ALGEBRA UND ZAHLENTHEORIE
MIT GRUNDLEGENDEN ABSCHNITTEN AUS DER LINEAREN ALGEBRA

Wolfgang Soergel

25. April 2024

Inhaltsverzeichnis

Diese Zusammenstellung ist ergänzt um die besonders relevanten Abschnitte der Skripte zur linearen Algebra. Dabei tritt aber das Problem auf, daß manche Verweise ins Leere laufen. Die Abschnitte bis zur Galois-Theorie einschließlich sollten in etwa den Standardstoff einer Algebra-Vorlesung für das dritte Semester abdecken. Ich habe mich bei der Entwicklung der Theorie besonders darum bemüht, die Verwendung des Zorn'schen Lemmas zu vermeiden. Mein Ziel war es, dem falschen Eindruck entgegenzuwirken, unsere Sätze über die Auflösbarkeit von polynomialen Gleichungen oder die Bestimmung quadratischer Reste oder die Konstruierbarkeit regelmäßiger Vielecke basierten auf Subtilitäten der Mengenlehre. Insbesondere wird der algebraische Abschluß in den Beweisen nicht verwendet und der Begriff eines maximalen Ideals wird gar nicht erst betrachtet. Ich bedanke mich bei vielen Freiburger Studierenden für Hinweise, die mir geholfen haben, die Darstellung zu klären und zu glätten und Fehler zu beheben.

1 Zahlen

1.1 Konstruktion der natürlichen Zahlen*

1.1.1. Im folgenden diskutiere ich die Beschreibung der natürlichen Zahlen im Rahmen der naiven Mengenlehre. Eine vollständig überzeugende Diskussion dieser Struktur ist meines Erachtens nur im Rahmen der Logik möglich.

1.1.2. Führt man die Mengenlehre axiomatisch ein, so definiert man eine Menge als **unendlich**, wenn es eine injektive aber nicht bijektive Abbildung von unserer Menge in sich selbst gibt. Eine Menge heißt **endlich**, wenn sie nicht unendlich ist. Die Existenz einer unendlichen Menge ist eines der Axiome der Zermelo-Fraenkel-Mengenlehre, wir nennen es das **Unendlichkeitsaxiom**. Bei Zermelo und Fraenkel ist diese Axiomatik noch formaler und präziser, aber so weit gehen wir hier nicht.

1.1.3. Es ist klar, daß jede Menge mit einer unendlichen Teilmenge auch selbst unendlich sein muß. Es folgt, daß jede Teilmenge einer endlichen Menge wieder endlich ist. Es ist klar, daß eine unendliche Menge unendlich bleibt, wenn wir ihr ein Element wegnehmen: Wir können ja unsere injektive aber nicht bijektive Abbildung leicht so abändern, daß ein vorgegebenes Element auf sich selber abgebildet wird. Es folgt, daß die Vereinigung einer endlichen Menge mit einer einelementigen Menge wieder endlich ist.

Ergänzung 1.1.4 (**Maximale Elemente endlicher teilgeordneter Mengen**). Jede nichtleere endliche teilgeordnete Menge $(E, \leq)$ besitzt mindestens ein maximales Element. Diese Erkenntnis haben wir bereits mehrfach als intuitiv klar verwendet, etwa im Beweis **??** der Tatsache, daß zwischen je zwei verschiedenen reellen Zahlen immer noch eine rationale Zahl liegt, oder beim Beweis des Basisexistenzsatzes für endlich erzeugte Vektorräume **??**, aber das war noch vor der Formalisierung des Begriffs einer endlichen Menge. Etwas formaler können wir durch Widerspruch argumentieren. In der Tat könnten wir andernfalls eine Abbildung $f : E \to E$ finden, die jedem Element ein echt größeres Element zuordnet. Halten wir dann $a \in E$ fest, so erhielten wir eine injektive aber nicht surjektive Abbildung von $\{x \in E \mid x \geq a\}$ zu sich selbst, und dieser Widerspruch zeigt die Behauptung.

Satz 1.1.5 (**Die natürlichen Zahlen**). *1. Es gibt Paare (N, s) aus einer Menge N und einer injektiven Abbildung $s : N \hookrightarrow N$ derart, daß $N \backslash s(N)$ aus einem einzigen Element o besteht und daß jede s-stabile Teilmenge von N, die o enthält, bereits ganz N sein muß;*

2. *Sei (N, s) solch ein Paar. Ist dann (X, x, f) ein Tripel bestehend aus einer Menge X, einem Element $x \in X$ und einer Abbildung $f : X \to X$, so gibt es genau eine Abbildung $\psi : N \to X$ mit $\psi(o) = x$ und $\psi s = f\psi$;*

3. *Ein Paar (N, s) wie im ersten Teil ist im wesentlichen eindeutig bestimmt. Ist genauer (N', s') ein weiteres derartiges Paar und $\{o'\} = N'\backslash s'(N')$, so ist die eindeutig bestimmte Abbildung $\psi : N \to N'$ mit $s'\psi = \psi s$ und $\psi(o) = o'$ eine Bijektion.*

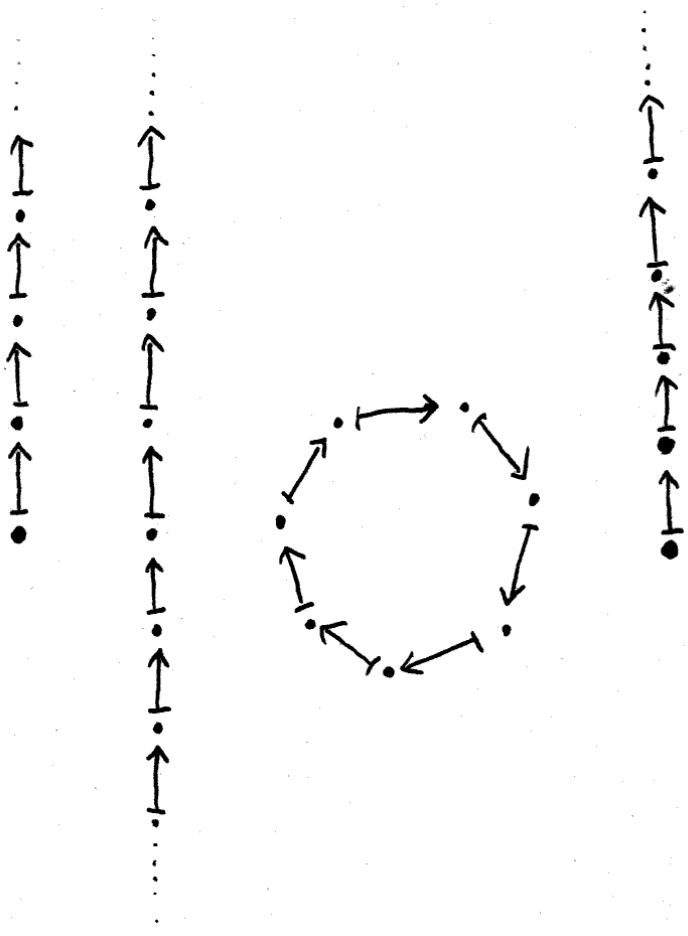
1.1.6. Sobald der Satz bewiesen ist, halten wir ein derartiges Paar ein für allemal fest, verwenden dafür die Notation $(\mathbb{N}, s)$, erlauben uns aufgrund der Eindeutigkeit den bestimmten Artikel und nennen $\mathbb{N}$ die Menge der **natürlichen Zahlen**. Gegeben $a \in \mathbb{N}$ heißt $s(a)$ der **Nachfolger** oder genauer der **unmittelbare Nachfolger** von a. Die Notation s steht für „successor“. Wir vereinbaren für das eindeutig bestimmte Element von $\mathbb{N}$, das kein Nachfolger ist und daß oben o hieß, die Notation $0 \in \mathbb{N}$ und die Bezeichnung **Null**.

1.1.7. Gegeben eine Menge X und zwei Abbildungen $\psi, \phi : \mathbb{N} \to X$ mit $\psi(0) = \phi(0)$ und $\big(\psi(b) = \phi(b)\big) \Rightarrow \big(\psi(s(b)) = \phi(s(b))\big)$ folgt $\psi = \phi$. In der Tat bedeuten unsere Annahmen, daß die Teilmenge $\{b \in \mathbb{N} \mid \psi(b) = \phi(b)\}$ das Element $0 \in \mathbb{N}$ enthält und stabil ist unter s und also aufgrund der charakterisierenden Eigenschaft der natürlichen Zahlen ganz $\mathbb{N}$ sein muß. Diese Umformulierung der Definition 1.1.6 heißt das **Prinzip der vollständigen Induktion**.

1.1.8. Die in diesem Satz gegebene Charakterisierung und im folgenden Beweis durchgeführte Konstruktion der natürlichen Zahlen gehen auf einen berühmten Artikel von Richard Dedekind zurück mit dem Titel „Was sind und was sollen die Zahlen?“. Eine alternative Charakterisierung besprechen wir in **??**.

Beweis. 1. Nach dem Unendlichkeitsaxiom 1.1.2 finden wir eine Menge A nebst einer injektiven Abbildung $s : A \hookrightarrow A$ und einem Element $o \in A\backslash s(A)$. Unter allen Teilmengen $M \subset A$ mit $o \in M$ und $s(M) \subset M$ gibt es sicher eine kleinste, nämlich den Schnitt N aller derartigen Teilmengen. Für diese gilt dann notwendig $N \subset \{o\} \cup s(N)$, da die rechte Seite auch eine mögliche Teilmenge M mit unseren Eigenschaften ist. Da die andere Inklusion eh klar ist, folgt $N = \{o\} \cup s(N)$. So haben wir bereits ein mögliches Paar (N, s) gefunden.

2. Gegeben (X, x, f) wie oben betrachten wir die Gesamtheit aller Teilmengen $G \subset N \times X$ mit $(o, x) \in G$ und $(n, y) \in G \Rightarrow (s(n), f(y)) \in G$. Sicher gibt es eine kleinste derartige Teilmenge $G_{\min} = \Gamma$, nämlich den Schnitt aller möglichen derartigen Teilmengen G. Wir zeigen nun, daß Γ der Graph einer Funktion ist. Dazu betrachten wir die Teilmenge M aller $m \in N$ derart, daß es genau ein $y \in X$ gibt mit $(m, y) \in \Gamma$. Sicher gilt $o \in M$, denn gäbe es $y \in X$ mit $x \neq y$ und $(o, y) \in \Gamma$, so könnten wir (o, y) ohne Schaden aus Γ entfernen im Widerspruch zur Minimalität von Γ. Ist ähnlich $m \in M$, so zeigen wir in derselben Weise $s(m) \in M$. Also gilt $M = N$ und Γ ist der Graph einer Funktion $f : N \to X$ mit den gewünschten Eigenschaften. Finden wir eine weitere Funktion mit den



Versuch der graphischen Darstellung einer Menge mit einer injektiven aber nicht surjektiven Abbildung in sich selbst.

gewünschten Eigenschaften, so ist deren Graph auch ein mögliches G und wir folgern erst $G \supset \Gamma$ und dann $G = \Gamma$.

3. Nach Teil 2 gibt es auch genau eine Abbildung $\varphi : N' \xrightarrow{\sim} N$ mit $s\varphi = \varphi s'$ und $\varphi : o' \mapsto o$. Nach Teil 2, diesmal der Eindeutigkeitsaussage, gilt dann $\psi\phi = \mathrm{id}$ und $\phi\psi = \mathrm{id}$. Also ist unser ψ in der Tat eine Bijektion. □

1.1.9. In unseren natürlichen Zahlen $(\mathbb{N}, s)$ erklären wir die **Eins** als den Nachfolger der Null und setzen in Formeln

$$1 := s(0)$$

1.1.10 (**Potenzen von Abbildungen**). Sei (X, x, f) ein Tripel bestehend aus einer Menge X, einem Element $x \in X$ und einer Abbildung $f : X \to X$. Für die Werte der Abbildung $\psi : \mathbb{N} \to X$ aus Teil 2 vereinbaren wir die Notation

$$f^n(x) := \psi(n)$$

Unser $f^n(x)$ wird also in Formeln charakterisiert durch $f^0(x) = x$ und $f^{s(n)}(x) = f(f^n(x))$. Indem wir es für alle $x \in X$ betrachten, erhalten wir für alle $n \in \mathbb{N}$ eine Abbildung

$$f^n : X \to X$$

Wir nennen f^n die **n-te Potenz von** f. Per definitionem gilt $f^0 = \mathrm{id}$ und $f^1 = f$. Vollständige Induktion zeigt $\mathrm{id}^n = \mathrm{id}$ für alle n.

Lemma 1.1.11. *Für alle $n \in \mathbb{N}$ gilt $n = s^n(0)$.*

Beweis. Wir argumentieren mit vollständiger Induktion über n. Für $n = 0$ sind beide Seiten 0 und die Behauptung stimmt. Gilt die Formel für ein n, so folgt $s(n) = s(s^n(0)) = s^{s(n)}(0)$ mit der ersten Gleichung durch Anwenden von s und der zweiten nach der definitorischen Gleichung $f(f^n(x)) = f^{s(n)}(x)$ für Potenzen 1.1.10. Damit ist unsere Behauptung bewiesen. □

1.1.12 (**Funktorialität von Potenzen**). Gegeben eine Abbildung $h : X \to Y$ und Abbildungen $f : X \to X$ sowie $g : Y \to Y$ mit $hf = gh$ gilt

$$hf^n = g^n h$$

für alle $n \in \mathbb{N}$. In der Tat reicht es, für alle $x \in X$ die Identität $hf^n(x) = g^n h(x)$ zeigen. Beide Seiten sind aber als Funktionen von n Abbildungen $\psi : \mathbb{N} \to Y$ mit demselben Wert $\psi(0) = h(x)$ für $n = 0$ und derselben charakterisierenden Eigenschaft $\psi s = g\psi$. Für je zwei Selbstabbildungen $f, g : X \to X$ einer Menge mit $fg = gf$ folgern wir $gf^a = f^a g$ und $g^b f^a = f^a g^b$ für alle $a, b \in \mathbb{N}$.

Definition 1.1.13. Für die Menge der natürlichen Zahlen mit Nachfolgerabbildung $(\mathbb{N}, s)$ aus 1.1.6 erklären wir die **Addition** $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $(a, b) \mapsto a + b$ durch die Vorschrift

$$a + b := s^a(b)$$

1.1.14. Wir finden $0 + b = s^0(b) = \mathrm{id}(b) = b$ und $1 + b = s^1(b) = s(b)$ für alle $b \in \mathbb{N}$. Anderersits finden wir $b + 0 = s^b(0) = b$ nach 1.1.11.

Lemma 1.1.15. *Die Addition natürlicher Zahlen ist eine kommutative Verknüpfung mit der Null als neutralem Element.*

Beweis. Aus der Funktorialität von Potenzen 1.1.12 folgt $s^a s^b = s^b s^a$ für alle $a, b \in \mathbb{N}$. Werten wir beide Seiten auf 0 aus, so erhalten wir mit 1.1.11 die Kommtativität $s^a(b) = s^b(a)$. Daß 0 ein neutrales Element ist alias die Identitäten $0 + b = b = b + 0$ kennen wir bereits aus 1.1.14. □

Lemma 1.1.16 (Produkt von Potenzen und Addition). *Gegeben eine Menge X und eine Abbildung $f : X \to X$ und $a, b \in \mathbb{N}$ gilt $f^{a+b} = f^a f^b$.*

1.1.17. Es folgt, daß die Addition natürlicher Zahlen assoziativ ist, denn gegeben $a, b, c \in \mathbb{N}$ finden wir $s^{(a+b)+c} = (s^a s^b)s^c = s^a s^b s^c = s^a(s^b s^c) = s^{a+(b+c)}$ und Auswerten bei 0 liefert die Behauptung.

Beweis. Wir zeigen das durch vollständige Induktion über a. Im Fall $a = 0$ ist es klar. Für den Induktionsschritt wenden wir f an und finden von der Mitte ausgehend

$$f^{s(a)+b} = f^{s(a+b)} = f f^{a+b} = f(f^a f^b) = (f f^a) f^b = f^{s(a)} f^b$$

Hier nutzen wir nach rechts die Assoziativität der Verknüpfung von Abbildungen und nach links die Identität $s(a) + b = s^{s(a)}(b) = s(s^a(b)) = s(a + b)$. □

Satz 1.1.18 (Eigenschaften der Addition natürlicher Zahlen). *Die Menge der natürlichen Zahlen wird mit der Verknüpfung $+$ ein kommutatives Monoid, in dem die* **Kürzungsregel** $(a + b = c + b) \Rightarrow (a = c)$ *gilt sowie die Regel* $(a + b = 0) \Rightarrow (a = b = 0)$.

Beweis. Kommutativität, neutrales Element und Assoziativität haben wir bereits in 1.1.15 und 1.1.17 erledigt. Was unsere Kürzungsregel angeht, enthält für $a \neq c$ die Menge aller b mit $a + b \neq c + b$ sicher $b = 0$ und ist stabil unter s, enthält also alle $b \in \mathbb{N}$. Aus $a + b = 0$ folgt zu guter Letzt $a = 0$, weil ja sonst die Null gar nicht im Bild der Abbildung $(a+) : \mathbb{N} \to \mathbb{N}$ liegt, und dann folgt auch $b = 0$ nach der Kürzungsregel. □

Satz 1.1.19 (Anordnung auf den natürlichen Zahlen). *Sei $(\mathbb{N}, s)$ die Menge der natürlichen Zahlen mit Nachfolgerabbildung aus 1.1.6 und Addition aus 1.1.18. Die Relation $\leq$ auf $\mathbb{N}$ gegeben durch die Vorschrift*

$$(a \leq b) \Leftrightarrow (\exists c \in \mathbb{N} \text{ mit } a + c = b)$$

ist eine Anordnung auf $\mathbb{N}$. Für diese Anordnung ist $0 \in \mathbb{N}$ das kleinste Element und jede nichtleere Teilmenge von $\mathbb{N}$ besitzt ein kleinstes Element.

Beweis. Bis auf die allerletzte Aussage folgt das alles leicht aus den in 1.1.18 gezeigten Eigenschaften der Addition. Ist nun $A \subset \mathbb{N}$ eine Teilmenge ohne kleinstes Element, so ist $\{n \in \mathbb{N} \mid n \leq a \ \forall a \in A\}$ stabil unter s und enthält die Null, ist also ganz $\mathbb{N}$, und es folgt $A = \emptyset$. □

Satz 1.1.20 (Zählen endlicher Mengen). *Eine Menge X ist genau dann endlich, wenn es ein $n \in \mathbb{N}$ und eine Bijektion $\mathbb{N}_{<n} \xrightarrow{\sim} X$ gibt. Dies n ist dann wohlbestimmt und heißt die* **Kardinalität** *von X und wird $n = |X|$ notiert.*

Beweis. Daß es eine Injektion $\mathbb{N}_{<a} \xrightarrow{\sim} \mathbb{N}_{<b}$ nur für $a \leq b$ geben kann, zeigt man leicht durch Induktion. Das zeigt die Eindeutigkeit von n. Umgekehrt liefert das Zorn'sche Lemma ein maximales Paar bestehend aus einem $a \in \mathbb{N} \sqcup \{\infty\}$ und einer injektiven Abbildung $\mathbb{N}_{<a} \hookrightarrow X$. Ist X endlich, so haben wir notwendig $a \neq \infty$ und unsere maximale injektive Abbildung muß eine Bijektion $\mathbb{N}_{<a} \xrightarrow{\sim} X$ gewesen sein. □

Lemma 1.1.21 (Potenzen einer Verknüpfung kommutierender Abbildungen). *Gegeben Abbildungen $f, g : X \to X$ mit $fg = gf$ gilt für alle $a \in \mathbb{N}$ die Identität $(fg)^a = f^a g^a$.*

Beweis. Durch vollständige Induktion. Der Fall $a = 0$ ist offensichtlich. Für den Induktionsschritt verwenden wir die Assoziativität der Verknüpfung von Abbildungen implizit, schalten wir fg auf beiden Seiten nach und entwickeln mit der Funktorialität von Potenzen 1.1.12 von der Mitte ausgehend

$$(fg)^{s(a)} = (fg)(fg)^a = fgf^a g^a = ff^a gg^a = f^{s(a)} g^{s(a)}$$ □

Lemma 1.1.22 (Iterierte Potenzen). *Gegeben eine Abbildung $f : X \to X$ gilt für alle $a, b \in \mathbb{N}$ die Identität*

$$(f^a)^b = (f^b)^a$$

Beweis. Induktion über a. Der Fall $a = 0$ ist offensichtlich. Für den Induktionsschritt schalten wir auf beiden Seiten f^b nach und finden von der Mitte ausgehend

$$(f^{s(a)})^b = (ff^a)^b = f^b (f^a)^b = f^b (f^b)^a = (f^b)^{s(a)}$$

Nach links haben wir dabei die Regel 1.1.21 für Potenzen einer Verknüpfung kommutierender Abbildungen verwendet. Das Kommutieren von f und f^a folgt aus der Funktorialität 1.1.12 von Potenzen. □

Satz 1.1.23 (Multiplikation natürlicher Zahlen). *Sei $(\mathbb{N}, s)$ die Menge der natürlichen Zahlen mit Nachfolgerabbildung aus 1.1.6 und bezeichne $+$ ihre Addition aus 1.1.18. Die Verknüpfung*

$$(a, b) \mapsto ab = a \cdot b := (b+)^a(0)$$

ist kommutativ mit neutralem Element dem Nachfolger $1 = s(0)$ der Null. Weiter folgt aus $a \neq 0$ und $b \neq 0$ bereits $ab \neq 0$.

1.1.24 (**Produkt mit Null**). Wir folgern $a \cdot 0 = (0+)^a(0) = \mathrm{id}^a(0) = \mathrm{id}(0) = 0$ wegen der Neutralität von Null für die Addition und unseren Erkenntnissen 1.1.10 zu Potenzen der Identität.

Beweis. Per definitionem gilt $(b+) = s^b$, also $ab = (b+)^a(0) = (s^b)^a(0)$. Sind weder a noch b Null, so ist das ein echter Nachfolger der Null und folglich nicht Null. Die Kommutativität der Multiplikation erhalten wir, indem wir die Identität $(s^a)^b = (s^b)^a$ aus 1.1.22 auf 0 anwenden. Um die Eins als neutral zu erkennen, erinnern wir $(1+) = s$ aus 1.1.14 und rechnen $a \cdot 1 = (1+)^a(0) = s^a(0) = a$. Mit der Kommutativität der Multiplikation folgt, daß 1 in der Tat neutral ist für die Multiplikation. □

Lemma 1.1.25 (Iterierte Potenzen und Multiplikation). *Gegeben eine Abbildung $f : X \to X$ und $a, b \in \mathbb{N}$ gilt $(f^a)^b = f^{ab}$.*

Beweis. Induktion über a. Im Fall $a = 0$ ist die Aussage klar wegen unseren Erkenntnissen $f^0 = \mathrm{id}$ und $\mathrm{id}^b = \mathrm{id}$ aus 1.1.10 und dem Verschwinden des Produkts mit Null 1.1.24. Für den Induktionsschritt rechnen wir $b+ab = (b+)((b+)^a(0)) = (b+)^{s(a)}(0) = s(a)b$ und damit

$$(f^{s(a)})^b = (f f^a)^b = f^b (f^a)^b = f^b f^{ab} = f^{b+ab} = f^{s(a)b}$$

nach Definition, der Regel für Potenzen von Verknüpfungen 1.1.21, der Induktionsannahme und der Regel für Produkte von Potenzen 1.1.16. Wir verwenden dabei implizit unsere stehende Vereinbarung „Punkt vor Strich“. □

1.1.26 (**Assoziativität der Multiplikation**). Gegeben $a, b, c \in \mathbb{N}$ finden wir mit unserer Formel für iterierte Potenzen 1.1.25 von der Mitte ausgehend die Identität

$$s^{a(bc)} = (s^a)^{bc} = \left((s^a)^b\right)^c = \left(s^{ab}\right)^c = s^{(ab)c}$$

Wenden wir beide Seiten auf $0 \in \mathbb{N}$ an, ergibt sich mit 1.1.11 wie gewünscht die Assoziativität der Multiplikation $a(bc) = (ab)c$. Unter der Multiplikation ist $\mathbb{N}$ also ein kommutatives Monoid mit der Eins als neutralem Element.

1.1.27 (**Distributivgesetz**). Wir finden mit unseren Regeln zum Produkt von Potenzen 1.1.16 beziehungsweise zu iterierten Potenzen 1.1.25 die Identitäten

$$s^{ab+ac} = s^{ab}s^{ac} = (s^a)^b(s^a)^c = (s^a)^{b+c} = s^{a(b+c)}$$

Das Distributivgesetz $ab + ac = a(b + c)$ ergibt sich, indem wir beide Seiten auf die Null anwenden und 1.1.11 beachten.

1.1.28. Zusammenfassend haben wir so auf unserer Menge mit Nachfolgerabbildung $(\mathbb{N}, s)$ ein Element Null ausgezeichnet als das einzige Element, das kein Nachfolger ist, und ein Element Eins als dessen Nachfolger. Wir haben weiter auf $\mathbb{N}$ eine Addition und Multiplikation eingeführt und gezeigt, daß beide assoziative und kommutative Verknüpfungen sind mit neutralen Elementen Null beziehungsweise Eins und daß das Distributivgesetz gilt.

1.1.29 (**Potenzgesetze**). Gegeben ein multiplikativ notiertes Monoid M und $a \in \mathbb{N}$ erklären wir für jedes $m \in M$ seine a**-te Potenz**

$$m^a := (m\cdot)^a(1_M)$$

als den Wert der a-ten Potenz der Linksmultiplikation mit m auf dem neutralen Element. Sie dürfen als Übung zeigen, daß es am Ergebnis nichts ändert, wenn wir stattdessen mit der Rechtsmultiplikation arbeiten. Im Spezialfall des Monoids $\mathrm{Ens}(X)$ aller Selbstabbildungen einer Menge erhalten wir unsere Potenzen von Selbstabbildungen aus 1.1.6 zurück. Gegeben ein multiplikativ notiertes Monoid M übersetzen sich unsere Regeln für das Potenzieren von Selbstabbildungen in die Regeln $m^0 = 1_M$, $m^1 = m$, $m^{a+b} = m^a m^b$, $(m^a)^b = m^{ab}$ und, im Fall von kommutierenden $m, n \in M$, die Zusatzregel $(mn)^a = m^a n^a$ in unserem Monoid. Im Fall eines additiv notierten Monoids, das nach unseren Konventionen stets als kommutativ angenommen wird, erhalten wir dahingegen die Regeln $0m = 0_M$, $1m = m$, $(a + b)m = am + bm$, $b(am) = (ab)m$ und $a(m + n) = am + an$. All diese Regeln gelten insbesondere auch für $\mathbb{N}$ selbst, auf dem wir ja sogar zwei Strukturen als kommutatives Monoid erklärt hatten, die additive und die multiplikative Struktur. Letztere Formeln hatten wir in diesem Fall auch bereits zuvor bereits gezeigt.

Satz 1.1.30 (Teilen mit Rest). *Sei $(\mathbb{N}, s)$ die Menge der natürlichen Zahlen mit Nachfolgerabbildung und Addition, Multiplikation und Anordnung wie in 1.1.23 und 1.1.19. Gegeben $a, b \in \mathbb{N}$ mit $b \neq 0$ gibt es eindeutig bestimmte $c, d \in \mathbb{N}$ mit $a = bc + d$ und $d < b$.*

Beweis. Übung. □

1.1.31. Die Nachfolger von 0 notieren wir der Reihe nach 1, 2, 3, 4, 5, 6, 7, 8, 9 und nennen sie der Reihe nach **Eins, Zwei, Drei, Vier, Fünf, Sechs, Sieben,**

Acht, Neun. Den Nachfolger von Neun nennen wir **Zehn** und notieren ihn vorerst $\mathrm{Z} \in \mathbb{N}$. Dann vereinbaren wir für $a_0, a_1, \ldots, a_r \in \{0, 1, \ldots, 9\}$ die **Dezimaldarstellung**

$$a_r \ldots a_1 a_0 := a_r \mathrm{Z}^r + \ldots + a_1 \mathrm{Z}^1 + a_0 \mathrm{Z}^0$$

So erhalten wir insbesondere für unsere natürliche Zahl Zehn die Dezimaldarstellung $\mathrm{Z} = 10 = 1\mathrm{Z}^1 + 0\mathrm{Z}^0$. Wenn ganz allgemein eine endliche Folge der Symbole $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$ ohne Punkt und Komma nebeneinandersteht und nichts anderes gesagt wird, ist davon auszugehen, daß eine natürliche Zahl in Dezimaldarstellung gemeint ist. In diesem Kontext dürfen Multiplikationssymbole natürlich nicht, wie sonst üblich, einfach weggelassen werden. Schließlich gilt es zu zeigen, daß jede natürliche Zahl eine eindeutig bestimmte Dezimaldarstellung hat mit $r > 0 \Rightarrow a_r \neq 0$, was wieder dem Leser zur Übung überlassen sei.

1.1.32 (**Zahldarstellungen**). Gegeben eine beliebige natürliche Zahl $b > 1$ hat jede natürliche Zahl n genau eine Darstellung der Form

$$n = a_r b^r + \ldots + a_1 b^1 + a_0 b^0$$

mit $a_0, a_1, \ldots, a_r \in \{0, 1, \ldots, b-1\}$ und $r > 0 \Rightarrow a_r \neq 0$. Wenn wir Symbole alias Ziffern für die Elemente dieser Menge vereinbaren, so können wir die Sequenz von Ziffern $a_r \ldots a_0$ als Darstellung der Zahl n interpretieren. Wir sagen dann auch, sie **stelle** n **im** b**-adischen System dar** und schreiben

$$a_r \ldots a_0 = [a_r, \ldots, a_0]_b = n$$

Wenn aber ganz links nicht eine Darstellung zur Basis zehn gemeint sein sollte, muß man das deutlich dazusagen. Das zehnadische Sytem heißt das **Dezimalsystem** und man spricht dann auch von der **Dezimaldarstellung** einer natürlichen Zahl und wir haben etwa

$$[2, 5, 5]_{10} = 255$$

Bei $b \leq 10$ wählt man als Ziffern meist die ersten b üblichen Ziffern des Dezimalsystems. Das 2-adische Sytem heißt das **Dualsystem** und man spricht dann auch von der **Binärdarstellung** einer natürlichen Zahl. So wäre

$$1010 = [1, 0, 1, 0]_2 = 2^3 + 2^1 = 10$$

die Darstellung der Zahl Zehn im Dualsystem, wo ganz links dazugesagt werden muß, daß 1010 als Binärdarstellung gemeint ist. Gebräuchlich sind auch Darstellungen im 16-adischen Sytem alias **Hexadezimalsystem** mit den üblicherweise verwendten Ziffern $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, \mathrm{A}, \mathrm{B}, \mathrm{C}, \mathrm{D}, \mathrm{E}, \mathrm{F}$. So hätten wir zum Beispiel

$$\mathrm{FF} = [\mathrm{F}, \mathrm{F}]_{16} = 15 \cdot 16 + 15 = 255$$

und müssen ganz links dazusagen, daß FF als Hexadesimaldarstellung gemeint ist. Wenn aber in so einer Ziffernfolge die ersten sechs Buchstaben des Alphabets als Großbuchstaben auftauchen, liegt der Verdacht einer Zahl in Hexadesimaldarstellung nahe.

Übungen

Übung 1.1.33. Man zeige, daß gilt $s(a) \neq a$ für alle $a \in \mathbb{N}$.

Übung 1.1.34. Man führe den Beweis für das Teilen mit Rest 1.1.30 aus.

Übung 1.1.35. Man zeige, daß die Vereinigung einer endlichen Menge mit einer einelementigen Menge wieder endlich ist. Man zeige durch vollständige Induktion über a, daß für alle $a \in \mathbb{N}$ die Menge $\mathbb{N}_{<a} := \{n \in \mathbb{N} \mid n < a\}$ endlich ist. Daß umgekehrt jede endliche Menge in Bijektion zu genau einer dieser Mengen ist, zeigen wir formal erst in **??**, obwohl wir es natürlich schon oft verwendet haben und weiter verwenden müssen. Der Beweis ist nicht schwer, aber alles zu seiner Zeit.

Übung 1.1.36. Gegeben eine endliche Menge X und eine Abbildung $f : X \to X$ und $x \in X$ zeige man, daß es natürliche Zahlen $n \neq m$ gibt mit $f^n(x) = f^m(x)$. Ist also X eine nichtleere endliche Menge und $f : X \to X$ eine Abbildung, so gibt es $y \in X$ und $r \geq 1$ mit $f^r(y) = y$.

Übung 1.1.37. Gegeben eine Menge X und eine Abbildung $f : \mathbb{N} \times X \to X$ und ein Element $a \in X$ gibt es genau eine Folge $\mathbb{N} \to X$, $n \mapsto x_n$ mit $x_0 = a$ und $x_{n+1} = f(n, x_n)\ \forall n \in \mathbb{N}$.

Übung 1.1.38. Gegeben ein multiplikativ notiertes Monoid M und $a \in \mathbb{N}$ zeige man $(m\cdot)^a(1_M) = (\cdot m)^a(1_M)$.

Übung 1.1.39. Man zeige die Iterationsregeln **??** für Mengen mit einer assoziativen Verknüpfung.

1.2 Äquivalenzrelationen und ganze Zahlen

1.2.1. Unter einer **Relation** R auf einer Menge X verstehen wir wie in **??** eine Teilmenge $R \subset X \times X$ des kartesischen Produkts von X mit sich selbst, also eine Menge von Paaren von Elementen von X. Statt $(x, y) \in R$ schreiben wir in diesem Zusammenhang meist xRy.

Definition 1.2.2. Eine Relation $R \subset X \times X$ auf einer Menge X heißt eine **Äquivalenzrelation**, wenn für alle Elemente $x, y, z \in X$ gilt:

1. **Transitivität:** (xRy und yRz) $\Rightarrow xRz$;

2. **Symmetrie:** $xRy \Leftrightarrow yRx$;

3. **Reflexivität:** xRx.

1.2.3. Ist eine Relation symmetrisch und transitiv und ist jedes Element in Relation zu mindestens einem weiteren Element, so ist unsere Relation bereits reflexiv. Ein Beispiel für eine Relation, die symmetrisch und transitiv ist, aber nicht reflexiv, wäre etwa die „leere Relation“ $R = \emptyset$ auf einer nichtleeren Menge $X \neq \emptyset$.

Beispiel 1.2.4. Gegeben eine Abbildung $f : X \to Z$ erhalten wir eine Äquivalenzrelation auf X durch die Vorschrift $(x \sim y) \Leftrightarrow (f(x) = f(y))$. Die Äquivalenzlassen sind dann genau die nichtleeren Fasern von f. Wir werden demnächst zeigen, daß jede Äquivalenzrelation auf diese Weise beschrieben werden kann.

1.2.5. Gegeben eine Äquivalenzrelation $\sim$ auf einer Menge X betrachtet man für $x \in X$ die Menge $A(x) := \{z \in X \mid z \sim x\}$ und nennt sie die **Äquivalenzklasse von** x. Eine Teilmenge $A \subset X$ heißt eine **Äquivalenzklasse** für unsere Äquivalenzrelation genau dann, wenn es ein $x \in X$ gibt derart, daß $A = A(x)$ die Äquivalenzklasse von x ist. Ein Element einer Äquivalenzklasse nennt man auch einen **Repräsentanten** der Klasse. Eine Teilmenge $Z \subset X$, die aus jeder Äquivalenzklasse genau ein Element enthält, heißt ein **Repräsentantensystem**. Aufgrund der Reflexivität gilt $x \in A(x)$, und man sieht leicht, daß für $x, y \in X$ die folgenden drei Aussagen gleichbedeutend sind:

1. $x \sim y$;

2. $A(x) = A(y)$;

3. $A(x) \cap A(y) \neq \emptyset$.

1.2.6. Gegeben eine Äquivalenzrelation $\sim$ auf einer Menge X bezeichnen wir die Menge aller Äquivalenzklassen, eine Teilmenge der Potenzmenge $\mathcal{P}(X)$, mit

$$(X/\sim) := \{A(x) \mid x \in X\}$$

und haben eine kanonische Abbildung $\mathrm{can} : X \to (X/\sim)$, $x \mapsto A(x)$. Diese kanonische Abbildung ist eine Surjektion und ihre Fasern sind genau die Äquivalenzklassen unserer Äquivalenzrelation.

1.2.7. Ist $f : X \to Z$ eine Abbildung mit $x \sim y \Rightarrow f(x) = f(y)$, so gibt es nach der universellen Eigenschaft von Surjektionen **??** genau eine Abbildung $\bar{f} : (X/\sim) \to Z$ mit $f = \bar{f} \circ \mathrm{can}$. Wir zitieren diese Eigenschaft manchmal als die **universelle Eigenschaft des Raums der Äquivalenzklassen**. Sagt man, eine Abbildung $g : (X/\sim) \to Z$ sei **wohldefiniert** durch eine Abbildung $f : X \to Z$, so ist gemeint, daß f die Eigenschaft $x \sim y \Rightarrow f(x) = f(y)$ hat und daß man $g = \bar{f}$ setzt.

1.2.8. Gegeben auf einer Menge X eine Relation $R \subset X \times X$ gibt es eine kleinste Äquivalenzrelation $T \subset X \times X$, die R umfaßt. Man kann diese Äquivalenzrelation entweder beschreiben als den Schnitt aller Äquivalenzrelationen, die R umfassen, oder auch als die Menge T aller Paare (x, y) derart, daß es ein $n \geq 0$ gibt und Elemente $x = x_0, x_1, \ldots, x_n = y$ von X mit $x_\nu R x_{\nu-1}$ oder $x_{\nu-1} R x_\nu$ für alle ν mit $1 \leq \nu \leq n$. Wir nennen T auch die **von der Relation R erzeugte Äquivalenzrelation auf X**.

Beispiel 1.2.9. Denken wir uns die Menge X als die „Menge aller Tiere“ und R als die Relation „könnten im Prinzip miteinander fruchtbaren Nachwuchs zeugen“, so wären die Äquivalenzklassen unter der von dieser Relation erzeugten Äquivalenzrelation eine mathematische Fassung dessen, was Biologen unter einer „Tierart“ verstehen würden.

Beispiel 1.2.10. Gegeben eine Menge X und eine Abbildung $f : X \to X$ betrachten wir die von der Relation $f(x) \sim x$ erzeugte Äquivalenzrelation. Man zeigt unschwer, daß sie explizit beschrieben werden kann durch

$$(x \sim y) \Leftrightarrow (\exists m, n \in \mathbb{N} \text{ mit } f^n(x) = f^m(y)).$$

Beispiel 1.2.11. Gegeben $M \supset N$ ein kommutatives Monoid mit einem Untermonoid erhält man eine Äquivalenzrelation auf der Menge $M \times N$ durch die Vorschrift

$$(a, s) \sim (b, t) \Leftrightarrow (\exists x \in N \text{ mit } atx = bsx)$$

Hier sind Symmetrie und Reflexivität offensichtlich. Um die Transitivität zu prüfen, müssen wir etwas rechnen: Gilt außerdem $(b, t) \sim (c, r)$, also $bry = cty$ für ein $y \in N$, so folgt $atxry = bsxry = ctysx$ und damit in der Tat $(a, s) \sim (c, r)$. Die Menge der Äquivalenzklassen notieren wir

$$N^{-1}M := (M \times N)/\sim$$

und notieren $s\backslash a$ die Äquivalenzklasse von (a, s). Man prüft, daß es auf $N^{-1}M$ eine Verknüpfung gibt mit $(s\backslash a)(t\backslash b) = (st\backslash ab)$ und daß $N^{-1}M$ mit dieser Verknüpfung ein kommutatives Monoid wird und $\mathrm{can} : M \to N^{-1}M$ gegeben durch $a \mapsto 1\backslash a$ ein Monoidhomomorphismus, unter dem jedes $s \in N$ auf ein invertierbares Element von $N^{-1}M$ abgebildet wird. Offensichtlich ist can genau dann ein Injektion $M \hookrightarrow N^{-1}M$, wenn N aus kürzbaren Elementen von M besteht. Schließlich induziert das Vorschalten von can für jedes weitere Monoid L eine Bijektion

$$\mathrm{Mon}(N^{-1}M, L) \tilde{\to} \{\varphi \in \mathrm{Mon}(M, L) \mid \varphi(N) \subset L^\times\}$$

wir sagen, das Monoid $N^{-1}M$ „gehe aus M durch formales Invertieren der Elemente von N hervor“. Im Spezialfall $N = M$ ist insbesondere $M^{-1}M$ stets eine Gruppe. Sie heißt die **einhüllende Gruppe** des kommutativen Monoids M.

1.2.12 (**Konstruktion des Rings der ganzen Zahlen**). Die einhüllende Gruppe unseres Monoids $(\mathbb{N}, +)$ der natürlichen Zahlen aus 1.1.18 heißt die additive Gruppe

$$\mathbb{Z}$$

der **ganzen Zahlen**. Aufgrund der Kürzungsregel 1.1.18 ist die kanonische Abbildung in diesem Fall eine Injektion $\mathbb{N} \hookrightarrow \mathbb{Z}$. Man prüft leicht, daß wir auf $\mathbb{Z}$ eine Anordnung erhalten durch die Vorschrift $(a \leq b) \Leftrightarrow$ (Es gibt $c \in \mathbb{N}$ mit $a+c = b$). Diese Anordnung hat die Eigenschaft $(a \leq b) \Rightarrow (a + x \leq b + x)$ und $\mathbb{N} = \mathbb{Z}_{\geq 0}$. Nach 1.1.23 induziert unsere Multiplikation auf $\mathbb{Z}_{\geq 0}$ eine Multiplikation auf $\mathbb{Z}_{>0}$ und diese ist nach 1.1.27 distributiv über der Addition. Aus **??** folgt dann schließlich, daß sich unsere Multiplikation auf $\mathbb{Z}_{>0}$ aus 1.1.23 auf eine und nur eine Weise zu einer kommutativen und über $+$ distributiven Multiplikation auf $\mathbb{Z}$ fortsetzen läßt. Von dieser Multiplikation ist a posteriori dann auch klar, daß sie unsere Multiplikation auf $\mathbb{N} \supset \mathbb{Z}_{>0}$ fortsetzt. Wenn wir in 2.1.1 lernen, was ein „Ring“ ist, werden sich unsere ganzen Zahlen mit dieser Addition und Multiplikation als eines der ersten Beispiele für einen Ring erweisen.

Ergänzung 1.2.13. Gegeben Relationen $R \subset X \times X$ und $S \subset Y \times Y$ ist auch das Bild von $(R \times S) \subset (X \times X) \times (Y \times Y)$ unter der durch Vertauschen der mittleren Einträge gegebenen Identifikation $(X \times X) \times (Y \times Y) \xrightarrow{\sim} (X \times Y) \times (X \times Y)$ eine Relation. Wir notieren diese Relation auf dem Produkt kurz $R \times S$. Sind R und S Äquivalenrelationen, so auch $R \times S$.

Übungen

Ergänzende Übung 1.2.14. Ist G eine Gruppe und $H \subset G \times G$ eine Untergruppe, die die Diagonale umfaßt, so ist H eine Äquivalenzrelation.

1.3 Untergruppen der Gruppe der ganzen Zahlen

Definition 1.3.1. Eine Teilmenge einer Gruppe heißt eine **Untergruppe**, wenn sie abgeschlossen ist unter der Verknüpfung und der Inversenbildung und zusätzlich das neutrale Element enthält. Ist G eine multiplikativ geschriebene Gruppe, so ist eine Teilmenge $U \subset G$ also eine Untergruppe, wenn in Formeln gilt: $a, b \in U \Rightarrow ab \in U$, $a \in U \Rightarrow a^{-1} \in U$ sowie $1 \in U$.

Ergänzung 1.3.2. Nach der reinen Lehre sollte eine Teilmenge einer Gruppe eine „Untergruppe“ heißen, wenn sie so mit der Struktur einer Gruppe versehen werden kann, daß die Einbettung ein Gruppenhomomorphismus wird. Da diese Definition jedoch für Anwendungen erst aufgeschlüsselt werden muß, haben wir gleich die aufgeschlüsselte Fassung als Definition genommen und überlassen den Nachweis der Äquivalenz zur Definition nach der reinen Lehre dem Leser zur Übung.

Beispiele 1.3.3. In jeder Gruppe ist die einelementige Teilmenge, die nur aus dem neutralen Element besteht, eine Untergruppe. Wir nennen sie die **triviale Untergruppe**. Ebenso ist natürlich die ganze Gruppe stets eine Untergruppe von sich selber. Gegeben ein Vektorraum V ist die Menge aller Automorphismen eine Untergruppe $\mathrm{Aut}(V) \subset \mathrm{Ens}^\times(V)$ der Gruppe aller Permutationen der zugrundeliegenden Menge.

Satz 1.3.4 (**Untergruppen der additiven Gruppe $\mathbb{Z}$ der ganzen Zahlen**). *Jede Untergruppe $H \subset \mathbb{Z}$ ist von der Form $H = m\mathbb{Z}$ für genau ein $m \in \mathbb{N}$. Die Abbildungsvorschrift $m \mapsto m\mathbb{Z}$ liefert mithin eine Bijektion*

$$\mathbb{N} \quad \tilde{\to} \quad \{H \subset \mathbb{Z} \mid H \textit{ ist Untergruppe von } \mathbb{Z}\}$$

Beweis. Im Fall $H = \{0\}$ ist $m = 0$ die einzige natürliche Zahl mit $H = m\mathbb{Z}$. Gilt $H \neq \{0\}$, so enthält H echt positive Elemente. Sei dann $m \in H$ das kleinste echt positive Element von H. Wir behaupten $H = m\mathbb{Z}$. Die Inklusion $H \supset m\mathbb{Z}$ ist hier offensichtlich. Aber gäbe es $n \in H \setminus m\mathbb{Z}$, so könnten wir n mit Rest teilen durch m und also schreiben $n = ms + r$ für geeignete $s, r \in \mathbb{Z}$ mit $0 < r < m$. Es folgte $r = n - ms \in H$ im Widerspruch zur Minimalität von m. Das zeigt die Surjektivität unserer Abbildung. Die Injektivität ist offensichtlich. □

1.3.5. Der Schnitt über eine beliebige Familie von Untergruppen einer gegebenen Gruppe ist selbst wieder eine Untergruppe. Für eine Teilmenge T einer Gruppe G definieren wir die **von T erzeugte Untergruppe**

$$\langle T \rangle \subset G$$

als die kleinste Untergruppe von G, die T umfaßt. Natürlich gibt es so eine kleinste Untergruppe, nämlich den Schnitt über alle Untergruppen von G, die T umfassen. Für $T \neq \emptyset$ können wir $\langle T \rangle$ konkret beschreiben als die Menge aller endlichen Produkte von Elementen aus T und deren Inversen. Für $T = \emptyset$ besteht $\langle T \rangle$ dahingegen nur aus dem neutralen Element. Ist T durch einen Ausdruck in Mengenklammern gegeben, so lassen wir diese meist weg und schreiben also zum Beispiel kürzer $\langle a_1, \ldots, a_n \rangle$ statt $\langle \{a_1, \ldots, a_n\} \rangle$. Ob der Ausdruck $\langle T \rangle$ in einem speziellen Fall die von einer Menge T erzeugte Untergruppe oder vielmehr die von der einelementigen Menge mit einzigem Element T erzeugte Untergruppe meint, muß der Leser meist selbst aus dem Kontext erschließen. Schreiben wir jedoch $\langle {}_!T \rangle$, so ist stets zu verstehen, daß T eine Menge von Erzeugern und nicht einen einzelnen Erzeuger meint.

1.3.6. Ist V ein k-Vektorraum und $T \subset V$ eine Teilmenge, so muß der Leser von nun an aus dem Kontext erschließen, ob mit $\langle T \rangle$ die von T erzeugte Untergruppe oder der von T erzeugte Untervektorraum gemeint ist. Zur Unterscheidung schreiben wir manchmal $\langle T \rangle_{\mathbb{Z}}$ für die von T erzeugte Untergruppe und $\langle T \rangle_k$ für den von T erzeugten Untervektorraum.

Übungen

Ergänzende Übung 1.3.7. Eine endliche nichtleere Teilmenge einer Gruppe, die mit je zwei Elementen auch die Verknüpfung der beiden enthält, ist notwendig bereits eine Untergruppe.

Übung 1.3.8. Sind $H, K \subset G$ zwei Untergruppen einer Gruppe mit $H \cap K = 1$, so induziert die Verknüpfung eine Injektion $H \times K \hookrightarrow G$.

Übung 1.3.9. Wieviele Untergruppen hat die additive Gruppe eines zweidimensionalen Vektorraums über dem Körper mit zwei Elementen? Wieviele Untergruppen hat die additive Gruppe eines n-dimensionalen Vektorraums über dem Körper mit zwei Elementen?

Ergänzende Übung 1.3.10. Sei G eine Gruppe und $\varphi : G \to G$ ein Gruppenhomomorphismus. Man zeige: Gilt für ein $n \in \mathbb{N}$ die Geichheit $\ker \varphi^n = \ker \varphi^{n+1}$, so folgt $\ker \varphi^n = \ker \varphi^{n+1} = \ker \varphi^{n+2} = \ldots$

Übung 1.3.11. Ist $\varphi : G \to H$ ein Gruppenhomomorphismus, so gilt die Formel $|G| = |\operatorname{im} \varphi| \cdot |\ker \varphi|$. Man bemerke, daß diese Formel im Fall linearer Abbildungen von Vektorräumen über endlichen Körpern äquivalent ist zur Dimensionsformel.

1.4 Primfaktorzerlegung

Definition 1.4.1. Eine **Primzahl** ist eine natürliche Zahl ≥ 2, die sich nicht als das Produkt von zwei echt kleineren natürlichen Zahlen erhalten läßt.

Beispiel 1.4.2. Die Primzahlen unterhalb von 50 sind 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47.

1.4.3. Eine Möglichkeit, alle Primzahlen zu finden, ist das sogenannte **Sieb des Eratosthenes**: Man beginnt mit der kleinsten Primzahl, der Zwei. Streicht man alle Vielfachen der Zwei, als da heißt, alle geraden Zahlen, so ist die erste Zahl unter den Übrigen die nächste Primzahl, die Drei. Streicht man nun auch noch alle Vielfachen der Drei, so ist die erste Zahl unter den Übrigen die nächste Primzahl, die Fünf, und so weiter. „Der Erste“ heißt auf lateinisch „Primus“ und auf griechisch ähnlich und es könnte sein, daß die Bezeichnung „Primzahl“ daher rührt.

Satz 1.4.4 (Existenz einer Primfaktorzerlegung). *Jede natürliche Zahl $n \geq 2$ kann als ein Produkt von Primzahlen $n = p_1 p_2 \ldots p_r$ dargestellt werden.*

1.4.5. Der Satz gilt in unserer Terminologie auch für die Zahl $n = 1$, wenn wir auch Produkte der Länge $r = 0$ erlauben und erinnern, daß nach unseren Konventionen die Eins durch das „leere Produkt“ mit $r = 0$ dargestellt wird. Eine Primzahl p ist darin als das Produkt $p = p_1$ mit nur einem Faktor zu verstehen.

Beweis. Das ist klar mit vollständiger Induktion: Ist eine Zahl nicht bereits selbst prim, so kann sie als Produkt echt kleinerer Faktoren geschrieben werden, von denen nach Induktionsannahme bereits bekannt ist, daß sie Primfaktorzerlegungen besitzen. □

Satz 1.4.6. *Es gibt unendlich viele Primzahlen.*

Beweis. Durch Widerspruch. Gäbe es nur endlich viele Primzahlen, so könnten wir deren Produkt betrachten und dazu Eins hinzuzählen. Die so neu entstehende Zahl müßte dann wie jede von Null verschiedene natürliche Zahl nach 1.4.4 eine Primfaktorzerlegung besitzen, aber keine unserer endlich vielen Primzahlen käme als Primfaktor in Frage. □

Ergänzung 1.4.7. Noch offen (2019) ist die Frage, ob es auch unendlich viele **Primzahlzwillinge** gibt, als da heißt, Paare von Primzahlen mit der Differenz Zwei, wie zum Beispiel $5, 7$ oder $11, 13$ oder $17, 19$. Ebenso offen ist die Frage, ob jede gerade Zahl $n > 2$ die Summe von zwei Primzahlen ist. Die Vermutung, daß das richtig sein sollte, ist bekannt als **Goldbach-Vermutung**. Bekannt ist, daß es unendlich viele Paare von Primzahlen mit einem Abstand ≤ 246 gibt.

Satz 1.4.8 (Eindeutigkeit der Primfaktorzerlegung). *Die Darstellung einer natürlichen Zahl $n \geq 1$ als ein Produkt von Primzahlen $n = p_1 p_2 \ldots p_r$ ist eindeutig bis auf die Reihenfolge der Faktoren. Nehmen wir zusätzlich $p_1 \leq p_2 \leq \ldots \leq p_r$ an, so ist unsere Darstellung mithin eindeutig.*

1.4.9. Dieser Satz ist einer von vielen Gründen, aus denen man bei der Definition des Begriffs einer Primzahl die Eins ausschließt, obwohl das die Definition verlängert: Hätten wir der Eins erlaubt, zu unseren Primzahlen dazuzugehören, so wäre der vorhergehende Satz in dieser Formulierung falsch. In obigem Satz ist $r \geq 0$ gemeint, genauer ist die Eins das leere Produkt und Primzahlen werden durch ein Produkt mit nur einem Faktor dargestellt.

Beweis. Der Beweis dieses Satzes braucht einige Vorbereitungen. Ich bitte Sie, gut aufzupassen, daß wir bei diesen Vorbereitungen den Satz über die Eindeutigkeit der Primfaktorzerlegung nirgends verwenden, bis er dann im Anschluß an Lemma 1.4.15 endlich bewiesen werden kann. □

Definition 1.4.10. Seien $a, b \in \mathbb{Z}$ ganze Zahlen. Wir sagen a **teilt** b oder a **ist ein Teiler von** b und schreiben $a|b$, wenn es $c \in \mathbb{Z}$ gibt mit $ac = b$.

Definition 1.4.11. Sind ganze Zahlen $a, b \in \mathbb{Z}$ nicht beide Null, so gibt es eine größte ganze Zahl $c \in \mathbb{Z}$, die sie beide teilt. Diese Zahl heißt der **größte gemeinsame Teiler** von a und b. Ganze Zahlen a und b heißen **teilerfremd**, wenn sie außer ± 1 keine gemeinsamen Teiler besitzen. Insbesondere sind also $a = 0$ und $b = 0$ nicht teilerfremd.

Satz 1.4.12 (über den größten gemeinsamen Teiler). *Gegeben zwei ganze Zahlen $a, b \in \mathbb{Z}$, die nicht beide Null sind, kann ihr größter gemeinsamer Teiler c als eine ganzzahlige Linearkombination unserer beiden Zahlen dargestellt werden. Es gibt also in Formeln $r, s \in \mathbb{Z}$ mit*

$$c = ra + sb$$

Teilt weiter $d \in \mathbb{Z}$ sowohl a als auch b, so teilt d auch den größten gemeinsamen Teiler von a und b.

1.4.13. Der letzte Teil dieses Satzes ist einigermaßen offensichtlich, wenn man die Eindeutigkeit der Primfaktorzerlegung als bekannt voraussetzt. Da wir besagte Eindeutigkeit der Primfaktorzerlegung jedoch erst aus besagtem zweiten Teil ableiten werden, ist es wichtig, auch für den zweiten Teil dieses Satzes einen eigenständigen Beweis zu geben.

Beweis. Man betrachte die Teilmenge $a\mathbb{Z} + b\mathbb{Z} = \{ar + bs \mid r, s \in \mathbb{Z}\} \subset \mathbb{Z}$. Sie ist offensichtlich eine von Null verschiedene Untergruppe von $\mathbb{Z}$. Also ist sie nach unserer Klassifikation 1.3.4 der Untergruppen von $\mathbb{Z}$ von der Form $a\mathbb{Z} + b\mathbb{Z} = \hat{c}\mathbb{Z}$ für genau ein $\hat{c} > 0$ und es gilt:

i. $\hat{c}$ teilt a und b. In der Tat haben wir ja $a, b \in \hat{c}\mathbb{Z}$;

ii. $\hat{c} = ra + sb$ für geeignete $r, s \in \mathbb{Z}$. In der Tat haben wir ja $\hat{c} \in a\mathbb{Z} + b\mathbb{Z}$;

iii. (d teilt a und b) $\Rightarrow$ (d teilt $\hat{c}$).

Daraus folgt sofort, daß $\hat{c}$ der größte gemeinsame Teiler von a und b ist, und damit folgt dann der Satz. □

1.4.14 (**Notation für größte gemeinsame Teiler**). Gegeben $a_1, \ldots, a_n \in \mathbb{Z}$ können wir mit der Notation 1.3.5 kürzer schreiben

$$a_1\mathbb{Z} + \ldots + a_n\mathbb{Z} = \langle a_1, \ldots, a_n \rangle$$

Üblich ist hier auch die Notation $(a_1, \ldots, a_n)$, die jedoch oft auch n-Tupel von ganzen Zahlen bezeichnet, also Elemente von $\mathbb{Z}^n$, und in der Analysis im Fall $n = 2$ meist ein offenes Intervall. Es gilt dann aus dem Kontext zu erschließen, was jeweils gemeint ist. Sind a und b nicht beide Null und ist c ihr größter gemeinsamer Teiler, so haben wir nach dem Vorhergehenden $\langle a, b \rangle = \langle c \rangle$. Wir benutzen von nun an diese Notation. Über die Tintenersparnis hinaus hat sie den Vorteil, auch im Fall $a = b = 0$ sinnvoll zu bleiben.

Lemma 1.4.15 (von Euklid). *Teilt eine Primzahl ein Produkt von zwei ganzen Zahlen, so teilt sie einen der Faktoren.*

1.4.16 (**Diskussion der Terminologie**). Dies Lemma findet sich bereits in Euklid's Elementen in Buch VII als Proposition 30.

1.4.17. Wenn wir die Eindeutigkeit der Primfaktorzerlegung als bekannt voraussetzen, so ist dies Lemma offensichtlich. Diese Argumentation hilft aber hier nicht weiter, da sie voraussetzt, was wir gerade erst beweisen wollen. Sicher ist Ihnen die Eindeutigkeit der Primfaktorzerlegung aus der Schule und ihrer Rechenerfahrung wohlvertraut. Um die Schwierigkeit zu sehen, sollten Sie vielleicht selbst einmal versuchen, einen Beweis dafür anzugeben. Im übrigen werden wir in 6.4.8 sehen, daß etwa im Ring $\mathbb{Z}[\sqrt{-5}]$ das Analogon zur Eindeutigkeit der Primfaktorzerlegung nicht mehr richtig ist.

Beweis. Sei p unsere Primzahl und seien $a, b \in \mathbb{Z}$ gegeben mit $p|ab$. Teilt p nicht a, so folgt für den größten gemeinsamen Teiler $\langle p, a\rangle = \langle 1\rangle$, denn die Primzahl p hat nur die Teiler ± 1 und $\pm p$. Der größte gemeinsame Teiler von p und a kann aber nicht p sein und muß folglich 1 sein. Nach 1.4.12 gibt es also $r, s \in \mathbb{Z}$ mit $1 = rp + sa$. Es folgt $b = rpb + sab$ und damit $p|b$, denn p teilt natürlich rpb und teilt nach Annahme auch sab. □

Beweis der Eindeutigkeit der Primfaktorzerlegung 1.4.8. Zunächst bemerken wir, daß aus Lemma 1.4.15 per Induktion dieselbe Aussage auch für Produkte beliebiger Länge folgt: Teilt eine Primzahl ein Produkt, so teilt sie einen der Faktoren. Seien $n = p_1 p_2 \ldots p_r = q_1 q_2 \ldots q_s$ zwei Primfaktorzerlegungen derselben Zahl $n \geq 1$. Da p_1 unser n teilt, muß es damit eines der q_i teilen. Da auch dies q_i prim ist, folgt $p_1 = q_i$. Wir kürzen den gemeinsamen Primfaktor und sind fertig per Induktion. □

1.4.18. Ich erkläre am Beispiel $a = 160$, $b = 625$ den sogenannten **euklidischen Algorithmus**, mit dem man den größten gemeinsamen Teiler c zweier positiver natürlicher Zahlen a, b bestimmen kann nebst einer Darstellung $c = ra + rb$. In unseren Gleichungen wird jeweils geteilt mit Rest.

$$\begin{aligned} 160 &= 1\cdot\ 145 \ +\ 15\\ 145 &= 9\cdot\ \ 15 \ +\ 10\\ 15 &= 1\cdot\ \ 10 \ +\ \ 5\\ 10 &= 2\cdot\ \ \ 5 \ +\ \ 0 \end{aligned}$$

Daraus folgt für den größten gemeinsamen Teiler $\langle 625, 160\rangle = \langle 160, 145\rangle = \langle 145, 15\rangle = \langle 15, 10\rangle = \langle 10, 5\rangle = \langle 5, 0\rangle = \langle 5\rangle$. Die vorletzte Zeile liefert eine Darstellung $5 = x \cdot 10 + y \cdot 15$ unseres größten gemeinsamen Teilers $5 = \mathrm{ggT}(10, 15)$ als ganzzahlige Linearkombination von 10 und 15. Die vorvorletzte Zeile eine Darstellung $10 = x' \cdot 15 + y' \cdot 145$ und nach Einsetzen in die vorherige Gleichung

eine Darstellung $5 = x(x' \cdot 15 + y' \cdot 145) + y \cdot 15$ unseres größten gemeinsamen Teilers $5 = \mathrm{ggT}(15, 145)$ als ganzzahlige Linearkombination von 15 und 145. Indem wir so induktiv hochsteigen, erhalten wir schließlich für den größten gemeinsamen Teiler die Darstellung $5 = -11 \cdot 625 + 43 \cdot 160$.

Ergänzung 1.4.19. Gegeben eine positive natürliche Zahl n bezeichne $\mathrm{rad}(n)$ das Produkt ohne Vielfachheiten aller Primzahlen, die n teilen. Die **ABC-Vermutung** besagt, daß es für jedes $\varepsilon > 0$ nur endlich viele Tripel von paarweise teilerfremden positiven natürlichen Zahlen a, b, c geben soll mit $a + b = c$ und

$$c > (\mathrm{rad}(abc))^{1+\varepsilon}$$

Es soll also salopp gesprochen sehr selten sein, daß für teilerfremde positive natürliche Zahlen a, b mit vergleichsweise kleinen Primfaktoren ihre Summe auch nur kleine Primfaktoren hat. Der Status der Vermutung ist zur Zeit (2019) noch ungeklärt. Man kann zeigen, daß es unendlich viele Tripel von paarweise teilerfremden positiven natürlichen Zahlen $a < b < c$ gibt mit $a + b = c$ und $c \geq \mathrm{rad}(abc)$. Diese sind jedoch bereits vergleichsweise selten, so gibt es etwa nur 120 mögliche Tripel mit $c < 10000$.

Übungen

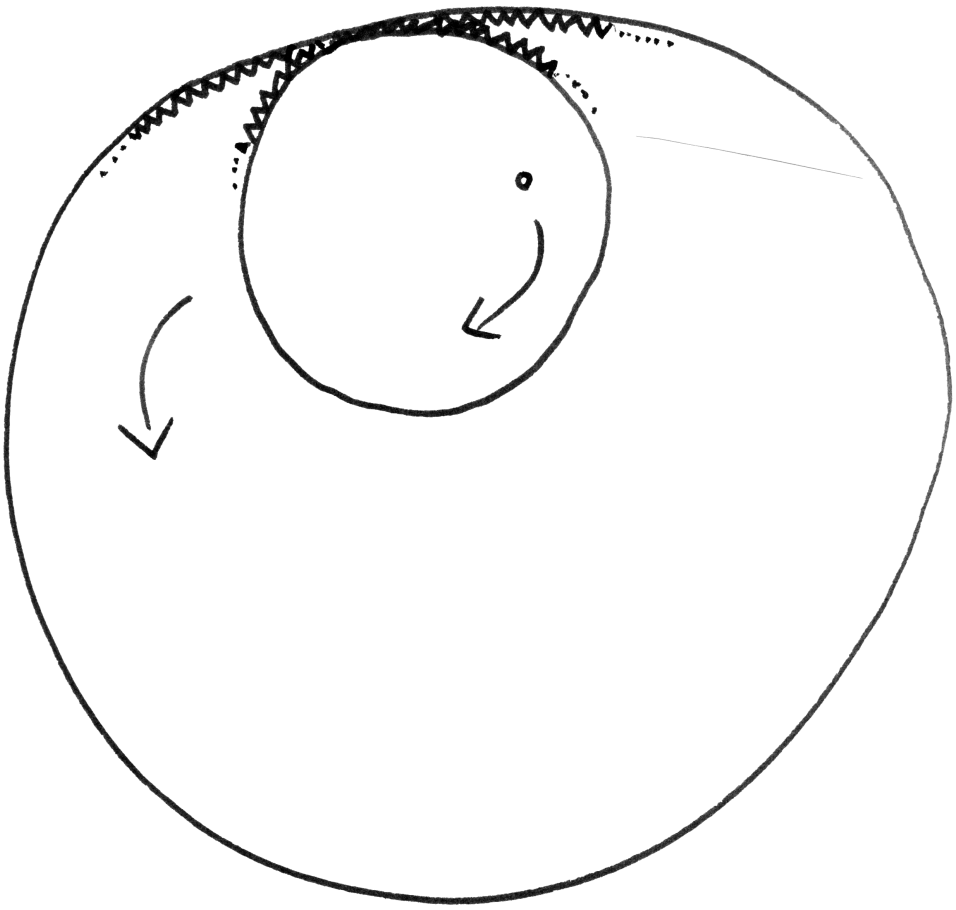
Übung 1.4.20. Man berechne den größten gemeinsamen Teiler von 3456 und 436 und eine Darstellung desselben als ganzzahlige Linearkombination unserer beiden Zahlen.

Übung 1.4.21. Gegeben zwei von Null verschiedene natürliche Zahlen a, b nennt man die kleinste von Null verschiedene natürliche Zahl, die sowohl ein Vielfaches von a als auch ein Vielfaches von b ist, das **kleinste gemeinsame Vielfache** von a und b und notiert sie $\mathrm{kgV}(a, b)$. Man zeige in dieser Notation die Formel $\mathrm{kgV}(a, b)\,\mathrm{ggT}(a, b) = ab$.

Ergänzende Übung 1.4.22. Beim sogenannten „Spirographen“, einem Zeichenspiel für Kinder, kann man an einem innen mit 105 Zähnen versehenen Ring ein Zahnrad mit 24 Zähnen entlanglaufen lassen. Steckt man dabei einen Stift durch ein Loch außerhalb des Zentrums des Zahnrads, so entstehen dabei die köstlichsten Figuren. Wie oft muß das Zahnrad auf dem inneren Zahnkranz umlaufen, bevor solch eine Figur fertig gemalt ist?

Ergänzende Übung 1.4.23. Berechnen Sie, wieviele verschiedene Strophen das schöne Lied hat, dessen erste Strophe lautet:

> Tomatensalat Tomatensalat Tooo-
> -matensalat Tomatensaaaaaaaa-
> -lat Tomatensalat Tomatensalat
> Tomatensalat Tomatensaaaaaaa-



Der Spirograph aus Übung 1.4.22

2 Ringe und Polynome

2.1 Ringe

Definition 2.1.1. Ein **Ring**, französisch **anneau**, ist eine Menge mit zwei Verknüpfungen $(R, +, \cdot)$ derart, daß gilt:

1. $(R, +)$ ist eine kommutative Gruppe;
2. $(R, \cdot)$ ist ein Monoid; ausgeschrieben heißt das nach **??**, daß auch die Verknüpfung $\cdot$ assoziativ ist und daß es ein Element $1 = 1_R \in R$ mit der Eigenschaft $1 \cdot a = a \cdot 1 = a \quad \forall a \in R$ gibt, das **Eins-Element** oder kurz die **Eins** unseres Rings;
3. Es gelten die Distributivgesetze, als da heißt, für alle $a, b, c \in R$ gilt

$$\begin{aligned} a \cdot (b + c) &= (a \cdot b) + (a \cdot c) \\ (a + b) \cdot c &= (a \cdot c) + (b \cdot c) \end{aligned}$$

Die beiden Verknüpfungen heißen die **Addition** und die **Multiplikation** in unserem Ring. Das Element $1 \in R$ aus unserer Definition ist wohlbestimmt als das neutrale Element des Monoids $(R, \cdot)$, vergleiche **??**. Ein Ring, dessen Multiplikation kommutativ ist, heißt ein **kommutativer Ring** und bei uns in unüblicher Verkürzung ein **Kring**.

2.1.2. Wir schreiben meist kürzer $a \cdot b = ab$ und vereinbaren die Regel „Punkt vor Strich“, so daß zum Beispiel das erste Distributivgesetz auch übersichtlicher in der Form $a(b + c) = ab + ac$ geschrieben werden kann.

Beispiel 2.1.3. Die ganzen Zahlen $\mathbb{Z}$ bilden mit der üblichen Multiplikation und Addition nach 1.2.12 einen kommutativen Ring.

2.1.4 (**Ursprung der Terminologie**). Der Begriff „Ring“ soll zum Ausdruck bringen, daß diese Struktur nicht in demselben Maße „geschlossen“ ist wie ein Körper, da wir nämlich nicht die Existenz von multiplikativen Inversen fordern. Er wird auch im juristischen Sinne für gewisse Arten weniger geschlossenener Körperschaften verwendet. So gibt es etwa den „Ring deutscher Makler“ oder den „Ring deutscher Bergingenieure“.

2.1.5 (**Diskussion der Terminologie**). Eine Struktur wie in der vorhergehenden Definition, bei der nur die Existenz eines Einselements nicht gefordert wird, bezeichnen wir im Vorgriff auf **??** als eine **assoziative $\mathbb{Z}$-Algebra**. In der Literatur wird jedoch auch diese Struktur oft als „Ring“ bezeichnet, sogar bei der von mir hochgeschätzten Quelle Bourbaki. Die Ringe, die eine Eins besitzen, heißen in dieser Terminologie „unitäre Ringe“.

Ergänzung 2.1.6. Allgemeiner als in **??** erklärt heißt ein Element a eines beliebigen Ringes, ja einer beliebigen assoziativen $\mathbb{Z}$-Algebra **nilpotent**, wenn es $d \in \mathbb{N}$ gibt mit $a^d = 0$.

Beispiele 2.1.7. Die einelementige Menge mit der offensichtlichen Addition und Multiplikation ist ein Ring, der **Nullring**. Jeder Körper ist ein Ring. Die ganzen Zahlen $\mathbb{Z}$ bilden einen Ring. Ist R ein Ring und X eine Menge, so ist die Menge $\mathrm{Ens}(X, R)$ aller Abbildungen von X nach R ein Ring unter punktweiser Multiplikation und Addition. Ist R ein Ring und $n \in \mathbb{N}$, so bilden die $(n \times n)$-Matrizen mit Einträgen in R einen Ring $\mathrm{Mat}(n; R)$ unter der üblichen Addition und Multiplikation von Matrizen; im Fall $n = 0$ erhalten wir den Nullring, im Fall $n = 1$ ergibt sich R selbst. Ist A eine abelsche Gruppe, so bilden die Gruppenhomomorphismen von A in sich selbst, die sogenannten **Endomorphismen** von A, einen Ring mit der Verknüpfung von Abbildungen als Multiplikation und der punktweisen Summe als Addition. Man notiert diesen Ring

$$\mathrm{End}A$$

und nennt ihn den **Endomorphismenring der abelschen Gruppe** A. Ähnlich bilden auch die Endomorphismen eines Vektorraums V über einem Körper k einen Ring $\mathrm{End}_k V$, den sogenannten **Endomorphismenring von** V. Oft notiert man auch den Endomorphismenring eines Vektorraums abkürzend $\mathrm{End}V$ in der Hoffnung, daß aus dem Kontext klar wird, daß die Endomorphismen von V als Vektorraum gemeint sind und nicht die Endomorphismen der V zugrundeliegenden abelschen Gruppe. Will man besonders betonen, daß die Endomorphismen als Gruppe gemeint sind, so schreibt man manchmal auch $\mathrm{End}_{\mathbb{Z}} A$ aus Gründen, die erst in **??** erklärt werden. Ich verwende für diesen Ring zur Vermeidung von Indizes lieber die Notation $\mathrm{End}_{\mathbb{Z}} A = \mathrm{Ab}A$, die sich aus den allgemeinen kategorientheoretischen Konventionen **??** ergibt.

Definition 2.1.8. Eine Abbildung $\varphi : R \to S$ von einem Ring in einen weiteren Ring heißt ein **Ringhomomorphismus**, wenn gilt $\varphi(1) = 1$ und $\varphi(a + b) = \varphi(a) + \varphi(b)$ sowie $\varphi(ab) = \varphi(a)\varphi(b)$ für alle $a, b \in R$. In anderen Worten ist ein Ringhomomorphismus also eine Abbildung, die sowohl für die Addition als auch für die Multiplikation ein Monoidhomomorphismus ist. Die Menge aller Ringhomomorphismen von einem Ring R in einen Ring S notieren wir

$$\mathrm{Ring}(R, S)$$

Ergänzung 2.1.9. Von Homomorphismen zwischen $\mathbb{Z}$-Algebren können wir natürlich nicht fordern, daß sie das Einselement auf das Einselement abbilden. Wir sprechen dann von **Algebrenhomomorphismen**. In der Terminologie, in der unsere assoziativen $\mathbb{Z}$-Algebren als Ringe bezeichnet werden, werden unsere Ringhomomorphismen „unitäre Ringhomomorphismen“ genannt.

Proposition 2.1.10. *Für jeden Ring R gibt es genau einen Ringhomomorphismus $\mathbb{Z} \to R$, in Formeln $|\operatorname{Ring}(\mathbb{Z}, R)| = 1$.*

Beweis. Nach **??** gibt es genau einen Gruppenhomomorphismus von additiven Gruppen $\varphi : \mathbb{Z} \to R$, der die $1 \in \mathbb{Z}$ auf $1_R \in R$ abbildet. Wir müssen nur noch zeigen, daß er mit der Multiplikation verträglich ist, in Formeln $\varphi(nm) = \varphi(n)\varphi(m)$ für alle $n, m \in \mathbb{Z}$. Mit 2.1.15 zieht man sich leicht auf den Fall $n, m > 0$ zurück. In diesem Fall beginnt man mit der Erkenntnis $\varphi(1 \cdot 1) = \varphi(1) = 1_R = 1_R \cdot 1_R = \varphi(1)\varphi(1)$ und argumentiert von da aus mit vollständiger Induktion und dem Distributivgesetz. □

2.1.11 (**Ganze Zahlen und allgemeine Ringe**). Gegeben ein Ring R notieren wir den Ringhomomorphismus $\mathbb{Z} \to R$ aus 2.1.10 manchmal $n \mapsto n_R$ und meist $n \mapsto n$. Ich will kurz diskutieren, warum das ungefährlich ist. Gegeben $r \in R$ und $n \in \mathbb{Z}$ gilt nämlich stets $nr = n_R r = r n_R$, wobei nr in Bezug auf die Struktur von R als additive abelsche Gruppe verstehen, also $nr = n^+ r = r + r \ldots + r$ mit n Summanden falls $n \geq 1$ und so weiter, wie in der Tabelle **??** und in **??** ausgeführt wird. Unsere Gleichung $nr = n_R r = r n_R$ bedeutet dann hinwiederum, daß es auf den Unterschied zwischen n_R und n meist gar nicht ankommt. Deshalb führt es auch selten zu Mißvertändnissen, wenn wir statt n_R nur kurz n schreiben.

2.1.12. Eine Teilmenge eines Rings heißt ein **Teilring**, wenn sie eine additive Untergruppe und ein multiplikatives Untermonoid ist. Ist also R unser Ring, so ist eine Teilmenge $T \subset R$ genau dann ein Teilring, wenn gilt $0_R, 1_R \in T$, $a \in T \Rightarrow (-a) \in T$ sowie $a, b \in T \Rightarrow a + b, ab \in T$. Wir diskutieren diesen Begriff hier nur im Vorbeigehen, da er in dieser Vorlesung nur eine Nebenrolle spielt.

Übungen

Übung 2.1.13 (**Quotientenring**). Gegeben ein Ring R und eine Surjektion $R \twoheadrightarrow Q$ von R auf eine Menge Q, die an die Multiplikation und Addition von R angepaßt ist im Sinne von **??**, ist Q mit der koinduzierten Addition und Multiplikation auch wieder ein Ring.

Ergänzende Übung 2.1.14. Auf der abelschen Gruppe $\mathbb{Z}$ gibt es genau zwei Verknüpfungen, die als Multiplikation genommen die Addition zu einer Ringstruktur ergänzen.

Übung 2.1.15. Man zeige, daß in jedem Ring R gilt $0a = 0\ \forall a \in R$; $-a = (-1)a\ \forall a \in R$; $(-1)(-1) = 1$; $(-a)(-b) = ab\ \forall a, b \in R$.

Übung 2.1.16. Gegeben eine Überdeckung einer endlichen Menge X durch Teilmengen $X = X_1 \cup \ldots \cup X_n$ zeige man die **Einschluß-Ausschluß-Formel**

$$0 = \sum_{I \subset \{1,\ldots,n\}} (-1)^{|I|} \left| \bigcap_{i \in I} X_i \right|$$

mit der Interpretation des leeren Schnitts als X. Im Fall $n = 3$ etwa können wir das ausschreiben zu

$$|X \cup Y \cup Z| = |X| + |Y| + |Z| - |X \cup Y| - |X \cup Z| - |Y \cup Z| + |X \cup Y \cup Z|$$

Hinweis: Sogar im Fall einer beliebigen Menge X mit beliebigen Teilmengen X_i mag man deren charakteristische Funktionen mit χ_i bezeichnen und im Ring der $\mathbb{Z}$-wertigen Funktionen auf X das Produkt $(1-\chi_1)\dots(1-\chi_n)$ ausmultiplizieren.

Übung 2.1.17. Für jeden Ring R gibt es höchstens einen Ringhomomorphismus $\mathbb{Q} \to R$, in Formeln $|\operatorname{Ring}(\mathbb{Q}, R)| \leq 1$.

2.2 Restklassenringe des Rings der ganzen Zahlen

Definition 2.2.1. Gegeben $G \supset H$ eine Gruppe mit einer Untergruppe definieren wir den **Quotienten** G/H, eine Teilmenge $G/H \subset \mathcal{P}(G)$, durch die Vorschrift

$$G/H := \{L \subset G \mid \exists g \in G \text{ mit } L = gH\}$$

Die Teilmenge $gH \subset G$ heißt die **H-Linksnebenklasse von g in G**. Unser Quotient ist also die Menge aller H-Linksnebenklassen in G. Jedes Element einer Linksnebenklasse heißt auch ein **Repräsentant** besagter Linksnebenklasse. Eine Teilmenge $R \subset G$ derart, daß die Vorschrift $g \mapsto gH$ eine Bijektion $R \xrightarrow{\sim} G/H$ induziert, heißt ein **Repräsentantensystem** für die Menge der Linksnebenklassen.

Vorschau 2.2.2. Diese Konstruktion wird in 3.1.2 noch sehr viel ausführlicher diskutiert werden.

Beispiel 2.2.3. Im Fall der additiven Gruppe $\mathbb{Z}$ mit der Untergruppe $m\mathbb{Z}$ haben wir speziell $\mathbb{Z}/m\mathbb{Z} = \{L \subset \mathbb{Z} \mid \exists a \in \mathbb{Z} \text{ mit } L = a + m\mathbb{Z}\}$. Die Linksnebenklasse von a heißt in diesem Fall auch die **Restklasse von a modulo m**, da zumindest im Fall $a \geq 0$ und $m > 0$ ihre nichtnegativen Elemente genau alle natürlichen Zahlen sind, die beim Teilen durch m denselben Rest lassen wie a. Wir notieren diese Restklasse auch $\bar{a}$. Natürlich ist $\bar{a} = \bar{b}$ gleichbedeutend zu $a - b \in m\mathbb{Z}$. Gehören a und b zur selben Restklasse, in Formeln $a + m\mathbb{Z} = b + m\mathbb{Z}$, so nennen wir sie **kongruent modulo** m und schreiben

$$a \equiv b \pmod{m}$$

Offensichtlich gibt es für $m > 0$ genau m Restklassen modulo m, in Formeln $|\mathbb{Z}/m\mathbb{Z}| = m$, und wir haben genauer

$$\mathbb{Z}/m\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{m-1}\}$$

Da in dieser Aufzählung keine Nebenklassen mehrfach genannt werden, ist die Teilmenge $\{0, 1, \ldots, m-1\}$ also ein Repräsentantensystem für die Menge von Nebenklassen $\mathbb{Z}/m\mathbb{Z}$. Ein anderes Repräsentantensystem wäre $\{1, \ldots, m\}$, ein Drittes $\{1, \ldots, m-1, 7m\}$.

Satz 2.2.4 (**Restklassenring**). *Für alle $m \in \mathbb{Z}$ gibt es auf der Menge $\mathbb{Z}/m\mathbb{Z}$ genau eine Struktur als Ring derart, daß die Abbildung $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/m\mathbb{Z}$ mit $a \mapsto \bar{a}$ ein Ringhomomorphismus ist.*

2.2.5. Das ist dann natürlich die Struktur als Quotientenring im Sinne unserer Übung 2.1.13.

Beweis. Daß es höchstens eine derartige Ringstruktur gibt, es eh klar. Zu zeigen bleibt nur deren Existenz. Nach **??** induziert jede Verknüpfung auf einer Menge A eine Verknüpfung auf ihrer Potenzmenge $\mathcal{P}(A)$. Für die so von der Verknüpfung $+$ auf $\mathbb{Z}$ induzierte Verknüpfung $+$ auf $\mathcal{P}(\mathbb{Z})$ gilt offensichtlich

$$\bar{a} + \bar{b} = (a + m\mathbb{Z}) + (b + m\mathbb{Z}) = (a + b) + m\mathbb{Z} = \overline{a+b} \quad \forall a, b \in \mathbb{Z}$$

Insbesondere induziert unsere Verknüpfung $+$ auf $\mathcal{P}(\mathbb{Z})$ eine Verknüpfung $+$ auf $\mathbb{Z}/m\mathbb{Z}$ und $a \mapsto \bar{a}$ ist für diese Verknüpfungen ein Morphismus von Magmas alias Mengen mit Verknüpfung. Ebenso können wir auf $\mathcal{P}(\mathbb{Z})$ eine Verknüpfung $\odot = \odot_m$ einführen durch die Vorschrift

$$T \odot S := T \cdot S + m\mathbb{Z} := \{ab + mr \mid a \in T, b \in S, r \in \mathbb{Z}\}$$

Wieder prüft man für die so erklärte Multiplikation mühelos die Formel

$$\bar{a} \odot \bar{b} = \overline{ab}$$

Daß $\mathbb{Z}/m\mathbb{Z}$ mit unseren beiden Verknüpfungen ein Ring wird und $a \mapsto \bar{a}$ ein Ringhomomorphismus, folgt ohne weitere Schwierigkeiten aus der Surjektivität der natürlichen Abbildung $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/m\mathbb{Z}$ alias Übung 2.1.13. □

2.2.6. Wir geben wir die komische Notation $\odot$ nun auch gleich wieder auf und schreiben stattdessen $\bar{a} \cdot \bar{b}$ oder noch kürzer $\bar{a}\bar{b}$. Auch die Notation $\bar{a}$ werden wir meist zu a vereinfachen, wie wir es ja in 2.1.11 eh schon vereinbart hatten.

Beispiel 2.2.7. Modulo $m = 2$ gibt es genau zwei Restklassen: Die Elemente der Restklasse von 0 bezeichnet man üblicherweise als **gerade Zahlen**, die Elemente der Restklasse von 1 als **ungerade Zahlen**. Der Ring $\mathbb{Z}/2\mathbb{Z}$ mit diesen beiden Elementen $\bar{0}$ und $\bar{1}$ ist offensichtlich sogar ein Körper.

Beispiel 2.2.8 (**Der Ring $\mathbb{Z}/12\mathbb{Z}$ der Uhrzeiten**). Den Ring $\mathbb{Z}/12\mathbb{Z}$ könnte man als „Ring von Uhrzeiten“ ansehen. Er hat die zwölf Elemente $\{\bar{0}, \bar{1}, \ldots, \overline{11}\}$ und wir haben $\overline{11} + \bar{5} = \overline{16} = \bar{4}$ alias „5 Stunden nach 11 Uhr ist es 4 Uhr“. Weiter haben wir in $\mathbb{Z}/12\mathbb{Z}$ etwa auch $\bar{3}\cdot\bar{8} = \overline{24} = \bar{0}$. In einem Ring kann es also durchaus passieren, daß ein Produkt von zwei von Null verschiedenen Faktoren Null ist.

Vorschau 2.2.9. Sei $m \geq 1$ eine natürliche Zahl. Eine Restklasse modulo m heißt eine **prime Restklasse**, wenn sie aus zu m teilerfremden Zahlen besteht. Wir zeigen in **??**, daß es in jeder primen Restklasse unendlich viele Primzahlen gibt. Im Fall $m = 10$ bedeutet das zum Beispiel, daß es jeweils unendlich viele Primzahlen gibt, deren Dezimaldarstellung mit einer der Ziffern $1, 3, 7$ und 9 endet.

Proposition 2.2.10 (**Teilbarkeitskriterien über Quersummen**)**.** *Eine natürliche Zahl ist genau dann durch Drei beziehungsweise durch Neun teilbar, wenn ihre Quersumme durch Drei beziehungsweise durch Neun teilbar ist.*

Beweis. Wir erklären das Argument nur an einem Beispiel. Das ist natürlich im Sinne der Logik kein Beweis. Dies Vorgehen schien mir aber in diesem Fall besonders gut geeignet, dem Leser den Grund dafür klarzumachen, aus dem unsere Aussage im Allgemeinen gilt. Und das ist es ja genau, was ein Beweis in unserem mehr umgangssprachlichen Sinne leisten soll! Also frisch ans Werk. Per definitionem gilt

$$1258 = 1 \cdot 10^3 + 2 \cdot 10^2 + 5 \cdot 10 + 8$$

Offensichtlich folgt

$$1258 \equiv 1 \cdot 10^3 + 2 \cdot 10^2 + 5 \cdot 10 + 8 \pmod 3$$

Da 10 kongruent ist zu 1 modulo 3 erhalten wir daraus

$$1258 \equiv 1 + 2 + 5 + 8 \pmod 3$$

Insbesondere ist die rechte Seite durch Drei teilbar genau dann, wenn die linke Seite durch Drei teilbar ist. Das Argument für Neun statt Drei geht genauso. □

2.2.11. In $\mathbb{Z}/12\mathbb{Z}$ gilt zum Beispiel $\bar{3} \cdot \bar{5} = \bar{3} \cdot \bar{1}$. In allgemeinen Ringen dürfen wir also nicht kürzen. Dies Phänomen werden wir nun begrifflich fassen. Dazu vereinbaren wir, daß bei Ringen unsere allgemeinen Konventionen **??** zu Kürzbarkeit und Teilen stets in Bezug auf die Multiplikation zu verstehen sein sollen. Wir schreiben das auch noch aus.

Definition 2.2.12. 1. Gegeben ein Ring R und Elemente $a, b \in R$ sagen wir, a **teilt** b oder auch a ist ein **Teiler von** b und schreiben $a|b$, wenn es $d \in R$ gibt mit $ad = b$. Ist unser Ring nicht kommutativ, so nennen wir a genauer einen **Linksteiler** von b und erklären analog **Rechtsteiler**;

2. Ein Element $a \in R$ eines Rings heißt **linkskürzbar**, wenn die Multiplikation mit a eine Injektion $(a\cdot) : R \hookrightarrow R$ liefert. Analog erklären wir die Eigenschaft **rechtskürzbar**. Ein Element, das linkskürzbar und rechtskürzbar ist, nennen wir **kürzbar**. Ein nicht kürzbares Element nennen wir **nichtkürzbar**;

3. Ein Ring heißt ein **Integritätsring** oder **Integritätsbereich**, wenn er nicht der Nullring ist und das Produkt von je zwei von Null verschiedenen Elementen von Null verschieden ist. Einen kommutativen Integritätsring nennen wir auch einen **Integritätskring**.

Beispiel 2.2.13. Die nichtkürzbaren Elemente in $\mathbb{Z}/12\mathbb{Z}$ sind $0, 2, 3, 4, 6, 8, 9, 10$.

2.2.14 (**Diskussion der Terminologie**). In der Literatur heißen die nichtkürzbaren Elemente eines Rings meist die „Nullteiler“. Mir gefiel diese Terminologie nicht, da ja nach unseren sonstigen Definitionen alle Elemente eines Rings Teiler der Null sind.

2.2.15 (**Kürzen in Ringen**). Sei R ein Ring. Natürlich ist der Gruppenhomomorphismus $(a\cdot) : R \to R$ genau dann injektiv, wenn sein Kern Null ist, wenn also gilt $ax = 0 \Rightarrow x = 0$.

Definition 2.2.16. Ein Element a eines Rings R heißt **invertierbar** oder genauer **invertierbar in** R oder auch eine **Einheit von** R, wenn es bezüglich der Multiplikation invertierbar ist im Sinne von **??**, wenn es also $b \in R$ gibt mit $ab = ba = 1$. Die Menge der invertierbaren Elemente eines Rings bildet unter der Multiplikation eine Gruppe, die man die **Gruppe der Einheiten von** R nennt und gemäß unserer allgemeinen Konventionen **??** mit $R^\times$ bezeichnet.

Beispiel 2.2.17. Der Ring $\mathbb{Z}$ der ganzen Zahlen hat genau zwei Einheiten, nämlich 1 und (-1). In Formeln haben wir also $\mathbb{Z}^\times = \{1, -1\}$. Dahingegen sind die Einheiten im Ring $\mathbb{Q}$ der rationalen Zahlen genau alle von Null verschiedenen Elemente, in Formeln $\mathbb{Q}^\times = \mathbb{Q}\backslash 0$.

2.2.18. Eine Einheit eines Krings teilt alle Elemente unseres Krings und ist sogar dasselbe wie ein Teiler der Eins.

Definition 2.2.19. Zwei Elemente eines Krings heißen **teilerfremd**, wenn sie außer Einheiten keine gemeinsamen Teiler haben.

2.2.20. Allgemeiner mag man eine Teilmenge eines Krings **teilerfremd** nennen, wenn es keine Nichteinheit unseres Krings gibt, die alle Elemente unserer Teilmenge teilt.

2.2.21 (**Kürzbare Elemente endlicher Kringe**). In einem endlichen Kring R sind die Einheiten genau die kürzbaren Elemente. In der Tat ist in diesem Fall die Multiplikation $(a\cdot) : R \to R$ genau dann injektiv, wenn sie bijektiv ist.

Beispiel 2.2.22. Die Einheiten von $\mathbb{Z}/12\mathbb{Z}$ sind mithin genau $1, 5, 7, 11$. Man prüft unschwer, daß sogar jedes dieser Elemente sein eigenes Inverses ist. Mithin ist die Einheitengruppe $(\mathbb{Z}/12\mathbb{Z})^\times$ des Uhrzeitenrings gerade unsere Klein'sche Vierergruppe. Im allgemeinen ein Inverses zu a in $\mathbb{Z}/m\mathbb{Z}$ zu finden, läuft auf die Lösung der Gleichung $ax = 1 + my$ hinaus, von der wir bereits gesehen hatten, daß der euklidische Algorithmus das leisten kann.

2.2.23 (**Ursprung der Terminologie**). A priori meint eine Einheit in der Physik das, was ein Mathematiker eine Basis eines eindimensionalen Vektorraums nennen würde. So wäre etwa die Sekunde s eine Basis des reellen Vektorraums $\vec{\mathbb{T}}$ aller Zeitspannen aus **??**. In Formeln ausgedrückt bedeutet das gerade, daß das Daranmultiplizieren von s eine Bijektion $\mathbb{R} \xrightarrow{\sim} \vec{\mathbb{T}}$ liefert. Mit den Einheiten eines kommutativen Ringes R verhält es sich nun genauso: Genau dann ist $u \in R$ eine Einheit, wenn das Daranmultiplizieren von u eine Bijektion $R \xrightarrow{\sim} R$ liefert. Daher rührt dann wohl auch die Terminologie.

Ergänzung 2.2.24. In der Chemie rechnet man oft mit **mol** und versteht darunter seit 2019 genau $6{,}02214076 \cdot 10^{23}$ und verwendet das als eine Einheit. Mathematisch gesehen sollte man das eigentlich eine Zahl nennen, aber natürlich ist $\mathbb{R}$ auch ein eindimensionaler reeller Vektorraum und in diesem Sinne mag man auch alle von Null verschiedenen Elemente von $\mathbb{R}$ Einheiten. Diese Konvention war früher noch sinnvoller, als man ein Mol als die Zahl der Kohlenstoffatome in einem Gramm des Standardisotops von Kohlenstoff erklärte und nicht so genau sagen konnte, wie viele Atome das nun genau sind.

2.2.25. Ein Körper kann in dieser Begrifflichkeit definiert werden als ein Integritätsring, in dem jedes von Null verschiedene Element eine Einheit ist.

Proposition 2.2.26 (Endliche Primkörper). *Sei $m \in \mathbb{N}$. Genau dann ist der Restklassenring $\mathbb{Z}/m\mathbb{Z}$ ein Körper, wenn m eine Primzahl ist.*

Beweis. Sei ohne Beschränkung der Allgemeinheit $m \geq 2$. Ist m keine Primzahl, so gibt es $a, b \in \mathbb{N}$ mit $a < m$ und $b < m$ aber $ab = m$. Dann gilt in $\mathbb{Z}/m\mathbb{Z}$ offensichtlich $\bar{a} \neq 0$ und $\bar{b} \neq 0$, aber ebenso offensichtlich gilt $\bar{a}\bar{b} = 0$ und $\mathbb{Z}/m\mathbb{Z}$ hat von Null verschiedene nicht invertierbare Elemente. Damit kann $\mathbb{Z}/m\mathbb{Z}$ kein Körper sein. Ist dahingegen $m = p$ eine Primzahl, so folgt aus dem Satz von Euklid 1.4.15, daß $\mathbb{Z}/p\mathbb{Z}$ ein Integritätsring ist. Dann aber sind nach 2.2.21 alle seine von Null verschiedenen Elemente Einheiten und $\mathbb{Z}/p\mathbb{Z}$ ist folglich ein Körper. □

2.2.27 (**Terminologie und Notation**). Die Körper $\mathbb{Z}/p\mathbb{Z}$ für Primzahlen p sowie der Körper $\mathbb{Q}$ sind die „kleinstmöglichen Körper" in einem Sinne, der in 7.1.6 präzisiert wird. Man nennt diese Körper deshalb auch **Primkörper**. Die endlichen Primkörper werden meist

$$\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$$

notiert, mit einem $\mathbb{F}$ für „field“ oder „finite“. Die Notation $\mathbb{F}_q$ verwendet man allerdings auch allgemeiner mit einer echten Primzahlpotenz q im Index als Bezeichnung für „den endlichen Körper mit q Elementen“, den wir erst in 7.7.1 kennenlernen werden, und der weder als Ring noch als abelsche Gruppe isomorph ist zu $\mathbb{Z}/q\mathbb{Z}$.

Ergänzung 2.2.28. Ich bespreche kurz das **Verfahren von Diffie-Hellman** zum öffentlichen Vereinbaren geheimer Schlüssel. Wir betrachten dazu das des folgende Schema:

Geheimbereich Alice	Öffentlicher Bereich	Geheimbereich Bob
	Bekanntgemacht wird eine Gruppe G und ein Element $g \in G$.	
Alice wählt $a \in \mathbb{N}$, berechnet g^a und macht es öffentlich.		Bob wählt $b \in \mathbb{N}$, berechnet g^b und macht es öffentlich.
	g^a, g^b	
Nach dem öffentlichen Austausch berechnet Alice $(g^b)^a = g^{ba} = g^{ab}$.		Nach dem öffentlichen Austauch berechnet Bob $(g^a)^b = g^{ab} = g^{ba}$.

Das Gruppenelement $g^{ba} = g^{ab}$ ist der gemeinsame hoffentlich geheime Schlüssel. Der Trick hierbei besteht darin, geeignete Paare (G, g) und eine geeignete Zahl a so zu finden, daß die Berechnung von g^a unproblematisch ist, daß jedoch kein schneller Algorithmus bekannt ist, der aus der Kenntnis von G, g und g^a ein mögliches a bestimmt, der also, wie man auch sagt, einen **diskreten Logarithmus von** g^a **zur Basis** g findet. Dann kann Alice g^a veröffentlichen und dennoch a geheim halten und ebenso kann Bob g^b veröffentlichen und dennoch b geheim halten. Zum Beispiel kann man für G die Einheitengruppe $G = (\mathbb{Z}/p\mathbb{Z})^\times$ des Primkörpers zu einer großen Primzahl p nehmen. Nun ist es natürlich denkbar, daß man aus der Kenntnis von g^a und g^b direkt g^{ab} berechnen kann, ohne zuvor a zu bestimmen, aber auch für die Lösung dieses sogenannten **Diffie-Hellman-Problems** ist in diesem Fall kein schneller Algorithmus bekannt. Mit den derzeitig verfügbaren Rechenmaschinen können also Alice und Bob mit einer Rechenzeit von unter einer Minute einen geheimen Schlüssel vereinbaren, dessen Entschlüsselung auf derselben Maschine beim gegenwärtigen Stand der veröffentlichten Forschung Millionen von Jahren bräuchte. Allerdings ist auch wieder nicht bewiesen, daß es etwa Fall der Einheitengruppe eines großen Primkörpers nicht doch einen effizienten Algorithmus zur Lösung des Diffie-Hellman-Problems geben könnte. Wenn wir Pech haben, sind die mathematischen Abteilungen irgendwelcher Geheimdienste

schon längst so weit.

Vorschau 2.2.29. Statt mit der Einheitengruppe endlicher Körper arbeitet man in der Praxis auch oft mit sogenannten „elliptischen Kurven“ alias Lösungsmengen kubischer Gleichungen, deren Gruppengesetz Sie in einer Vorlesung über algebraische Geometrie kennenlernen können.

Definition 2.2.30. Gegeben ein Ring R gibt es nach 2.1.10 genau einen Ringhomomorphismus $\mathbb{Z} \to R$. Dessen Kern alias das Urbild der Null ist nach **??** eine Untergruppe von $\mathbb{Z}$ und hat nach 1.3.4 folglich die Gestalt $m\mathbb{Z}$ für genau ein $m \in \mathbb{N}$. Diese natürliche Zahl m nennt man die **Charakteristik des Rings** R und notiert sie $m = \operatorname{char} R$.

2.2.31 (**Bestimmung der Charakteristik eines Rings**). Um die Charakteristik eines Rings R zu bestimmen, müssen wir anders gesagt sein Einselement $1 \in R$ nehmen und bestimmen, wiewiele Summanden wir mindestens brauchen, damit gilt $1 + 1 + \ldots + 1 = 0$ mit einer positiven Zahl von Summanden links. Kriegen wir da überhaupt nie Null heraus, so ist die Charakteristik Null, wir haben also etwa $\operatorname{char}\mathbb{Z} = \operatorname{char}\mathbb{Q} = \operatorname{char}\mathbb{R} = \operatorname{char}\mathbb{C} = 0$. Gilt bereits $1 = 0$, so ist die Charakteristik 1 und wir haben den Nullring vor uns. Für $p \in \mathbb{N}$ gilt allgemein $\operatorname{char}(\mathbb{Z}/p\mathbb{Z}) = p$.

2.2.32 (**Die Charakteristik eines Körpers ist stets prim**). Es ist leicht zu sehen, daß die Charakteristik eines Körpers, wenn sie nicht Null ist, stets eine Primzahl sein muß: Da der Nullring kein Körper ist, kann die Charakteristik nicht 1 sein. Hätten wir aber einen Körper der Charakteristik $m = ab > 0$ mit natürlichen Zahlen $a < m$ und $b < m$, so wären die Bilder von a und b in unserem Körper von Null verschiedene Elemente mit Produkt Null. Widerspruch!

Ergänzung 2.2.33. Im Körper $\mathbb{F}_7$ ist (-1) kein Quadrat, wie man durch Ausprobieren schnell prüft. Einen Körper mit 49 Elementen kann man deshalb nach **??** zum Beispiel erhalten, indem man analog wie bei der Konstruktion der komplexen Zahlen aus den reellen Zahlen formal eine Wurzel aus (-1) adjungiert.

Übungen

Ergänzende Übung 2.2.34. Gegeben eine abelsche Gruppe V und ein Körper K induziert die kanonische Identifikation $\operatorname{Ens}(K \times V, V) \xrightarrow{\sim} \operatorname{Ens}(K, \operatorname{Ens}(V, V))$ aus **??** eine Bijektion

$$\left\{ \begin{array}{c} \text{Strukturen als } K\text{-Vektorraum} \\ \text{auf der abelschen Gruppe } V \end{array} \right\} \xrightarrow{\sim} \left\{ \begin{array}{c} \text{Ringhomomorphismen} \\ K \to \operatorname{Ab} V \end{array} \right\}$$

Wir verwenden hier unsere alternative Notation $\operatorname{Ab} V$ für den Endomorphismenring der abelschen Gruppe V, um jede Verwechslung mit dem Endomorphismenring als Vektorraum auszuschließen.

Übung 2.2.35. Man finde das multiplikative Inverse der Nebenklasse von 22 im Körper $\mathbb{F}_{31}$. Hinweis: Euklidischer Algorithmus.

Ergänzende Übung 2.2.36. Man konstruiere einen Körper mit 49 Elementen und einen Körper mit 25 Elementen. Hinweis: **??** und **??**.

Ergänzende Übung 2.2.37. Sei R ein Kring, dessen Charakteristik eine Primzahl p ist, für den es also einen Ringhomomorphismus $\mathbb{Z}/p\mathbb{Z} \to R$ gibt. Man zeige, daß dann der sogenannte **Frobenius-Homomorphismus** $F : R \to R$, $a \mapsto a^p$ ein Ringhomomorphismus von R in sich selber ist. Hinweis: Man verwende, daß die binomische Formel **??** offensichtlich in jedem Kring gilt, ja sogar für je zwei Elemente a, b eines beliebigen Rings mit $ab = ba$.

Ergänzende Übung 2.2.38. Wieviele Untergruppen hat die abelsche Gruppe $\mathbb{Z}/4\mathbb{Z}$? Wieviele Untergruppen hat die abelsche Gruppe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$?

Ergänzende Übung 2.2.39. Eine natürliche Zahl ist durch 11 teilbar genau dann, wenn ihre „alternierende Quersumme“ durch 11 teilbar ist.

Ergänzende Übung 2.2.40. Eine natürliche Zahl, die kongruent zu sieben ist modulo acht, kann nicht eine Summe von drei Quadraten sein.

Ergänzende Übung 2.2.41. Eine Zahl mit einer Dezimaldarstellung der Gestalt $abcabc$ wie zum Beispiel 349349 ist stets durch 7 teilbar.

Ergänzende Übung 2.2.42. Es kann in Ringen durchaus Elemente a geben, für die es zwar ein b gibt mit $ba = 1$ aber kein c mit $ac = 1$: Man denke etwa an Endomorphismenringe unendlichdimensionaler Vektorräume. Wenn es jedoch b und c gibt mit $ba = 1$ und $ac = 1$, so folgt bereits $b = c$ und a ist eine Einheit.

Übung 2.2.43. Jeder Ringhomomorphismus macht Einheiten zu Einheiten. Jeder Ringhomomorphismus von einem Körper in einen vom Nullring verschiedenen Ring ist injektiv.

Übung 2.2.44. Sei p eine Primzahl. Eine abelsche Gruppe G kann genau dann mit der Struktur eines $\mathbb{F}_p$-Vektorraums versehen werden, wenn in additiver Notation gilt $pg = 0$ für alle $g \in G$, und die fragliche Vektorraumstruktur ist dann durch die Gruppenstruktur eindeutig bestimmt.

Ergänzende Übung 2.2.45. Wieviele Untervektorräume hat ein zweidimensionaler Vektorraum über einem Körper mit fünf Elementen? Wieviele angeordnete Basen?

Ergänzende Übung 2.2.46. Gegeben ein Vektorraum über einem endlichen Primkörper sind seine Untervektorräume genau die Untergruppen der zugrundeliegenden abelschen Gruppe.

Ergänzende Übung 2.2.47. Man zeige: In jedem endlichen Körper ist das Produkt aller von Null verschiedenen Elemente (-1). Hinweis: Man zeige zunächst, daß

nur die Elemente ± 1 ihre eigenen Inversen sind. Als Spezialfall erhält man die Kongruenz $(p-1)! \equiv -1 \pmod p$ für jede Primzahl p. Diese Aussage wird manchmal auch als **Satz von Wilson** zitiert. Ist $n \in \mathbb{N}_{\geq 1}$ keine Primzahl, so zeigt man im übrigen leicht $(n-1)! \equiv 0 \pmod n$.

Übung 2.2.48. Gegeben $m \geq 1$ sind die Einheiten des Restklassenrings $\mathbb{Z}/m\mathbb{Z}$ genau die Restklassen derjenigen Zahlen a mit $0 \leq a < m$, die zu m teilerfremd sind, in anderen Worten die primen Restklassen. In Formeln haben wir also $(\mathbb{Z}/m\mathbb{Z})^\times = \{\bar{a} \mid 0 \leq a < m,\ \langle m, a\rangle = \langle 1\rangle\}$. Hinweis: 1.4.12.

Übung 2.2.49. Man zeige für Binomialkoeffizienten im Körper $\mathbb{F}_p$ die Identität $\binom{p-1}{i} = (-1)^i$.

2.3 Polynome

2.3.1. Ist R ein Ring, so bildet die Menge $R[X]$ aller „formalen Ausdrücke“ der Gestalt $a_n X^n + \ldots + a_1 X + a_0$ mit $a_i \in R$ unter der offensichtlichen Addition und Multiplikation einen Ring, den **Polynomring über R in einer Variablen X**, und wir haben eine offensichtliche Einbettung $\mathrm{can} : R \hookrightarrow R[X]$. Die Herkunft der Bezeichnung diskutieren wir in **??**. Die a_ν heißen in diesem Zusammenhang die **Koeffizienten** unseres Polynoms, genauer heißt a_ν der **Koeffizient von X^ν**. Das X heißt die **Variable** unseres Polynoms und kann auch schon mal mit einem anderen Buchstaben bezeichnet werden. Besonders gebräuchlich sind hierbei Großbuchstaben vom Ende des Alphabets. Diese Beschreibung des Polynomrings ist hoffentlich verständlich, sie ist aber nicht so exakt, wie eine Definition es sein sollte. Deshalb geben wir auch noch eine exakte Variante.

Definition 2.3.2. Sei R ein Ring. Wir bezeichnen mit $R[X]$ die Menge aller Abbildungen $\varphi : \mathbb{N} \to R$, die nur an endlich vielen Stellen von Null verschiedene Werte annehmen, und definieren auf $R[X]$ eine Addition und eine Multiplikation durch die Regeln

$$\begin{array}{rcl} (\varphi + \psi)(n) & := & \varphi(n) + \psi(n) \\ (\varphi \cdot \psi)(n) & := & \sum_{i+j=n} \varphi(i)\psi(j) \end{array}$$

Mit diesen Verknüpfungen wird $R[X]$ ein Ring, der **Polynomring über R**. Ordnen wir jedem $a \in R$ die Abbildung $\mathbb{N} \to R$ zu, die bei 0 den Wert a annimmt und sonst den Wert Null, so erhalten wir eine Einbettung, ja einen injektiven Ringhomomorphismus

$$\mathrm{can} : R \hookrightarrow R[X]$$

Wir notieren ihn schlicht $a \mapsto a$ und nennen die Polynome im Bild dieser Einbettung **konstante Polynome**. Bezeichnen wir weiter mit X die Abbildung $\mathbb{N} \to R$, die bei 1 den Wert 1 annimmt und sonst nur den Wert Null, so können wir jede

Abbildung $\varphi \in R[X]$ eindeutig schreiben in der Form $\varphi = \sum_\nu \varphi(\nu) X^\nu$ und sind auf einem etwas formaleren Weg wieder am selben Punkt angelangt.

Ergänzung 2.3.3. Im Fall eines Körpers K ist insbesondere $K[X]$ als Gruppe per definitionem der freie K-Vektorraum $K[X] := K\langle\mathbb{N}\rangle$ über der Menge $\mathbb{N}$ der natürlichen Zahlen.

2.3.4. Die wichtigste Eigenschaft eines Polynomrings ist, daß man „für die Variable etwas einsetzen darf“. Das wollen wir nun formal aufschreiben.

Proposition 2.3.5 (Einsetzen in Polynome). *Seien R ein Kring und $b \in R$ ein Element. So gibt es genau einen Ringhomomorphismus*

$$\mathrm{E}_b : R[X] \to R$$

mit $\mathrm{E}_b(X) = b$ und $\mathrm{E}_b \circ \mathrm{can} = \mathrm{id}_R$. Wir nennen E_b den **Einsetzungshomomorphismus zu** *b.*

Beweis. Dieser eindeutig bestimmte Ringhomomorphismus E_b ist eben gegeben durch die Vorschrift $\mathrm{E}_b(a_n X^n + \ldots + a_1 X + a_0) = a_n b^n + \ldots + a_1 b + a_0$. □

2.3.6. Es ist üblich, das Bild unter dem Einsetzungshomomorphismus E_b eines Polynoms $P \in R[X]$ abzukürzen als

$$P(b) := \mathrm{E}_b(P)$$

Ich verwende später meist die Notation $\mathrm{E}_b = \delta_b$, die die Interpretation als „Dirac-Maß“ anklingen läßt.

2.3.7. Unsere übliche Darstellung einer Zahl in Ziffernschreibweise läuft darauf hinaus, die Koeffizienten eines Polynoms anzugeben, das an der Stelle 10 die besagte Zahl als Wert ausgibt, also etwa $7258 = P(10)$ für $P(X)$ das Polynom $7X^3 + 2X^2 + 5X + 8$.

2.3.8. Es geht auch noch allgemeiner, man darf etwa über einem Körper auch quadratische Matrizen in Polynome einsetzen. Um das zu präzisieren, vereinbaren wir die Sprechweise, daß zwei Elemente b und c eines Rings **kommutieren**, wenn gilt $bc = cb$. Das bedeutet also, daß sie in Bezug auf die Multiplikation kommutieren im Sinne von **??**.

Proposition 2.3.9 (Einsetzen in Polynome, Variante). *Seien $\varphi : R \to S$ ein Ringhomomorphismus und $b \in S$ ein Element derart, daß b für alle $a \in R$ mit $\varphi(a)$ kommutiert. So gibt es genau einen Ringhomomorphismus*

$$\mathrm{E}_{\varphi,b} = \mathrm{E}_b : R[X] \to S$$

mit $\mathrm{E}_b(X) = b$ und $\mathrm{E}_b \circ \mathrm{can} = \varphi$. Wir nennen $\mathrm{E}_{\varphi,b}$ den **Einsetzungshomomorphismus zu** *b* **über** *φ.*

Beweis. Dieser eindeutig bestimmte Ringhomomorphismus E_b ist gegeben durch die Vorschrift $\mathrm{E}_b(a_nX^n+\ldots+a_1X+a_0) := \varphi(a_n)b^n+\ldots+\varphi(a_1)b+\varphi(a_0)$. □

2.3.10. Es ist auch in dieser Allgemeinheit üblich, das Bild unter dem Einsetzungshomomorphismus $\mathrm{E}_{\varphi,b}$ eines Polynoms $P \in R[X]$ abzukürzen als

$$P(b) := \mathrm{E}_{\varphi,b}(P)$$

So schreiben wir im Fall eines Krings R zum Beispiel $P(A)$ für die Matrix, die beim Einsetzen einer quadratischen Matrix $A \in \mathrm{Mat}(n;R)$ in das Polynom P ensteht. In diesem Fall hätten wir $S = \mathrm{Mat}(n;R)$ und φ wäre der Ringhomomorphismus, der jedem $a \in R$ das a-fache der Einheitsmatrix zuordnet.

2.3.11 (**Wechsel der Koeffizienten**). Ist $\varphi : R \to S$ ein Ringhomomorphismus, so erhalten wir einen Ringhomomorphismus $\varphi = \varphi_{[X]} : R[X] \to S[X]$ der zugehörigen Polynomringe durch das „Anwenden von φ auf die Koeffizienten“. Formal können wir ihn als das „Einsetzen von X für X über φ“ beschreiben, also als den Ringhomomorphismus $\varphi_{[X]} = \mathrm{E}_{\varphi,X}$.

Definition 2.3.12. Seien R ein Kring und $P \in R[X]$ ein Polynom. Ein Element $a \in R$ heißt eine **Nullstelle** oder auch eine **Wurzel** von P, wenn gilt $P(a) = 0$.

Definition 2.3.13. Sei R ein Ring. Jedem Polynom $P \in R[X]$ ordnen wir seinen **Grad** $\operatorname{grad} P \in \mathbb{N} \sqcup \{-\infty\}$ (englisch **degree**, französisch **degré**) durch die Vorschrift

$$\begin{array}{ll} \operatorname{grad} P = n & \text{für } P = a_nX^n + \ldots + a_1X + a_0 \text{ mit } a_n \neq 0; \\ \operatorname{grad} P = -\infty & \text{für } P \text{ das Nullpolynom.} \end{array}$$

Für ein von Null verschiedenes Polynom $P = a_nX^n + \ldots + a_1X + a_0$ mit $n = \operatorname{grad} P$ nennt man $a_n \in R\backslash 0$ seinen **Leitkoeffizienten**. Den Leitkoeffizienten des Nullpolynoms erklären wir als die Null von R. Ein Polynom heißt **normiert**, wenn sein Leitkoeffizient 1 ist. Das Nullpolynom ist demnach nur über dem Nullring normiert, hat aber auch dort den Grad $-\infty$. Auf Englisch heißen unsere normierten Polynome **monic polynomials**. Ein Polynom vom Grad Eins heißt **linear**, ein Polynom vom Grad Zwei **quadratisch**, ein Polynom vom Grad Drei **kubisch**.

Lemma 2.3.14 (Grad eines Produkts). *Ist R ein Integritätsring, so ist auch der Polynomring $R[X]$ ein Integritätsring und der Grad eines Produkts ist die Summe der Grade der Faktoren, in Formeln*

$$\operatorname{grad}(PQ) = \operatorname{grad} P + \operatorname{grad} Q$$

Beweis. Ist R ein Integritätsring, so ist offensichtlich der Leitkoeffizient von PQ das Produkt der Leitkoeffizienten von P und von Q. □

Lemma 2.3.15 (Polynomdivision mit Rest). *Sei R ein Ring. Gegeben Polynome $P, Q \in R[X]$ mit Q normiert gibt es eindeutig bestimmte Polynome A, B mit $P = AQ + B$ und* $\operatorname{grad} B \leq (\operatorname{grad} Q) - 1$.

Beispiel 2.3.16. Die Polynomdivision mit Rest des Polynoms $X^4 + 2X^2$ durch $X^2 + 2X + 1$ liefert

$$\begin{aligned} X^4 + 2X^2 &= X^2(X^2 + 2X + 1) - 2X^3 + X^2 \\ &= X^2(X^2 + 2X + 1) - 2X(X^2 + 2X + 1) + 5X^2 + 2X \\ &= (X^2 - 2X + 5)(X^2 + 2X + 1) - 8X - 5 \end{aligned}$$

Beweis. Ich habe mir bei der Formulierung des Lemmas Mühe gegeben, daß es auch im Fall des Nullrings $R = 0$ richtig ist, wenn wir $-\infty - 1 = -\infty$ verstehen. Für den Beweis dürfen wir damit annehmen, daß R nicht der Nullring ist. Wir suchen ein Polynom A mit $\operatorname{grad}(P - AQ)$ kleinstmöglich. Gälte dennoch $\operatorname{grad}(P - AQ) \geq (\operatorname{grad}(Q))$, sagen wir $B := P - AQ = aX^r + \ldots + c$ mit $a \neq 0$ und $r > d = \operatorname{grad}(Q)$, so hätte $P - (A + aX^{r-d})Q$ echt kleineren Grad als B, im Widerspruch zur Wahl von A. Das zeigt die Existenz. Für den Nachweis der Eindeutigkeit gehen wir aus von einer weiteren Gleichung $P = A'Q + B'$ mit $\operatorname{grad} B' < d$. Es folgt zunächst $(A - A')Q = B' - B$ und wegen der offensichtlichen Formel für den Grad des Produkts eines beliebigen Polynoms mit einem normierten Polynom weiter $A - A' = 0$ und dann auch $B' - B = 0$. □

Korollar 2.3.17 (Abspalten von Linearfaktoren bei Nullstellen). *Sei R ein Ring und $P \in R[X]$ ein Polynom. Genau dann ist $\lambda \in R$ eine Nullstelle von P, wenn das Polynom $(X - \lambda)$ das Polynom P teilt, in Formeln*

$$P(\lambda) = 0 \;\Leftrightarrow\; (X - \lambda) | P$$

Beweis. Nach Lemma 2.3.15 über die Division mit Rest finden wir ein Polynom $A \in R[X]$ und eine Konstante $b \in R$ mit $P = A(X - \lambda) + b$. Einsetzen von λ für X liefert dann $b = 0$. □

2.3.18. Der im Sinne von 2.3.13 lineare Faktor $(X - \lambda)$ unseres Polynoms heißt auch ein **Linearfaktor**, daher der Name des Korollars.

Satz 2.3.19 (Zahl der Nullstellen eines Polynoms). *Ist K ein Körper oder allgemeiner ein kommutativer Integritätsring, so hat ein von Null verschiedenes Polynom $P \in K[X]$ höchstens* $\operatorname{grad} P$ *Nullstellen in K.*

Beweis. Ist $\lambda \in K$ eine Nullstelle, so finden wir nach 2.3.17 eine Darstellung $P = A(X - \lambda)$ mit $\operatorname{grad} A = \operatorname{grad} P - 1$. Eine von λ verschiedene Nullstelle von P ist für K ein Integritätsring notwendig eine Nullstelle von A und der Satz folgt mit Induktion. □

Beispiel 2.3.20. In einem Körper K oder allgemeiner einem kommutativer Integritätsring gibt es zu jedem Element $b \in K$ höchstens zwei Elemente $a \in K$ mit $a^2 = b$. Ist nämlich a eine Lösung dieser Gleichung, so gilt $X^2 - b = (X - a)(X + a)$, und wenn wir da für X etwas von $\pm a$ Verschiedenes einsetzen, kommt sicher nicht Null heraus.

Ergänzung 2.3.21. Die Kommutativität ist hierbei wesentlich. In 2.6.4 werden wir den sogenannten „Schiefkörper der Quaternionen“ einführen, einen Ring, der außer der Kommutativität der Multiplikation alle unsere Körperaxiome erfüllt. In diesem Ring hat die Gleichung $X^2 = -1$ dann offensichtlich die sechs Lösungen $\pm \mathrm{i}, \pm \mathrm{j}, \pm \mathrm{k}$ und nicht ganz so offensichtlich **??** sogar unendlich viele Lösungen.

2.3.22. Ist K ein Körper oder allgemeiner ein Kring, $P \in K[X]$ ein Polynom und $\lambda \in K$ eine Nullstelle von P, so nennen wir das Supremum über alle $n \in \mathbb{N}$ mit $(X - \lambda)^n | P$ die **Vielfachheit der Nullstelle** λ oder auch ihre **Ordnung**. Das Nullpolynom hat insbesondere an jeder Stelle eine Nullstelle der Vielfachheit ∞ und gar keine Nullstelle bei λ ist dasselbe wie eine „Nullstelle der Vielfachheit Null“. Durch Abspalten von Nullstellen wie in 2.3.17 zeigt man, daß im Fall eines Körpers oder allgemeiner eines kommutativen Integritätsrings auch die Zahl der mit ihren Vielfachheiten gezählten Nullstellen eines von Null verschiedenen Polynoms beschränkt ist durch seinen Grad.

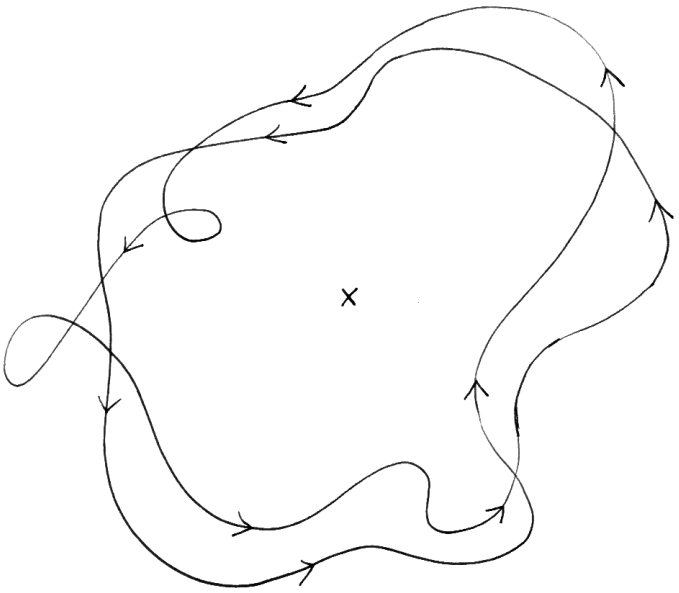
Definition 2.3.23. Ein Körper K heißt **algebraisch abgeschlossen**, wenn jedes nichtkonstante Polynom $P \in K[X] \backslash K$ mit Koeffizienten in unserem Körper K eine Nullstelle in unserem Körper K hat.

Beispiel 2.3.24. Der Körper $K = \mathbb{R}$ ist nicht algebraisch abgeschlossen, denn das Polynom $X^2 + 1$ hat keine reelle Nullstelle.

Vorschau 2.3.25. Der Körper $\mathbb{C}$ der komplexen Zahlen ist algebraisch abgeschlossen. Das ist die Aussage des sogenannten **Fundamentalsatzes der Algebra**, für den wir mehrere Beweise geben werden: Einen besonders elementaren Beweis nach Argand in der Analysis in **??**, einen sehr eleganten mit den Methoden der Funktionentheorie in **??**, und einen mehr algebraischen Beweis, bei dem die Analysis nur über den Zwischenwertsatz eingeht, in 8.3.8. Mir selbst gefällt der noch wieder andere Beweis mit den Mitteln der Topologie **??** am besten, da er meine Anschauung am meisten anspricht. Er wird in analytischer Verkleidung bereits in **??** vorgeführt. Eine heuristische Begründung wird in nebenstehendem Bild gegeben.

Satz 2.3.26. *Ist K ein algebraisch abgeschlossener Körper, so hat jedes von Null verschiedene Polynom $P \in K[X] \backslash 0$ eine* **Zerlegung in Linearfaktoren** *der Gestalt*

$$P = c(X - \lambda_1) \ldots (X - \lambda_n)$$



Heuristische Begründung für den Fundamentalsatz der Algebra. Ein Polynom n-ten Grades wird eine sehr große Kreislinie in der komplexen Zahlenebene mit Zentrum im Ursprung abbilden auf einen Weg in der komplexen Zahlenebene, der „den Ursprung n-mal umläuft“. Angedeutet ist etwa das Bild einer sehr großen Kreislinie unter einem Polynom vom Grad Zwei. Schrumpfen wir nun unsere sehr große Kreislinie zu immer kleineren Kreislinien bis auf einen Punkt, so schrumpfen auch diese Wege zu einem konstanten Weg zusammen. Unsere n-fach um einen etwa am Ursprung aufgestellten Pfahl laufende Seilschlinge kann jedoch offensichtlich nicht auf einen Punkt zusammengezogen werden, ohne daß wir sie über den Pfahl heben, anders gesagt: Mindestens eines der Bilder dieser kleineren Kreislinien muß durch den Ursprung laufen, als da heißt, unser Polynom muß auf mindestens einer dieser kleineren Kreislinien eine Nullstelle habe. In **??** oder besser **??** werden wir diese Heuristik zu einem formalen Beweis ausbauen.

mit $n \geq 0$, $c \in K^\times$ und $\lambda_1, \ldots, \lambda_n \in K$. Darüber hinaus ist diese Zerlegung eindeutig bis auf die Reihenfolge der Faktoren.

2.3.27. Gegeben eine Nullstelle μ von P ist in diesem Fall die Zahl der Indizes i mit $\lambda_i = \mu$ die Vielfachheit der Nullstelle μ. In der Sprache der Multimengen aus **??** erhalten wir für jeden algebraisch abgeschlossenen Körper K eine Bijektion zwischen der Menge aller „endlichen Multimengen von Elementen von K“ und der Menge aller normierten Polynome mit Koeffizienten in K, indem wir einer Multimenge ${}_\mu\{\lambda_1, \ldots, \lambda_n\}$ das Polynom $(X - \lambda_1) \ldots (X - \lambda_n)$ zuordnen.

Beweis. Ist P ein konstantes Polynom, so ist nichts zu zeigen. Ist P nicht konstant, so gibt es nach Annahme eine Nullstelle $\lambda \in K$ von P und wir finden genau ein Polynom $\tilde{P}$ mit $P = (X - \lambda)\tilde{P}$. Der Satz folgt durch vollständige Induktion über den Grad von P. □

Korollar 2.3.28 (**Faktorisierung reeller Polynome**). *Jedes von Null verschiedene Polynom P mit reellen Koeffizienten besitzt eine Zerlegung in Faktoren der Gestalt*

$$P = c(X - \lambda_1) \ldots (X - \lambda_r)(X^2 + \mu_1 X + \nu_1) \ldots (X^2 + \mu_s X + \nu_s)$$

mit $c, \lambda_1, \ldots, \lambda_r, \mu_1, \ldots, \mu_s, \nu_1, \ldots, \nu_s \in \mathbb{R}$ derart, daß die quadratischen Faktoren keine reellen Nullstellen haben. Diese Zerlegung ist eindeutig bis auf die Reihenfolge der Faktoren.

Beweis. Da unser Polynom invariant ist unter der komplexen Konjugation, müssen sich seine mit ihren Vielfachheiten genommenen komplexen Nullstellen so durchnummerieren lassen, daß $\lambda_1, \ldots, \lambda_r$ reell sind und daß eine gerade Zahl nicht reeller Nullstellen übrigbleibt mit $\lambda_{r+2t-1} = \bar{\lambda}_{r+2t}$ für $1 \leq t \leq s$ und $r, s \geq 0$. Die Produkte $(X - \lambda_{r+2t-1})(X - \lambda_{r+2t})$ haben dann reelle Koeffizienten, da sie ja invariant sind unter der komplexen Konjugation, haben jedoch keine reellen Nullstellen. □

Vorschau 2.3.29. In der Algebra 6.4.1 können Sie lernen, inwiefern sowohl die vorhergehenden Aussagen über die Faktorisierung von Polynomen als auch die Primfaktorzerlegung natürlicher Zahlen Spezialfälle eines allgemeinen Satzes über die „Faktorialität euklidischer Ringe“ sind.

2.3.30 (**Polynomringe in mehreren Variablen**). Ähnlich wie den Polynomring in einer Variablen 2.3.2 konstruiert man auch Polynomringe in mehr Variablen über einem gegebenen Grundring R. Ist die Zahl der Variablen endlich, so kann man induktiv definieren

$$R[X_1, \ldots, X_n] = (R[X_1, \ldots, X_{n-1}])[X_n]$$

Man kann aber auch für eine beliebige Menge I den Polynomring $R[X_i]_{i\in I}$ bilden als die Menge aller „endlichen formalen Linearkombinationen mit Koeffizienten aus R von endlichen Monomen in den X_i“. Ich verzichte an dieser Stelle auf eine formale Definition.

Ergänzung 2.3.31. Bei Hochster kann man ein Beispiel für nichtisomorphe kommutative Ringe $A \ncong B$ finden, deren Polynomringe in einer Variablen doch isomorph sind, $A[T] \cong B[T]$. Die Konstruktion eines derartigen Beispiels ist aber bereits höhere Mathematik und für uns an dieser Stelle nicht relevant.

Übungen

Übung 2.3.32. Welche Matrix entsteht beim Einsetzen der quadratischen Matrix $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ in das Polynom $X^2 + 1$?

Ergänzende Übung 2.3.33. Man zeige, daß jede Nullstelle $\alpha \in \mathbb{C}$ eines normierten Polynoms mit komplexen Koeffizienten $X^n + a_{n-1}X^{n-1} + \ldots + a_0$ die Abschätzung $|\alpha| \leq 1 + |a_{n-1}| + \ldots + |a_0|$ erfüllt. Hinweis: Sonst gilt erst $|\alpha| > 1$ und dann $|\alpha|^n > |a_{n-1}\alpha^{n-1}| + \ldots + |a_0|$. Umgekehrt zeige man auch, daß aus der Abschätzung $|\alpha| \leq C$ für alle komplexen Wurzeln die Abschätzung $|a_k| \leq \binom{n}{k} C^{n-k}$ für die Koeffizienten folgt.

Übung 2.3.34. Ist $P \in \mathbb{R}[X]$ ein Polynom mit reellen Koeffizienten und $\mu \in \mathbb{C}$ eine komplexe Zahl, so gilt $P(\mu) = 0 \Rightarrow P(\bar{\mu}) = 0$. Ist also eine komplexe Zahl Nullstelle eines Polynoms mit reellen Koeffizienten, so ist auch die konjugiert komplexe Zahl eine Nullstelle desselben Polynoms.

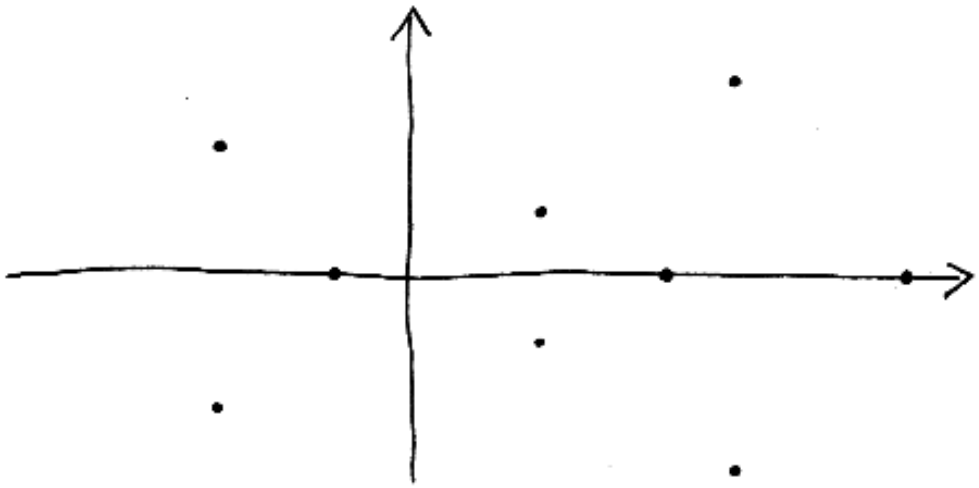
Ergänzende Übung 2.3.35. Seien k, K kommutative Ringe, $i : k \to K$ ein Ringhomomorphismus und $i : k[X] \to K[X]$ der induzierten Ringhomomorphismus zwischen den zugehörigen Polynomringen. Man zeige: Ist $\lambda \in k$ eine Nullstelle eines Polynoms $P \in k[X]$, so ist $i(\lambda) \in K$ eine Nullstelle des Polynoms $i(P)$.

Ergänzende Übung 2.3.36. Ist K ein Integritätsbereich, so induziert die kanonische Einbettung $K \hookrightarrow K[X]$ auf den Einheitengruppen eine Bijektion $K^\times \xrightarrow{\sim} K[X]^\times$. Im Ring $(\mathbb{Z}/4\mathbb{Z})[X]$ aber ist etwa auch $\bar{1} + \bar{2}X$ eine Einheit.

Übung 2.3.37. Man zeige, daß es in einem endlichen Körper $\mathbb{F}$ einer von 2 verschiedenen Charakteristik genau $(|\mathbb{F}| + 1)/2$ Quadrate gibt, wohingegen in einem endlichen Körper der Charakteristik 2 jedes Element das Quadrat eines weiteren Elements ist.

Übung 2.3.38. Man zerlege das Polynom $X^4 + 2$ in $\mathbb{R}[X]$ in der in 2.3.28 beschriebenen Weise in ein Produkt quadratischer Faktoren ohne Nullstelle.

Ergänzende Übung 2.3.39. Ein reelles Polynom hat bei $\lambda \in \mathbb{R}$ eine mehrfache Nullstelle genau dann, wenn auch seine Ableitung bei λ verschwindet.



Die komplexen Nullstellen eines Polynoms mit reellen Koeffizienten, die nicht reell sind, tauchen immer in Paaren aus einer Wurzel und ihrer komplex Konjugierten auf, vergleiche auch Übung 2.3.34.

Ergänzende Übung 2.3.40. Gegeben ein reelles Polynom, dessen komplexe Nullstellen bereits sämtlich reell sind, ist jede Nullstelle seiner Ableitung reell und wenn sie keine Nullstelle der Funktion selbst ist, eine einfache Nullstelle der Ableitung. Hinweis: Zwischen je zwei Nullstellen unserer Funktion muß mindestens eine Nullstelle ihrer Ableitung liegen.

Ergänzende Übung 2.3.41. Man zeige: Die rationalen Nullstellen eines normierten Polynoms mit ganzzahligen Koeffizienten $P \in \mathbb{Z}[X]$ sind bereits alle ganz. In Formeln folgt aus $P(\lambda) = 0$ für $\lambda \in \mathbb{Q}$ also bereits $\lambda \in \mathbb{Z}$.

Ergänzende Übung 2.3.42. Gegeben ein Ring R bilden auch die **formalen Potenzreihen mit Koeffizienten in** R der Gestalt $\sum_{n\geq 0} a_n X^n$ mit $a_n \in R$ einen Ring, der meist $R[\![X]\!]$ notiert wird. Man gebe eine exakte Definition dieses Rings und zeige, daß seine Einheiten genau diejenigen Potenzreihen sind, deren konstanter Term eine Einheit in R ist, in Formeln

$$R[\![X]\!]^\times = R^\times + XR[\![X]\!]$$

Man verallgemeinere die Definition und Beschreibung der Einheiten auf Potenzreihenringe $R[\![X_1, \ldots, X_n]\!]$ in mehreren Variablen und konstruiere einen Ringisomorphismus

$$(R[\![X_1, \ldots, X_n]\!])[\![X_{n+1}]\!] \tilde{\to} R[\![X_1, \ldots, X_n, X_{n+1}]\!]$$

Ergänzende Übung 2.3.43. Gegeben ein Ring R bilden auch die **formalen Laurentreihen mit Koeffizienten in** R der Gestalt $\sum_{n\geq -N} a_n X^n$ mit $a_n \in R$ und $N \in \mathbb{N}$ einen Ring, der meist $R(\!(X)\!)$ notiert wird. Man gebe eine exakte Definition dieses Rings und zeige, daß im Fall $R \neq 0$ seine Einheiten genau diejenigen von Null verschiedenen Reihen sind, bei denen der Koeffizient der kleinsten mit von Null verschiedenem Koeffizienten auftauchenden Potenz von X eine Einheit in R ist, in Formeln

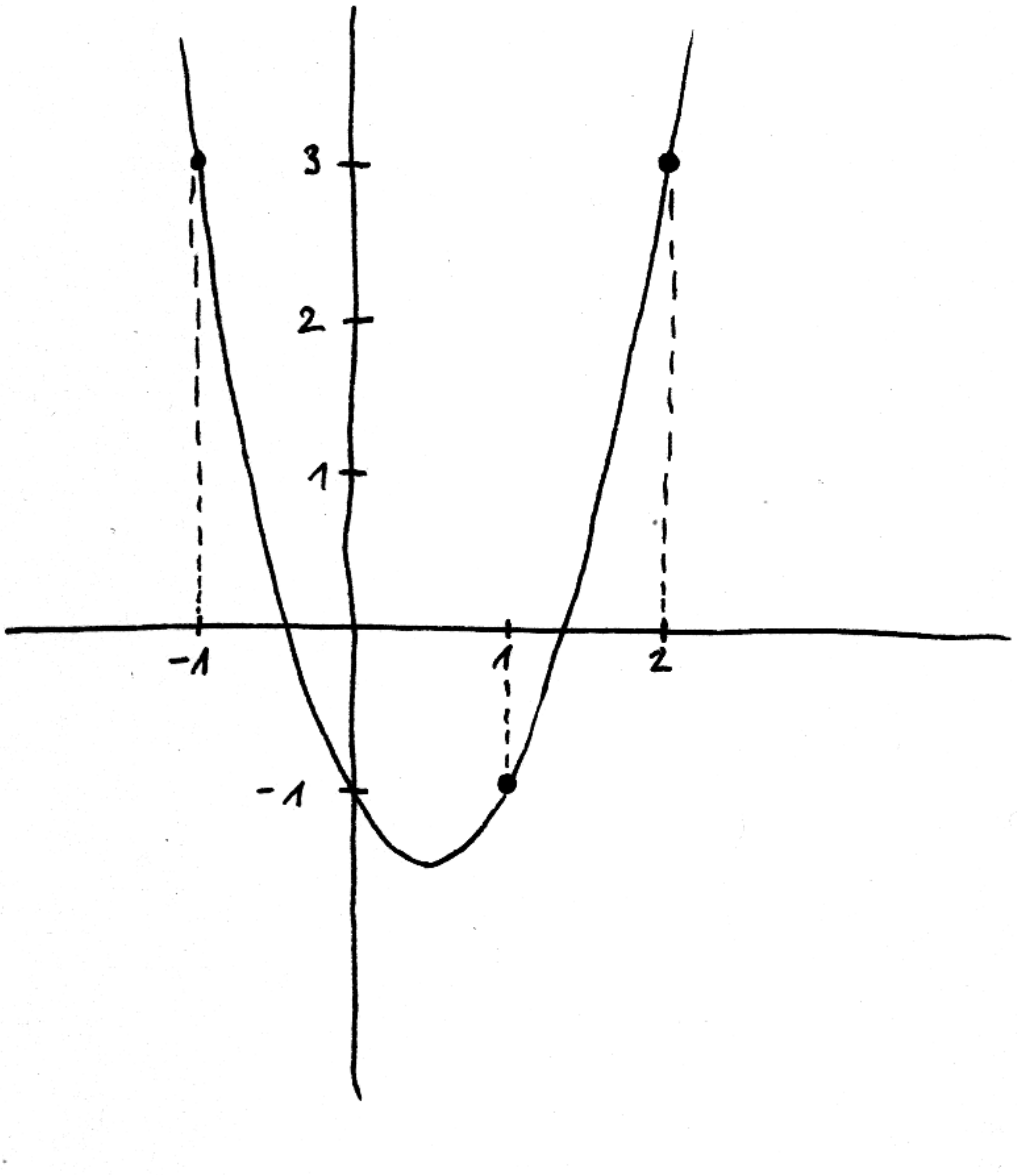
$$R(\!(X)\!)^\times = \bigcup_{n\in\mathbb{Z}} X^n R[\![X]\!]^\times$$

Insbesondere ist im Fall eines Körpers K auch $K(\!(X)\!)$ ein Körper.

Ergänzung 2.3.44. Wir verwenden hier die Terminologie, nach der bei **formalen Laurentreihen** im Gegensatz zu den Laurentreihen der Funktionentheorie nur endlich viele Terme mit negativen Exponenten erlaubt sind.

2.4 Polynome als Funktionen*

Lemma 2.4.1 (Interpolation durch Polynome). *Seien K ein Körper und $x_0, \ldots, x_n \in K$ paarweise verschiedene* **Stützstellen** *und $y_0, \ldots, y_n \in K$ beliebig vorgegebene Werte. So gibt es genau ein Polynom $P \in K[X]$ vom Grad $\leq n$ mit $P(x_0) = y_0, \ldots, P(x_n) = y_n$.*



Das Polynom $P(X) = 2X^2 - 2X - 1$ mit reellen Koeffizienten, das die an den Stützstellen $-1, 1, 2$ vorgegebenen Werte $3, -1, 3$ interpoliert.

Beweis. Zunächst ist sicher $(X - x_1) \dots (X - x_n) =: A_0(X)$ ein Polynom vom Grad n, das bei $x_1, \dots, x_n$ verschwindet und an allen anderen Stellen von Null verschieden ist, insbesondere auch bei x_0. Dann ist $L_0(X) := A_0(X)/A_0(x_0)$ ein Polynom vom Grad n, das bei x_0 den Wert Eins annimmt und bei $x_1, \dots, x_n$ verschwindet. In derselben Weise konstruieren wir auch Polynome $L_1(X), \dots, L_n(X)$ und erhalten ein mögliches Interpolationspolynom als

$$P(X) = y_0 L_0(X) + \dots + y_n L_n(X) = \sum_{i=0}^{n} y_i \frac{\prod_{j \neq i}(X - x_j)}{\prod_{j \neq i}(x_i - x_j)}$$

Das zeigt die Existenz. Ist Q eine weitere Lösung derselben Interpolationsaufgabe vom Grad $\leq n$, so ist $P - Q$ ein Polynom vom Grad $\leq n$ mit $n + 1$ Nullstellen, eben bei den Stützstellen $x_0, \dots, x_n$. Wegen 2.3.19 muß dann aber $P - Q$ das Nullpolynom sein, und das zeigt die Eindeutigkeit. □

2.4.2. Um die bisher eingeführten algebraischen Konzepte anschaulicher zu machen, will ich sie in Bezug setzen zu geometrischen Konzepten. Ist K ein Kring, so können wir jedem Polynom $f \in K[X_1, \dots, X_n]$ die Funktion $\tilde{f} : K^n \to K$, $(x_1, \dots, x_n) \mapsto f(x_1, \dots, x_n)$ zuordnen. Wir erhalten so einen Ringhomomorphismus

$$K[X_1, \dots, X_n] \to \mathrm{Ens}(K^n, K)$$

Dieser Homomorphismus ist im Allgemeinen weder injektiv noch surjektiv. Schon für $n = 1$, $K = \mathbb{R}$ läßt sich ja keineswegs jede Abbildung $\mathbb{R} \to \mathbb{R}$ durch ein Polynom beschreiben, also ist sie in diesem Fall nicht surjektiv. Im Fall eines endlichen Körpers K kann weiter für $n \geq 1$ unsere K-lineare Auswertungsabbildung vom unendlichdimensionalen K-Vektorraum $K[X_1, \dots, X_n]$ in den endlichdimensionalen K-Vektorraum $\mathrm{Ens}(K^n, K)$ unmöglich injektiv sein. Wir haben jedoch den folgenden Satz.

Satz 2.4.3 (Polynome als Funktionen). *1. Ist K ein unendlicher Körper, ja allgemeiner ein unendlicher Integritätskring, so ist für alle $n \in \mathbb{N}$ die Auswertungsabbildung eine Injektion $K[X_1, \dots, X_n] \hookrightarrow \mathrm{Ens}(K^n, K)$;*

2. Ist K ein endlicher Körper, so ist für alle $n \in \mathbb{N}$ die Auswertungsabbildung eine Surjektion $K[X_1, \dots, X_n] \twoheadrightarrow \mathrm{Ens}(K^n, K)$. Den Kern dieser Surjektion beschreibt Übung 3.3.19.

Beweis. 1. Durch Induktion über n. Der Fall $n = 0$ ist eh klar. Für $n = 1$ folgt die Behauptung aus der Erkenntnis, das jedes von Null verschiedene Polynom in $K[X]$ nur endlich viele Nullstellen in K haben kann. Der Kern der Abbildung

$$K[X] \to \mathrm{Ens}(K, K)$$

besteht also nur aus dem Nullpolynom. Für den Induktionsschritt setzen wir $X_n = Y$ und schreiben unser Polynom in der Gestalt

$$P = a_d Y^d + \ldots + a_1 Y + a_0$$

mit $a_i \in K[X_1, \ldots, X_{n-1}]$. Halten wir $(x_1, \ldots, x_{n-1}) = x \in K^{n-1}$ fest, so ist $a_d(x)Y^d + \ldots + a_1(x)Y + a_0(x) \in K[Y]$ das Nullpolynom nach dem Fall $n = 1$. Also verschwinden $a_d(x), \ldots, a_1(x), a_0(x)$ für alle $x \in K^{n-1}$, mit Induktion sind somit alle a_i schon das Nullpolynom und wir haben $P = 0$.

2. Das bleibt dem Leser überlassen. Man mag sich beim Beweis an 2.4.1 orientieren. Wir folgern in 6.3.8 eine allgemeinere Aussage aus dem abstrakten chinesischen Restsatz. □

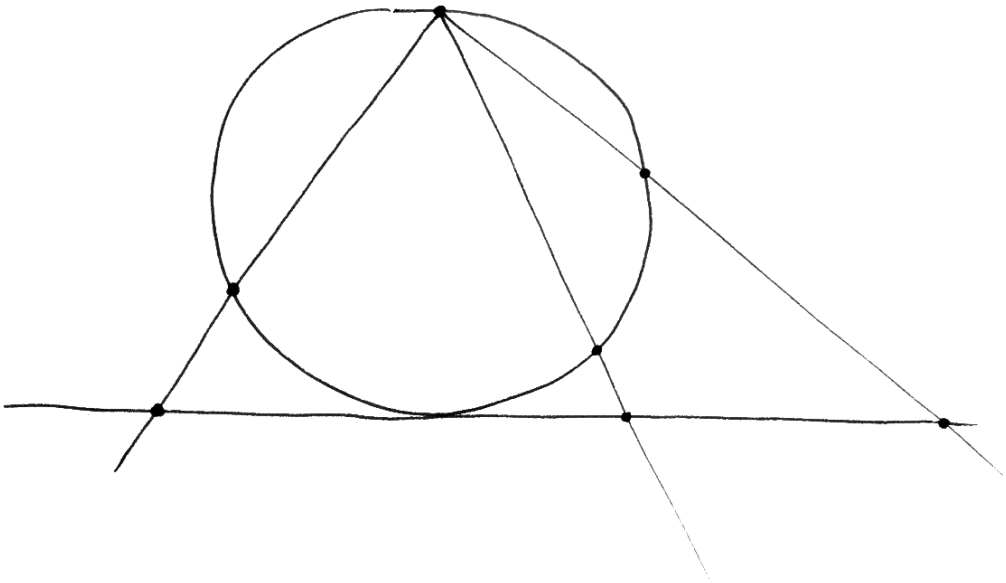
Übungen

Ergänzende Übung 2.4.4. Man zeige, daß jeder algebraisch abgeschlossene Körper unendlich ist. Hinweis: Im Fall $1 \neq -1$ reicht es, Quadratwurzeln zu suchen. Man zeige, daß jedes nichtkonstante Polynom $P \in K[X, Y]$ in zwei Veränderlichen über einem algebraisch abgeschlossenen Körper unendlich viele Nullstellen in K^2 hat.

Ergänzende Übung 2.4.5 (**Nullstellensatz für Hyperebenen**). Sei K ein unendlicher Körper. Verschwindet ein Polynom im Polynomring in d Variablen über K auf einer affinen Hyperebene in K^d, so wird es von jeder linearen Gleichung besagter Hyperebene geteilt. Hinweis: Ohne Beschränkung der Allgemeinheit mag man unsere Hyperebene als eine der Koordinatenhyperebenen annehmen. Man zeige auch allgemeiner: Verschwindet ein Polynom in d Veränderlichen über einem unendlichen Körper auf der Vereinigung der paarweise verschiedenen affinen Hyperebenen $H_1, \ldots, H_n \subset K^d$, so wird es vom Produkt der linearen Gleichungen unserer Hyperebenen geteilt.

Ergänzende Übung 2.4.6 (**Pythagoreische Zahlen**). Man zeige: Stellen wir eine Lampe oben auf den Einheitskreis und bilden jeden von $(0, 1)$ verschiedenen Punkt des Einheitskreises ab auf denjenigen Punkt der Parallelen zur x-Achse durch $(0, -1)$, auf den sein Schatten fällt, so entsprechen die Punkte mit rationalen Koordinaten auf dem Einheitskreis genau den Punkten mit rationalen Koordinaten auf unserer Parallelen. Hinweis: Hat ein Polynom in $\mathbb{Q}[X]$ vom Grad drei zwei rationale Nullstellen, so ist auch seine dritte Nullstelle rational. Geben wir das Bild vom Schattenwurf auf und nehmen den Schnitt des Lichtstrahls mit der x-Achse, so steht eine explizite Formel für die Umkehrabbildung in **??**.

Ergänzung 2.4.7. Unter einem **pythagoreischen Zahlentripel** versteht man ein Tripel (a, b, c) von positiven natürlichen Zahlen mit $a^2 + b^2 = c^2$, die also als



Wir stellen eine Lampe oben auf den Einheitskreis und bilden jeden von $(0,1)$ verschiedenen Punkt des Einheitskreises ab auf denjenigen Punkt der Parallelen zur x-Achse durch $(0,-1)$, auf den sein Schatten fällt. So entsprechen nach Übung 2.4.6 die Punkte mit rationalen Koordinaten auf dem Einheitskreis genau den Punkten mit rationalen Koordinaten auf unserer Parallelen. Ein Tripel $a,b,c \in \mathbb{Z}$ mit $a^2+b^2=c^2$ heißt ein **pythagoreisches Zahlentripel**. Die pythagoreischen Zahlentripel mit größtem gemeinsamen Teiler $\langle a,b,c\rangle = \langle 1\rangle$ und $c>0$ entsprechen nun offensichtlich eineindeutig den Punkten mit rationalen Koordinaten auf dem Einheitskreis vermittels der Vorschrift $(a,b,c) \mapsto (a/c, b/c)$. In dieser Weise liefert unser Bild also einen geometrischen Zugang zur Klassifikation der pythagoreischen Zahlentripel.

Seitenlängen eines rechtwinkligen Dreiecks auftreten können. Es scheint mir offensichtlich, daß die Bestimmung aller pythagoreischen Zahlentripel im wesentlichen äquivalent ist zur Bestimmung aller Punkte mit rationalen Koordinaten auf dem Einheitskreis, also aller Punkte $(x, y) \in \mathbb{Q}^2$ mit $x^2 + y^2 = 1$.

Übung 2.4.8. Man zeige, daß die Menge der Polynome in $\mathbb{Q}[X]$, die an allen Punkten aus $\mathbb{N}$ ganzzahlige Werte annehmen, übereinstimmt mit der Menge aller Linearkombinationen mit ganzzahligen Koeffizienten der mithilfe der Binomialkoeffizienten gebildeten Polynome

$$\binom{X}{k} := \frac{X(X-1)\ldots(X-k+1)}{k(k-1)\ldots 1} \quad \text{falls } k \geq 1 \text{ und } \binom{X}{0} := 1.$$

Hinweis: Man berechne die Werte unserer Polynome bei $X = 0, 1, 2, \ldots$ Die Übung zeigt, daß diejenigen Polynome in $\mathbb{Q}[X]$, die an allen Punkten aus $\mathbb{N}$ ganzzahlige Werte annehmen, sogar an allen Punkten aus $\mathbb{Z}$ ganzzahlige Werte annehmen müssen. Sie heißen **ganzwertige** oder **numerische Polynome**. Man zeige weiter für jedes Polynom in $\mathbb{Q}[X]$ vom Grad $d \geq 0$, das an fast allen Punkten aus $\mathbb{N}$ ganzzahlige Werte annimmt, daß es ein ganzwertiges Polynom sein muß und daß das $(d!)$-fache seines Leitkoeffizienten mithin eine ganze Zahl sein muß.

Ergänzende Übung 2.4.9. Man zeige, daß die Menge aller Polynome mit rationalen Koeffizienten in $\mathbb{Q}[X_1, \ldots, X_r]$, die an allen Punkten aus $\mathbb{N}^r$ ganzzahlige Werte annehmen, übereinstimmt mit der Menge aller Linearkombinationen mit ganzzahligen Koeffizienten von Produkten der Gestalt

$$\binom{X_1}{k_1} \cdots \binom{X_r}{k_r}$$

mit $k_1, \ldots, k_r \geq 0$. Hinweis: Man argumentiere wie in 2.4.8.

2.5 Quotientenkörper und Partialbruchzerlegung

2.5.1. Die Konstruktion des Körpers $\mathbb{Q}$ der Bruchzahlen aus dem Integritätsbereich $\mathbb{Z}$ der ganzen Zahlen hatten wir bisher noch nicht formal besprochen. Hier holen wir das gleich in größerer Allgemeinheit nach und zeigen, wie man zu jedem Integritätsbereich seinen „Quotientenkörper“ konstruieren kann.

Definition 2.5.2. Gegeben ein kommutativer Integritätsbereich R konstruieren wir seinen **Quotientenkörper**

$$\mathrm{Quot}(R)$$

wie folgt: Wir betrachten die Menge $R \times (R \backslash 0)$ und definieren darauf eine Relation $\sim$ durch die Vorschrift

$$(a, s) \sim (b, t) \text{ genau dann, wenn gilt } at = bs.$$

Diese Relation ist eine Äquivalenzrelation, wie man leicht prüft. Wir bezeichnen die Menge der Äquivalenzklassen mit $\mathrm{Quot}(R)$ und die Äquivalenzklasse von (a,s) mit $\frac{a}{s}$ oder a/s. Dann definieren wir auf $\mathrm{Quot}(R)$ Verknüpfungen $+$ und $\cdot$ durch die Regeln

$$\frac{a}{s}+\frac{b}{t}=\frac{at+bs}{st} \quad \text{und} \quad \frac{a}{s}\cdot\frac{b}{t}=\frac{ab}{st}$$

und überlassen dem Leser den Nachweis, daß diese Verknüpfungen wohldefiniert sind und $\mathrm{Quot}(R)$ zu einem Körper machen und daß die Abbildung $\mathrm{can}: R \to \mathrm{Quot}(R)$, $r \mapsto r/1$ ein injektiver Ringhomomorphismus ist. Er heißt die **kanonische Einbettung** unseres Integritätsbereichs in seinen Quotientenkörper.

Ergänzung 2.5.3. Auf Englisch bezeichnet man den Quotientenkörper als **fraction field** und auf Französisch als **corps de fractions**. Dort verwendet man folgerichtig statt unserer Notation $\mathrm{Quot}(R)$ die Notation $\mathrm{Frac}(R)$. Die noch allgemeinere Konstruktion der „Lokalisierung“ lernen wir erst in **??** kennen.

Beispiel 2.5.4. Der Körper der rationalen Zahlen $\mathbb{Q}$ wird formal definiert als der Quotientenkörper des Rings der ganzen Zahlen, in Formeln

$$\mathbb{Q} := \mathrm{Quot}\,\mathbb{Z}$$

Sicher wäre es unter formalen Aspekten betrachtet eigentlich richtig gewesen, diese Definition schon viel früher zu geben. Es schien mir jedoch didaktisch ungeschickt, gleich am Anfang derart viel Zeit und Formeln auf die exakte Konstruktion einer Struktur zu verwenden, die Ihnen bereits zu Beginn ihres Studiums hinreichend vertraut sein sollte. Wie bereits bei rationalen Zahlen nennt man auch im allgemeinen bei einem Bruch g/h das g den **Zähler** und das h den **Nenner** des Bruchs.

Satz 2.5.5 (Universelle Eigenschaft des Quotientenkörpers). *Sei R ein kommutativer Integritätsbereich. Ist $\varphi: R \to A$ ein Ringhomomorphismus, unter dem jedes von Null verschiedene Element von R auf eine Einheit von A abgebildet wird, so faktorisiert φ eindeutig über $\mathrm{Quot}\,R$, es gibt also in Formeln genau einen Ringhomomorphismus $\tilde{\varphi}: \mathrm{Quot}\,R \to A$ mit $\varphi(r) = \tilde{\varphi}(r/1)\ \forall r \in R$.*

Beweis. Für jedes mögliche $\tilde{\varphi}$ muß gelten $\tilde{\varphi}(r/s) = \varphi(r)\varphi(s)^{-1}$. Das zeigt bereits die Eindeutigkeit von $\tilde{\varphi}$. Um auch seine Existenz zu zeigen, betrachten wir die Abbildung $\hat{\varphi}: R \times (R\backslash 0) \to A$ gegeben durch $\hat{\varphi}(r,s) = \varphi(r)\varphi(s)^{-1}$ und prüfen, daß sie konstant ist auf Äquivalenzklassen. Dann muß sie nach 1.2.6 eine wohlbestimmte Abbildung $\mathrm{Quot}\,R \to A$ induzieren, von der der Leser leicht selbst prüfen wird, daß sie ein Ringhomomorphismus ist. □

2.5.6 (**Brüche mit kontrollierten Nennern**). Gegeben ein kommutativer Integritätsbereich R und eine Teilmenge $S \subset R\backslash 0$ betrachten wir im Quotientenkörper von R den Teilring

$$S^{-1}R := \{(r/s) \in \operatorname{Quot} R \mid s \text{ ist ein Produkt von Elementen von } S\}$$

Hierbei ist die Eins auch als Produkt von Elementen von S zu verstehen, eben als das leere Produkt. Insbesondere erhalten wir eine Einbettung $R \hookrightarrow S^{-1}R$ durch $r \mapsto (r/1)$. Ist nun $\varphi : R \to A$ ein Ringhomomorphismus, unter dem jedes Element von S auf eine Einheit von A abgebildet wird, so faktorisiert φ mit demselben Beweis wie zuvor eindeutig über $S^{-1}R$, es gibt also in Formeln genau einen Ringhomomorphismus $\tilde{\varphi} : S^{-1}R \to A$ mit $\varphi(r) = \tilde{\varphi}(r/1)\ \forall r \in R$.

Beispiel 2.5.7 (**Auswerten rationaler Funktionen**). Ist K ein Körper, so bezeichnet man den Quotientenkörper des Polynomrings mit $K(X) := \operatorname{Quot} K[X]$ und nennt ihn den **Funktionenkörper zu** K und seine Elemente **rationale Funktionen**. Man lasse sich durch die Terminologie nicht verwirren, Elemente dieses Körpers sind per definitionem formale Ausdrücke und eben gerade keine Funktionen. Inwiefern man sie zumindest für unendliches K doch als Funktionen verstehen darf, soll nun ausgeführt werden. Gegeben $\lambda \in K$ betrachten wir dazu die Menge $S_\lambda := \{P \mid P(\lambda) \neq 0\}$ aller Polynome, die bei λ keine Nullstelle haben, und bezeichnen mit

$$K[X]_\lambda := S_\lambda^{-1}K[X] \subset K(X)$$

der Teilring aller Quotienten von Polynomen, die sich darstellen lassen als ein Bruch, dessen Nenner bei λ keine Nullstelle hat. Auf diesem Teilring ist das Auswerten bei λ nach 2.5.6 ein wohlbestimmter Ringhomomorphismus $K[X]_\lambda \to K$, den wir notieren als $f \mapsto f(\lambda)$. Er ist der einzige derartige Ringhomomorphismus mit $X \mapsto \lambda$. Gegeben $f \in K(X)$ heißen die Punkte $\lambda \in K$ mit $f \notin K[X]_\lambda$ die **Polstellen von** f und das kleinste n mit $(X-\lambda)^n f \in K[X]_\lambda$ heißt die **Polstellenordnung von** f **bei** λ. Natürlich hat jedes Element $f \in K(X)$ höchstens endlich viele Polstellen. Für jede rationale Funktion $f \in K(X)$ erklärt man ihren **Definitionsbereich** $D(f) \subset K$ als die Menge aller Punkte $a \in K$, die keine Polstellen von f sind. Durch „Kürzen von Nullstellen“ überzeugt man sich leicht, daß jede rationale Funktion so als Quotient $f = g/h$ geschrieben werden kann, daß Zähler und Nenner keine gemeinsamen Nullstellen in K haben, und daß dann die Polstellen gerade die Nullstellen des Nenners sind. Vereinbart man, daß f diesen Stellen als Wert ein neues Symbol ∞ zuweisen soll, so erhält man für jeden unendlichen Körper K sogar eine wohlbestimmte Injektion $K(X) \hookrightarrow \operatorname{Ens}(K, K \sqcup \{\infty\})$.

2.5.8. In der Schule mögen Sie gelernt haben, daß etwa die Funktion x/x bei $x = 0$ nicht definiert ist. Von unserem Standpunkt aus ist das nicht so klar. Es gibt einerseits den Begriff einer Funktion als einer Abbildung, und um eine Abbildung anzugeben müssen bei uns im Prinzip Definitionsbereich, Wertebereich

und Abbildungsvorschrift gleich mit angegeben werden, und die Abbildungsvorschrift $x \mapsto x/x$ kann in der Tat bei $x = 0$ nicht sinnvoll in der Art „setze erst $x = 0$ für die Variable ein und führe dann die vorgeschriebenen Operationen im Körper $\mathbb{R}$ aus“ ausgewertet werden. Im Sinne unserer obigen Definition gilt im Funktionenköper $\mathbb{R}(X)$ dahingegen $1 = X/X$ und die Null gehört durchaus zum Defintionsbereich dieser rationalen Funktion im in 2.5.7 erklärten Sinne.

Ergänzung 2.5.9. Es ist sogar richtig, daß jede rationale Funktion eine eindeutige maximal gekürzte Darstellung mit normiertem Nenner hat. Um das einzusehen, benötigt man ein Analogon der eindeutigen Primfaktorzerlegung für Polynomringe, das wir für allgemeines K erst in 6.4.19 zeigen.

2.5.10. Wir erinnern aus 2.3.42 und 2.3.43 die Ringe der Potenzreihen und der Laurentreihen. Gegeben ein Körper K liefert die Verknüpfung von Einbettungen $K[X] \hookrightarrow K[\![X]\!] \hookrightarrow K(\!(X)\!)$ offensichtlich einen Ringhomomorphismus und nach der universellen Eigenschaft 2.5.5 mithin eine Einbettung $K(X) \hookrightarrow K(\!(X)\!)$. Das Bild von $(1 - X)^{-1}$ unter dieser Einbettung wäre etwa die „formale geometrische Reihe“ $1 + X + X^2 + X^3 + \ldots$

Ergänzung 2.5.11. Sei K ein Körper. Ist $p \in K$ fest gewählt und $K(T) \xrightarrow{\sim} K(X)$ der durch $T \mapsto (X + p)$ gegebene Isomorphismus, so bezeichnet man das Bild von $f \in K(T)$ unter der Komposition $K(T) \xrightarrow{\sim} K(X) \hookrightarrow K(\!(X)\!)$ auch als die **Laurententwicklung von f um den Entwicklungspunkt** p. Meist schreibt man in einer Laurententwicklung statt X auch $(T - p)$. So wäre die Laurententwicklung von $f = T^2/(T - 1)$ um den Entwicklungspunkt $T = 1$ etwa die endliche Laurentreihe $(T - 1)^{-1} + 2 + (T - 1)$.

Satz 2.5.12 (Partialbruchzerlegung). *Gegeben ein algebraisch abgeschlossener Körper K wird eine K-Basis des Funktionenkörpers $K(X)$ gebildet von erstens den Potenzen der Variablen $(X^n)_{n\geq 1}$ mitsamt zweitens den Potenzen der Inversen der Linearfaktoren $((X - a)^{-n})_{n\geq 1,\, a\in K}$ zuzüglich drittens der Eins $1 \in K(X)$.*

2.5.13. Eine Darstellung einer rationalen Funktion als Linearkombination der Elemente dieser Basis nennt man eine **Partialbruchzerlegung** unserer rationalen Funktion. Anschaulich scheint mir zumindest die lineare Unabhängigkeit der behaupteten Basis recht einsichtig: Polstellen an verschiedenen Punkten können sich ebensowenig gegenseitig aufheben wie Polstellen verschiedener Ordnung an einem vorgegebenen Punkt. Alle rationalen Funktionen mag man auffassen als Funktionen auf der projektiven Gerade $\mathbb{P}^1 K$ aus **??** und die $(X^n)_{n\geq 1}$ als Funktionen, die „eine Polstelle der Ordnung n im Unendlichen haben“. Das ist auch der Grund dafür, daß ich die 1 im Satz oben extra aufgeführt habe und nicht stattdessen einfach kürzer $(X^n)_{n\geq 0}$ schreibe.

2.5.14. Ist K ein algebraisch abgeschlossener Körper, so sind die Polstellen eines Elements $f \in K(X)$ im Sinne von 2.5.7 genau die Elemente $a \in K$ mit der

Eigenschaft, daß für ein $n \geq 1$ der Term $(X-a)^{-n}$ mit von Null verschiedenem Koeffizienten in der Partialbruchzerlegung von f auftritt.

Ergänzung 2.5.15. In Büchern zur Analysis findet man oft eine Variante dieses Satzes für den Körper $K = \mathbb{R}$: In diesem Fall werden die im Satz beschriebenen Elemente ergänzt zu einer Basis durch die Elemente $1/((X-\lambda)(X-\bar{\lambda}))^n$ und die Elemente $X/((X-\lambda)(X-\bar{\lambda}))^n$ für $\lambda \in \mathbb{C}$ mit positivem Imaginärteil und $n \geq 1$ beliebig, wie der Leser zur Übung selbst zeigen mag. Eine Verallgemeinerung auf den Fall eines beliebigen Körpers K wird in 7.7.16 diskutiert.

Beweis. Wir zeigen zunächst, daß unsere Familie den Funktionenkörper als K-Vektorraum erzeugt. Sei also $f \in K(X)$ dargestellt als Quotient von zwei Polynomen $f = P/Q$ mit $Q \neq 0$. Wir argumentieren mit Induktion über den Grad von Q. Ist Q konstant, so haben wir schon gewonnen. Sonst besitzt Q eine Nullstelle $\mu \in K$ und wir können schreiben $Q(x) = (X-\mu)^m \tilde{Q}(x)$ mit $m \geq 1$ und $\tilde{Q}(\mu) \neq 0$. Dann nehmen wir $c = P(\mu)/\tilde{Q}(\mu)$ und betrachten die Funktion

$$\frac{P}{Q} - \frac{c}{(X-\mu)^m} = \frac{P - c\tilde{Q}}{(X-\mu)^m \tilde{Q}}$$

Aufgrund unserer Wahl von c hat der Zähler auf der rechten Seite eine Nullstelle bei $X = \mu$, wir können im Bruch also $(X-\mu)$ kürzen, und eine offensichtliche Induktion über dem Grad des Polynoms Q beendet den Beweis. Zum Beweis der linearen Unabhängigkeit betrachten wir eine Linearkombination unserer Basis in spe, die die Nullfunktion darstellt. Sei $c(X-a)^{-n}$ ein Summand darin mit $n \geq 1$ größtmöglich für die gewählte Polstelle a. So multiplizieren wir mit $(X-a)^n$ und werten aus bei a im Sinne von 2.5.6 und finden, daß schon $c = 0$ gegolten haben muß. So argumentieren wir alle Polstellen weg, und daß die nichtnegativen Potenzen von X linear unabhängig sind folgt ja schon aus der Definition des Polynomrings. □

2.5.16 (**Berechnung einer Partialbruchzerlegung**). Will man konkret eine Partialbruchzerlegung bestimmen, so rate ich dazu, mit einer Polynomdivision zu beginnen und $P = AQ + R$ zu schreiben mit Polynomen A und R derart, daß der Grad von R echt kleiner ist als der Grad von Q. Wir erhalten $P/Q = A + R/Q$, und in der Partialbruchzerlegung von R/Q tritt dann kein polynomialer Summand mehr auf. Die Polstellen-Summanden gehören dann alle zu Nullstellen von Q und ihr Grad ist beschränkt durch die Vielfachheit der entsprechenden Nullstelle von Q. Nun setzen wir die Koeffizienten unserer Linearkombination als Unbestimmte an, für die wir dann ein lineares Gleichungssystem erhalten, das wir mit den üblichen Verfahren lösen.

Beispiel 2.5.17. Wir bestimmen von $(X^4 + 2X^2)/(X^2 + 2X + 1)$ die Partialbruchzerlegung. Die Polynomdivision haben wir bereits in 2.3.16 durchgeführt

und $X^4+2X^2=(X^2-2X+5)(X^2+2X+1)-8X-5$ erhalten, so daß sich unser Bruch vereinfacht zu

$$\frac{X^4+2X^2}{X^2+2X+1}=X^2-2X+5-\frac{8X+5}{X^2+2X+1}$$

Jetzt zerlegen wir den Nenner in Linearfaktoren $X^2+2X+1=(X+1)^2$ und dürfen nach unserem Satz über die Partialbruchzerlegung

$$\frac{8X+5}{(X+1)^2}=\frac{a}{X+1}+\frac{b}{(X+1)^2}$$

ansetzen, woraus sich ergibt $8X+5=aX+a+b$ und damit $a=8$ und $b=-3$. Die Partialbruchzerlegung unserer ursprünglichen Funktion hat also die Gestalt

$$\frac{X^4+2X^2}{X^2+2X+1}=X^2-2X+5-\frac{8}{X+1}+\frac{3}{(X+1)^2}$$

2.5.18 (**Geschlossene Darstellung der Fibonacci-Zahlen**). Wir bilden die sogenannte **erzeugende Funktion** der Fibonacci-Folge alias die formale Potenzreihe $f(x)=\sum_{n\geq 0} f_n x^n$ mit den Fibonacci-Zahlen aus **??** als Koeffizienten. Die Rekursionsformel für Fibonacci-Zahlen $f_{n+2}=f_{n+1}+f_n$ liefert unmittelbar $xf(x)+x^2f(x)=f(x)-x$. Wir folgern $(1-x-x^2)f(x)=x$. Umgekehrt hat jede formale Potenzreihe, die diese Identität erfüllt, die Fibonacci-Zahlen als Koeffizienten. Es gilt also, die Funktion $x/(1-x-x^2)$ in eine Potenzreihe zu entwickeln. Dazu erinnern wir Satz 2.5.12 über die Partialbruchzerlegung, schreiben $x^2+x-1=(x+\alpha)(x+\beta)$ mit $\alpha=\frac{1}{2}+\frac{1}{2}\sqrt{5}$ und $\beta=\frac{1}{2}-\frac{1}{2}\sqrt{5}$ und dürfen $x/(1-x-x^2)=a/(x+\alpha)+b/(x+\beta)$ ansetzen. Zur Vereinfachung der weiteren Rechnungen erinnern wir $\alpha\beta=-1$ und variieren unseren Ansatz zu $x/(1-x-x^2)=c/(1-x\alpha)+d/(1-x\beta)$. Das führt zu $c+d=0$ alias $c=-d$ und $\alpha c+\beta d=-1$ alias $c=1/(\beta-\alpha)=1/\sqrt{5}$. Die Entwicklung unserer Brüche in eine geometrische Reihe nach 2.5.10 liefert damit im Ring der formalen Potenzreihen die Identität

$$\frac{x}{1-x-x^2}=\sum_{i\geq 0}\frac{(x\alpha)^i}{\sqrt{5}}-\frac{(x\beta)^i}{\sqrt{5}}$$

und für den Koeffizienten von x^i alias die i-te Fibonacci-Zahl f_i ergibt sich wie in **??** die Darstellung

$$f_i=\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^i-\frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^i$$

Übungen

Übung 2.5.19. Man zeige: Besitzt ein kommutativer Integritätsbereich R eine Anordnung $\leq$, unter der er im Sinne von **??** ein angeordneter Ring wird, so besitzt sein Quotientenkörper $\operatorname{Quot} R$ genau eine Struktur als angeordneter Körper, für die die kanonische Einbettung $R \hookrightarrow \operatorname{Quot} R$ mit der Anordnung verträglich alias monoton wachsend ist. Speziell erhalten wir so die übliche Anordnung auf $\mathbb{Q} = \operatorname{Quot} \mathbb{Z}$.

Ergänzende Übung 2.5.20. Gegeben ein unendlicher Körper K und eine von Null verschiedene rationale Funktion $f \in K(X)^\times$ sind die Polstellen von f genau die Nullstellen von $(1/f)$, als da heißt, die Stellen aus dem Definitionsbereich von $(1/f)$, an denen diese Funktion den Wert Null annimmt. Fassen wir genauer f als Abbildung $f : K \to K \sqcup \{\infty\}$ auf, so entspricht $(1/f)$ der Abbildung $a \mapsto f(a)^{-1}$, wenn wir $0^{-1} = \infty$ und $\infty^{-1} = 0$ vereinbaren.

Übung 2.5.21. Ist K ein algebraisch abgeschlossener Körper, so nimmt eine von Null verschiedene rationale Funktion $f \in K(X)^\times$ auf ihrem Definitionsbereich fast jeden Wert an gleichviel Stellen an, genauer an $n = \max(\operatorname{grad} g, \operatorname{grad} h)$ Stellen für $f = g/h$ eine unkürzbare Darstellung als Quotient zweier Polynome. In anderen Worten haben unter $f : D(f) \to K$ fast alle Punkte $a \in K$ genau n Urbilder.

Übung 2.5.22. Sei $P \in \mathbb{Q}(X)$ gegeben. Man zeige: Gibt es eine Folge ganzer Zahlen aus dem Definitionsbereich unserer rationalen Funktion $a_n \in \mathbb{Z} \cap D(P)$ mit $a_n \to \infty$ und $P(a_n) \in \mathbb{Z}$ für alle n, so ist P bereits ein Polynom $P \in \mathbb{Q}[X]$.

Übung 2.5.23. Sei K ein Köper und seien $f, g \in K(X)$ gegeben. Man zeige: Gibt es unendlich viele Punkte aus dem gemeinsamen Definitionsbereich $D(f) \cap D(g)$, an denen f und g denselben Wert annehmen, so gilt bereits $f = g$ in $K(X)$.

Ergänzende Übung 2.5.24. Man zeige, daß im Körper $\mathbb{Q}(\!(X)\!)$ jede formale Potenzreihe mit konstantem Koeffizienten Eins eine Quadratwurzel besitzt. Die Quadratwurzel von $(1 + X)$ kann sogar durch die binomische Reihe **??** explizit angegeben werden, aber das sieht man leichter mit den Methoden der Analysis.

Übung 2.5.25. Man bestimme die Partialbruchzerlegung von $1/(1+X^4)$ in $\mathbb{C}(X)$.

Übung 2.5.26. Man zeige, daß bei einem Bruch $P(T)/(T^n(T-1)^m)$ mit Zähler $P(T) \in \mathbb{Z}[T]$ auch alle Koeffizienten bei der Partialbruchzerlegung ganze Zahlen sind.

Übung 2.5.27. Man bearbeite nocheinmal die Übungen **??** und **??**.

Übung 2.5.28 (**Verknüpfung rationaler Funktionen**). Ist K ein Körper und $P \in K[X]$ ein von Null verschiedenes Polynom, so liegt jede Nullstelle von P im größeren Körper $K(Y) \supset K$ bereits im Teilkörper K. Gegeben $f \in K(X)$ gehört

mithin jedes $g \in K(Y)\backslash K$ zum Definitionsbereich von f und wir können mithin setzen

$$f \circ g := f(g) \in K(Y)$$

Man zeige, daß die K-linearen Körperhomomorphismen $\varphi : K(X) \to K(Y)$ alle die Gestalt $\varphi : f \mapsto f \circ g$ haben für $g = \varphi(X) \in K(Y)\backslash K$. Sind f und g beide nicht konstant, so ist auch $f \circ g$ nicht konstant. Gegeben $f, g, h \in K(X)\backslash K$ zeige man die Assoziativität $(f \circ g) \circ h = f \circ (g \circ h)$. Unsere Abbildung $K(X) \to \mathrm{Ens}(K, K \sqcup \{\infty\})$ kann zu einer Abbildung $K(X) \to \mathrm{Ens}(K \sqcup \{\infty\})$ fortgesetzt werden, indem wir für $f = P/Q$ den Wert $f(\infty)$ erklären als den Quotienten a_n/b_n der Leitkoeffizienten, falls P und Q denselben Grad n haben, und ∞ falls der Grad von P größer ist als der von Q, und 0 falls er kleiner ist. So erhalten wir einen Monoidhomomorphismus $(K(X), \circ) \to (\mathrm{Ens}(K \sqcup \{\infty\}), \circ)$, der im Fall eines unendlichen Körpers K injektiv ist.

Übung 2.5.29 (**Quotientenkörper von Ringen formaler Potenzreihen**). Gegeben ein kommutativer Integritätsbereich R zeige man, daß die universelle Eigenschaft des Quotientenkörpers einen Körperisomorphismus

$$\mathrm{Quot}(R[\![X]\!]) \xrightarrow{\sim} (\mathrm{Quot}\, R)(\!(X)\!)$$

induziert. Induktiv erhalten wir so etwa für jeden Körper K einen Körperisomorphismus

$$\big(K(\!(X)\!)\big)(\!(Y)\!) \xrightarrow{\sim} \big(K(\!(Y)\!)\big)(\!(X)\!)$$

Zum Beispiel ist $(X - Y)^{-1} = X^{-1}(1 - Y/X)^{-1} = \sum_{n\geq 0} X^{-n-1}Y^n$ die Darstellung eines Elements auf der linken Seite, das auf der rechten Seite auf den Ausdruck $\sum_{n\geq 0} -Y^{-n-1}X^n$ abgebildet wird.

2.6 Quaternionen*

2.6.1. Dieser Abschnitt ist für den Rest der Vorlesung unerheblich. Allerdings gehören die Quaternionen zur mathematischen Allgemeinbildung.

Definition 2.6.2. Ein **Schiefkörper** ist ein Ring R, der nicht der Nullring ist und in dem alle von Null verschiedenen Elemente Einheiten sind. Auf englisch sagt man **skew field**, auf französisch **corps gauche**. Gleichbedeutend spricht man auch von einem **Divisionsring**.

Satz 2.6.3 (Quaternionen). *Es gibt Fünftupel* $(\mathbb{H}, \mathrm{i}, \mathrm{j}, \mathrm{k}, \kappa)$ *bestehend aus einem Ring* $\mathbb{H}$*, Elementen* $\mathrm{i}, \mathrm{j}, \mathrm{k} \in \mathbb{H}$ *und einem Ringhomomorphismus* $\kappa : \mathbb{R} \to \mathbb{H}$ *derart, daß gilt*

$$\mathrm{i}^2 = \mathrm{j}^2 = \mathrm{k}^2 = \mathrm{i}\,\mathrm{j}\,\mathrm{k} = -1$$

und $\kappa(a)q = q\kappa(a)\ \forall a \in \mathbb{R}$, $q \in \mathbb{H}$ *und daß* $1, \mathrm{i}, \mathrm{j}, \mathrm{k}$ *eine Basis von* $\mathbb{H}$ *bilden für die durch die Vorschrift* $\mathbb{R} \times \mathbb{H} \to \mathbb{H}$, $(a, q) \mapsto \kappa(a)q$ *auf* $\mathbb{H}$ *gegebene Struktur als* $\mathbb{R}$*-Vektorraum. Des weiteren ist in einem derartigem Fünftupel der Ring* $\mathbb{H}$ *ein Schiefkörper.*

2.6.4. Ein derartiges Fünftupel ist im wesentlichen eindeutig bestimmt in der offensichtlichen Weise. Um das zu sehen beachten wir, daß durch Multiplikation der letzten Gleichung von rechts mit k folgt $\mathrm{i}\,\mathrm{j} = \mathrm{k}$ und durch Invertieren beider Seiten weiter $\mathrm{j}\,\mathrm{i} = -\mathrm{k}$. Von da ausgehend erhalten wir unmittelbar die Formeln

$$\mathrm{i}\,\mathrm{j} = \mathrm{k} = -\mathrm{j}\,\mathrm{i}, \quad \mathrm{j}\,\mathrm{k} = \mathrm{i} = -\mathrm{k}\,\mathrm{j}, \quad \mathrm{k}\,\mathrm{i} = \mathrm{j} = -\mathrm{i}\,\mathrm{k},$$

und so die Eindeutigkeit. Wegen dieser Eindeutigkeit erlauben wir uns den bestimmten Artikel und nennen $\mathbb{H}$ den Schiefkörper der **Quaternionen**, da er nämlich als Vektorraum über den reellen Zahlen die Dimension Vier hat, oder auch den Schiefkörper der **Hamilton'schen Zahlen** nach seinem Erfinder Hamilton. Weiter kürzen wir für reelle Zahlen $a \in \mathbb{R}$ meist $\kappa(a) = a$ ab. Jedes Element $q \in \mathbb{H}$ hat also die Gestalt

$$q = a + b\,\mathrm{i} + c\,\mathrm{j} + d\,\mathrm{k}$$

mit wohlbestimmten $a, b, c, d \in \mathbb{R}$. Die Abbildung $\mathbb{C} \hookrightarrow \mathbb{H}$ mit $a + b\mathrm{i}_{\mathbb{C}} \mapsto a + b\mathrm{i}$ ist ein Ringhomomorphismus und wir machen auch für komplexe Zahlen meist in der Notation keinen Unterschied zwischen unserer Zahl und ihrem Bild in $\mathbb{H}$ unter obiger Einbettung. In 7.12.2 diskutieren wir, warum und in welcher Weise $\mathbb{R}, \mathbb{C}$ und $\mathbb{H}$ bis auf Isomorphismus die einzigen Schiefkörper endlicher Dimension „über dem Körper $\mathbb{R}$" sind.

2.6.5. Auch die Abbildungen $\mathbb{C} \to \mathbb{H}$ mit $a+b\mathrm{i}_{\mathbb{C}} \mapsto a+b\mathrm{j}$ oder mit $a+b\mathrm{i}_{\mathbb{C}} \mapsto a+b\mathrm{k}$ sind Ringhomomorphismen, und wir werden bald sehen, daß es sogar unendlich viele $\mathbb{R}$-lineare Ringhomomorphismen, ja eine ganze 3-Sphäre von $\mathbb{R}$-linearen Ringhomomorphismen $\mathbb{C} \to \mathbb{H}$ gibt.

2.6.6. Hamilton war von seiner Entdeckung so begeistert, daß er eine Gedenktafel an der Dubliner Broom Bridge anbringen ließ, auf der zu lesen ist: „Here as he walked by on the 16th of October 1843 Sir William Rowan Hamilton in a flash of genius discovered the fundamental formula for quaternion multiplication $\mathrm{i}^2 = \mathrm{j}^2 = \mathrm{k}^2 = \mathrm{i}\,\mathrm{j}\,\mathrm{k} = -1$ & cut it on a stone of this bridge".

Beweis. Bezeichne $\mathbb{H}$ die Menge aller komplexen (2×2)-Matrizen der Gestalt

$$\mathbb{H} = \left\{ \begin{pmatrix} z & -y \\ \bar{y} & \bar{z} \end{pmatrix} \middle| \, z, y \in \mathbb{C} \right\} \subset \mathrm{Mat}(2; \mathbb{C})$$

Die Addition und Multiplikation von Matrizen induziert offensichtlich eine Addition und Multiplikation auf $\mathbb{H}$ und wir erhalten eine Einbettung $\mathbb{C} \hookrightarrow \mathbb{H}$ vermittels

$z \mapsto \operatorname{diag}(z, \bar{z})$. Das Bilden der konjugierten transponierten Matrix definiert einen Antiautomorphismus $q \mapsto \bar{q}$ von $\mathbb{H}$, in Formeln $\overline{qw} = \bar{w}\bar{q}$, und $q\bar{q}$ ist für $q \neq 0$ stets positiv und reell. Folglich ist $\mathbb{H}$ ein Schiefkörper. Wir fassen $\mathbb{C}$ meist als Teilmenge von $\mathbb{H}$ auf vermittels der eben erklärten Einbettung, aber vorerst unterscheiden wir noch zwischen den komplexen Zahlen $1_{\mathbb{C}}$, $\mathrm{i}_{\mathbb{C}}$ und den Matrizen $1 = \operatorname{diag}(1_{\mathbb{C}}, 1_{\mathbb{C}})$, $\mathrm{i} = \operatorname{diag}(\mathrm{i}_{\mathbb{C}}, -\mathrm{i}_{\mathbb{C}})$. Unser $\mathbb{H}$ hat dann über $\mathbb{R}$ die Basis $1, \mathrm{i}, \mathrm{j}, \mathrm{k}$ mit $\mathrm{i} := \operatorname{diag}(\mathrm{i}_{\mathbb{C}}, -\mathrm{i}_{\mathbb{C}})$ und

$$\mathrm{j} := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ und } \mathrm{k} := \begin{pmatrix} 0 & \mathrm{i}_{\mathbb{C}} \\ \mathrm{i}_{\mathbb{C}} & 0 \end{pmatrix}$$

und es gilt

$$\mathrm{i}^2 = \mathrm{j}^2 = \mathrm{k}^2 = \mathrm{i}\,\mathrm{j}\,\mathrm{k} = -1 \qquad \square$$

2.6.7. Jede zyklische Vertauschung von $\mathrm{i}, \mathrm{j}, \mathrm{k}$ liefert einen Automorphismus der Quaternionen. Die Konjugation $q \mapsto \bar{q}$ aus der im Beweis gegebenen Konstruktion hat in der Basis $1, \mathrm{i}, \mathrm{j}, \mathrm{k}$ die Gestalt

$$\overline{a + b\,\mathrm{i} + c\,\mathrm{j} + d\,\mathrm{k}} = a - b\,\mathrm{i} - c\,\mathrm{j} - d\,\mathrm{k}$$

und hat wie bereits erwähnt die Eigenschaft $\overline{qw} = \bar{w}\bar{q}$. Gegeben ein Quaternion $q = a + b\,\mathrm{i} + c\,\mathrm{j} + d\,\mathrm{k}$ nennt man $a = (q + \bar{q})/2$ seinen **Realteil** und schreibt $a = \operatorname{Re}(q)$. Für $q = a + b\,\mathrm{i} + c\,\mathrm{j} + d\,\mathrm{k}$ ist $q\bar{q} = \bar{q}q = a^2 + b^2 + c^2 + d^2$ und man setzt $|q| = \sqrt{q\bar{q}}$ und nennt diese reelle Zahl den **Betrag** unseres Quaternions. Offensichtlich kann für $q \neq 0$ sein Inverses durch die Formel $q^{-1} = \bar{q}/|q|^2$ angegeben werden. Offensichtlich gilt dann $|qw| = |q||w|$ für alle $q, w \in \mathbb{H}$ und die Gruppe aller Quaternionen der Länge Eins besteht genau aus allen unitären (2×2)-Matrizen mit Determinante Eins. Darin enthalten ist die Untergruppe der acht Quaternionen $\{\pm 1, \pm \mathrm{i}, \pm \mathrm{j}, \pm \mathrm{k}\}$, die sogenannte **Quaternionengruppe**, von deren Multiplikationstabelle Hamilton bei seiner Konstruktion ausgegangen war.

Vorschau 2.6.8. Gegeben ein Kring R mitsamt einem selbstinversen Ringhomomorphismus $R \to R$, $r \mapsto \bar{r}$ und einem Element $v \in R$ mit $\bar{v} = v$ bildet allgemeiner die Menge aller (2×2)-Matrizen der Gestalt

$$\mathbb{H} = \left\{ \begin{pmatrix} z & vy \\ \bar{y} & \bar{z} \end{pmatrix} \middle| \, z, y \in R \right\} \subset \operatorname{Mat}(2; R)$$

einen Teilring des Matrizenrings. Derartige Ringe heißen **Quaternionenringe**.

2.6.9. Es gibt außer der Identität nur einen $\mathbb{R}$-linearen Körperhomomorphismus $\mathbb{C} \to \mathbb{C}$, nämlich die komplexe Konjugation. Im Fall der Quaternionen liefert dahingegen jede von Null verschiedene Quaternion $q \in \mathbb{H}^\times$ einen $\mathbb{R}$-linearen Ringhomomorphismus $\operatorname{int} q : \mathbb{H} \to \mathbb{H}$, $w \mapsto qwq^{-1}$, und $\operatorname{int} q = \operatorname{int} q'$ impliziert bereits $\mathbb{R}q = \mathbb{R}q'$.

Übungen

Übung 2.6.10. Man zeige, daß es für jedes Quaternion q mit Realteil $\operatorname{Re} q = 0$ und Betrag $|q| = 1$ einen $\mathbb{R}$-linearen Ringhomomorphismus $\mathbb{C} \to \mathbb{H}$ gibt mit $\mathrm{i}_{\mathbb{C}} \mapsto q$.

Ergänzende Übung 2.6.11. Man zeige: Sind zwei natürliche Zahlen jeweils eine Summe von vier Quadraten, so auch ihr Produkt. Diese Erkenntnis ist ein wichtiger Schritt bei einem Beweis des sogenannten **Vier-Quadrate-Satzes** von Lagrange, nach dem jede natürliche Zahl eine Summe von vier Quadratzahlen ist, etwa $3 = 1^2 + 1^2 + 1^2 + 0^2$ oder $23 = 3^2 + 3^2 + 2^2 + 1^2$.

3 Quotienten

In diesem Abschnitt wird die Gruppentheorie weiter ausgebaut. Insbesondere lernen Sie die Klassifikation der endlich erzeugten abelschen Gruppen kennen. Man versteht unter solch einer Klassifikation die Angabe einer Liste von endlich erzeugten abelschen Gruppen derart, daß jede endlich erzeugte abelsche Gruppe zu genau einer Gruppe dieser Liste isomorph ist. Die Klassifikation endlich erzeugter Vektorräume über einem vorgegebenen Körper K kennen Sie bereits: Jeder solche Vektorraum K ist isomorph zu genau einem K^n mit $n \in \mathbb{N}$, und dieses n heißt dann auch die Dimension des K-Vektorraums V. Wir werden sehen, daß die Klassifikation der endlich erzeugten abelschen Gruppen raffinierter ist.

3.1 Nebenklassen

3.1.1. Ist $(G, \perp)$ eine Menge mit Verknüpfung und sind $A, B \subset G$ Teilmengen, so schreiben wir $A \perp B = \{a \perp b \mid a \in A,\ b \in B\} \subset G$ und erhalten auf diese Weise eine Verknüpfung auf der Menge aller Teilmengen von G, der sogenannten Potenzmenge $\mathcal{P}(G)$. Ist unsere ursprüngliche Verknüpfung assoziativ, so auch die induzierte Verknüpfung auf der Potenzmenge. Wir kürzen in diesem Zusammenhang oft die einelementige Menge $\{a\}$ mit a ab, so daß also zum Beispiel $a \perp B$ als $\{a\} \perp B$ zu verstehen ist.

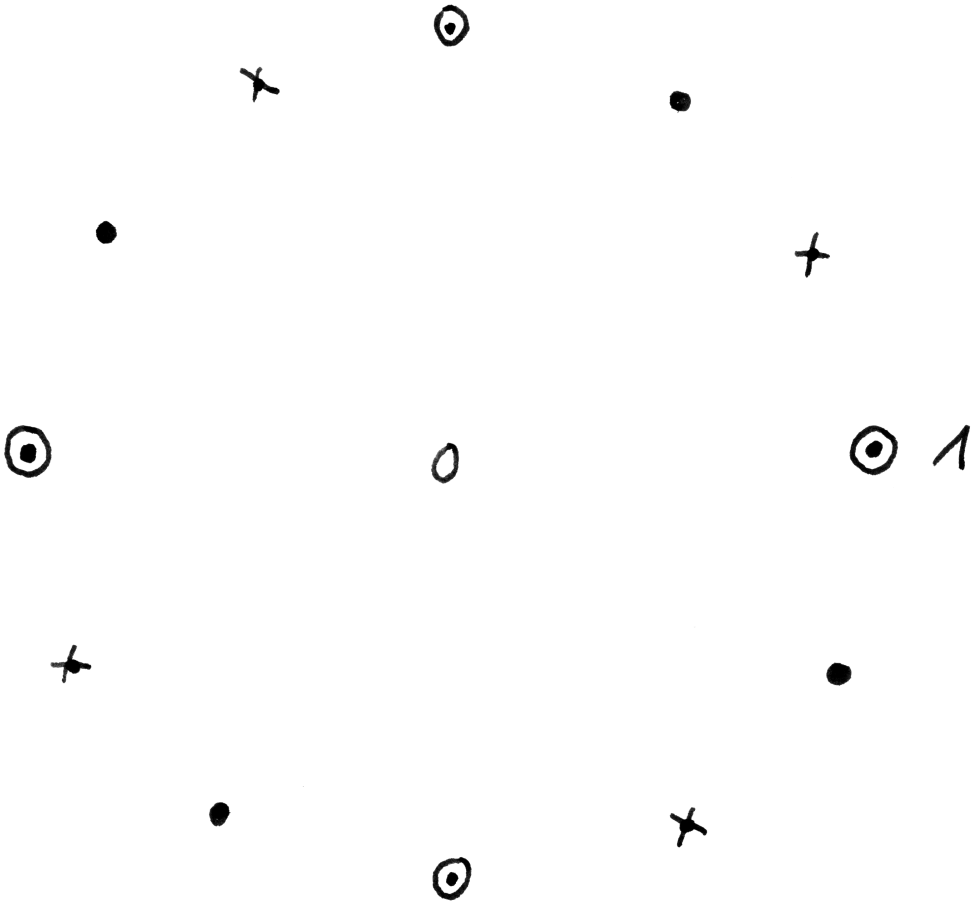
Definition 3.1.2. Ist G eine Gruppe, $H \subset G$ eine Untergruppe und $g \in G$ ein Element, so nennen wir die Menge gH die **Linksnebenklasse von** g **unter** H und die Menge Hg die **Rechtsnebenklasse von** g **unter** H. Diese Nebenklassen sind also Teilmengen von G. Ein Element einer Nebenklasse nennt man einen **Repräsentanten** der besagten Nebenklasse. Weiter betrachten wir in G die beiden Mengensysteme

$$\begin{aligned} G/H &= \{gH \mid g \in G\} \\ H\backslash G &= \{Hg \mid g \in G\} \end{aligned}$$

aller Links- beziehungsweise Rechtsnebenklassen von H in G. Die Elemente von G/H und von $H\backslash G$ sind also Teilmengen von G. Die Symbole G/H sowie $H\backslash G$ bezeichnen dementsprechend Teilmengen der Potenzmenge $\mathcal{P}(G)$ von G.

3.1.3 (**Disjunktheit der Nebenklassen**). Gegeben $G \supset H$ eine Gruppe mit einer Untergruppe sind die H-Rechtsnebenklassen in G paarweise disjunkt. In der Tat folgt aus $g \in xH$ alias $g = xh$ für $h \in H$ bereits $gH = xhH = xH$. Analoges gilt für die Linksnebenklassen.

Beispiel 3.1.4. Im Fall $G = \mathbb{Z} \supset H = m\mathbb{Z}$ haben wir die Menge der Nebenklassen $\mathbb{Z}/m\mathbb{Z}$ bereits in 2.2.4 diskutiert und sogar selbst mit der Struktur einer Gruppe, ja sogar mit der Struktur eines Rings versehen. Im allgemeinen trägt G/H



Die drei Nebenklassen der Gruppe $\{\pm 1, \pm \mathrm{i}\}$ der vierten Einheitswurzeln in der Gruppe der zwölften Einheitswurzeln. Da diese Gruppe kommutativ ist, fallen hier Rechtsnebenklassen und Linksnebenklassen zusammen.

nur dann eine natürliche Gruppenstruktur, wenn wir an unsere Untergruppe H zusätzliche Forderungen stellen, vergleiche 3.2.

Satz 3.1.5 (**Lagrange**). *Gegeben eine endliche Gruppe teilt die Kardinalität jeder Untergruppe die Kardinalität der ganzen Gruppe. Ist G eine endliche Gruppe und $H \subset G$ eine Untergruppe, so gilt genauer*

$$|G| = |H| \cdot |G/H| = |H| \cdot |H\backslash G|$$

Beweis. Jedes Element von G gehört zu genau einer Links- beziehungsweise Rechtsnebenklasse unter H, und jede dieser Nebenklassen hat genau $|H|$ Elemente. □

3.1.6. In anderen Worten kann man diesen Beweis etwa im Fall der Linksnebenklassen auch dahingehend formulieren, daß alle Fasern der offensichtlichen Abbildung $\mathrm{can} : G \to G/H$ genau $|H|$ Elemente haben, denn diese Fasern sind gerade die Linksnebenklassen von H in G.

Definition 3.1.7. Gegeben eine Gruppe G mit einer Untergruppe H heißt die Zahl $|G/H|$ der Restklassen auch der **Index von H in G**.

Übungen

Ergänzende Übung 3.1.8. Haben zwei Untergruppen ein- und derselben Gruppe endlichen Index, so hat auch ihr Schnitt endlichen Index.

Ergänzende Übung 3.1.9. Seien $G \supset H$ eine Gruppe und eine Untergruppe. Man zeige, daß es eine Bijektion zwischen G/H und $H\backslash G$ gibt.

Ergänzende Übung 3.1.10. Haben zwei endliche Untergruppen einer Gruppe teilerfremde Kardinalitäten, so besteht ihr Schnitt nur aus dem neutralen Element.

Übung 3.1.11. Sei $\varphi : G \to L$ ein Gruppenhomomorphismus und seien $H \subset G$ sowie $H' \subset G'$ Untergruppen. Gilt $\varphi(H) \subset H'$, so gibt es genau eine Abbildung $\bar{\varphi} : G/H \to G'/H'$ derart, daß im Diagramm

$$\begin{array}{ccccc} H & \longrightarrow & G & \longrightarrow & G/H \\ \downarrow & & \downarrow & & \downarrow \\ H' & \longrightarrow & G' & \longrightarrow & G'/H' \end{array}$$

auch das rechte Rechteck kommutiert, und die nichtleeren Fasern dieser Abbildung $\bar{\varphi}$ sind die Mengen $\bar{\varphi}^{-1}(\varphi(g)H') = \{gxH \mid x \in \varphi^{-1}(H')\}$ und haben insbesondere alle dieselbe Kardinalität wie $\varphi^{-1}(H')/H$. Sind weiter zwei der vertikalen Abbildungen unseres Diagramms Bijektionen, so auch die Dritte. Allgemeinere Aussagen liefert später das Neunerlemma 3.7.5.

Ergänzende Übung 3.1.12 (**Zu unipotenten oberen Dreiecksmatrizen**). Sei R ein Ring und $n \geq 2$. Gegeben $i, j \leq n$ mit $i \neq j$ betrachten wir die Untergruppen $U_{ij} := \mathrm{I} + RE_{ij} \subset \mathrm{GL}(n;R)$ und die Untergruppe $U \subset \mathrm{GL}(n;R)$ aller oberen Dreiecksmatrizen mit Einträgen in R. Man zeige, daß das Aufmultiplizieren in beliebiger aber fest gewählter Reihenfolge stets eine Bijektion

$$\prod_{i<j} U_{ij} \xrightarrow{\sim} U$$

induziert. Hinweis: Man betrachte rechts die Folge von Untergruppen $U_\nu := \{A \mid A_{ij} = 0 \text{ für } 0 < |i-j| \leq \nu\}$ und verwende 3.1.11. Allgemeiner zeige man, daß für jede Permutation $w \in \mathcal{S}_n$ die Multiplikation bei beliebiger aber fester Reihenfolge der Faktoren eine Bijektion $\prod_{i<j,\, w(i)<w(j)} U_{ij} \xrightarrow{\sim} U \cap w^{-1}Uw$ liefert. Hinweis: Natürlich gilt stets $U_{w(i)w(j)}w = wU_{ij}$.

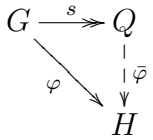
3.2 Normalteiler und Nebenklassengruppen

Satz 3.2.1 (Universelle Eigenschaft surjektiver Gruppenhomomorphismen). *Seien G eine Gruppe, $s : G \twoheadrightarrow Q$ ein surjektiver Gruppenhomomorphismus und $\varphi : G \to H$ ein beliebiger Gruppenhomomorphismus. Genau dann existiert ein Gruppenhomomorphismus $\bar{\varphi} : Q \to H$ mit $\varphi = \bar{\varphi} \circ s$, wenn gilt* $\ker(\varphi) \supset \ker(s)$.

3.2.2. Dieser Gruppenhomomorphismus $\bar{\varphi}$ ist dann natürlich eindeutig bestimmt. In diesem Sinne kann man unseren Satz auch dahingehend zusammenfassen, daß das Vorschalten eines surjektiven Gruppenhomomorphismus $s : G \twoheadrightarrow Q$ für jede weitere Gruppe H eine Bijektion

$$(\circ s) : \mathrm{Grp}(Q,H) \xrightarrow{\sim} \{\varphi \in \mathrm{Grp}(G,H) \mid \ker(\varphi) \supset \ker(s)\}$$

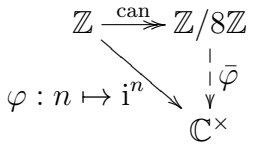
liefert. Der Übersichtlichkeit halber stelle ich die in diesem Satz auftauchenden Gruppen und Morphismen auch noch wieder anders in einem Diagramm dar:



Man sagt dann, φ **faktorisiere in eindeutiger Weise über** s.

Beweis. Offensichtlich gilt $s^{-1}(s(x)) = x\ker(s)$ für alle $x \in G$. Die Fasern von unseres surjektiven Gruppenhomomorphismus s sind also genau die Nebenklassen unter $\ker(s)$. Damit ist φ konstant auf den Fasern von s und wir finden nach der universellen Eigenschaft von Surjektionen **??** schon einmal genau eine Abbildung $\bar{\varphi}$ wie behauptet. Man prüft ohne weitere Schwierigkeiten, daß sie sogar ein Gruppenhomomorphismus sein muß. □

Beispiel 3.2.3. Wir haben etwa



oder in Worten: Die Abbildung $\varphi : n \mapsto \mathrm{i}^n$ faktorisiert über $\mathbb{Z}/8\mathbb{Z}$ und induziert so einen Gruppenhomomorphismus $\bar{\varphi} : \mathbb{Z}/8\mathbb{Z} \to \mathbb{C}^\times$, $\bar{n} \mapsto \mathrm{i}^n$.

3.2.4 (**Surjektive Gruppenhomomorphismen mit demselben Kern**). Gegeben eine Gruppe G und zwei surjektive Gruppenhomomorphismus $s : G \twoheadrightarrow Q$ und $t : G \twoheadrightarrow P$ mit demselben Kern $\ker(s) = \ker(t)$ sind die Gruppenhomomorphismen $\bar{t} : Q \to P$ mit $\bar{t} \circ s = t$ und $\bar{s} : P \to Q$ mit $\bar{s} \circ t = s$ nach 3.2.1 zueinander inverse Isomorphismen $Q \xrightarrow{\sim} P \xrightarrow{\sim} Q$. Salopp gesprochen wird also bei einem surjektiven Gruppenhomomorphismus „das Ziel bereits durch die Ausgangsgruppe und den Kern festgelegt bis auf eindeutigen Isomorphismus“.

3.2.5. Die vorstehenden Überlegungen legen die Frage nahe, welche Untergruppen einer gegebenen Gruppe denn als Kerne von von unserer Gruppe ausgehenden Gruppenhomomorphismen in Frage kommen. Das diskutieren wir im folgenden.

Definition 3.2.6. Eine Untergruppe N einer Gruppe G heißt **normal** oder auch ein **Normalteiler von** G, wenn in G die N-Rechtsnebenklassen mit den N-Linksnebenklassen übereinstimmen, wenn also gilt

$$gN = Ng \; \forall g \in G$$

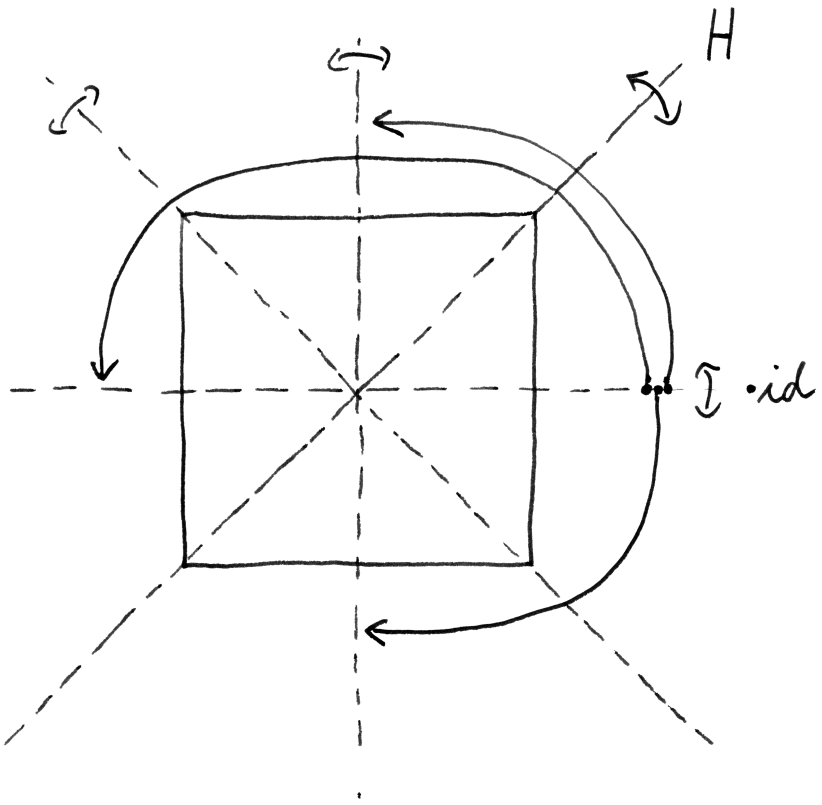
Die Aussage „$N \subset G$ ist ein Normalteiler“ kürzt man oft ab mit $N \triangleleft G$.

Beispiele 3.2.7. In einer kommutativen Gruppe ist jede Untergruppe ein Normalteiler. In der Gruppe $\mathcal{S}_3$ der Permutationen von 3 Elementen ist die Untergruppe $\mathcal{S}_2 \subset \mathcal{S}_3$ aller Permutationen, die die dritte Stelle festhalten, kein Normalteiler.

3.2.8 (**Diskussion der Terminologie**). Normal zu sein ist für eine Untergruppe etwas ganz Besonderes. In diesem Licht betrachtet ist unsere Terminologie gewöhnungsbedürftig. Aber gut, vielleicht ist ja bei Menschen auch normal zu sein etwas ganz Besonderes.

3.2.9. Man sieht leicht, daß der Kern eines Gruppenhomomorphismus stets ein Normalteiler sein muß. Wir zeigen nun, daß auch umgekehrt jeder Normalteiler der Kern eines surjektiven Gruppenhomomorphismus ist.

Satz 3.2.10. *Seien G eine Gruppe und $N \subset G$ ein Normalteiler. So gilt:*



Die acht Symmetrien des Quadrats. Eine Linksnebenklasse gH der von der Spiegelung an der Nordost-Diagonalen erzeugten Untergruppe besteht aus den beiden Symmetrien des Quadrats, die die obere rechte Ecke in eine vorgegebene weitere Ecke überführen. Eine Rechtsnebenklasse Hg besteht dahingegen aus den beiden Symmetrien des Quadrats, bei denen die obere rechte Ecke von einer vorgegebenen weiteren Ecke herkommt. Insbesondere ist H kein Normalteiler in der Gruppe der acht Symmetrien des Quadrats.

1. *Die Menge G/N der Nebenklassen ist abgeschlossen unter der induzierten Verknüpfung auf der Potenzmenge $\mathcal{P}(G)$ von G und wird mit dieser Verknüpfung eine Gruppe, die* **Nebenklassengruppe** *oder auch der* **Quotient von G nach N;**

2. *Die Abbildung $G \twoheadrightarrow G/N$, die jedem Element seine Nebenklasse zuordnet, ist ein surjektiver Gruppenhomomorphismus mit Kern N.*

Beweis. Es gilt $(gN)(g_1N) = gNg_1N = gg_1NN = gg_1N$, also ist unsere Menge stabil unter der Verknüpfung. Das Assoziativgesetz gilt eh, das neutrale Element ist N, und das Inverse zu gN ist $g^{-1}N$. Die zweite Aussage ist eh klar. □

Beispiel 3.2.11. Die Nebenklassengruppe $\mathbb{Z}/m\mathbb{Z}$ kennen wir bereits aus 2.2.4, wo wir darauf sogar noch eine Multiplikation erklärt hatten, die sie zu einem Ring macht. Sie hat genau m Elemente.

Satz 3.2.12 (Isomorphiesatz). *Jeder Homomorphismus $\varphi : G \to H$ von Gruppen induziert einen Isomorphismus $\bar{\varphi} : G/\ker\varphi \xrightarrow{\sim} \operatorname{im}\varphi$.*

Beispiel 3.2.13. In unserem Beispiel 3.2.3 liefert uns der Isomorphiesatz einen Isomorphismus $\mathbb{Z}/4\mathbb{Z} \xrightarrow{\sim} \{\mathrm{i}^n \mid n \in \mathbb{Z}\} \subset \mathbb{C}^\times$.

Beispiel 3.2.14. Die Abbildung $\varphi = 2\,\mathrm{can} : \mathbb{Z} \to \mathbb{Z}/10\mathbb{Z}$, $n \mapsto (2n + 10\mathbb{Z})$ hat den Kern $\ker\varphi = 5\mathbb{Z}$ und das Bild $\operatorname{im}\varphi = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\} \subset \mathbb{Z}/10\mathbb{Z}$. Der Isomorphiesatz liefert in diesem Fall also einen Gruppenisomorphismus

$$\mathbb{Z}/5\mathbb{Z} \xrightarrow{\sim} \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\}$$

Beweis. Das folgt sofort aus unserern Erkenntnissen 3.2.4 über surjektive Gruppenhomomorphismen mit demselben Kern, denn wir finden surjektive Gruppenhomomorphismen von G auf beide Seiten, die ein kommutatives Dreieck entstehen lassen und denselben Kern haben. □

Korollar 3.2.15 (Noether'scher Isomorphiesatz). *Ist G eine Gruppe und sind $K \subset H \subset G$ zwei Normalteiler von G, so induziert die Komposition von kanonischen Abbildungen $G \twoheadrightarrow (G/K) \twoheadrightarrow (G/K)/(H/K)$ einen Isomorphismus*

$$G/H \xrightarrow{\sim} (G/K)/(H/K)$$

3.2.16. Ist G eine Gruppe und sind $K \subset H \subset G$ Untergruppen mit K normal in H, so werden wir bald $(G/K)/(H/K)$ als „Raum der Bahnen einer Operation der Gruppe H/K auf der Menge G/K" verstehen können, und unsere Abbildung ist dann immer noch wohldefiniert und nach 4.1.26 eine Bijektion.

Beweis. Nach unserern Erkenntnissen 3.2.4 über surjektive Gruppenhomomorphismen mit demselben Kern3.2.4 reicht es zu zeigen, daß unsere Kompsition den Kern H hat. Das ist jedoch klar. □

Übungen

Übung 3.2.17. Man zeige, daß in der symmetrischen Gruppe $\mathcal{S}_4$ die Doppeltranspositionen aus **??** zusammen mit dem neutralen Element einen Normalteiler $D \subset \mathcal{S}_4$ bilden, und konstruiere einen Isomorphismus $\mathcal{S}_4/D \xrightarrow{\sim} \mathcal{S}_3$.

Ergänzende Übung 3.2.18. Sei $m \in \mathbb{N}$ eine natürliche Zahl. Man zeige, daß die Vorschrift $\varphi \mapsto \varphi(\bar{1})$ für eine beliebige Gruppe G eine Bijektion

$$\mathrm{Grp}(\mathbb{Z}/m\mathbb{Z}, G) \xrightarrow{\sim} \{g \in G \mid g^m = 1\}$$

liefert. Man beachte, daß hierbei $\bar{1}$ nicht das neutrale Element der additiv notierten Gruppe $\mathbb{Z}/m\mathbb{Z}$ bezeichnet, sondern die Nebenklasse der Eins, einen Erzeuger, wohingegen $1 \in G$ das neutrale Element der multiplikativ notierten Gruppe G meint. Wieviele Gruppenhomomorphismen gibt es von $\mathbb{Z}/m\mathbb{Z}$ nach $\mathbb{Z}/n\mathbb{Z}$?

Übung 3.2.19. Gegeben ein surjektiver Gruppenhomomorphismus $\varphi : G \twoheadrightarrow \bar{G}$ und ein Normalteiler $\bar{N} \subset \bar{G}$ mit Urbild $\varphi^{-1}(\bar{N}) = N \subset G$ induziert φ einen Gruppenisomorphismus

$$\varphi : G/N \xrightarrow{\sim} \bar{G}/\bar{N}$$

Übung 3.2.20. Der Kern eines Gruppenhomomorphismus ist stets ein Normalteiler. Allgemeiner ist das Urbild eines Normalteilers unter einem Gruppenhomomorphismus stets ein Normalteiler, und das Bild eines Normalteilers unter einem surjektiven Gruppenhomomorphismus ist wieder ein Normalteiler.

Ergänzende Übung 3.2.21. Jede Untergruppe vom Index Zwei ist ein Normalteiler.

Ergänzende Übung 3.2.22. Jede Untergruppe von endlichem Index umfaßt einen Normalteiler von endlichem Index.

Ergänzende Übung 3.2.23. Man nennt einen Gruppenhomomorphismus $A \to A''$ **linksspaltend**, wenn er ein Rechtsinverses besitzt, und nennt solch ein Rechtsinverses dann eine **Spaltung**. Man zeige: Jeder linksspaltende Gruppenhomomorphismus ist surjektiv. Ist $\varphi : A \to A''$ ein Homomorphismus von abelschen Gruppen, $A' \subset A$ sein Kern und $\psi : A'' \to A$ ein Rechtsinverses von φ alias $\varphi\psi = \mathrm{id}$, so erhalten wir vermittels der Vorschrift $(a', a'') \mapsto a' + \psi(a'')$ einen Isomorphismus $A' \times A'' \xrightarrow{\sim} A$. Verallgemeinerungen auf den Fall nichtabelscher Gruppen besprechen wir in 5.2.10.

Ergänzende Übung 3.2.24. Man nennt einen Gruppenhomomorphismus $A' \to A$ **rechtsspaltend**, wenn er ein Linksinverses besitzt, und nennt solch ein Linksinverses dann eine **Spaltung**. Man zeige: Jeder rechtsspaltende Gruppenhomomorphismus ist injektiv. Ist $\psi : A' \to A$ ein Homomorphismus von abelschen Gruppen und $\phi : A \to A'$ ein Linksinverses alias $\phi\psi = \mathrm{id}$ und $A'' \subset A$ dessen Kern, so ist ϕ linksspaltend und wir erhalten für $A'' := \ker \phi$ wie in 3.2.23 einen Isomorphismus $A' \times A'' \xrightarrow{\sim} A$.

Ergänzende Übung 3.2.25. Jede Surjektion von einer abelschen Gruppe auf $\mathbb{Z}^r$ besitzt ein Rechtsinverses. Man gebe ein Beispiel für einen surjektiven Gruppenhomomorphismus, der kein Rechtsinverses besitzt.

Übung 3.2.26. Man zeige, daß das Multiplizieren von Matrizen mit Spaltenvektoren eine Bijektion $\mathrm{Mat}(n \times m; \mathbb{Z}) \xrightarrow{\sim} \mathrm{Grp}(\mathbb{Z}^m, \mathbb{Z}^n)$, $A \mapsto (A\circ)$ zwischen der Menge aller $(n \times m)$-Matrizen mit ganzzahligen Einträgen und der Menge aller Gruppenhomomorphismen $\mathbb{Z}^m \to \mathbb{Z}^n$ liefert.

Ergänzende Übung 3.2.27. Seien A, B, C abelsche Gruppen. Eine Abbildung $\varphi : A \times B \to C$ heißt **biadditiv**, wenn jedes feste $b \in B$ einen Gruppenhomomorphismus $A \to C$, $a \mapsto \varphi(a, b)$ liefert und jedes feste $a \in A$ einen Gruppenhomomorphismus $B \to C$, $b \mapsto \varphi(a, b)$. Man zeige: Gegeben eine biadditive Abbildung $\varphi : A \times B \to C$ und surjektive Homomorphismen $s : A \twoheadrightarrow P$ sowie $t : B \twoheadrightarrow Q$ mit $\varphi(\ker(s) \times B) = 0 = \varphi(A \times \ker(t))$ gibt es genau eine biadditive Abbildung $\bar{\varphi} : P \times Q \to C$ derart, daß das folgende Diagramm kommutiert:

$$\begin{array}{ccc} A \times B & \xrightarrow{\varphi} & C \\ {\scriptstyle s\times t}\downarrow & & \| \\ P \times Q & \xrightarrow{\bar{\varphi}} & C \end{array}$$

Analog erklärt man multiadditive Abbildungen für abelsche Gruppen und zeigt für diese eine analoge Aussage.

3.3 Zyklische Gruppen

Definition 3.3.1. Eine Gruppe heißt **zyklisch**, wenn sie im Sinne von 1.3.5 von einem einzigen Element erzeugt wird.

Definition 3.3.2. Sei g ein Element einer Gruppe G. Die **Ordnung** $\mathrm{ord}\, g$ von g ist die kleinste natürliche Zahl $n \geq 1$ mit $g^n = 1_G$. Gibt es kein solches n, so setzen wir $\mathrm{ord}\, g = \infty$ und sagen, g habe **unendliche Ordnung**.

3.3.3. In jeder Gruppe ist das einzige Element der Ordnung 1 das neutrale Element. Elemente der Ordnung ≤ 2 heißen auch **Involutionen**.

Proposition 3.3.4 (Struktur zyklischer Gruppen). *Ist G eine Gruppe und $g \in G$ ein Element, so stimmt die Ordnung von g überein mit der Kardinalität der von g erzeugten Untergruppe, in Formeln $\mathrm{ord}\, g = |\langle g \rangle|$. Genauer gilt:*

1. *Hat g unendliche Ordnung, so ist die Abbildung $\nu \mapsto g^\nu$ ein Isomorphismus $\mathbb{Z} \xrightarrow{\sim} \langle g \rangle$;*

2. *Hat g endliche Ordnung $\operatorname{ord} g = n$, so induziert $\nu \mapsto g^\nu$ einen Isomorphismus $\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \langle g\rangle$.*

Beweis. Wir betrachten den Gruppenhomomorphismus $\varphi : \mathbb{Z} \to G$, $\nu \mapsto g^\nu$. Nach dem Isomorphiesatz 3.2.12 haben wir einen Isomorphismus

$$\mathbb{Z}/\ker\varphi \xrightarrow{\sim} \operatorname{im}\varphi = \langle g\rangle$$

Nach der Klassifikation 1.3.4 der Untergruppen von $\mathbb{Z}$ ist $\ker\varphi$ von der Form $\ker\varphi = n\mathbb{Z}$ für eindeutig bestimmtes $n \in \mathbb{N}$, und dann gilt notwendig $n = \operatorname{ord} g$ für g von endlicher Ordnung beziehungsweise $n = 0$ für g von unendlicher Ordnung. □

3.3.5. Motiviert durch diese Proposition nennt man die Kardinalität einer Gruppe oft die **Ordnung der Gruppe**. Wir haben mit unserer Proposition im Übrigen auch bewiesen, daß jede Gruppe mit genau 5 Elementen isomorph ist zu $\mathbb{Z}/5\mathbb{Z}$, denn für jedes vom neutralen Element verschiedene Element unserer Gruppe ist $\langle g\rangle$ eine Untergruppe mit mindestens zwei Elementen, also nach Lagrange bereits die ganze Gruppe. Wir formulieren das gleich noch allgemeiner.

Ergänzung 3.3.6 (**Diskussion der Notation**). Für die endlichen zyklischen Gruppen $\mathbb{Z}/n\mathbb{Z}$ mit $n \geq 1$ sind viele alternative Notationen gebräuchlich. Ich kenne insbesondere die alternativen Notationen C_n, Z_n und $\mathbb{Z}_n$, von denen ich die letzte am wenigsten mag, da sie im Fall einer Primzahl $n = p$ auch für die sogenannten p-adischen Zahlen benutzt wird.

Korollar 3.3.7. *Jede Gruppe von Primzahlordnung ist zyklisch. Ist genauer p eine Primzahl und G eine Gruppe mit $|G| = p$ Elementen, so gibt es für jedes Element $g \in G\backslash 1_G$ genau einen Gruppenisomorphismus $\mathbb{Z}/p\mathbb{Z} \xrightarrow{\sim} G$ mit $\bar{1} \mapsto g$.*

Beweis. Nach dem Satz von Lagrange 3.1.5 teilt die Ordnung jeder Untergruppe die Ordnung der ganzen Gruppe. Eine Gruppe von Primzahlordnung hat also nur genau zwei Untergruppen, nämlich die einelementige Untergruppe, die nur aus dem neutralen Element besteht, und die ganze Gruppe als Untergruppe von sich selbst. Die von einem Element, das nicht das neutrale Element ist, erzeugte Untergruppe muß also notwendig bereits die ganze Gruppe sein. □

Korollar 3.3.8. *Bei einer endlichen Gruppe G teilt die Ordnung jedes Elements $g \in G$ die Ordnung der ganzen Gruppe und es gilt mithin*

$$g^{|G|} = 1$$

Beweis. Man wende den Satz von Lagrange 3.1.5 an auf die von unserem Element erzeugte Untergruppe. Es folgt, daß $r := \operatorname{ord} g = |\langle g\rangle|$ ein Teiler von $|G|$ ist, $|G| = ra$ mit $a \in \mathbb{N}$. Damit erhalten wir aber

$$g^{|G|} = g^{ra} = (g^r)^a = 1^a = 1$$ □

Korollar 3.3.9. *Ist p eine Primzahl, so gilt für alle ganzen Zahlen $a \in \mathbb{Z}$ die* **Fermat'sche Kongruenz**

$$a^p \equiv a \pmod{p}$$

Beweis. Die multiplikative Gruppe $(\mathbb{Z}/p\mathbb{Z})^\times$ des Körpers $\mathbb{Z}/p\mathbb{Z}$ hat genau $p-1$ Elemente, nach 3.3.8 gilt also $b^{p-1} = 1$ für alle $b \in (\mathbb{Z}/p\mathbb{Z})^\times$. Es folgt $b^p = b$ für alle $b \neq 0$, und für $b = 0$ gilt diese Gleichung eh. Mit $b = a + p\mathbb{Z}$ ergibt sich dann die Behauptung. □

3.3.10. Gibt es natürliche Zahlen $n \in \mathbb{N}$, die

bei Division durch 6 Rest 4 lassen,

bei Division durch 13 Rest 2, und

bei Division durch 11 Rest 9?

Da $\langle 6, 13\rangle = \langle 13, 11\rangle = \langle 6, 11\rangle = \langle 1\rangle$ lautet die Antwort ja, wie man aus dem anschließenden Korollar 3.3.13 folgert.

Satz 3.3.11. *Ist $m = ab$ ein Produkt von zwei zueinander teilerfremden positiven natürlichen Zahlen, so liefert die Abbildung $\kappa : n \mapsto (n + a\mathbb{Z}, n + b\mathbb{Z})$ einen Isomorphismus*

$$\mathbb{Z}/m\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$$

3.3.12. Übung 3.4.25 zeigt, daß die fraglichen Gruppen im Fall nicht teilerfremder Faktoren auch nicht isomorph sind.

Beweis. Der Kern unserer Abbildung

$$\begin{array}{rccc} \kappa: & \mathbb{Z} & \to & \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \\ & n & \mapsto & (n + a\mathbb{Z}, n + b\mathbb{Z}) \end{array}$$

besteht aus allen $n \in \mathbb{Z}$, die durch a und b teilbar sind, also aus allen Vielfachen von m. Unser Isomorphiesatz 3.2.12 liefert mithin einen Isomorphismus $\mathbb{Z}/m\mathbb{Z} \xrightarrow{\sim} \operatorname{im}\kappa$. Daraus folgt hinwiederum $\operatorname{im}\kappa = \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$, da unsere Untergruppe $\operatorname{im}\kappa$ bereits selbst $m = ab$ Elemente hat. □

Korollar 3.3.13 (Chinesischer Restsatz). *Ist $m = q_1 \ldots q_s$ ein Produkt von paarweise teilerfremden ganzen Zahlen, so liefert die offensichtliche Abbildung einen Isomorphismus*

$$\mathbb{Z}/m\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/q_1\mathbb{Z} \times \ldots \times \mathbb{Z}/q_s\mathbb{Z}$$

Beweis. Das folgt induktiv aus dem in 3.3.11 behandelten Fall $s = 2$. Die Details mag der Leser als Übung selbst ausführen. □

Ergänzung 3.3.14. Ein Element endlicher Ordnung in einer Gruppe heißt ein **Torsionselement**. Eine Gruppe, in der alle Elemente außer dem neutralen Element unendliche Ordnung haben, heißt **torsionsfrei**. Zum Beispiel sind die abelschen Gruppen $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$ torsionsfrei. Die Menge aller Torsionselemente ist in jeder abelschen Gruppe A eine Untergruppe, die **Torsionsuntergruppe** A_{tor}. In der Tat folgt, wenn wir unsere Gruppe einmal additiv notieren, für $x, y \in A$ aus $nx = 0$ und $my = 0$ bereits $nm(x + y) = 0$.

Satz 3.3.15 (**Primzahltorsion in abelschen Gruppen**). *Gegeben eine abelsche Gruppe A gilt:*

1. *Für jede Primzahl p ist die Teilmenge $A(p)$ aller Elemente von p-Potenz-Ordnung eine Untergruppe;*

2. *Sind $p_1, \ldots, p_r$ paarweise verschiedene Primzahlen, so liefert das Verknüpfen einen injektiven Gruppenhomomorphismus*

$$A(p_1) \times \ldots \times A(p_r) \hookrightarrow A$$

3. *Das Bild unseres Gruppenhomomorphismus aus Teil 2 besteht genau aus den Elementen von A, deren Ordnung endlich ist und von keinen von p_i verschiedenen Primzahlen geteilt wird.*

Vorschau 3.3.16. Dieser Satz wird sich in **??** ebenso wie der Satz **??** über die Direktheit der Summe der Haupträume als Spezialfall desselben allgemeinen Resultats zu „Moduln über Kringen“ erweisen.

Beweis. (1) Wir notieren unsere abelsche Gruppe A additiv. Gegeben $x, y \in A$ der Ordnungen p^r und p^s liefert die Vorschrift $(n, m) \mapsto nx + my$ einen Gruppenhomomorphismus $\mathbb{Z}/p^r\mathbb{Z} \times \mathbb{Z}/p^s\mathbb{Z} \to A$. Offensichtlich landet er sogar in $A(p)$ und sein Bild enthält x und y. Das zeigt die erste Behauptung.

(2) Es gilt zu zeigen, daß der Kern Null ist. Sei sonst $(x_1, \ldots, x_r)$ im Kern aber nicht Null. Ohne Beschränkung der Allgemeinheit dürfen wir $x_1 \neq 0$ annehmen. die Gleichung

$$-x_1 = x_2 + \ldots + x_r$$

zeigt dann $(p_2 \ldots p_r)^N x_1 = 0$ für hinreichend großes N, im Widerspruch zu unserer Annahme, daß die Ordnung von x_1 eine Potenz von p_1 sein soll.

(3) Es reicht, das für zyklische Torsionsgruppen zu zeigen. In diesem Fall folgt es aber unmittelbar aus dem chinesischen Restsatz. □

Korollar 3.3.17 (**Primzerlegung endlicher abelscher Gruppen**). *Sei E eine endliche abelsche Gruppe.*

1. *Gegeben eine Primzahl p ist die Teilmenge $E(p)$ aller Elemente, deren Ordnung eine p-Potenz ist, eine Untergruppe von p-Potenzordnung;*

2. *Sind $p_1, \ldots, p_r$ die paarweise verschiedenen Primzahlen, die in der Primfaktorzerlegung von $|E|$ mindestens einmal vorkommen, so liefert die Verknüpfung einen Gruppenisomorphismus*

$$E(p_1) \times \ldots \times E(p_r) \xrightarrow{\sim} E$$

Beweis. Unser Korollar folgt unmittelbar aus Satz 3.3.15 über Primzahltorsion in abelschen Gruppen mit Ausnahme der Aussage, daß $E(p)$ eine Gruppe von p-Potenzordnung ist. Das folgt aber für alle endlichen abelschen Gruppen, in denen jedes Element p-Potenzordnung hat, durch Induktion über die Gruppenordnung. Unser Korollar wird alternativ auch unmittelbar aus dem Klassifikationssatz für endlich erzeugte abelsche Gruppen 3.4.5 folgen. □

Ergänzung 3.3.18 (**Satz von Cauchy im abelschen Fall**). Teilt eine Primzahl p die Ordnung einer endlichen abelschen Gruppe E, so gibt es insbesondere in E ein Element der Ordnung p : In der Tat ist dann $E(p)$ nicht trivial; es gibt darin also ein vom neutralen Element verschiedenes Element a; dessen Ordnung ist etwa p^r mit $r \geq 1$; und dann ist in additiver Notation $p^{r-1}a$ das gesuchte Element der Ordnung p. Dieselbe Aussage gilt auch für beliebige endliche Gruppen und heißt der „Satz von Cauchy“, aber der Beweis ist dann schwieriger, vergleiche 4.1.35 oder 5.4.8.

Übungen

Ergänzende Übung 3.3.19 (**Polynomfunktionen über endlichen Körpern**). Sei k ein endlicher Körper mit $|k| = q$ Elementen. Man zeige $a^q = a$ für alle $a \in k$. Man zeige weiter, daß der Kern unserer Surjektion $k[X_1, \ldots, X_n] \to \mathrm{Ens}(k^n, k)$ aus 2.4.3 genau aus denjenigen Polynomen besteht, die sich als Summe $P_1(X_1^q - X_1) + \ldots + P_n(X_n^q - X_n)$ der Produkte von irgendwelchen Polynomen $P_i \in k[X_1, \ldots, X_n]$ mit den Polynomen $(X_i^q - X_i)$ schreiben lassen. Hinweis: Unsere Summen von Produkten bilden einen Untervektorraum, zu dem der Untervektorraum aller Polynome, in denen kein X_i in der Potenz q oder höher vorkommt, komplementär ist.

Übung 3.3.20 (**Untergruppen zyklischer Gruppen**). Man zeige: Jede Untergruppe einer zyklischen Gruppe ist zyklisch. Genauer haben wir für beliebiges $m \in \mathbb{N}$ eine Bijektion

$$\begin{array}{ccc} \{\text{Teiler } d \in \mathbb{N} \text{ von } m\} & \xrightarrow{\sim} & \{\text{Untergruppen von } \mathbb{Z}/m\mathbb{Z}\} \\ d & \mapsto & d\mathbb{Z}/m\mathbb{Z} \end{array}$$

Man folgere, daß jede echte, als da heißt von der ganzen Gruppe verschiedene Untergruppe einer zyklischen Gruppe von Primzahlpotenzordnung $\mathbb{Z}/p^r\mathbb{Z}$ in der Untergruppe $p\mathbb{Z}/p^r\mathbb{Z} \subset \mathbb{Z}/p^r\mathbb{Z}$ enthalten sein muß. Hinweis: 1.3.4.

Ergänzende Übung 3.3.21. Man zeige: Jede endlich erzeugte Untergruppe von $\mathbb{Q}$ ist zyklisch.

Ergänzende Übung 3.3.22. Man zeige, daß die additive Gruppe aller Gruppenhomomorphismen $\mathrm{Grp}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Q}/\mathbb{Z})$ unter punktweiser Addition isomorph ist zu $\mathbb{Z}/n\mathbb{Z}$, für alle $n \geq 1$.

Übung 3.3.23. Man gebe alle Zahlen an, die bei Division durch 6 Rest 4 lassen, bei Division durch 13 Rest 2, und bei Division durch 11 Rest 9. Hinweis: Der euklidische Algorithmus liefert schon mal Lösungen, wenn ein Rest 1 ist und die anderen Null.

Übung 3.3.24. Man zeige, daß es in einer zyklischen Gruppe der Ordnung n genau dann Elemente der Ordnung d gibt, wenn d ein Teiler von n ist.

Übung 3.3.25. Gibt es ein Vielfaches von 17, dessen letzte Ziffern 39 lauten?

Ergänzende Übung 3.3.26. Gegeben x, y zwei Elemente endlicher Ordnung in einer abelschen Gruppe G teilt die Ordnung ihres Produkts das kleinste gemeinsame Vielfache ihrer Ordnungen, und sind die Ordnungen von x und y teilerfremd, so gilt sogar $\mathrm{ord}(xy) = (\mathrm{ord}\, x)(\mathrm{ord}\, y)$.

Ergänzende Übung 3.3.27. In jeder endlichen abelschen Gruppe wird die maximal von einem Gruppenelement erreichte Ordnung geteilt von den Ordnungen aller Gruppenelemente. Hinweis: Bezeichnet $M \subset \mathbb{N}$ die Menge aller Ordnungen von Elementen unserer Gruppe, so enthält M mit jeder Zahl auch alle ihre Teiler. Weiter enthält M nach 3.3.26 mit je zwei teilerfremden Zahlen auch ihr Produkt.

Übung 3.3.28 (**Verallgemeinerte Fermat'sche Kongruenz**). Gegeben Primzahlen $p_1, \ldots, p_r$ und eine Zahl e mit $e \equiv 1 \pmod{(p_i - 1)}\ \forall i$ zeige man für alle $a \in \mathbb{Z}$ die Kongruenz $a^e \equiv a \pmod{(p_1 \ldots p_r)}$. Hinweis: Man folgere das zunächst im Fall $r = 1$ aus dem Kleinen Fermat. Für den allgemeinen Fall kombiniere man den Chinesischen Restsatz mit dem Kleinen Fermat.

Ergänzung 3.3.29 (**Verschlüsselung nach dem RSA-Verfahren**). Ich will versuchen, das sogenannte **RSA-Verfahren** nach Rivest, Shamir und Adleman zum öffentlichen Vereinbaren geheimer Schlüssel anhand des folgenden Schemas zu erklären.

Geheimbereich Alice	Öffentlicher Bereich	Geheimbereich Bob
Alice wählt zwei große Primzahlen p, q und berechnet das Produkt $N = pq$. Sie wählt Zahlen $s, t \in \mathbb{N}$ mit $st \equiv 1 \pmod{(p-1)(q-1)}$. Sie macht N und t öffentlich.		
	N, t	
		Bob wählt eine Restklasse $a \in \mathbb{Z}/N\mathbb{Z}$, berechnet a^t, und macht es öffentlich.
	$a^t \in \mathbb{Z}/N\mathbb{Z}$	
Alice berechnet $(a^t)^s = a$.		

Die Restklasse $a \in \mathbb{Z}/N\mathbb{Z}$ ist dann der gemeinsame geheime Schlüssel. Die behauptete Gleichheit von Restklassen $(a^t)^s = a$ prüft man mit Hilfe des Ringisomorphismus

$$\mathbb{Z}/N\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$$

In $\mathbb{Z}/p\mathbb{Z}$ haben wir ja $a^x = a$ wann immer gilt $x \equiv 1 \pmod{p-1}$. In $\mathbb{Z}/q\mathbb{Z}$ haben wir ebenso $a^x = a$ wann immer gilt $x \equiv 1 \pmod{q-1}$. Falls beides gilt und erst recht falls gilt $x \equiv 1 \pmod{(p-1)(q-1)}$ haben wir also $a^x = a$ in $\mathbb{Z}/N\mathbb{Z}$. Diese Identität ist ein Spezialfall unserer verallgemeinerten Fermat'schen Kongruenz 3.3.28. Der Trick beim RSA-Verfahren besteht darin, daß alle derzeit bekannten Verfahren zum Faktorisieren einer großen Zahl wie N sehr viel Rechenzeit brauchen. Es ist also möglich, N zu veröffentlichen und dennoch p, q geheim zu halten, die hinwiederum für die Berechnung von s benötigt werden. Des weiteren braucht es mit allen derzeit bekannten Verfahren auch sehr viel Rechenzeit, um aus a^t auf a zurückzuschließen, also eine „t-te Wurzel modulo N" zu finden.

3.4 Endlich erzeugte abelsche Gruppen

Proposition 3.4.1. *Jede Untergruppe einer endlich erzeugten abelschen Gruppe ist endlich erzeugt, und für die Untergruppe benötigt man höchstens soviele Erzeuger wie für die ganze Gruppe.*

Ergänzung 3.4.2. Eine Untergruppe einer nicht abelschen endlich erzeugten Gruppe muß im allgemeinen keineswegs endlich erzeugt sein. Ein Beispiel geben wir in **??**.

Beweis. Induktion über die Zahl der Erzeuger. Im Fall einer zyklischen Gruppe wissen wir nach 3.3.20 oder eigentlich 1.3.4 bereits, daß auch jede Untergruppe zyklisch ist. Sei nun unsere Gruppe X additiv notiert und sei $x_0, \ldots, x_n$ ein Erzeugendensystem. Sei $Y \subset X$ eine Untergruppe. Nach 3.3.20 ist $Y \cap \langle x_0 \rangle$ zyklisch, etwa erzeugt von y_0. Nach Induktionsannahme ist das Bild von Y in $X/\langle x_0 \rangle$ endlich erzeugt, etwa von den Nebenklassen $\bar{y}_1, \ldots, \bar{y}_n$ gewisser Elemente $y_1, \ldots, y_n \in Y$. Der Leser wird nun in Anlehnung an den Beweis von **??** unschwer zeigen können, daß $y_0, y_1, \ldots, y_n$ bereits ganz Y erzeugen. □

3.4.3. Unter einer **Primzahlpotenz** oder kurz **Primpotenz** verstehen wir eine natürliche Zahl der Gestalt $q = p^e$ für p prim und $e \geq 0$. Unter einer **echten Primzahlpotenz** verstehen wir eine von 1 verschiedene Primzahlpotenz. Gegeben eine Primzahl p verstehen wir unter einer **p-Potenz** eine natürliche Zahl der Gestalt $q = p^e$ für p prim und $e \geq 0$. Die beiden folgenden Sätze geben zwei **Klassifikationen der endlich erzeugten abelschen Gruppen**.

Satz 3.4.4 (Klassifikation durch Teilerfolgen). *Für jede endlich erzeugte abelsche Gruppe X gibt es genau ein $s \geq 0$ und ein s-Tupel von von 1 verschiedenen natürlichen Zahlen $(a_1, \ldots, a_s) \in \{0, 2, 3, \ldots\}^s$ mit $a_i | a_{i+1}$ für $1 \leq i < s$ derart, daß gilt*

$$X \cong \mathbb{Z}/a_1\mathbb{Z} \times \ldots \times \mathbb{Z}/a_s\mathbb{Z}$$

Satz 3.4.5 (Klassifikation durch Rang und Primzahlpotenzen). *Für jede endlich erzeugte abelsche Gruppe X gibt es echte Primzahlpotenzen $q_1, \ldots, q_t$ und eine natürliche Zahl $r \in \mathbb{N}$ mit*

$$X \cong \mathbb{Z}/q_1\mathbb{Z} \times \ldots \times \mathbb{Z}/q_t\mathbb{Z} \times \mathbb{Z}^r$$

Die Zahl r wird durch X eindeutig festgelegt und heißt der **Rang** *von X. Wir notieren sie $r = \operatorname{rang}(X)$. Die Primzahlpotenzen q_τ sind eindeutig bis auf Reihenfolge.*

Vorschau 3.4.6. Die zweite Klassifikation wird sich in **??** zusammen mit der Jordan'schen Normalform als Spezialfall derselben Klassifikation von „Moduln über Hauptidealringen“ erweisen. Auch die erste Klassifikation läßt sich in dieser Allgemeinheit formulieren und beweisen, vergleiche **??**.

3.4.7. Es wird im zweiten Satz nicht gefordert, daß die Primzahlpotenzen paarweise verschieden sein sollen. Ich erinnere daran, daß wir in **??** eine Multimenge von Elementen einer Menge P erklärt hatten als eine Abbildung $P \to \mathbb{N}$. In diesem Sinne werden also die endlich erzeugten abelschen Gruppen klassifiziert durch ihren Rang, eine natürliche Zahl, zusammen mit einer endlichen Multimenge von echten Primzahlpotenzen.

3.4.8 (**Übergang zwischen beiden Klassifikationen**). Um von der Darstellung im ersten Klassifikationssatz zu der im Zweiten überzugehen, kann man sich auf den Fall endlicher Gruppen beschränken, indem man die Nullen an der Ende der Folge der a_i abschneidet, die eben für den Faktor $\mathbb{Z}^r$ verantwortlich sind. Die anderen a_i zerlegt man in ein Produkt von echten Primzahlpotenzen, und die zugehörigen Faktoren $\mathbb{Z}/a_i\mathbb{Z}$ zerfallen dann nach dem chinesischen Restsatz entsprechend in ein Produkt zyklischer Gruppen von Primzahlpotenzordnung. Um von der Darstellung im zweiten Klassifikationssatz zu der im Ersten überzugehen, kann man sich wieder auf den Fall endlicher Gruppen beschränken. Gegeben ein Produkt zyklischer Gruppen von Primzahlpotenzordnung betrachtet man zunächst von jeder dabei auftauchenden Primzahl die höchste jeweils vorkommende Potenz und multipliziert diese zusammen: Das gibt a_s. Dann streicht man alle „verbrauchten“ Potenzen und macht genauso weiter.

Korollar 3.4.9. *Jede endliche abelsche Gruppe ist ein endliches Produkt von zyklischen Gruppen von Primzahlpotenzordnung, und die dabei auftretenden echten Primzahlpotenzen und ihre Vielfachheiten sind wohlbestimmt bis auf Reihenfolge. In Formeln erhalten wir so eine Bijektion*

$$\begin{array}{ccc} \left\{ \begin{array}{c} \textit{Endliche Multimengen} \\ \textit{von echten Primzahlpotenzen} \end{array} \right\} & \xrightarrow{\sim} & \left\{ \begin{array}{c} \textit{Endliche abelsche Gruppen} \\ \textit{bis auf Isomorphismus} \end{array} \right\} \\ {}_{\mu}\{q_1, q_2, \ldots, q_t\} & \mapsto & \mathbb{Z}/q_1\mathbb{Z} \times \mathbb{Z}/q_2\mathbb{Z} \times \ldots \times \mathbb{Z}/q_t\mathbb{Z} \end{array}$$

3.4.10. Man beachte bei den vorhergehenden Sätzen, daß die Faktoren keineswegs eindeutig sind „als Untergruppen unserer abelschen Gruppe“. Partielle Eindeutigkeitsaussagen liefern 3.3.15 und 3.3.17. Die Beweise werden uns bis zum Ende des Abschnitts beschäftigen. Eine erste wesentliche Zutat ist der gleich folgende Elementarteilersatz 3.4.13.

Beispiel 3.4.11. Die Gruppen $(\mathbb{Z}/9\mathbb{Z})^2 \times \mathbb{Z}/4\mathbb{Z}$ und $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ sind nicht isomorph, denn sie entsprechen den beiden unterschiedlichen Multimengen von Primzahlpotenzen ${}_{\mu}\{9, 9, 4\}$ und ${}_{\mu}\{3, 27, 4\}$ oder alternativ den beiden unterschiedlichen Teilerfolgen $9|36$ und $3|108$. Man kann das aber auch ohne alle Theorie unschwer einsehen: Die zweite Gruppe enthält Elemente der Ordnung 27, die erste nicht. Der Beweis, daß die explizit angegebenen Gruppen in unseren Klassifikationssätzen jeweils paarweise nicht isomorph sind, verfeinert diese Grundidee.

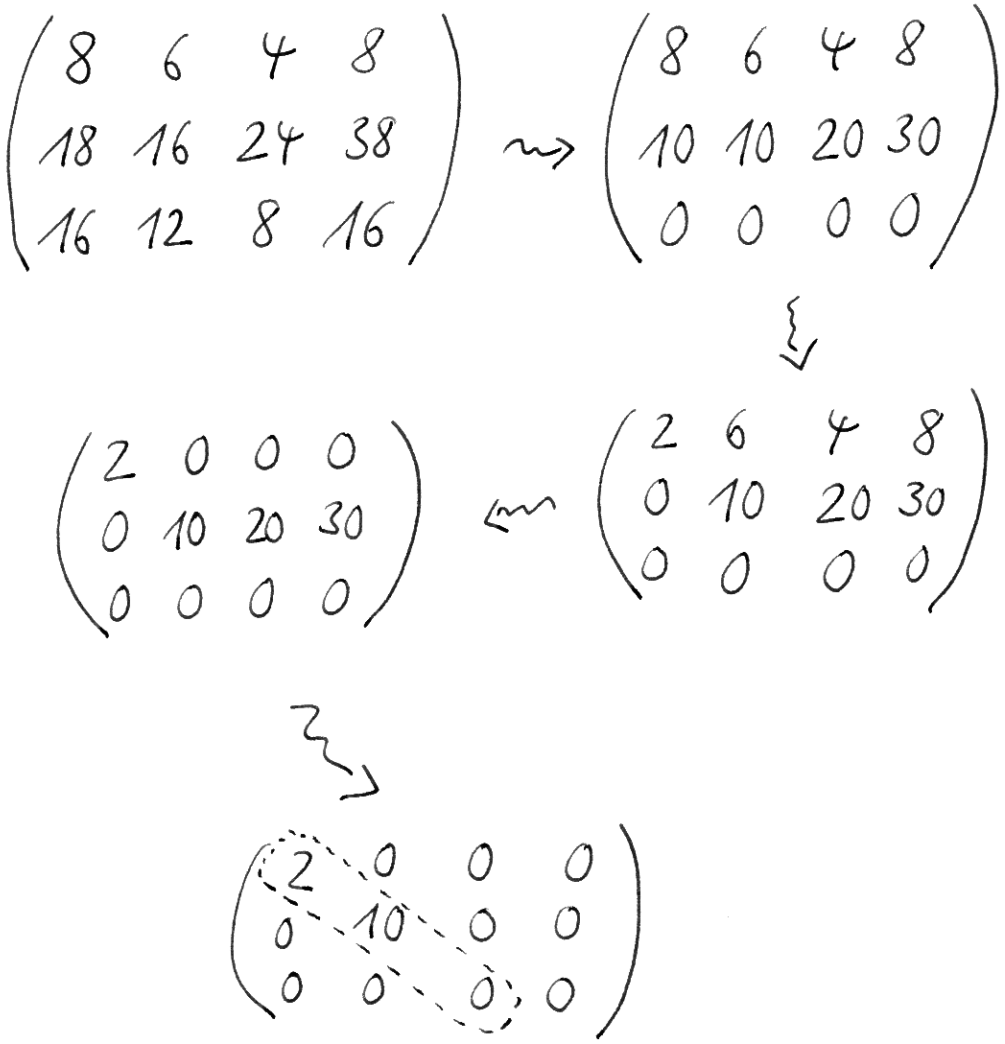
3.4.12 (**Endlich erzeugte torsionsfreie abelsche Gruppen**). Jede endlich erzeugte torsionsfreie abelsche Gruppe ist nach jeder unserer beiden Klassifikationen 3.4.4 und 3.4.5 isomorph zu $\mathbb{Z}^r$ für genau ein $r \in \mathbb{N}$.

Satz 3.4.13 (Elementarteilersatz). *1. Gegeben eine nicht notwendig quadratische Matrix A mit ganzzahligen Einträgen gibt es stets quadratische ganzzahlig invertierbare Matrizen mit ganzzahligen Einträgen P und Q derart, daß $B := PAQ$ eine Matrix mit Nullen außerhalb der Diagonalen ist, in der die Diagonaleinträge weiter vorn jeweils die Diagonaleinträge weiter hinten teilen, in Formeln $i \neq j \Rightarrow B_{i,j} = 0$ und $B_{i,i}|B_{i+1,i+1}\ \forall i$;*

2. Wir können durch geeignete Wahl von P und Q sogar zusätzlich erreichen, daß alle Diagonaleinträge nichtnegativ sind, und unter dieser Zusatzannahme werden besagte Diagonaleinträge durch die Matrix A bereits eindeutig festgelegt.

3.4.14. Ich nenne die Multimenge der Diagonaleinträge von B die Multimenge der **Elementarteiler der Matrix** A. Den Beweis der analogen Aussage für Polynomringe dürfen Sie selbst als Übung 3.4.30 ausarbeiten. Eine gemeinsame Verallgemeinerung für sogenannte „Hauptidealringe“ wird in **??** dargestellt.

Beweis. Wir beginnen mit dem Nachweis der Existenz. Ist A die Nullmatrix, so ist nichts zu zeigen. Sonst finden wir P, Q invertierbar derart, daß PAQ oben links einen positiven Eintrag hat. Es gibt dann natürlich auch $P_{\min}, Q_{\min}$ derart, daß $P_{\min}AQ_{\min}$ den kleinstmöglichen positiven Eintrag hat unter allen PAQ mit positivem Eintrag dort. Dann teilt dieser Eintrag notwendig alle anderen Einträge der ersten Spalte, da wir sonst durch Zeilenoperationen, genauer durch Subtraktion eines Vielfachen der ersten Zeile von einer anderen Zeile, Multiplikation einer Zeile mit -1 und Vertauschung zweier Zeilen, einen noch kleineren positiven Eintrag oben links erzeugen könnten. Ebenso teilt unser Eintrag auch alle anderen Einträge in der ersten Zeile. Durch entsprechende Zeilen- und Spaltenoperationen können wir also zusätzlich die erste Zeile und Spalte bis auf den ersten Eintrag als genullt annehmen. Teilt nun unser positiver Eintrag oben links nicht alle anderen Einträge unserer Matrix, sagen wir nicht den Eintrag $a_{i,j}$ mit $i \neq 1 \neq j$, so könnten wir durch Addieren der ersten Zeile zur i-ten Zeile gefolgt von einer Subtraktion eines Vielfachen der ersten Spalte von von der j-ten Spalte einen noch kleineren positiven Eintrag an der Stelle (i, j) erzeugen, und ihn durch Zeilen- und Spaltenvertauschung in die linke obere Ecke bringen im Widerspruch zu unserer Annahme. Also teilt unser positiver Eintrag oben links alle anderen Einträge unserer Matrix und eine offensichtliche Induktion beendet den Beweis der Existenz. Um die Eindeutigkeit zu zeigen, betrachten wir für jedes r die sogenannten r**-Minoren** unserer Matrix. Man versteht darunter die Determinanten aller derjenigen $(r \times r)$-Matrizen, die wir aus unserer Matrix durch das Streichen von Zeilen und Spalten erhalten können. Dann bemerken wir, daß sich für gegebenes $r \geq 1$ der größte gemeinsame Teiler G_r aller $(r \times r)$-Minoren unter Zeilen- und Spal-



Berechnung der Elementarteiler einer ganzzahligen Matrix durch ganzzahlige ganzzahlig invertierbare Zeilen- und Spaltenoperationen. Wir finden die Elementarteiler 2, 10, 0 jeweils mit der Vielfachheit Eins.

tenoperationen nicht ändert. Folglich sind die $G_r = d_1 \dots d_r$ wohlbestimmt durch A, und dasselbe gilt dann auch für die d_i. □

3.4.15 (**Herkunft der Terminologie**). Der Begriff der „Minoren einer Matrix“ wurde meines Wissens in einer Arbeit von Arthur Cayley in Crelles Journal im Jahre 1855, Band 50, Seite 282, mit dem Titel „Sept différents mémoires d'analyse. No 3: Remarques sur la notation des fonctions algébriques“ eingeführt. Cayley war mit Sylvester befreundet, auf den wie bereits in **??** erwähnt die Verwendung des Begriffs einer „Matrix“ in der Mathematik zurückgeht.

Beweis der Klassifikationen 3.4.4 und 3.4.5. Wir notieren die abelsche Gruppe X im folgenden additiv. Gegeben ein Erzeugendensystem $x_1, \dots, x_n$ von X erklären wir durch die Vorschrift $(a_1, \dots, a_n) \mapsto a_1x_1 + \dots + a_nx_n$ einen surjektiven Gruppenhomomorphismus

$$\mathbb{Z}^n \twoheadrightarrow X$$

Dessen Kern ist nach 3.4.1 wieder eine endlich erzeugte abelsche Gruppe K, für die wir wieder einen surjektiven Gruppenhomomorphismus $\mathbb{Z}^m \twoheadrightarrow K$ finden können. Mit der Notation ψ für die Komposition $\mathbb{Z}^m \twoheadrightarrow K \hookrightarrow \mathbb{Z}^n$ erhalten wir also einen Isomorphismus abelschen Gruppen

$$\mathbb{Z}^n / \operatorname{im} \psi \cong X$$

Genau wie bei Vektorräumen überlegt man sich, daß die Gruppenhomomorphismen $\mathbb{Z}^m \to \mathbb{Z}^n$ genau die Multiplikationen von links mit ganzzahligen $(n \times m)$-Matrizen sind, falls Elemente aus $\mathbb{Z}^m$ beziehungsweise $\mathbb{Z}^n$ als Spaltenvektoren aufgefaßt werden, vergleiche 3.2.26. Weiter überlegt man sich, daß auch in dieser Situation die Verknüpfung von Homomorphismen der Multiplikation von Matrizen entspricht. Bezeichnet nun A die Matrix unserer Abbildung $\mathbb{Z}^m \to \mathbb{Z}^n$, und wählen wir P und Q wie im Elementarteilersatz, so ergibt sich ein kommutatives Diagramm von abelschen Gruppen

$$\begin{array}{ccc} \mathbb{Z}^m & \xrightarrow{A} & \mathbb{Z}^n \\ {\scriptstyle Q}\uparrow\wr & & \wr\downarrow{\scriptstyle P} \\ \mathbb{Z}^m & \xrightarrow{D} & \mathbb{Z}^n \end{array}$$

für eine nicht notwendig quadratische Diagonalmatrix D mit nichtnegativen Einträgen $d_1|d_2|\dots|d_r$ für $r = \min(m, n)$. In anderen Worten bildet der Gruppenisomorphismus $P : \mathbb{Z}^n \xrightarrow{\sim} \mathbb{Z}^n$ in dieser Situation $\operatorname{im} \psi = \operatorname{im} A$ bijektiv auf $\operatorname{im} D$ ab und wir erhalten Isomorphismen

$$X \cong \mathbb{Z}^n / \operatorname{im} \psi = \mathbb{Z}^n / \operatorname{im} A \cong \mathbb{Z}^n / \operatorname{im} D$$

Für die Diagonalmatrix D mit Diagonaleinträgen d_i ist aber klar, daß $\mathbb{Z}^n/\operatorname{im} D$ isomorph ist zu einem Produkt der Gruppen $\mathbb{Z}/d_i\mathbb{Z}$ mit soviel Kopien von $\mathbb{Z}$, wie es in unserer Matrix D mehr Spalten als Zeilen gibt, also mit $(n-r)$ Kopien von $\mathbb{Z}$. Formaler kann das auch mit dem allgemeinen Resultat 3.6.13 begründet werden, nach dem „Produkte exakter Sequenzen wieder exakt sind“. Lassen wir von unserer Folge $d_1|d_2|\ldots|d_r$ nun alle Einsen vorne weg und ergänzen am Ende $(n-r)$ Nullen, so erhalten wir eine Folge $a_1|\ldots|a_s$ wie in der Klassifikation durch Teilerfolgen 3.4.4 gefordert, und die Existenz dort ist gezeigt. Mit dem Chinesischen Restsatz 3.3.13 folgt dann auch sofort die Existenzaussage der Klassifikation durch Primzahlpotenzen 3.4.5. Um die Eindeutigkeit in unseren Klassifikationen zu zeigen bemerken wir, daß für jede endlich erzeugte abelsche Gruppe X und jede Primzahl p und alle $n \geq 1$ der Quotient $p^{n-1}X/p^nX$ nach 2.2.44 ein endlichdimensionaler Vektorraum über $\mathbb{F}_p$ ist. Wir notieren seine Dimension

$$D_p^n(X) := \dim_{\mathbb{F}_p}(p^{n-1}X/p^nX)$$

Alternativ mag man $D_p^n(X)$ auch als die eindeutig bestimmte natürliche Zahl $D \in \mathbb{N}$ mit $|p^{n-1}X/p^nX| = p^D$ charakterisieren. Man sieht nun leicht oder folgert formal mit 3.6.13 die Formel $D_p^n(X \times Y) = D_p^n(X) + D_p^n(Y)$ für je zwei endlich erzeugte abelsche Gruppen X und Y. Für zyklische Gruppen $X \cong \mathbb{Z}/a\mathbb{Z}$ finden wir schließlich

$$D_p^n(\mathbb{Z}/a\mathbb{Z}) \quad = \quad \begin{cases} 1 & \text{falls } p^n \text{ teilt } a; \\ 0 & \text{sonst.} \end{cases}$$

In der Tat ist das klar für $a = p^m$, für a teilerfremd zu p ist es eh klar, und mit dem Chinesischen Restsatz 3.3.11 folgt es im allgemeinen. Für jede Zerlegung $X \cong \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_t\mathbb{Z}$ finden wir also

$$D_p^n(X) = |\{i \mid p^n \text{ teilt } d_i\}|$$

Für $X \cong \mathbb{Z}^r \times \mathbb{Z}/q_1\mathbb{Z} \times \ldots \times \mathbb{Z}/q_t\mathbb{Z}$ wie in 3.4.5 finden wir insbesondere mit den Notationen von dort

$$D_p^n(X) = r + |\{i \mid p^n \text{ teilt } q_i\}|$$

Wenden wir diese Erkenntnis an auf alle Primzahlen p, so folgt die im Satz behauptete Eindeutigkeit ohne weitere Schwierigkeiten: Wir erhalten genauer für jede Primzahl p und jedes $n \geq 1$ die nur von unserer Gruppe abhängenden Darstellungen $|\{i \mid q_i = p^n\}| = D_p^n(X) - D_p^{n+1}(X)$ und $r = \lim_{n\to\infty} D_p^n(X)$ für die Zahl der zyklischen Faktoren von vorgegebener Primzahlpotenzordnung und den Rang r des freien Anteils. Die Eindeutigkeit in 3.4.4 hinwiederum kann man leicht aus der Eindeutigkeit in 3.4.5 folgern: Verschiedene Teilerfolgen führen offensichtlich zu verschiedenen Multimengen von echten Primzahlpotenzen oder verschiedenen Rängen. □

Definition 3.4.16. Gegeben eine Gruppe G heißt die kleinste Zahl $e \geq 1$ mit $g^e = 1 \ \ \forall g \in G$ der **Exponent** unserer Gruppe. Gibt es kein solches e, so sagen wir, die Gruppe habe unendlichen Exponenten.

Satz 3.4.17 (Endliche Gruppen von Einheitswurzeln). *Jede endliche Untergruppe der multiplikativen Gruppe eines Körpers ist zyklisch.*

3.4.18. Die Elemente ζ endlicher Ordnung in der multiplikativen Gruppe eines Körpers sind per definitionem genau diejenigen Elemente, die eine Gleichung der Gestalt $\zeta^n = 1$ erfüllen. Man nennt sie deshalb auch die **Einheitswurzeln** des Körpers.

Beispiel 3.4.19. Um uns auf den gleich folgenden Beweis einzustimmen zeigen wir zunächst beispielhaft, daß jede 18-elementige Untergruppe der multiplikativen Gruppe eines Körpers zyklisch ist. Nach 3.4.4 muß unsere Gruppe ja isomorph sein zu genau einer der beiden Gruppen $\mathbb{Z}/18\mathbb{Z}$ und $\mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$. Es gilt also nur, die zweite Möglichkeit auszuschließen. Im zweiten Fall gäbe es jedoch in unserer Gruppe 8 Elemente der Ordnung drei und 9 Elemente, deren Ordnung drei teilt, und das steht im Widerspruch dazu, daß das Polynom $X^3 - 1$ in unserem Körper höchstens drei Nullstellen haben kann.

Beweis. In jeder endlichen kommutativen Gruppe wird die maximale von einem Gruppenelement erreichte Ordnung n geteilt von den Ordnungen aller Gruppenelemente, zum Beispiel nach dem Klassifikationssatz 3.4.4 oder direkter nach Übung 3.3.27. Wäre eine endliche Untergruppe E der multiplikativen Gruppe eines Körpers nicht zyklisch, so gäbe es also $n < |E|$ mit $\zeta^n = 1 \ \forall \zeta \in E$ im Widerspruch dazu, daß das Polynom $X^n - 1$ in unserem Körper höchstens n Nullstellen haben kann. □

Ergänzung 3.4.20 (**Nichtspalten der Einbettung der Torsionsuntergruppe**). Gegeben eine abelsche Gruppe A bilden die Elemente endlicher Ordnung nach 3.3.14 stets eine Untergruppe $A_{\text{tor}} \subset A$ und der Quotient A/A_{tor} ist offensichtlich torsionsfrei. Allerdings gibt es im Gegensatz zum Fall endlich erzeugter abelscher Gruppen im allgemeinen keinen Gruppenisomorphismus zwischen A und $A_{\text{tor}} \times (A/A_{\text{tor}})$. Betrachten wir etwa in der Gruppe A aller Folgen a_n mit $a_n \in \mathbb{Z}/p^n\mathbb{Z}$, die wir später einmal $A = \prod_{n=0}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$ notieren, das Element

$$v = (\overline{p^0}, 0, \overline{p^1}, 0, \overline{p^2}, 0, \ldots),$$

So ist v kein Torsionselement und seine Nebenklasse $\bar{v} \in A/A_{\text{tor}}$ ist folglich nicht Null und für alle $i \geq 0$ gibt es $w = w_i \in A/A_{\text{tor}}$ mit $p^i w = v$. Das einzige Element von A, das in dieser Weise „durch alle p-Potenzen teilbar ist“, ist jedoch die Null. Folglich existiert kein Gruppenisomorphismus zwischen A und $A_{\text{tor}} \times (A/A_{\text{tor}})$. Dies Beispiel ist im übrigen eine Variation von **??**.

Übungen

Übung 3.4.21. Sei k ein Körper. Die Matrizen vom Rang $< r$ in $\mathrm{Mat}(m \times n; k)$ sind genau die Matrizen, bei denen alle r-Minoren verschwinden.

Ergänzende Übung 3.4.22. Der Rang einer endlich erzeugten abelschen Gruppe X kann beschrieben werden als die Dimension des $\mathbb{Q}$-Vektorraums $\mathrm{Grp}(X, \mathbb{Q})$ aller Gruppenhomomorphismen von X nach $\mathbb{Q}$, mit seiner Vektorraumstruktur als Teilraum des $\mathbb{Q}$-Vektorraums $\mathrm{Ens}(X, \mathbb{Q})$.

Ergänzende Übung 3.4.23. Man gebe ein dreielementiges bezüglich Inklusion minimales Erzeugendensystem der Gruppe $\mathbb{Z}$ an.

Übung 3.4.24 (**Untergruppen freier endlich erzeugter abelscher Gruppen**). Gegeben eine Untergruppe $U \subset \mathbb{Z}^n$ gibt es stets einen Automorphismus φ von $\mathbb{Z}^n$ und $0 \leq r \leq n$ und positive natürliche Zahlen $d_1|d_2|\ldots|d_r$ mit $\varphi(U) = \langle d_1\mathrm{e}_1, d_2\mathrm{e}_2, \ldots, d_r\mathrm{e}_r\rangle$. Eine analoge Aussage für Polynomringe in einer Veränderlichen mögen Sie selber formulieren und beweisen. Eine gemeinsame Verallgemeinerung für „Hauptidealringe“ diskutueren wir in **??**.

Ergänzende Übung 3.4.25. Gegeben $a, b \in \mathbb{N}_{\geq 1}$ gibt es einen Gruppenisomorphismus $\mathbb{Z}/ab\mathbb{Z} \cong \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ genau dann, wenn a und b teilerfremd sind.

Ergänzende Übung 3.4.26. Man zeige, daß für jede nichttriviale zyklische Gruppe gerader Ordnung $2n$ in additiver Notation die Multiplikation mit n als Bild die einzige Untergruppe mit zwei Elementen hat und als Kern die einzige Untergruppe vom Index Zwei. Des weiteren zeige man, daß es nur einen surjektiven Gruppenhomomorphismus von unserer zyklischen Gruppe gerader Ordnung auf „die“ zweielementige Gruppe gibt.

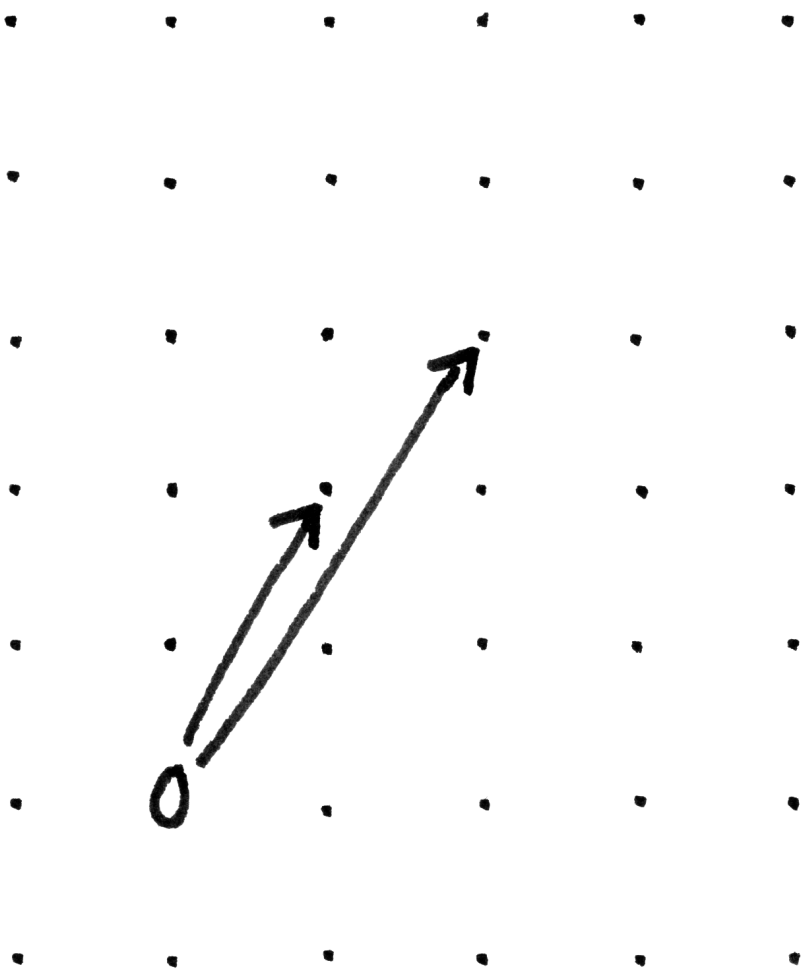
Ergänzende Übung 3.4.27. Man berechne die Elementarteiler der Matrix

$$\begin{pmatrix} 2 & 3 & 4 & 5 \\ 6 & 7 & 8 & 9 \\ 5 & 5 & 5 & 5 \end{pmatrix}$$

Ergänzende Übung 3.4.28. Man zeige, daß jede von Null verschiedene Zeilenmatrix als einzigen Elementarteiler den größten gemeinsamen Teiler der Matrixeinträge hat.

Ergänzende Übung 3.4.29. Sind $a, b \in \mathbb{Z}$ teilerfremd, in Formeln $\langle a, b\rangle = \langle 1\rangle$, so läßt sich das Element $(a, b) \in \mathbb{Z}^2$ ergänzen zu einem Erzeugendensystem von $\mathbb{Z}^2$. Man formuliere und zeige auch die analoge Aussage für $\mathbb{Z}^n$.

Ergänzende Übung 3.4.30 (**Smith-Zerlegung**). Gegeben eine nicht notwendig quadratische Matrix A mit Einträgen im Polynomring $k[X]$ mit Koeffizienten in



Ein Erzeugendensystem von $\mathbb{Z}^2$

einem Körper k zeige man: (1) Es gibt quadratische im Matrizenring über $k[X]$ invertierbare Matrizen mit polynomialen Einträgen P und Q derart, daß $B = PAQ$ eine Matrix mit Nullen außerhalb der Diagonalen ist, in der die Diagonaleinträge weiter vorn jeweils die Diagonaleinträge weiter hinten teilen, in Formeln $i \neq j \Rightarrow B_{i,j} = 0$ und $B_{i,i} | B_{i+1,i+1}$ $\forall i$; (2) Wir können durch geeignete Wahl von P und Q sogar zusätzlich erreichen, daß alle von Null verschiedenen Diagonaleinträge normiert sind, und unter dieser Zusatzannahme werden besagte Diagonaleinträge durch die Matrix A bereits eindeutig festgelegt.

Vorschau 3.4.31. Die Smith-Zerlegung aus der vorhergehenden Übung wird sich in **??** als ein Spezialfall des „Elementarteilersatzes für Hauptidealringe“ erweisen. Die Smith-Zerlegung ist der Schlüssel zum vertieften Verständnis der Jordan'schen Normalform und liefert auch Verallgemeinerungen über nicht notwendig algebraisch abgeschlossenen Körpern, vergleiche etwa **??** folgende.

Übung 3.4.32 (**Einheitengruppen von Restklassenringen**). Nach dem chinesischen Restsatz kennen wir die Einheitengruppen $(\mathbb{Z}/m\mathbb{Z})^\times$, sobald wir sie für jede Primzahlpotenz m kennen. In dieser Übung sollen sie zeigen:

$$(\mathbb{Z}/p^r\mathbb{Z})^\times \cong \begin{cases} \mathbb{Z}/p^{r-1}\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} & p \text{ ist eine ungerade Primzahl, } r \geq 1; \\ \mathbb{Z}/2^{r-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & p = 2,\ r \geq 2. \end{cases}$$

Man beachte, daß hier links die Multiplikation als Verknüpfung zu verstehen ist, rechts dahingegen die Addition. Hinweis: Nach 3.4.17 ist $(\mathbb{Z}/p\mathbb{Z})^\times$ stets zyklisch. Bei ungeradem p gehe man von der Abbildung $(\mathbb{Z}/p^r\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$ aus und zeige, daß sie surjektiv ist und daß die Restklasse von $1+p$ den Kern erzeugt. Dazu beachte man, daß für alle $b \in \mathbb{Z}$ und $n \geq 1$ gilt $(1 + p^n + bp^{n+1})^p \in 1 + p^{n+1} + p^{n+2}\mathbb{Z}$. Dann beachte man, daß diese Formel unter der stärkeren Annahme $n \geq 2$ auch für $p = 2$ gilt, und folgere, daß der Kern der Abbildung $(\mathbb{Z}/2^r\mathbb{Z})^\times \to (\mathbb{Z}/4\mathbb{Z})^\times$ für $r \geq 2$ von der Restklasse von 5 erzeugt wird. In diesem Fall kann eine Spaltung unserer Abbildung leicht explizit angegeben werden.

Übung 3.4.33. Gibt es eine Potenz von 17, deren Dezimaldarstellung mit den Ziffern 37 endet?

Übung 3.4.34 (**Primitivwurzeln in Restklassenringen**). Man zeige, daß für $m \geq 2$ die Einheitengruppe $(\mathbb{Z}/m\mathbb{Z})^\times$ des Restklassenrings $\mathbb{Z}/m\mathbb{Z}$ zyklisch ist genau dann, wenn m eine Potenz einer ungeraden Primzahl oder das Doppelte einer Potenz einer ungeraden Primzahl oder Zwei oder Vier ist. Hinweis: Man beachte 3.4.32, den chinesischen Restsatz 3.3.11, und die Tatsache, daß eine zyklische Gruppe nie $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ als Quotienten haben kann. Ein Erzeuger der Einheitengruppe $(\mathbb{Z}/m\mathbb{Z})^\times$ heißt im übrigen auch eine **Primitivwurzel modulo** m und die vorhergehende Aussage darüber, modulo welcher natürlichen Zahlen m Primitivwurzeln existieren, wird als der **Satz von Euler** zitiert. Bis heute (2011) ungelöst

ist die **Vermutung von Artin**, nach der die 2 modulo unendlich vieler Primzahlen eine Primitivwurzel sein sollte.

Ergänzende Übung 3.4.35. Eine Untergruppe eines endlichdimensionalen $\mathbb{Q}$-Vektorraums heißt ein **$\mathbb{Z}$-Gitter**, wenn sie von einer Basis unseres $\mathbb{Q}$-Vektorraums erzeugt wird. Man zeige: Eine endlich erzeugte Untergruppe eines endlichdimensionalen $\mathbb{Q}$-Vektorraums ist ein $\mathbb{Z}$-Gitter genau dann, wenn sie besagten Vektorraum als $\mathbb{Q}$-Vektorraum erzeugt. Ist $\Gamma \subset V$ ein $\mathbb{Z}$-Gitter eines endlichdimensionalen $\mathbb{Q}$-Vektorraums und $\varphi : V \twoheadrightarrow W$ eine surjektive lineare Abbildung, so ist $\varphi(\Gamma)$ ein $\mathbb{Z}$-Gitter in W. Ist $U \subset V$ ein Untervektorraum, so ist $U \cap \Gamma$ ein $\mathbb{Z}$-Gitter in U.

Übung 3.4.36 (**Klassifikation ganzzahliger symmetrischer Bilinearformen**). Die Klassifikation von Paaren (Γ, s) bestehend aus einer endlich erzeugten freien abelschen Gruppe Γ und einer symmetrischen biadditiven Abbildung $s : \Gamma \times \Gamma \to \mathbb{Z}$ ist eine interessante Aufgabe. Man zeige, daß sich für Γ vom Rang zwei und s positiv definit stets ein Repräsentant $(\mathbb{Z}^2, s)$ finden läßt, dessen quadrierte Längenfunktion die Gestalt $ax^2 + 2bxy + cy^2$ hat mit $0 \leq 2b \leq a \leq c$. Hinweis: Man suche in Γ ein von Null verschiedenes Element v kleinstmöglicher Länge; Man zeige, daß es sich zu einer Basis von Γ ergänzen läßt, sagen wir durch einen weiteren Vektor u; Man mache nun für den verbesserten zweiten Basisvektor w den Ansatz $w = \pm(u + nv)$. Hat zusätzlich die Fundamentalmatrix von s die Determinante Eins, so finden wir unmittelbar $a = 1$, $b = 0$ und $c = 1$ und damit gibt es bis auf Isomorphismus nur ein mögliches Paar mit diesen Eigenschaften, nämlich $\mathbb{Z}^2$ mit dem Standardskalarprodukt.

Ergänzung 3.4.37. In der Literatur wird statt der in 3.4.36 erklärten Aufgabe oft implizit die Klassifikation von Tripeln (Γ, s, ω) besprochen mit dem zusätzlichen Datum einer Orientierung ω. Dann läßt sich in derselben Weise zumindest noch $-a < 2b \leq a < c$ oder $0 \leq 2b \leq a = c$ erreichen. Hat zusätzlich die Fundamentalmatrix von s die Determinante Eins, so finden wir immer noch $a = 1$, $b = 0$ und $c = 1$ und damit gibt es bis auf Isomorphismus nur ein mögliches Tripel mit diesen Eigenschaften.

Übung 3.4.38 (**Ternäre ganzzahlige symmetrische Bilinearformen**). Zur Klassifikation von Paaren (Γ, s) bestehend aus einer endlich erzeugten freien abelschen Gruppe Γ vom Rang drei und einer positiv definiten symmetrischen biadditiven Abbildung $s : \Gamma \times \Gamma \to \mathbb{Z}$ zeige man ähnlich, daß sich stets ein Repräsentant $(\mathbb{Z}^3, s)$ finden läßt, für dessen Fundamentalmatrix gilt

$$0 \leq 2m_{13} \leq 2m_{12} \leq m_{11} < 2\sqrt[3]{\det M}$$

Hinweis: Man suche in Γ ein von Null verschiedenes Element v kleinstmöglicher Länge; Man zeige, daß es sich zu einer Basis von Γ ergänzen läßt, sagen

wir durch weitere Vektoren u_1, u_2; Man mache nun für die verbesserten weiteren Basisvektoren w_1, w_2 den Ansatz $w_i = \pm(u_i + n_i v)$. So erreicht man die ersten Ungleichungen. Für die letzte Ungleichung beachte man, daß $\sqrt{\det M}$ nach **??** das Volumen des von einer und jeder Basis von Γ im Skalarproduktraum $V := \Gamma \otimes_{\mathbb{Z}} \mathbb{R}$ aufgespannten Parallelpipeds ist. Hat die Kugel mit Radius r mindestens das Volumen der Grundmasche, in Formeln $4\pi r^3/3 \geq \sqrt{\det M}$, so können die Kugeln um die Punkte aus Γ nicht paarweise disjunkt sein und es gibt einen von Null verschiedenen Gittervektor der Länge $\leq 2r$. So einen Vektor gibt es also für $(2r)^6(\pi/6)^2 \geq \det M$ alias $(2r)^2 \geq (6/\pi)^{2/3}\sqrt[3]{\det M}$ und wir finden $m_{11} < 2\sqrt[3]{\det M}$. Hat zusätzlich die Fundamentalmatrix von s die Determinante Eins, so finden wir unmittelbar einen Repräsentanten mit $m_{11} = 1$ und $m_{12} = m_{13} = 0$ und sehen mit 3.4.36, daß es bis auf Isomorphismus nur ein mögliches Paar mit diesen Eigenschaften gibt, nämlich $\mathbb{Z}^3$ mit dem Standardskalarprodukt.

Ergänzung 3.4.39. In der Literatur wird statt der in 3.4.38 erklärten Aufgabe oft implizit die Klassifikation von Tripeln (Γ, s, ω) besprochen mit dem zusätzlichen Datum einer Orientierung ω. Das verkompliziert dann die Argumentation und die Ergebnisse. Mit expliziten aber weniger anschaulichen Abschätzungen läßt sich darüber hinaus unschwer $m_{11} < (4/3)\sqrt[3]{\det M}$ zeigen.

Ergänzung 3.4.40 (**Symmetrische Bilinearformen und quadratische Formen**). Gegeben ein Kring K und ein K-Modul V verstehe ich unter einer **quadratischen Form auf** V wie im Fall eines Körpers K aus **??** eine Abbildung $q : V \to K$ derart, daß es eine Bilinearform b auf V gibt mit $q(v) = b(v, v)$. In der Literatur versteht man darunter auch oft eine symmetrische Bilinearform, aber die natürliche Abbildung $s \mapsto q_s$ von symmetrischen Bilinearformen zu quadratischen Formen gegeben durch $q_s(v) := s(v, v)$ ist nur dann eine Bijektion, wenn die Zwei in K invertierbar ist, in Formeln $2 \in K^\times$. In unserer Terminologie ist etwa XY eine quadratische Form über $\mathbb{Z}$, die nicht von einer symmetrischen Bilinearform herkommt.

3.5 Quotientenvektorräume

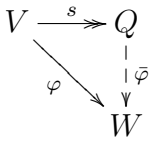
Satz 3.5.1 (Universelle Eigenschaft surjektiver Homomorphismen). *Seien $s : V \twoheadrightarrow Q$ eine surjektive lineare Abbildung und $\varphi : V \to W$ eine beliebige lineare Abbildung. Genau dann existiert ein Homomorphismus $\bar{\varphi} : Q \to W$ mit $\varphi = \bar{\varphi} \circ s$, wenn gilt* $\ker(\varphi) \supset \ker(s)$.

3.5.2. Dieser Homomorphismus $\bar{\varphi}$ ist dann natürlich eindeutig bestimmt. In diesem Sinne kann man diesen Satz auch dahingehend zusammenfassen, daß das Vorschalten eines surjektiven Homomorphismus $s : V \twoheadrightarrow Q$ für jeden weiteren

Vektorraum W eine Bijektion

$$(\circ s) : \mathrm{Hom}_k(Q, W) \tilde{\to} \{\varphi \in \mathrm{Hom}_k(V, W) \mid \ker(\varphi) \supset \ker(s)\}$$

liefert. Der Übersichtlichkeit halber stelle ich die in diesem Satz auftauchenden Gruppen und Morphismen auch noch wieder anders in einem Diagramm dar:



Man formuliert diesen Satz auch mit den Worten, φ **faktorisiere in eindeutiger Weise über** s.

Beweis. Offensichtlich ist φ konstant auf den Fasern von s. Damit finden wir schon mal eine Abbildung $\bar{\varphi}$ wie behauptet. Man prüft leicht, daß sie ein Homomorphismus ist. □

3.5.3 (**Surjektive Homomorphismen mit gleichem Kern**). Gegeben ein Vektorraum V und zwei surjektive Homomorphismus $s : V \twoheadrightarrow Q$ und $t : V \twoheadrightarrow P$ mit demselben Kern $\ker(s) = \ker(t)$ sind die Homomorphismen $\bar{t} : Q \to P$ mit $\bar{t} \circ s = t$ und $\bar{s} : P \to Q$ mit $\bar{s} \circ t = s$ nach 3.5.1 offensichtlich zueinander inverse Isomorphismen $Q \tilde{\to} P \tilde{\to} Q$. Salopp gesprochen wird also bei einem surjektiven Homomorphismus „das Ziel bereits durch den Ausgangsraum und den Kern festgelegt bis auf eindeutigen Isomorphismus“.

Satz 3.5.4 (**Quotientenvektorraum**)**.** *Sei k ein Körper. Gegeben $V \supset U$ ein k-Vektorraum mit einem Teilraum existiert auf der Restklassengruppe V/U aus 3.2.10 genau eine Struktur als k-Vektorraum $k \times V/U \to V/U$ derart, daß die kanonische Projektion*

$$\mathrm{can} : V \twoheadrightarrow V/U$$

aus 3.2.10 eine k-lineare Abbildung wird. Mit dieser Vektorraumstruktur heißt V/U der **Quotient von V nach U**.

Beweis. Wir betrachten die Abbildung

$$\begin{array}{ccc} k \times \mathcal{P}(V) & \to & \mathcal{P}(V) \\ (\lambda\ ,\ A) & \mapsto & \lambda.A := \lambda A + U \end{array}$$

Für $A = v + U$ finden wir $\lambda.A = \lambda A + U = \lambda v + U$, so daß unsere Abbildung eine Abbildung $k \times V/U \to V/U$ induziert, die die Eigenschaft $\overline{\lambda v} = \lambda.\bar{v}$ hat für alle $\lambda \in k$, $v \in V$. Damit folgt sofort, daß unsere Abbildung $k \times V/U \to V/U$ auf der abelschen Gruppe V/U eine Struktur als k-Vektorraum definiert, und daß

die Projektion $V \twoheadrightarrow V/U$ für diese Struktur k-linear ist. Umgekehrt ist auch klar, daß das die einzige Struktur als k-Vektorraum auf der abelschen Gruppe V/U ist, für die die Projektion $V \twoheadrightarrow V/U$ eine k-lineare Abbildung sein kann. □

Zweiter Beweis. Wir betrachten das Diagramm

$$\begin{array}{ccc} k \times V & \xrightarrow{m} & V \\ \downarrow & & \downarrow \\ k \times V/U & \xrightarrow{\bar{m}} & V/U \end{array}$$

mit der Skalarmultiplikation in der oberen Horizontalen. Nach Übung 3.2.27 und wegen $m(k \times U) \subset U$ gibt es genau eine biadditive Abbildung in der unteren Horizontalen, die dies Diagramm zum Kommutieren bringt. Daß die Nebenklassengruppe V/U mit dieser Abbildung als Skalarmultiplikation ein k-Vektorraum mit den geforderten Eigenschaften ist, prüft man dann ohne weitere Schwierigkeiten. □

3.5.5 (**Isomorphiesatz für Vektorräume**). Jeder Vektorraumhomomorphismus $f : V \to W$ induziert einen Vektorraumisomorphismus $V/\ker f \xrightarrow{\sim} \operatorname{im} f$. Das folgt unmittelbar aus dem Isomorphiesatz für Gruppen 3.2.12.

3.5.6. Gegeben Vektorräume $V \supset W \supset U$ induziert die Komposition von kanonischen Abbildungen $V \twoheadrightarrow V/U \twoheadrightarrow (V/U)/(W/U)$ einen Vektorraumisomorphismus $V/W \xrightarrow{\sim} (V/U)/(W/U)$. Das folgt unmittelbar aus dem Noether'schen Isomorphiesatz 3.2.15.

Definition 3.5.7. Gegeben $V \supset U$ ein Vektorraum mit einem Untervektorraum heißt die Dimension des Quotienten V/U auch die **Kodimension von** U **in** V und wird notiert als $\operatorname{codim}(U \subset V) := \dim(V/U)$.

3.5.8. Ist V endlichdimensional, so haben wir nach dem Isomorphiesatz 3.5.5 und der Dimensionsformel **??** die Identität

$$\operatorname{codim}(U \subset V) = \dim(V) - \dim(U)$$

Es gibt aber auch in unendlichdimensionalen Räumen durchaus Teilräume endlicher Kodimension. Eine Teilmenge eines Vektorraums ist eine lineare Hyperebene im Sinne von **??** genau dann, wenn sie ein Untervektorraum der Kodimension Eins ist.

Übungen

Übung 3.5.9 (**Auf Quotienten induzierte multilineare Abbildungen**). Gegeben eine bilineare Abbildung $b : V \times W \to L$ und surjektive lineare Abbildungen $s : V \twoheadrightarrow P$ und $t : W \twoheadrightarrow Q$ mit der Eigenschaft $b(\ker(s) \times W) = 0 = b(V \times \ker(t))$ gibt es genau eine bilineare Abbildung $\bar{b} : P \times Q \to L$ derart, daß das Diagramm

$$\begin{array}{ccc} V \times W & \xrightarrow{b} & L \\ {\scriptstyle s\times t}\downarrow & & \| \\ P \times Q & \xrightarrow{\bar{b}} & L \end{array}$$

kommutiert. Analoges gilt für multilineare Abbildungen.

Übung 3.5.10. Gegeben ein Vektorraum V mit Untervektorräumen U, W zeige man, daß sich jede Linearform auf V, die auf $U \cap W$ verschwindet, schreiben läßt als Summe einer Linearform, die auf U verschwindet, und einer Linearform, die auf W verschwindet.

Übung 3.5.11 (**Simultane Trigonalisierbarkeit**). Eine Menge von paarweise kommutierenden trigonalisierbaren Endomorphismen eines endlichdimensionalen Vektorraums ist stets simultan trigonalisierbar, als da heißt, es gibt eine Basis, bezüglich derer alle unsere Endomorphismen eine Matrix von oberer Dreiecksgestalt haben. Hinweis: Existenz eines simultanen Eigenvektors **??** und vollständige Induktion durch betrachen des Quotienten nach dem davon erzeugten Teilraum.

Ergänzende Übung 3.5.12 (**Quotienten affiner Räume**). Gegeben eine surjektive affine Abbildung von affinen Räumen $\varphi : E \twoheadrightarrow F$ zeige man, daß jede affine Abbildung $\eta : E \to G$ mit $\ker \vec{\eta} \supset \ker \vec{\varphi}$ in eindeutiger Weise über φ faktorisiert. Gegeben ein affiner Raum E und ein Teilraum $U \subset \vec{E}$ zeige man andererseits, daß es eine surjektive affine Abbildung $\varphi : E \twoheadrightarrow F$ gibt mit $\ker \vec{\varphi} = U$. Man mag F konstruieren als den Bahnenraum von U in E und mag diesen affinen Raum E/U notieren. Die zu diesem Datum gehörige surjektive affine Abbildung mag $\mathrm{can} : E \twoheadrightarrow E/U$ notiert werden.

3.6 Exakte Sequenzen

3.6.1. Beim Arbeiten mit Quotienten ermöglicht der Formalismus der „exakten Sequenzen“ oft besonders transparente Formulierungen. Wir führen deshalb im folgenden auch diese Sprache ein.

Definition 3.6.2. Eine Menge mit einem ausgezeichneten Element heißt eine **bepunktete Menge**. Das ausgezeichnete Element einer bepunkteten Menge heißt der **Basispunkt**.

Definition 3.6.3. Eine Sequenz $X \xrightarrow{f} Y \xrightarrow{g} Z$ von bepunkteten Mengen mit basispunkterhaltenden Abbildungen heißt **exakt**, wenn das Urbild in Y des ausgezeichneten Punktes $z \in Z$ mit dem Bild von $X \to Y$ zusammenfällt, in Formeln $f(X) = g^{-1}(z)$. Eine längere Sequenz von bepunkteten Mengen heißt exakt, wenn sie an jeder Stelle exakt ist.

Beispiel 3.6.4. Sei ens die einelementige Menge. Eine Sequenz $X \to Y \to \mathrm{ens}$ ist exakt genau dann, wenn ihre erste Abbildung surjektiv ist. Eine Sequenz $\mathrm{ens} \to Y \to Z$ ist exakt genau dann, wenn ihre zweite Abbildung injektiv ist.

Definition 3.6.5. Eine **kurze exakte Sequenz** von bepunkteten Mengen ist eine Sequenz $X \to Y \to Z$ derart, daß die Sequenz $\mathrm{ens} \to X \to Y \to Z \to \mathrm{ens}$ exakt ist oder gleichbedeutend, daß $X \to Y \to Z$ exakt ist sowie $X \to Y$ injektiv und $Y \to Z$ surjektiv. Wir notieren kurze exakte Sequenzen meist

$$X \hookrightarrow Y \twoheadrightarrow Z$$

3.6.6 (**Exakte Sequenzen von Gruppen**). Eine Gruppe fassen wir in diesem Kontext stets auf als eine bepunktete Menge mit dem neutralen Element als ausgezeichnetem Punkt. Eine Sequenz von Gruppen und Gruppenhomomorphismen

$$X \xrightarrow{f} Y \xrightarrow{g} Z$$

heißt also exakt, wenn das Bild der ersten Abbildung zusammenfällt mit dem Kern der zweiten Abbildung, in Formeln $\operatorname{im} f = \ker g$.

Beispiel 3.6.7. Für jeden Homomorphismus $x : M \to N$ von additiv notierten abelschen Gruppen ist die Sequenz

$$0 \to (\ker x) \to M \to N \to (N/\operatorname{im} x) \to 0$$

exakt. Man nennt wegen dieser Symmetrie den Quotienten nach dem Bild auch den **Kokern** unseres Morphismus von abelschen Gruppen. Wir verwenden für den Kokern die Notation $\operatorname{cok} x := (N/\operatorname{im} x)$.

3.6.8. Die Dimensionsformel **??** kann in dieser Terminologie auch dahingehend formuliert werden, daß für jede kurze exakte Sequenz $V' \hookrightarrow V \twoheadrightarrow V''$ von Vektorräumen gilt

$$\dim V = \dim V' + \dim V''$$

Definition 3.6.9. Gegeben Sequenzen $A \xrightarrow{r} B \xrightarrow{s} C$ und $A' \xrightarrow{r'} B' \xrightarrow{s'} C'$ verstehen wir unter einem **Homomorphismus von Sequenzen** ein Tripel (f, g, h) von Homomophismen derart, daß das folgende Diagramm kommutiert:

$$\begin{array}{ccccc} A & \xrightarrow{r} & B & \xrightarrow{s} & C \\ \downarrow f & & \downarrow g & & \downarrow h \\ A' & \xrightarrow{r'} & B' & \xrightarrow{s'} & C' \end{array}$$

Solch ein Morphismus heißt ein **Isomorphismus von Sequenzen**, wenn alle drei vertikalen Abbildungen f, g und h Isomorphismen sind. Je nach Kontext meinen wir mit Homomorphismen hier Vektorraumhomomorphismen, Gruppenhomomorphismen oder schlicht Abbildungen.

3.6.10. Gegeben eine kurze exakte Sequenz von abelschen Gruppen $A \overset{r}{\hookrightarrow} B \overset{s}{\twoheadrightarrow} C$ sind gleichbedeutend: (1) r besitzt ein Linksinverses, (2) s besitzt ein Rechtsinverses und (3) es gibt einen Isomorphismus der Gestalt $(\mathrm{id}_A, f, \mathrm{id}_C)$ von unserer Sequenz mit der Sequenz

$$A \overset{\mathrm{in}_1}{\hookrightarrow} A \oplus C \overset{\mathrm{pr}_2}{\twoheadrightarrow} C$$

Das ist eine Umformulierung der Übungen 3.2.23 und 3.2.24. Eine kurze exakte Sequenzen mit diesen Eigenschaften heißt eine **spaltende** kurze exakte Sequenz von abelschen Gruppen. Die kurze exakte Sequenz von abelschen Gruppen $\mathbb{Z} \hookrightarrow \mathbb{Z} \twoheadrightarrow \mathbb{Z}/2\mathbb{Z}$ mit der Multiplikation mit Zwei als erster Abbildung spaltet nicht.

3.6.11 (**Kurze exakte Sequenzen von Vektorräumen spalten**). Arbeiten wir speziell mit Vektorräumen, so finden wir mit **??** für jeden Untervektorraum $N \subset A$ einen zu N komplementären Teilraum U und nach **??** induziert die kanonische Abbildung einen Isomorphismus $U \xrightarrow{\sim} A/N$. In diesem Fall erhalten wir also zusätzlich einen Isomorphismus von kurzen exakten Sequenzen

$$\begin{array}{ccccc} N & \hookrightarrow & N \oplus U & \twoheadrightarrow & U \\ \| & & \wr\downarrow g & & \wr\downarrow h \\ N & \hookrightarrow & A & \twoheadrightarrow & A/N \end{array}$$

Implizit ist dabei zu verstehen, daß die Morphismen der oberen Horizontale die kanonische Injektion und Projektion sein sollen.

3.6.12 (**Die Duale einer kurzen exakten Sequenz ist exakt**). Gegeben eine kurze exakte Sequenz von Vektorräumen ist auch die duale Sequenz eine kurze exakte Sequenz. Das ist in der Tat offensichtlich im Fall einer kurzen exakten Sequenz der Gestalt $N \hookrightarrow N \oplus U \twoheadrightarrow U$ und folgt dann mit 3.6.11 im allgemeinen. Speziell ist die Transponierte einer Injektion eine Surjektion und die Transponierte einer Surjektion eine Injektion.

Übungen

Übung 3.6.13 (**Quotienten und Produkte**). Gegeben zwei Sequenzen von bepunkteten Mengen $A \to B \to C$ und $A' \to B' \to C'$ ist ihr **Produkt**

$$(A \times A') \to (B \times B') \to (C \times C')$$

exakt genau dann, wenn die beiden Ausgangssequenzen exakt sind. Analoges gilt sowohl für das Produkt als auch für die direkte Summe einer beliebigen Familie

von Sequenzen von bepunkteten Mengen. Diese Aussage präzisiert unter anderem die etwas vage Aussage, daß das „Bilden von Produkten mit dem Bilden von Quotienten kommutiert“.

Ergänzende Übung 3.6.14 (**Additivität der Spur**). Gegeben ein kommutatives Diagramm von endlichdimensionalen Vektorräumen mit zweimal derselben kurzen exakten Zeile

$$\begin{array}{ccccc} V' & \hookrightarrow & V & \twoheadrightarrow & V'' \\ f'\downarrow & & f\downarrow & & f''\downarrow \\ V' & \hookrightarrow & V & \twoheadrightarrow & V'' \end{array}$$

gilt für die Spuren der Vertikalen die Identität $\operatorname{tr}(f) = \operatorname{tr}(f') + \operatorname{tr}(f'')$. Hat allgemeiner im Fall beliebiger Vektorräume der Homomorphismus f endlichen Rang, so haben auch f' und f'' endlichen Rang, und unter dieser Voraussetzung gilt für die Spuren der Vertikalen auch wieder die Identität $\operatorname{tr}(f) = \operatorname{tr}(f') + \operatorname{tr}(f'')$.

3.7 Mehr zu exakten Sequenzen*

Proposition 3.7.1 (**Exakte Vektorraumsequenzen bis auf Isomorphismus**). *Jede exakte drei-Term-Sequenz von Vektorräumen ist isomorph zu einer Sequenz der Gestalt*

$$\begin{matrix} V_2 \\ \oplus \\ V_3 \end{matrix} \xleftarrow{\left(\begin{smallmatrix} 0 & \mathrm{id} \\ 0 & 0 \end{smallmatrix}\right)} \begin{matrix} V_1 \\ \oplus \\ V_2 \end{matrix} \xleftarrow{\left(\begin{smallmatrix} 0 & \mathrm{id} \\ 0 & 0 \end{smallmatrix}\right)} \begin{matrix} V_0 \\ \oplus \\ V_1 \end{matrix}$$

3.7.2. Wir verwenden hier die Matrixnotation **??**.

Beweis. Sei $C \xleftarrow{r} B \xleftarrow{s} A$ unsere Sequenz. Wir setzen $V_0 := \ker s$ und wählen ein Komplement $V_1 \subset A$ zu V_0. Dann induziert s einen Isomorphismus $s : V_1 \xrightarrow{\sim} \operatorname{im} s = \ker r$ und wir wählen ein Komplement $V_2 \subset B$ zu $\ker r$. Nun induziert r einen Isomorphismus $r : V_2 \xrightarrow{\sim} \operatorname{im} r$ und wir wählen ein Komplement $V_3 \subset C$ zu $\operatorname{im} r$. Insgesamt erhalten wir dann mit der Notation i_ν für die Einbettung von V_ν ein kommutatives Diagramm

$$\begin{array}{ccccc} \begin{matrix} V_2 \\ \oplus \\ V_3 \end{matrix} & \xleftarrow{\left(\begin{smallmatrix} 0 & \mathrm{id} \\ 0 & 0 \end{smallmatrix}\right)} & \begin{matrix} V_1 \\ \oplus \\ V_2 \end{matrix} & \xleftarrow{\left(\begin{smallmatrix} 0 & \mathrm{id} \\ 0 & 0 \end{smallmatrix}\right)} & \begin{matrix} V_0 \\ \oplus \\ V_1 \end{matrix} \\ {\scriptstyle (r,i_3)}\downarrow\wr & & {\scriptstyle (s,i_2)}\downarrow\wr & & {\scriptstyle (i_0,i_1)}\downarrow\wr \\ C & \longleftarrow & B & \longleftarrow & A \end{array}$$

□

Korollar 3.7.3 (**Erhaltung der Exaktheit unter** Hom). *Gegeben eine exakte Sequenz $U \xrightarrow{r} V \xrightarrow{s} W$ von Vektorräumen erhalten wir für jeden weiteren Vektorraum L exakte Sequenzen*

$$\begin{array}{ccccc} \operatorname{Hom}(W,L) & \xrightarrow{\circ s} & \operatorname{Hom}(V,L) & \xrightarrow{\circ r} & \operatorname{Hom}(U,L) \\ \operatorname{Hom}(L,U) & \xrightarrow{r\circ} & \operatorname{Hom}(L,V) & \xrightarrow{s\circ} & \operatorname{Hom}(L,W) \end{array}$$

Beweis. Das folgt unmittelbar aus der vorhergehenden Proposition 3.7.1 zusammen mit der Erkenntnis, daß das Bilden des Homomorphismenraums, wie in **??** und **??** ausgeführt wird, „mit endlichen direkten Summen vertauscht“. □

3.7.4 (**Die Duale einer exakten Sequenz ist exakt**). Nehmen wir in diesem Korollar als L den Grundkörper, so folgt insbesondere, daß jede exakte Sequenz von Vektorräumen beim Dualisieren wieder eine exakte Sequenz liefert.

Lemma 3.7.5 (**Neunerlemma**)**.** *Sei gegeben ein Diagramm von Gruppen mit kurzen exakten Zeilen der Gestalt*

$$\begin{array}{ccccc} A' & \hookrightarrow & A & \twoheadrightarrow & A'' \\ \downarrow & & \downarrow & & \downarrow \\ B' & \hookrightarrow & B & \twoheadrightarrow & B'' \\ \downarrow & & \downarrow & & \downarrow \\ C' & \hookrightarrow & C & \twoheadrightarrow & C'' \end{array}$$

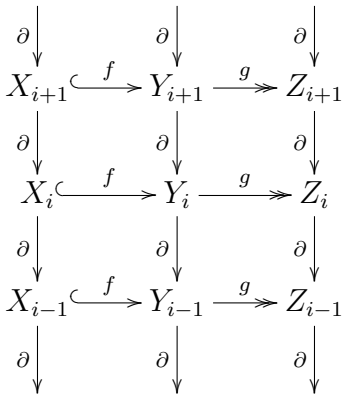
und seien die senkrechten Kompositionen jeweils trivial. Sei unser Diagramm **kommutativ** *in dem Sinne, daß alle vier Quadrate „kommutieren“, daß also die Komposition $A' \to A \to B$ übereinstimmt mit der Komposition $A' \to B' \to B$ etcetera. Sind unter diesen Voraussetzungen zwei der Spalten kurze exakte Sequenzen, so auch die dritte.*

3.7.6. Wir brauchen gar nicht zu fordern, daß die Abbildungen der rechten Vertikale Gruppenhomomorphismen sind, und noch nicht einmal, daß sie Gruppen sind, wenn wir nur annehmen, daß alle Horizontalen als Sequenzen von bepunkteten Mengen isomorph sind zu Sequenzen der Gestalt $H \hookrightarrow G \twoheadrightarrow G/H$ für eine Gruppe G mit einer Untergruppe H und dem neutralen Element von G als ausgezeichnetem Punkt in der Mitte. Der Beweis bleibt derselbe und 3.1.11 zeigt, daß auch in der rechten Spalte alle nichtleeren Fasern gleich viele Elemente haben. Die letzte Aussage von 3.1.11 etwa ist ein Spezialfall des so verallgemeinerten Neunerlemmas.

3.7.7. Das Neunerlemma kann als eine Verallgemeinerung des Noether'schen Isomorphiesatzes 3.2.15 verstanden werden, den man im Fall $A' = A$ zurückgewinnt. Im Fall abelscher Gruppen werden Sie eine noch allgemeinere Aussage eventuell später einmal als „lange exakte Homologiesequenz“ **??** kennenlernen. Der folgende Beweis ist ein schönes Beispiel für eine Beweismethode, die als **Diagrammjagd** bekannt ist.

Beweis. Es ist einfacher, eine allgemeinere Aussage zu zeigen: Sei ein kommuta-

tives Diagramm von Gruppen mit kurzen exakten Zeilen



gegeben derart, daß die Komposition aufeinanderfolgender Pfeile in den Spalten jeweils einwertig ist. Sind dann zwei der Spalten exakt, so auch die Dritte. Das Neunerlemma folgt durch die Erweiterung seines Diagramms durch triviale Gruppen nach oben und unten. Wir schreiben den Beweis gleich so auf, daß auch für die allgemeinere Situation 3.7.6 funktioniert, und notieren dazu die ausgezeichneten Punkte der rechten Spalte mit $\bar{1}$. Wir diskutieren die drei Fälle der Reihe nach.

Fall 1: Die letzten beiden Spalten sind exakt und es gilt, die Exaktheit der ersten bei X_i zu zeigen. Sei also $x_i \in X_i$ mit $\partial x_i = 1$. Für $y_i := fx_i$ folgt $\partial y_i = 1$, also $y_i = \partial y_{i+1}$. Für $z_{i+1} := gy_{i+1}$ folgt weiter $\partial z_{i+1} = \bar{1}$, also $z_{i+1} = \partial z_{i+2}$. Wir finden nun y_{i+2} mit $gy_{i+2} = z_{i+2}$, also $g\partial y_{i+2} = z_{i+1} = gy_{i+1}$, woraus für $\tilde{y}_{i+1} := (\partial y_{i+2})^{-1} y_{i+1}$ folgt $y_i = \partial \tilde{y}_{i+1}$ und $g\tilde{y}_{i+1} = \bar{1}$. Dann aber gibt es $\tilde{x}_{i+1}$ mit $f\tilde{x}_{i+1} = \tilde{y}_{i+1}$ und es folgt $f\partial\tilde{x}_{i+1} = y_i$ und somit $\partial\tilde{x}_{i+1} = x_i$.

Fall 2: Die beiden äußeren Spalten sind exakt und es gilt, die Exaktheit der mittleren bei Y_i zu zeigen. Sei $y_i \in Y_i$ mit $\partial y_i = 1$. Für $z_i := gy_i$ folgt $\partial z_i = \bar{1}$, also gibt es z_{i+1} mit $\partial z_{i+1} = z_i$ und dann y_{i+1} mit $gy_{i+1} = z_{i+1}$ und $g\partial y_{i+1} = z_i = gy_i$. Für $\tilde{y}_i := (\partial y_{i+1})^{-1} y_i$ folgt also $\partial\tilde{y}_i = 1$ und $g\tilde{y}_i = \bar{1}$. Also gibt es $\tilde{x}_i$ mit $f\tilde{x}_i = \tilde{y}_i$ und notwendig $\partial\tilde{x}_i = 1$, also $\tilde{x}_i = \partial\tilde{x}_{i+1}$ und $\tilde{y}_i = \partial f\tilde{x}_{i+1}$. So erhalten wir schließlich $y_i = \partial(y_{i+1} f(\tilde{x}_{i+1}))$.

Fall 3: Die ersten beiden Spalten sind exakt und es gilt, die Exaktheit der letzten bei z_i zu zeigen. Sei also $\partial z_i = \bar{1}$. Sicher gibt es y_i mit $gy_i = z_i$ und es folgt $g\partial y_i = \bar{1}$, also gibt es x_{i-1} mit $fx_{i-1} = \partial y_i$. Es folgt $f\partial x_{i-1} = 1$, also $\partial x_{i-1} = 1$, also gibt es x_i mit $\partial x_i = x_{i-1}$. Für $\tilde{y}_i := y_i (fx_i)^{-1}$ folgt $\partial\tilde{y}_i = 1$ und $g(\tilde{y}_i) = z_i$. Also gibt es $\tilde{y}_{i+1}$ mit $\tilde{y}_i = \partial\tilde{y}_{i+1}$ und dann gilt $z_i = \partial g\tilde{y}_{i+1}$. □

Übungen

Übung 3.7.8. Man folgere den Noether'schen Isomorphiesatz 3.2.15 aus dem Neunerlemma.

4 Symmetrie*

Symmetrie ist ein grundlegendes Konzept in Mathematik und Physik. Wir haben es bei der Modellierung des Anschauungsraums bereits in Aktion gesehen. Hier soll es in einem allgemeineren und formaleren Rahmen diskutiert und mit andersartigen Beispielen illustriert werden.

4.1 Gruppenwirkungen

Definition 4.1.1. Eine **Operation** oder **Wirkung** eines Monoids M auf einer Menge X ist eine Abbildung

$$\begin{array}{ccc} M \times X & \to & X \\ (g,x) & \mapsto & gx \end{array}$$

derart, daß gilt $g(hx) = (gh)x$ für alle $g, h \in M$, $x \in X$ sowie $ex = x$ für das neutrale Element $e \in M$ und alle $x \in X$. Eine Menge mit einer Operation eines Monoids M nennt man eine M-**Menge**. Die Aussage „X ist eine M-Menge“ schreiben wir in Formeln

$$M \backslash X$$

4.1.2. Die erste Eigenschaft werde ich auch als die **Assoziativität** der Operation ansprechen und beide Eigenschaften zusammen als **Unitärassoziativität**. Ich ziehe die Bezeichnung als Operation an dieser Stelle vor, da das Wort „Wirkung“ in der Physik in einer anderen Bedeutung verwendet wird.

Ergänzung 4.1.3. In derselben Weise erklärt man noch allgemeiner auch den Begriff der **Operation einer Menge** Ω **auf einer Menge** X als einer Abbildung $\Omega \times X \to X$, von der nichts weiter zu fordern ist.

Beispiele 4.1.4.

1. Das Anwenden einer Abbildung definiert für jede Menge X eine Operation $\mathrm{Ens}(X) \times X \to X$ des Monoids $\mathrm{Ens}(X)$ auf X und eine Operation $\mathrm{Ens}^\times(X) \times X \to X$ der Gruppe $\mathrm{Ens}^\times(X)$ auf X. Insbesondere operiert so die symmetrische Gruppe $\mathcal{S}_n$ auf der Menge $\{1, 2, \ldots, n\}$.

2. Das Anwenden einer linearen Abbildung definiert für jeden Vektorraum V eine Operation $\mathrm{End}(V) \times V \to V$ des Monoids $\mathrm{End}(V)$ auf V und eine Operation $\mathrm{GL}(V) \times V \to V$ der Gruppe $\mathrm{GL}(V)$ auf V.

3. Jedes Monoid M operiert vermittels seiner Verknüpfung $M \times M \to M$ auf sich selbst.

4. Jedes Monoid M operiert auf jeder Menge X vermittels der **trivialen Operation** $ax = x \; \forall a \in M, x \in X$.

5. Ist M ein Monoid und X eine M-Menge und $N \subset M$ ein Untermonoid, so ist X auch eine N-Menge in offensichtlicher Weise. Ist allgemeiner X eine M-Menge und $N \to M$ ein Monoidhomomorphismus, so kann X in offensichtlicher Weise mit einer Operation von N versehen werden.

6. Ist X ein M-Menge, so ist auch die Potenzmenge $\mathcal{P}(X)$ eine M-Menge in natürlicher Weise.

4.1.5. Gegeben ein Monoid M und eine Menge X induziert das Exponentialgesetz $\mathrm{Ens}(M \times X, X) \xrightarrow{\sim} \mathrm{Ens}(M, \mathrm{Ens}(X, X))$ aus **??** eine Bijektion

$$\left\{ \begin{array}{c} \text{Operationen des Monoids } M \\ \text{auf der Menge } X \end{array} \right\} \xrightarrow{\sim} \left\{ \begin{array}{c} \text{Monoidhomomorphismen} \\ M \to \mathrm{Ens}(X) \end{array} \right\}$$

In gewisser Weise ist also eine Operation eines Monoids M auf einer Menge X „dasselbe“ wie ein Monoidhomomorphismus $M \to \mathrm{Ens}(X)$. Ist G eine Gruppe, so erhalten wir insbesondere eine Bijektion

$$\left\{ \begin{array}{c} \text{Operationen der Gruppe } G \\ \text{auf der Menge } X \end{array} \right\} \xrightarrow{\sim} \left\{ \begin{array}{c} \text{Gruppenhomomorphismen} \\ G \to \mathrm{Ens}^\times(X) \end{array} \right\}$$

In gewisser Weise ist also eine Operation einer Gruppe G auf einer Menge X „dasselbe“ wie ein Gruppenhomomorphismus $G \to \mathrm{Ens}^\times(X)$.

4.1.6. Ist ganz allgemein $X \times Y \to Z$ eine Abbildung, etwa $(x, y) \mapsto x \top y$, und sind $A \subset X$ und $B \subset Y$ Teilmengen, so notieren wir $(A \top B) \subset Z$ die Teilmenge

$$(A \top B) = \{x \top y \mid x \in A,\ y \in B\}$$

Wir haben diese Notationen in Spezialfällen bereits oft verwendet, zum Beispiel, wenn wir das Erzeugnis eines Vektors in einem reellen Vektorraum als $\langle v \rangle = \mathbb{R}v$ schreiben, oder wenn wir das Erzeugnis von zwei Teilräumen U, W eines Vektorraums V als $U + W$ schreiben.

Definition 4.1.7. Sei X eine Menge mit einer Operation eines Monoids M, also eine M-Menge.

1. Die Menge aller **Fixpunkte von M in X** notiert man

   $$X^M := \{x \in X \mid ax = x\ \forall a \in M\}$$

   In vielen Situationen nennt man die Fixpunkte auch **Invarianten**.

2. Der **Fixator** oder auch **Stabilisator** eines Punktes $x \in X$ ist die Menge

   $$M_x := \{a \in M \mid ax = x\}$$

   Sie ist ein Untermonoid von M. Im Fall einer Gruppenwirkung ist sie sogar eine Untergruppe und heißt die **Standgruppe** oder **Isotropiegruppe** des Punktes x.

3. Gegeben eine Teilmenge $Y \subset X$ unterscheiden wir zwischen ihrem **Stabilisator** $\{a \in M \mid aY \subset Y\}$, ihrem **Fixator** oder **mengenweisen Fixator** $\{a \in M \mid aY = Y\}$ und schließlich ihrem **punktweisen Fixator** $\{a \in M \mid ay = y \ \forall y \in Y\}$. Alle drei sind Untermonoide und die letzten beiden im Fall einer Gruppenoperation sogar Untergruppen. Den Fixator nennen wir insbesondere im Fall, daß Y mehr als nur ein Element besitzt und daß eine Gruppe operiert, die **Symmetriegruppe von** Y. Natürlich kann der Fixator von $Y \subset X$ auch beschrieben werden als der Fixator des Punktes $Y \in \mathcal{P}(X)$ für die auf der Potenzmenge $\mathcal{P}(X)$ induzierte Operation. Wir notieren ihn M_Y.

4. Eine M-Menge X heißt **frei**, wenn es eine Teilmenge $Z \subset X$ gibt derart, daß die Operation $M \times X \to X$ eine Bijektion $M \times Z \xrightarrow{\sim} X$ induziert. Sie mögen als Übung zeigen, daß eine Menge mit Gruppenwirkung genau dann frei ist, wenn die Standgruppen aller ihrer Punkte trivial sind, in Formeln $(gx = x \text{ für ein } x \in X) \Rightarrow (g = e)$.

5. Für $Z \subset X$, $N \subset M$ schreiben wir kurz NZ für die Menge $NZ := \{bz \mid b \in N, z \in Z\}$. Für jede Teilmenge $Z \subset X$ ist MZ eine M-Menge in offensichtlicher Weise. Eine Teilmenge $Z \subset X$ heißt N**-stabil**, wenn gilt $NZ \subset Z$, wenn also N im Stabilisator der Teilmenge Z liegt. Ist $N = G$ eine Untergruppe von M, so wird jede G-stabile Teilmenge Z sogar von allen Elementen von G festgehalten, in Formeln

$$(GZ \subset Z) \Rightarrow (g(Z) = Z \ \forall g \in G)$$

6. Sei $x \in X$. Die Menge

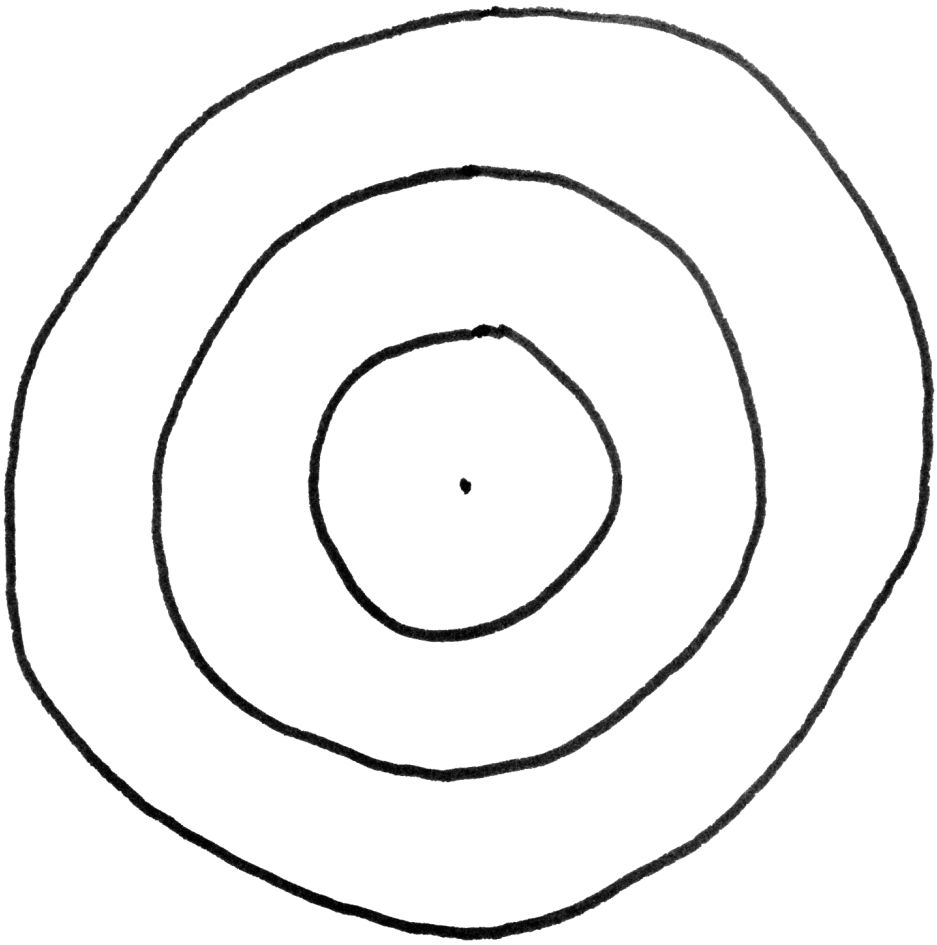
$$Mx := \{ax \mid a \in M\} \subset X$$

heißt die **Bahn** von x. Auf Englisch und Französisch sagt man dazu **orbit**.

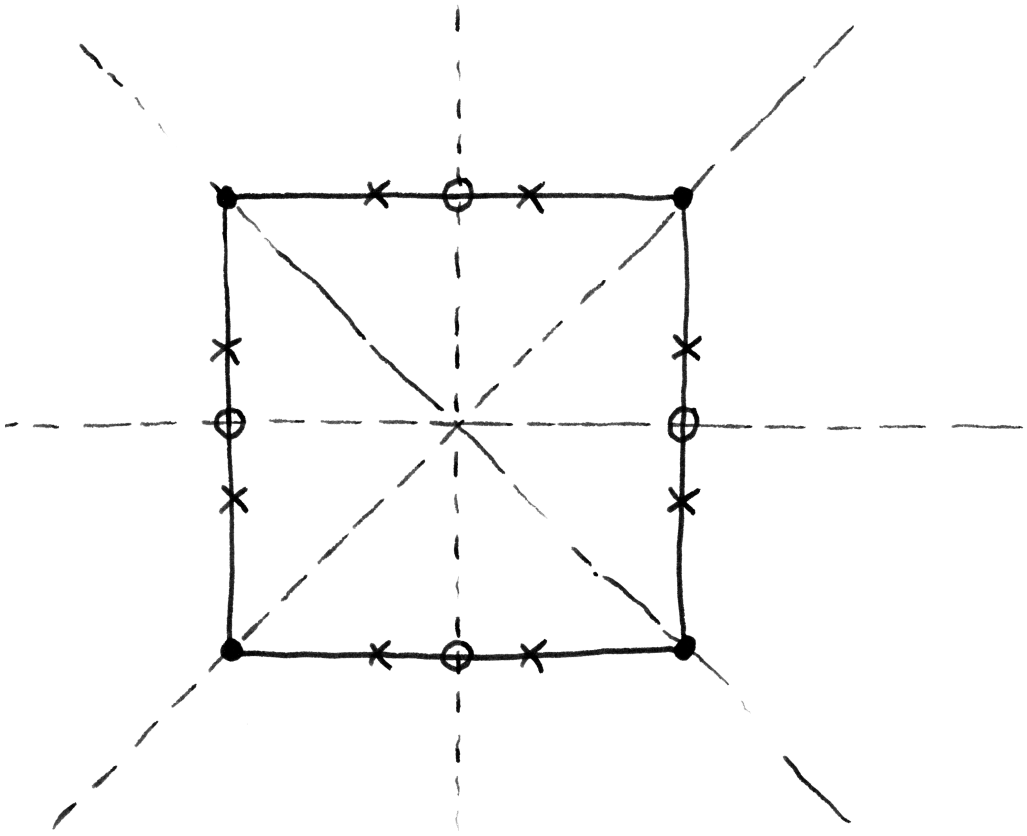
7. Eine Operation heißt **transitiv**, wenn es ein $x \in X$ gibt mit $X = Mx$. Im Fall einer Gruppenwirkung gilt dann $X = Gx$ für alle $x \in X$ und X heißt ein **homogener Raum** für G.

8. Eine Menge X mit einer freien transitiven Operation einer Gruppe G heißt ein **prinzipaler homogener** G**-Raum** oder auch ein G**-Torsor**.

4.1.8. Ist G eine Gruppe und $H \subset G$ eine Untergruppe, so sind per definitionem die Rechtsnebenklassen von H in G genau die Bahnen der durch Multiplikation gegebenen Operation von H auf G.



Einige Bahnen von S^1 auf $\mathbb{C}$



Einige Bahnen der Symmetriegruppe eines Quadrats

4.1.9. Ist G eine Gruppe und $H \subset G$ eine Untergruppe, so ist die Menge der Linksnebenklassen $X = G/H$ eine G-Menge in offensichtlicher Weise.

Beispiele 4.1.10. In jedem eindimensionalen Vektorraum über einem Körper k bilden die von Null verschiedenen Vektoren einen Torsor über der multiplikativen Gruppe $k^\times$ unseres Körpers. Jeder affine Raum ist ein Torsor über seinem Richtungsraum. Jede Menge mit genau zwei Elementen ist in natürlicher Weise ein $(\mathbb{Z}/2\mathbb{Z})$-Torsor. Jede Gruppe G kann in offensichtlicher Weise aufgefaßt werden als ein G-Torsor.

4.1.11 (**Diskussion der Terminologie**). Die Wirkung eines Monoids auf der leeren Menge ist in unseren Konventionen nicht transitiv. Hier sind jedoch auch andere Konventionen gebräuchlich, zum Beispiel nennt Bourbaki die Wirkung einer Gruppe auf der leeren Menge durchaus transitiv. Noch mehr Terminologie zu Mengen mit Gruppenwirkung führen wir in **??** ein.

Ergänzung 4.1.12 (**Begriff eines Torsors, Varianten**). Es gibt auch Varianten des Torsor-Begriffs, bei denen man nicht auf eine vorgegebene Gruppe Bezug nimmt.

1. Man kann einen **Torsor** definieren als eine Menge X mitsamt einer ausgezeichneten Untergruppe $G \subset \mathrm{Ens}^\times(X)$, die frei und transitiv auf X wirkt.

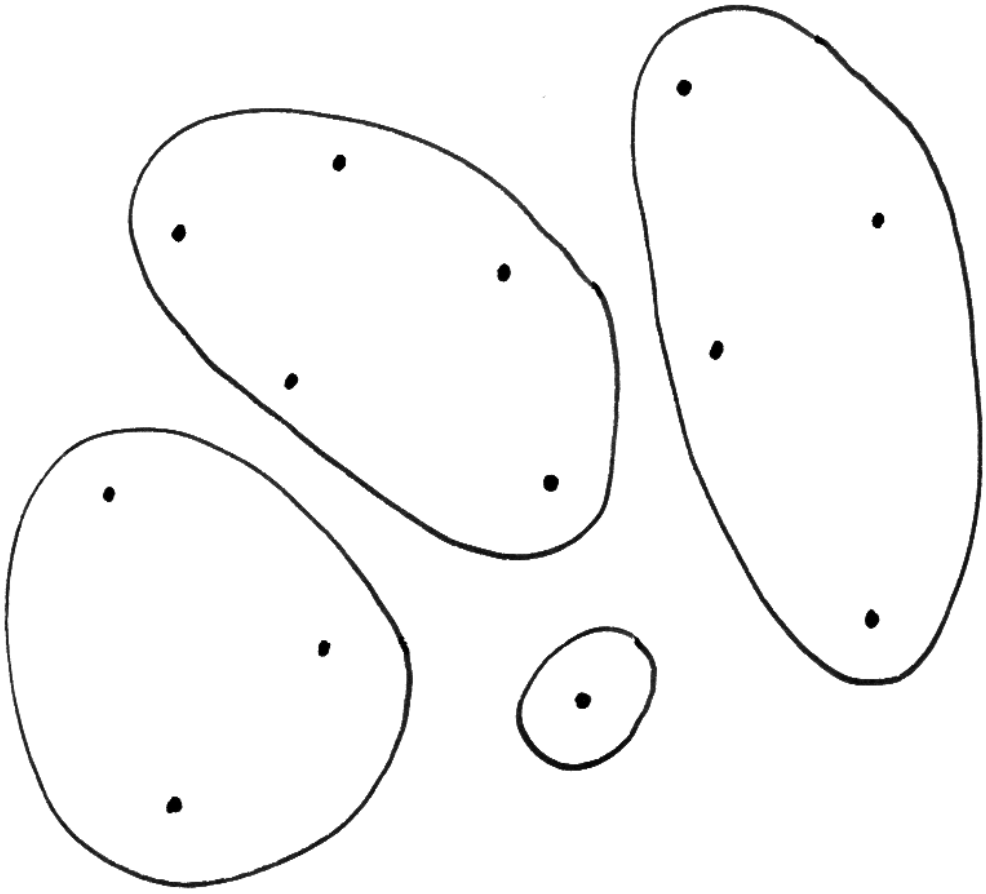
2. Man kann einen Torsor auch definieren als eine Menge X nebst einer Äquivalenzrelation auf $X \times X$ mit gewissen Eigenschaften, die ich hier nicht ausschreibe. Von der üblichen Definition aus gesehen erklären wir dabei die Äquivalenzrelation dadurch, daß ihre Äquivalenzklassen genau die Graphen der durch die Gruppenelemente gegebenen Selbstabbildungen von X sind.

3. Man kann einen Torsor schließlich auch definieren kann als eine Menge X nebst einer Abbildung $\varphi : X \times X \times X \to X$ mit gewissen Eigenschaften, die ich hier nicht ausschreibe. Von der üblichen Definition aus gesehen setzen wir dazu $\varphi(x, gx, y) = gy$.

Lemma 4.1.13 (**Zerlegung in Bahnen**). *Gegeben eine Menge mit Gruppenoperation sind je zwei Bahnen entweder gleich oder disjunkt.*

Ergänzung 4.1.14. Im Fall der Operation eines Monoids gibt im allgemeinen keine Zerlegung in Bahnen: Man betrachte für ein Gegenbeispiel etwa die Operation durch Addition des additiven Monoids $\mathbb{N}$ auf $\mathbb{Z}$.

4.1.15. Unter einer **Partition einer Menge** X versteht man ein System $\mathcal{U} \subset \mathcal{P}(X)$ von paarweise disjunkten nichtleeren Teilmengen, deren Vereinigung ganz X ist. In dieser Terminologie besagt unser Lemma also, daß die Bahnen unter der Operation einer Gruppe auf einer Menge eine Partition besagter Menge bilden.



Eine Partition einer Menge mit dreizehn Elementen durch vier Teilmengen.

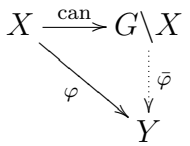
Beweis. Sei $G\backslash\!\!\backslash X$ unsere Menge mit Gruppenoperation. Wegen unserer Forderung $ex = x$ an eine Gruppenoperation liegt jedes $x \in X$ in einer G-Bahn, nämlich in der G-Bahn Gx. Andererseits folgt aus $Gx \cap Gy \neq \emptyset$ schon $Gx = Gy$: In der Tat liefert $gx = hy$ wegen $Gg = G$ unter Verwendung der Assoziativitätsbedingung an eine Gruppenoperation ja $Gx = Ggx = Ghy = Gy$. Die Bahnen sind also auch paarweise disjunkt. □

Definition 4.1.16. Gegeben eine Menge mit Gruppenoperation bezeichnet man das Mengensystem der Bahnen auch als den **Bahnenraum**. Ist $G\backslash\!\!\backslash X$ unsere Menge mit Gruppenoperation, so ist der Bahnenraum in Formeln ausgedrückt also die Teilmenge $\{Gx \mid x \in X\} \subset \mathcal{P}(X)$ der Potenzmenge von X. Wir notieren den Bahnenraum meist $G\backslash X$ oder $X/_l G$ oder X/G. Wir haben eine kanonische Surjektion $\mathrm{can} : X \twoheadrightarrow G\backslash X$, $x \mapsto Gx$, die jedem Element von X seine Bahn zuordnet.

4.1.17 (**Diskussion der Notation**). Alle Notationen für den Bahnenraum haben ihre Tücken: Die Notation $G\backslash X$ könnte auch die in **??** eingeführte Differenzmenge bedeuten, die Notation X/G hinwiederum könnte auch für den Bahnenraum einer Rechtsoperation stehen, wie wir ihn gleich einführen werden. Was im Einzelfall gemeint ist, muß aus dem Kontext erschlossen werden. Die Notation $X/_l G$ vermeidet zwar diese Probleme, ist aber unüblich und umständlich.

Beispiel 4.1.18. Wir betrachten die Menge $X = \mathbb{C}$ der komplexen Zahlen mit der Operation von $G = S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ durch Multiplikation. Die Standgruppen sind $G_x = 1$ falls $x \neq 0$ und $G_0 = S^1$. Die Bahnen sind genau alle Kreise um den Nullpunkt mit Radius $r \geq 0$. Die Einbettung $\mathbb{R}_{\geq 0} \hookrightarrow \mathbb{C}$ induziert eine Bijektion mit dem Bahnenraum $\mathbb{R}_{\geq 0} \xrightarrow{\sim} (S^1\backslash\mathbb{C})$.

4.1.19 (**Universelle Eigenschaft des Bahnenraums**). Gegeben eine Menge mit Gruppenoperation $G\backslash\!\!\backslash X$ und eine Abbildung in eine weitere Menge $\varphi : X \to Y$ mit der Eigenschaft $\varphi(gx) = \varphi(x)$ für alle $g \in G, x \in X$ existiert genau eine Abbildung $\bar{\varphi} : G\backslash X \to Y$ mit $\bar{\varphi} \circ \mathrm{can} = \varphi$, im Diagramm



In der Tat können und müssen wir $\bar{\varphi}(Gx)$ als das einzige Element der Menge $\varphi(Gx)$ definieren. Das ist ein Spezialfall der universellen Eigenschaft von Surjektionen **??**. Man mag es auch als einen Spezialfall der universellen Eigenschaft des Raums der Äquivalenzklassen einer Äquivalenzrelation im Sinne von 1.2.6 verstehen.

Definition 4.1.20. Sei X eine Menge und M ein Monoid. Eine **Rechtsoperation von M auf X** ist eine Abbildung

$$\begin{array}{ccc} X \times M & \to & X \\ (x,a) & \mapsto & xa \end{array}$$

derart, daß $x(ab) = (xa)b$ für alle $a, b \in M$, $x \in X$, und daß gilt $xe = x$ für das neutrale Element $e \in M$ und alle $x \in X$. Eine Menge mit einer Rechtsoperation eines Monoids M nennt man auch eine M-**Rechtsmenge**.

Beispiel 4.1.21. Ist M ein Monoid und X eine M-Menge und E eine weitere Menge, so wird der Abbildungsraum $\mathrm{Ens}(X, E)$ zu einer M-Rechtsmenge vermittels der Operation „durch Vorschalten“ $(fa)(x) := f(ax)$.

4.1.22 (**Beziehung von Rechts- und Linksoperationen**). Ist G eine Gruppe, so wird jede G-Rechtsmenge X zu einer G-Menge durch die Operation $gx = xg^{-1}$, die Begriffsbildung einer G-Rechtsmenge ist also für Gruppen in gewisser Weise obsolet. Sie dient im wesentlichen dem Zweck, in manchen Situationen suggestivere Notationen zu ermöglichen. Unsere Begriffe für Linksoperationen wie Bahn, Standgruppe et cetera verwenden wir analog auf für Rechtsoperationen. Den Bahnenraum notieren wir in diesem Fall stets X/G. Die kanonische Abbildung $X \twoheadrightarrow X/G$ hat dann offensichtlich eine zu 4.1.19 analoge universelle Eigenschaft.

4.1.23. Unter dem Exponentialgesetz $\mathrm{Ens}(X \times M, X) \xrightarrow{\sim} \mathrm{Ens}(M, \mathrm{Ens}(X, X))$ aus **??** entsprechen die Rechtsoperationen eines Monoids M auf einer Menge X gerade den Monoidhomomorphismen $M^{\mathrm{opp}} \to \mathrm{Ens}^\times(X)$. Hierbei meint M^{opp} das opponierte Monoid nach **??**, die entsteht, indem wir die Menge M mit der opponierten Verknüpfung $a^\circ b^\circ = (ba)^\circ$ versehen. In diesem Sinne ist also eine M-Rechtsoperation dasselbe wie eine Linksoperation von M^{opp}.

Ergänzung 4.1.24. Sei G eine Gruppe. Eine freie transitive G-Rechtsmenge nennen wir einen G-**Rechtstorsor** oder auch kurz einen G-**Torsor** in der Hoffnung, daß der Leser aus dem Kontext erschließen kann, ob im jeweils vorliegenden Fall eine Menge mit freier und transitiver Rechts- oder mit freier und transitiver Linksoperation gemeint ist.

4.1.25 (**Operationen auf dem projektiven Raum**). Wir erinnern für einen Körper K und $n \in \mathbb{N}$ aus **??** den projektiven Raum

$$\mathbb{P}^n K := (K^{n+1} \backslash 0)/K^\times$$

Sicher operiert die Gruppe $\mathrm{GL}(n+1; K)$ auf dem projektiven Raum $\mathbb{P}^n K$. Die offensichtliche Operation von $\mathrm{GL}(2; K)$ auf $\mathbb{P}^1 K$ entspricht unter unserer Identifikation von $K \sqcup \{\infty\}$ mit $\mathbb{P}^1 K$ durch $x \mapsto \langle 1, x\rangle$ und $\infty \mapsto \langle 0, 1\rangle$ der Operation

von $\mathrm{GL}(2;K)$ auf $K \sqcup \{\infty\}$, unter der eine Matrix durch die Transformation

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : x \mapsto \frac{c+dx}{a+bx}$$

wirkt. Der Punkt ∞ muß hier mit etwas Sorgfalt ins Spiel gebracht werden und ich schreibe nicht alle Fälle aus. Man sie jedoch leicht erschließen, wenn man weiß, daß diese Operation im Fall $K = \mathbb{R}$ stetig ist für die natürliche Topologie aus **??**. Zum Beispiel geht ∞ im Fall $b \neq 0$ nach d/b.

Übungen

Übung 4.1.26 (**Noether'scher Isomorphiesatz, Variante**). Seien $H \supset N$ eine Gruppe mit einem Normalteiler und X eine Menge mit H-Operation. So gibt es auf dem Bahnenraum X/N genau eine Operation der Quotientengruppe H/N mit der Eigenschaft $(hN)(Nx) = Nhx$. Ist speziell $G \supset H \supset N$ eine Gruppe mit zwei Untergruppen und ist N ein Normalteiler in H, so induziert die Komposition $G \twoheadrightarrow G/N \twoheadrightarrow (G/N)/(H/N)$ eine Bijektion $G/H \xrightarrow{\sim} (G/N)/(H/N)$.

Übung 4.1.27. Unter der Operation von $\mathrm{GL}(n+1;\mathbb{Q})$ auf dem projektiven Raum $\mathbb{P}^n\mathbb{Q}$ operiert bereits die Gruppe $\mathrm{SL}(n;\mathbb{Z})$ aller $(n\times n)$-Matrizen mit ganzzahligen Einträgen und Determinante Eins transitiv. Hinweis: 3.4.29.

Übung 4.1.28. Ist E ein affiner Raum über einem Körper der Charakteristik Null und $G \subset \mathrm{Aff}^\times E$ eine endliche Untergruppe seiner Automorphismengruppe, so besitzt G stets einen Fixpunkt in E. Hinweis: Man betrachte den Schwerpunkt einer Bahn.

Übung 4.1.29 (**Smith-Normalformen als Bahnrepräsentanten**). Sei K ein Körper. Man zeige, daß wir eine Operation der Gruppe $\mathrm{GL}(n;K) \times \mathrm{GL}(m;K)$ auf der Menge $\mathrm{Mat}(n \times m; K)$ erhalten durch die Vorschrift $(A,B)M = AMB^{-1}$. Man zeige weiter, daß die Bahnen unserer Operation genau die nichtleeren Fasern der durch den Rang gegebenen Abbildung $\mathrm{rk} : \mathrm{Mat}(n \times m; K) \to \mathbb{N}$ sind. Hinweis: Smith-Normalform **??**.

Übung 4.1.30 (**Jordan-Normalformen als Bahnrepräsentanten**). Sei K ein Körper. Man zeige, daß wir eine Operation der Gruppe $\mathrm{GL}(n;K)$ auf der Menge $\mathrm{Mat}(n;K)$ erhalten durch die Vorschrift $A.M := AMA^{-1}$. Man zeige, wie für einen algebraisch abgeschlossenen Körper K die Theorie der Jordan'schen Normalform eine Bijektion liefert zwischen dem Bahnenraum zu dieser „Operation durch Konjugation" und der Menge aller endlichen Multimengen von Paaren aus $\mathbb{N}_{\geq 1} \times K$, deren erste Komponenten sich zu n aufaddieren.

Ergänzende Übung 4.1.31. Sei K ein Körper. Man zeige, daß der Teilraum der quadratischen Formen $Q \subset \mathrm{Ens}(K^n, K)$ stabil ist unter der Rechtsoperation der

Gruppe $\mathrm{GL}(n;K)$ durch Vorschalten auf $\mathrm{Ens}(K^n,K)$. Man diskutiere, inwiefern die Frage nach der Klassifikation der quadratischen Formen im wesentlichen die Frage nach einem Repräsentantensystem für die Bahnen dieser Operation ist.

Ergänzende Übung 4.1.32. Man gebe für jedes ungerade n einen Gruppenisomorphismus $\mathrm{SO}(n) \times \mathbb{Z}/2\mathbb{Z} \xrightarrow{\sim} \mathrm{O}(n)$ an; Man zeige, daß es für gerades n keinen derartigen Isomorphismus gibt.

Ergänzende Übung 4.1.33. Ein Gitter in $\mathbb{C}$ ist eine Untergruppe $\Gamma \subset \mathbb{C}$, die man als Gruppenerzeugnis einer $\mathbb{R}$-Basis von $\mathbb{C}$ erhalten kann. Auf der Menge Gitt aller Gitter in $\mathbb{C}$ operiert $\mathbb{C}^\times$ in offensichtlicher Weise. Man zeige, daß es genau zwei $\mathbb{C}^\times$-Bahnen in Gitt gibt, deren Elemente nichttriviale Isotopiegruppen haben, nämlich die Bahnen der beiden Gitter $\mathbb{Z}+\mathbb{Z}\mathrm{i}$ und $\mathbb{Z}+\mathbb{Z}\mathrm{e}^{\pi\mathrm{i}/3}$.

Ergänzende Übung 4.1.34. Man finde ein Repräsentantensystem für die Bahnen unter der offensichtlichen Wirkung von $\mathrm{GL}(n;\mathbb{Z}) \times \mathrm{GL}(m;\mathbb{Z})$ auf dem Matrizenraum $\mathrm{Mat}(n \times m;\mathbb{Q})$. Hinweis: 3.4.13.

Übung 4.1.35. In dieser Übung sollen Sie den **Satz von Cauchy** zeigen: Jeder Primfaktor der Ordung einer endlichen Gruppe tritt auch als Ordnung eines Elements besagter Gruppe auf. Man zeige der Reihe nach:

1. Für eine Primzahl p und $G = \mathrm{GL}(n;\mathbb{F}_p)$ und die Untergruppe $N \subset G$ der unipotenten oberen Dreiecksmatrizen ist p kein Teiler von $|G/N|$ und $|N|$ eine Potenz von p;

2. Jede endliche Untergruppe $\Gamma \subset G$ ohne Elemente der Ordnung p operiert mit trivialen Standgruppen auf G/N, folglich muß ihre Ordnung $|\Gamma|$ zu p teilerfremd sein;

3. Jede endliche Gruppe Γ läßt sich als Untergruppe in $\mathrm{GL}(n;\mathbb{F}_p)$ für $n = |\Gamma|$ oder kanonischer in $\mathrm{GL}(\mathbb{F}_p\langle\Gamma\rangle)$ einbetten.

Einen anderen Beweis, bei dem vollständig innerhalb der Gruppentheorie argumentiert wird, können Sie in 5.4.8 finden. Er scheint mir jedoch im ganzen eher komplizierter.

4.2 Bahnformel

Lemma 4.2.1 (Bahnen als Quotienten). *Seien G eine Gruppe, X eine G-Menge und $x \in X$ ein Punkt. So induziert die Abbildung $G \to X$, $g \mapsto gx$ eine Bijektion*

$$G/G_x \xrightarrow{\sim} Gx$$

zwischen dem Quotienten nach der Standgruppe von x und der Bahn von x.

Beweis. Für jede G_x-Linksnebenklasse $L \subset G$ im Sinne von 3.1.2 besteht die Menge Lx nur aus einem Punkt, für $L = gG_x$ haben wir genauer $Lx = gG_xx = \{gx\}$. Die Abbildung im Lemma wird nun definiert durch die Bedingung, daß sie jeder Nebenklasse $L \in G/G_x$ das einzige Element von Lx zuordnet. Diese Abbildung ist offensichtlich surjektiv. Sie ist aber auch injektiv, denn aus $gG_xx = hG_xx$ folgt $gx = hx$, also $h^{-1}g \in G_x$, also $gG_x = hG_x$. □

Zweiter Beweis. Die durch das Anwenden auf $x \in X$ gegebene Abbildung $G \twoheadrightarrow Gx$ und die kanonische Surjektion $G \twoheadrightarrow G/G_x$ sind Surjektionen mit denselben Fasern. Die Behauptung folgt so aus **??**. □

4.2.2. Ist G eine endliche Gruppe und X eine G-Menge, so folgt mit dem vorhergehenden Lemma 4.2.1 aus dem Satz von Lagrange 3.1.5 für alle $x \in X$ insbesondere die sogenannte **Bahnformel**

$$|G| = |G_x| \cdot |Gx|$$

Die Kardinalität jeder Bahn teilt also die Kardinalität der ganzen Gruppe, und die Kardinalität der Standgruppen ist konstant auf den Bahnen. Genauer prüft man für beliebiges G die Formel $G_{gx} = gG_xg^{-1}$ für $g \in G$, $x \in X$. Ist weiter X endlich und $X = X_1 \sqcup \ldots \sqcup X_n$ seine Zerlegung in Bahnen und $x(i) \in X_i$ jeweils ein Element, so folgt

$$|X| = |X_1| + \ldots + |X_n| = |G|/|G_{x(1)}| + \ldots + |G|/|G_{x(n)}|$$

Beispiel 4.2.3. Seien $k \leq n$ natürliche Zahlen. Auf der Menge X aller k-elementigen Teilmengen der Menge $\{1, 2, \ldots, n\}$ operiert die symmetrische Gruppe $\mathcal{S}_n$ transitiv. Die Standgruppe des Punktes $x \in X$, der durch die k-elementige Teilmenge $\{1, 2, \ldots, k\}$ gegeben wird, ist isomorph zu $\mathcal{S}_k \times \mathcal{S}_{n-k}$. Die Bahnformel liefert folglich $|X| = n!/(k!(n-k)!)$ in Übereinstimmung mit unseren Erkenntnissen aus **??**. Ähnlich kann man auch die in **??** diskutierten Formeln für die Multinomialkoeffizienten herleiten.

Beispiel 4.2.4 (**Zahl der Drehsymmetrien eines Würfels**). Wir können unsere Bahnformel auch umgekehrt anwenden. Nehmen wir zum Beispiel an, wir wollten die Drehungen zählen, die einen Würfel in sich überführen. Die Gruppe G dieser Drehungen operiert sicher transitiv auf der Menge E der acht Ecken des Würfels und die Standgruppe jeder Ecke p hat drei Elemente. Wir folgern $|G| = |G_p| \cdot |E| = 3 \cdot 8 = 24$.

Übungen

Ergänzende Übung 4.2.5. Sind Q, H Untergruppen einer Gruppe G, so induziert die Einbettung $Q \hookrightarrow G$ eine Bijektion $Q/(Q \cap H) \xrightarrow{\sim} QH/H$. Gemeint ist auf

der rechten Seite der Bahnenraum der Operation von rechts durch Multiplikation der Gruppe H auf der Teilmenge $QH \subset G$.

Ergänzende Übung 4.2.6. Ist G eine Gruppe und X eine G-Menge und Y eine G-Rechtsmenge, so erklärt man ihr **balanciertes Produkt**

$$Y \times_{/G} X$$

als die Menge aller G-Bahnen in $Y \times X$ unter der Operation $g(y,x) = (yg^{-1}, gx)$. Man zeige: Sind P, Q Untergruppen einer Gruppe G mit Schnitt $S := P \cap Q$, so induziert die Multiplikation eine Bijektion

$$P \times_{/S} Q \xrightarrow{\sim} PQ$$

Ergänzende Übung 4.2.7. Ist in der Bruhat-Zerlegung 4.6.1 der Köper k ein endlicher Körper $k = \mathbb{F}_q$, so wird die Kardinalität der Doppelnebenklasse BxB für $x \in \mathcal{S}_n$ und B die oberen Dreicksmatrizen gegeben durch die Formel

$$|BxB| = |B|q^{l(x)}$$

mit $l(x)$ der Zahl der Fehlstände der Permutation x. Hinweis: Man wende auf die $(B \times B)$-Bahnen von $x \in \mathcal{S}_n \subset G$ die Bahnformel an.

4.3 Konjugationsklassen

Definition 4.3.1. Ist G eine Gruppe und $x \in G$ ein Element, so ist die Abbildung

$$\begin{array}{rccc} \mathrm{int}_x : & G & \to & G \\ & g & \mapsto & xgx^{-1} \end{array}$$

ein Isomorphismus der Gruppe G mit sich selber. Er heißt die **Konjugation mit** x. Ganz allgemein nennt man einen Isomorphismus einer Gruppe mit sich selber auch einen **Automorphismus** der Gruppe. Die Automorphismen einer Gruppe G bilden selber eine Gruppe mit der Verknüpfung von Abbildungen als Verknüpfung. Sie heißt die **Automorphismengruppe** von G und wir verwenden für sie die beiden Notationen $\mathrm{Aut}(G) = \mathrm{Grp}^{\times}(G)$. Diejenigen Automorphismen einer Gruppe, die sich als Konjugation mit einem geeigneten Gruppenelement schreiben lassen, heißen **innere Automorphismen** und auf englisch **interior automorphisms**, daher die Notation int. Sicher gilt $\mathrm{int}_x \circ \mathrm{int}_y = \mathrm{int}_{xy}$, folglich ist $\mathrm{int} : x \mapsto \mathrm{int}(x) := \mathrm{int}_x$ ein Gruppenhomomorphismus $\mathrm{int} : G \to \mathrm{Grp}^{\times}(G)$ und insbesondere eine Operation der Gruppe G auf der Menge G, die **Operation durch Konjugation**

$$\begin{array}{ccc} G \times G & \to & G \\ (x,y) & \mapsto & \mathrm{int}_x(y) = xyx^{-1} \end{array}$$

Die Bahnen dieser Operation heißen die **Konjugationsklassen** unserer Gruppe.

Beispiele 4.3.2. Die Konjugationsklassen in einer kommutativen Gruppe sind einelementig. Die Theorie der Jordan'schen Normalform beschreibt die Konjugationsklassen in $\mathrm{GL}(n;\mathbb{C})$, vergleiche 4.1.30.

Übungen

Ergänzende Übung 4.3.3. Sei A eine zyklische Gruppe der Ordnung $n \in \mathbb{N}$. So gibt es genau einen Ringisomorphismus $\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \mathrm{End}\, A$, und dieser Ringisomorphismus induziert einen Isomorphismus zwischen der Einheitengruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ und der Automorphismengruppe von A.

Ergänzende Übung 4.3.4. Man gebe jeweils ein Repräsentantensystem an für die Konjugationsklassen der Gruppe aller Isometrien des affinen Skalarproduktraums $\mathbb{R}^2$ und der Untergruppe ihrer orientierungserhaltenden Isometrien.

Ergänzende Übung 4.3.5. Wir betrachten die Gruppen $G \supset K$ der Ähnlichkeiten und der Kongruenzen einer euklidischen Ebene. Man zeige, daß K stabil ist unter der Konjugation mit $g \in G$ und daß die Konjugationsklassen von G, die in K enthalten sind, wie folgt beschrieben werden können:

1. Die Identität bildet für sich allein eine Konjugationsklasse;
2. Alle Verschiebungen, die nicht die Identität sind, bilden eine Konjugationsklasse;
3. Alle Spiegelungen an affinen Geraden bilden eine Konjugationsklasse;
4. Alle Gleitspiegelungen, die keine Spiegelungen sind, bilden eine Konjugationsklasse;
5. Für jeden Winkel θ mit $0 < \theta \leq 180°$ bilden alle Drehungen um einen beliebigen Punkt und um einen Winkel mit dem Betrag θ eine Konjugationsklasse.

Darüber hinaus gibt es keine weiteren Konjugationsklassen von G in K. Hinweis: **??**.

Ergänzende Übung 4.3.6. Wir betrachten die Gruppen $G \supset B$ der Ähnlichkeiten und der Bewegungen eines dreidimensionalen euklidischen Raums. Man zeige, daß B stabil ist unter der Konjugation mit $g \in G$ und daß die Konjugationsklassen von G, die in B enthalten sind, wie folgt beschrieben werden können:

1. Die Identität bildet für sich allein eine Konjugationsklasse;
2. Alle Verschiebungen, die nicht die Identität sind, bilden eine Konjugationsklasse;

3. Für jeden Winkel θ mit $0 < \theta \leq 180°$ bilden alle Drehungen um eine beliebige Achse und um einen Winkel mit dem Betrag θ eine Konjugationsklasse;

4. Für jeden Winkel θ mit $0 < \theta \leq 180°$ bilden alle Verschraubungen um einen Winkel mit dem Betrag θ, die keine Drehungen sind, eine Konjugationsklasse.

Darüber hinaus gibt es keine weiteren Konjugationsklassen von G in B. Hinweis: **??**.

4.4 Endliche Untergruppen von Bewegungsgruppen

4.4.1. Die orthogonalaffinen orientierungserhaltenden Automorphismen eines euklidischen Raums R der Dimension drei nennen wir seine **Bewegungen**. Die Gruppe B aller Bewegungen von R nennen wir die **Bewegungsgruppe von** R. Gegeben eine Teilmenge des Raums $T \subset R$ nennen wir eine Bewegung $b \in B$ mit $b(T) = T$ eine **Symmetriebewegung von** T. Die Symmetriebewegungen einer Teilmenge $T \subset R$ bilden eine Untergruppe seiner Bewegungsgruppe. Bis auf Isomorphismus gibt es nur einen dreidimensionalen euklidischen Raum und man mag sich darunter den Anschauungsraum denken. Der folgende Satz ist in dieser Anschauung und in Bezug auf die aus der Schule bekannten platonischen Körper formuliert in der Hoffnung, daß er durch diesen Stilbruch verständlicher wird. Das exakte Formulieren im Rahmen der in dieser Vorlesung entwickelten Sprache holen wir später nach.

Satz 4.4.2 (**Endliche Untergruppen von Bewegungsgruppen**). *Jede endliche Untergruppe der Bewegungsgruppe ist genau eine der folgenden Gruppen:*

1. *Eine* **zyklische Gruppe** C_k *mit* $k \geq 1$ *Elementen, bestehend aus allen Drehungen zu einer festen Drehachse um Winkel der Gestalt* $2\pi n/k$*. Der Fall* $k = 1$ *deckt hier den Fall der trivialen Gruppe ab, die nur aus der Identität besteht.*

2. *Eine* **Diedergruppe** D_k *mit* $2k$ *Elementen für* $k \geq 2$*. Im Fall* $k > 2$ *ist das die Gruppe aller Symmetriebewegungen eines ebenen gleichseitigen* k*-Ecks, aufgefaßt als räumliche Figur. Im Fall* $k = 2$ *ist es die Gruppe aller derjenigen Drehungen, die von einem Paar sich schneidender orthogonaler Geraden jede in sich überführen.*

3. *Eine* **Tetraedergruppe** T *aller* 12 *Symmetriebewegungen eines Tetraeders.*

4. *Eine* **Würfelgruppe** W *aller* 24 *Symmetriebewegungen eines Würfels.*

5. *Eine* **Ikosaedergruppe** I *aller* 60 *Symmetriebewegungen eines Ikosaeders.*

4.4.3. Will man diesen Satz einem Laien erklären, der mit dem Gruppenbegriff nicht vertraut ist, so mag man nach 1.3.7 auch einfacher von endlichen Mengen von Bewegungen reden, die mit je zwei Bewegungen stets auch deren Hintereinanderausführung enthalten. Vom mathematischen Standpunkt aus mag man das Resultat als eine Aufzählung der „Konjugationsklassen von endlichen Untergruppen der Bewegungsgruppe“ ansehen, also der Bahnen unter der Operation durch Konjugation unserer Bewegungsgruppe auf der Menge ihrer endlichen Untergruppen. Die endlichen Untergruppen der Isometriegruppe des Anschauungsraums werden in 4.4.25 diskutiert.

4.4.4. Das Evozieren der platonischen Körper stellt insofern einen Stilbruch dar, als wir uns zumindest implizit darauf verständigt hatten, alle unsere Überlegungen ausschließlich im Rahmen der Mengenlehre durchzuführen. Ein möglicher **Würfel** ist schnell beschrieben, man mag als Ecken für irgendeine Orthonormalbasis $(\vec{v}_1, \vec{v}_2, \vec{v}_3)$ die acht Vektoren $\pm\vec{v}_1 \pm \vec{v}_2 \pm \vec{v}_3$ nehmen, im $\mathbb{R}^3$ also etwa $(\pm 1, \pm 1, \pm 1)$. Die Ecken eines **Tetraeders** erhält man, wenn man nur die vier Ecken dieses Würfels nimmt, bei denen das Produkt der Koordinaten Eins ist. Den **Ikosaeder** besprechen wir in 4.4.12 noch ausführlich. Zu den fünf sogenannten „platonischen Körpern“ rechnet man außer diesen dreien noch den **Oktaeder** und den **Dodekaeder**. Die Eckenmenge eines Oktaeders bilden etwa die drei Vektoren der Standardbasis des $\mathbb{R}^3$ mitsamt ihren Negativen. Die Eckenmenge eines Dodekaeders mag man anschaulich als die Menge der „Flächenmitten eines Ikosaeders“ beschreiben und formal als die Menge der „Pole der Polordnung drei“ im Sinne des gleich folgenden Beweises im Fall der Symmetriegruppe eines Ikosaeders. Die Bezeichnungen Tetraeder, Oktaeder, Dodekaeder und Ikosaeder für die platonischen Körper außer dem Würfel kommen von den griechischen Worten für die Anzahlen 4, 8, 12 und 20 ihrer Flächen und dem griechischen Wort $\varepsilon\delta\rho\alpha$ für „Sitz“ und dann auch „Sitzfläche“ her. Man findet für den Würfel wegen seiner 6 Flächen manchmal auch die Bezeichnung „Hexaeder“. „Dieder“ heißt eigentlich „Zweiflach“, womit wohl gemeint ist, daß er in gewisser Weise zwei Flächen hat, da man ihn ja wie einen Bierdeckel von beiden Seiten verschieden anmalen könnte.

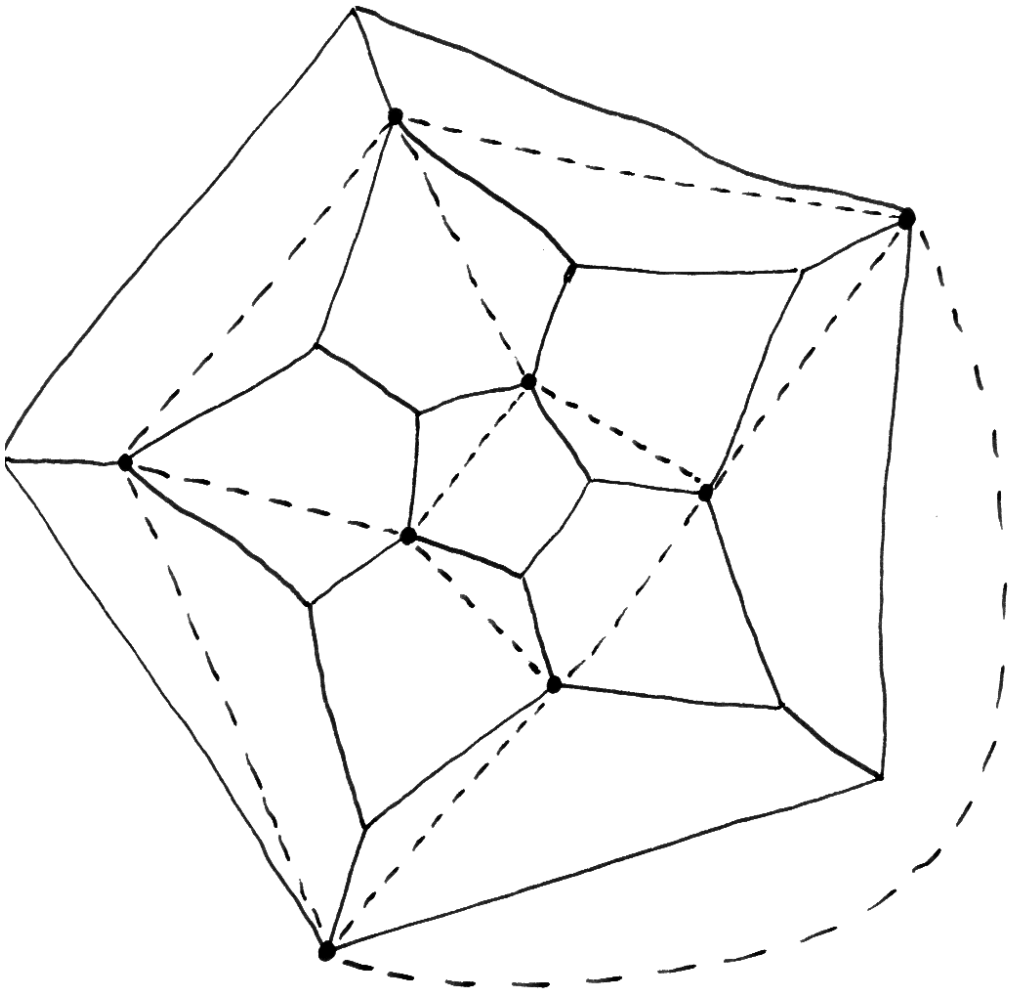
4.4.5. Die Diedergruppe D_4 mag man sich auch als die Gruppe aller acht räumlichen Bewegungen veranschaulichen, die einen Bierdeckel in sich überführen. Sie wird deshalb auch die **Bierdeckelgruppe** genannt.

Ergänzung 4.4.6 (**Beziehungen zur Kristallographie**). Unser Satz 4.4.2 ist ein möglicher Ausgangspunkt der Kristallographie: Unter einem **n-dimensionalen Kristall** verstehen wir hier eine Teilmenge K eines n-dimensionalen euklidischen Raums E, etwa die Menge der Orte der Atome eines Kristallgitters, mit der Eigenschaft, daß (1) die Translationen aus ihrer Symmetriegruppe den Richtungsraum

aufspannen und daß es (2) eine positive untere Schranke gibt für die Längen aller von Null verschiedenen Translationen aus besagter Symmetriegruppe. Die zweite Eigenschaft schließt etwa den Fall aus, daß unsere Teilmenge einfach der ganze besagte Raum ist. Unter der **Punktgruppe** P eines Kristalls verstehen wir die Untergruppe $P \subset \mathrm{O}(\vec{E})$ aller linearen Anteile von Symmetrien unseres Kristalls, unter seiner **Drehgruppe** $D \subset \mathrm{SO}(\vec{E})$ die Menge aller orientierungserhaltenden Elemente der Punktgruppe. Man zeigt, daß die Punktgruppe eines Kristalls stets endlich sein muß, und daß als Drehgruppen von räumlichen, als da heißt dreidimensionalen Kristallen nur die Gruppen C_k und D_k mit $k \in \{1, 2, 3, 4, 6\}$ sowie die Tetraedergruppe und die Würfelgruppe auftreten können. Die Einteilung nach Drehgruppen entspricht in etwa, aber leider nicht ganz genau, der in der Kristallographie gebräuchlichen Einteilung in die sieben **Kristallsysteme**. Genauer entsprechen dem „kubischen System“ die Würfelgruppe und die Tetraedergruppe, dem „tetragonalen System“ die Drehgruppen C_4 und D_4, dem „hexagonalen System“ die Drehgruppen C_6 und D_6, dem „trigonalen System“ die Drehgruppen C_3 und D_3, aber das „orthorhombische“, „monokline“ und „trikline System“ lassen sich erst anhand ihrer Punktgruppen unterscheiden. Auch in den übrigen Fällen liefert die Punktgruppe eine feinere Klassifikation. Für sie gibt es 32 Möglichkeiten, nach denen die Kristalle in die sogenannten **Kristallklassen** eingeteilt werden. Die eigentliche Klassifikation beschreibt alle als Symmetriegruppen von räumlichen Kristallen möglichen Bewegungsgruppen des Anschauungsraums bis auf Konjugation mit orientierungstreuen Automorphismen des unserem euklidischen Raum zugrundeliegenden affinen Raums. Das darf nicht dahingehend mißverstanden werden, daß diese Automorphismengruppe durch Konjugation auf der Menge der möglichen Symmetriegruppen räumlicher Kristalle operieren würde, aber in vielen Fällen sind eben doch zwei derartige Symmetriegruppen konjugiert zueinander, und dann betrachtet man sie als zur selben Klasse gehörig. Es gibt im Raum genau 230 Kristallklassen. Erlaubt man auch Konjugation mit nicht orientierungstreuen Automorphismen, so sinkt die Zahl der Klassen auf 219. Das **achtzehnte Hilbert'sche Problem** fragte unter anderem danach, ob es analog in jeder Dimension nur endlich viele Möglichkeiten für wesentlich verschiedene Kristalle gibt. Bieberbach konnte dafür einen Beweis geben.

4.4.7 (**Beziehungen zwischen den Symmetriegruppen platonischer Körper**). Eine Würfelgruppe kann auch als die Gruppe aller Symmetriebewegungen desjenigen Oktaeders aufgefaßt werden, dessen Ecken die Mittelpunkte der Flächen des Würfels sind. Ähnlich kann eine Ikosaedergruppe auch als Gruppe aller Symmetriebewegungen eines Dodekaeders aufgefaßt werden. Die Kantenmitten eines Tetraeders bilden die Ecken eines Oktaeders, so erhält man eine Einbettung der Tetraedergruppe in die Würfelgruppe.

4.4.8 (**Symmetriegruppen platonischer Körper als abstrakte Gruppen**). Die



Einer der fünf eingeschriebenen Würfel eines Dodekaeders, mit gestrichelt eingezeichneten Kanten.

Diedergruppe D_2 ist isomorph zur Klein'schen Vierergruppe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Sie kann vielleicht übersichtlicher auch beschrieben werden als die Gruppe aller Drehungen, die von einem Tripel paarweise orthogonaler Geraden jede in sich überführen. Neben der Identität liegen darin also die Drehungen um $180°$ um jede dieser drei Geraden. Die Tetraedergruppe kann man in die symmetrische Gruppe $\mathcal{S}_4$ einbetten vermittels ihrer Operation auf den Ecken des Tetraeders. Wir erhalten so einen Isomorphismus der Tetraedergruppe mit der alternierenden Gruppe A_4 aller geraden Permutationen von vier Elementen. Die Würfelgruppe operiert auf der Menge der vier räumlichen Diagonalen des Würfels und wir erhalten so einen Isomorphismus $W \cong \mathcal{S}_4$. Die Ikosaedergruppe operiert auf der Menge der fünf eingeschriebenen Würfel eines Dodekaeders, von denen einer in nebenstehendem Bild schematisch dargestellt ist. Mit etwas Geduld kann man direkt einsehen, daß diese Operation einen Isomorphismus der Ikosaedergruppe I mit der alternierenden Gruppe A_5 aller geraden Permutationen von 5 Elementen liefert. In 5.2.5 werden wir erklären, wie man das auch mit weniger Geduld aber mehr Gruppentheorie einsehen kann, und in 5.6.10 werden wir zusätzlich einen Isomorphismus dieser Gruppe mit der Gruppe $\mathrm{SL}(2;\mathbb{F}_5)/\{\pm \mathrm{id}\}$ herleiten.

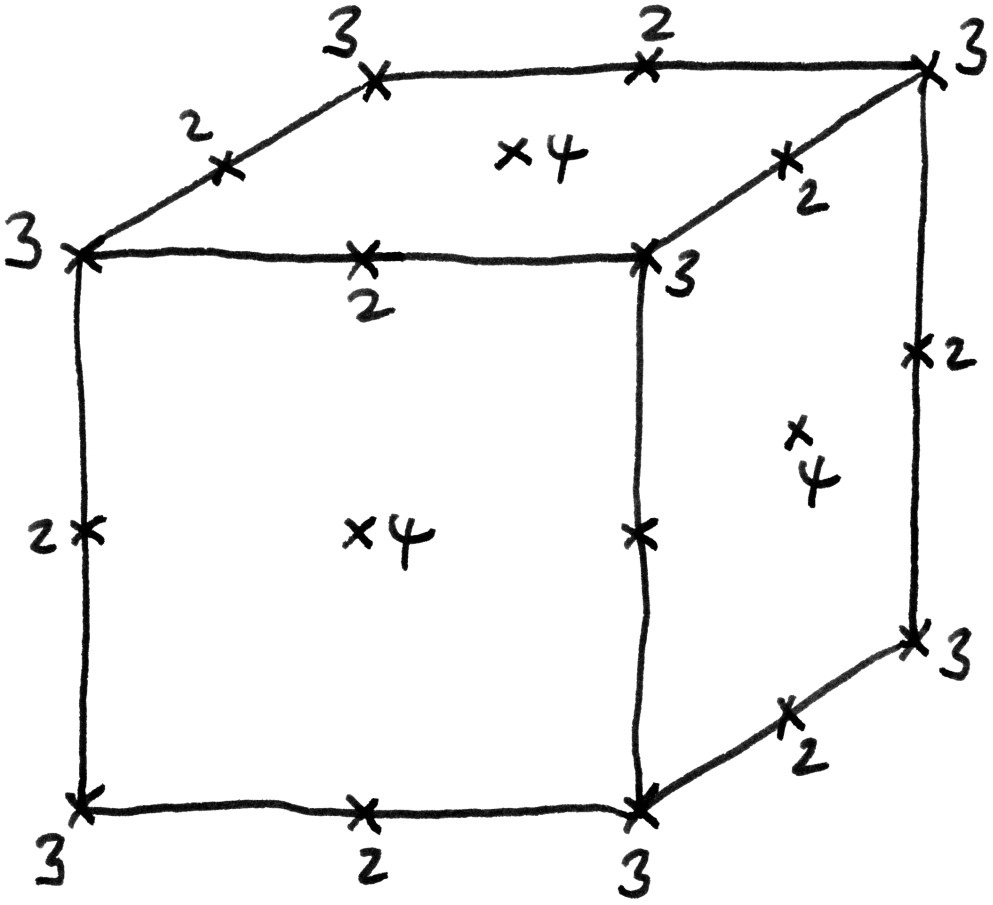
Beweis von Satz 4.4.2. Nach 4.1.28 besitzt jede endliche Gruppe von Automorphismen eines reellen affinen Raums mindestens einen Fixpunkt, genauer ist der Schwerpunkt **??** jeder Bahn ein Fixpunkt. Folglich reicht es, die endlichen Untergruppen der Drehgruppe $\mathrm{SO}(3)$ zu klassifizieren. Sei also $G \subset \mathrm{SO}(3)$ eine endliche Untergruppe. Für jede nichttriviale Drehung $g \in \mathrm{SO}(3)\backslash 1$ erklären wir ihre „Pole" als die beiden Schnittpunkte ihrer Drehachse mit der Einheitssphäre S^2. Sei P die Menge aller Pole von Elementen von $G\backslash 1$. Natürlich ist P eine endliche Menge und G operiert auf P. Wir zählen nun die Menge

$$M := \{(g,p) \in G \times S^2 \mid g \neq 1, gp = p\}$$

aller Paare (g,p) mit $g \in G\backslash 1$ und p einem Pol von g auf zwei Weisen. Einerseits gehört jedes von 1 verschiedene Gruppenelement $g \in G\backslash 1$ zu genau zwei Polen, andererseits gehört jeder Pol $p \in P$ mit Standgruppe G_p zu genau $|G_p| - 1$ von 1 verschiedenen Gruppenelementen. Zusammen erhalten wir so

$$2(|G| - 1) = |M| = \sum_{p \in P} (|G_p| - 1)$$

Sei nun $P = P_1 \sqcup \ldots \sqcup P_r$ die Bahnzerlegung von P und seien $p_i \in P_i$ fest gewählt. Die Standgruppe von p_i habe sagen wir $n_i \geq 2$ Elemente. Die zugehörige Bahn hat dann $|P_i| = |G|/n_i$ Elemente und alle Standgruppen zu Polen $p \in P_i$ haben $|G_p| = n_i$ Elemente. Die Kardinalität der Standgruppe eines Pols nennen wir abkürzend auch die **Polordnung**. Insbesondere ist also n_i die Polordnung des Pols



Die „von vorne sichtbaren“ Pole der Würfelgruppe mit den Kardinalitäten der jeweiligen Standgruppen

p_i. Fassen wir dann die Pole jeder Bahn in unserer Summe zu einem Summanden zusammen, so können wir in unserer Gleichung die rechte Seite umformen zu $\sum_{i=1}^{r}(|G|/n_i)(n_i-1)$ und Wegteilen von $|G|$ liefert die Gleichung

$$2-\frac{2}{|G|}=\sum_{i=1}^{r}\left(1-\frac{1}{n_i}\right)$$

Jeder Summand auf der rechten Seite ist mindestens $1/2$, der Ausdruck links ist aber kleiner als 2. Es kommen also nur bis zu drei Bahnen von Polen in Betracht. Wir machen nun eine Fallunterscheidung nach der Zahl r der Bahnen von Polen.

Fall 0: Es gibt überhaupt keine Pole. In diesem Fall besteht G nur aus dem neutralen Element und wir haben die triviale Gruppe C_1 vor uns.

Fall 1: Ganz P ist eine Bahn. Das ist unmöglich, denn es muß gelten $|G|\geq 2$ wenn es überhaupt Pole geben soll, und damit hätten wir $2-\frac{2}{|G|}\geq 1>1-\frac{1}{n_1}$ im Widerspruch zu unserer Gleichung.

Fall 2: Es gibt genau zwei Bahnen P_1 und P_2 in P. Wir haben dann

$$\frac{2}{|G|}=\frac{1}{n_1}+\frac{1}{n_2}$$

Natürlich haben wir $n_i\leq|G|$ und damit notwendig $n_1=n_2=|G|$. Alle Pole werden also von der Gruppe festgehalten, es gibt folglich nur zwei Pole, die sich notwendig gegenüberliegen müssen. Damit sind wir im Fall der zyklischen Gruppen C_k mit $k=n_1=n_2>1$.

Fall 3: Es gibt genau drei Bahnen P_1, P_2 und P_3 in P, wir haben also

$$\frac{2}{|G|}=\frac{1}{n_1}+\frac{1}{n_2}+\frac{1}{n_3}-1$$

Wir dürfen annehmen $n_1\leq n_2\leq n_3$. Sicher gilt dann $n_1=2$, sonst wäre die rechte Seite ≤ 0. Haben wir auch $n_2=2$, so kann n_3 beliebige Werte annehmen und wir haben $|G|=2n_3$. Die Bahn P_3 besteht dann aus zwei Polen, die sich notwendig gegenüberliegen müssen, da sonst bereits die Bewegung eines dieser beiden Pole mit einer nichttrivialen Drehung und den anderen ein drittes Element der Bahn P_3 liefern würde. Alle Gruppenelemente permutieren die beiden Pole aus P_3 und unsere Gruppe wird damit eine Diedergruppe. Bleibt der Fall $n_2>2$. Hier sind $(2,4,4)$ und $(2,3,6)$ unmöglich für (n_1,n_2,n_3), da ja gilt $\frac{1}{2}+\frac{1}{4}+\frac{1}{4}=1=\frac{1}{2}+\frac{1}{3}+\frac{1}{6}$. Also bleiben nur die Fälle $(2,3,3),(2,3,4)$ und $(2,3,5)$ und man berechnet leicht die zugehörigen Gruppenordnungen zu $12,24$, und 60.

Den Stand unseres Beweises bis hierher können wir wie folgt zusammenfassen: Wir haben eine Abbildung konstruiert – man mag sie die **Bahnpolordnungsabbildung** nennen – die jeder endlichen Untergruppe der Drehgruppe eine endliche Multimenge natürlicher Zahlen zuordnet, und haben gezeigt, daß in ihrem Bild höchstens die folgenden Multimengen liegen:

$$\emptyset,\ {}_\mu\{k,k\} \text{ und } {}_\mu\{2,2,k\} \text{ für } k \geq 2,\ {}_\mu\{2,3,3\},\ {}_\mu\{2,3,4\},\ \text{ und } {}_\mu\{2,3,5\}.$$

Wir müssen nun noch zeigen, daß (1) die angegebenen Multimengen genau das Bild unserer Bahnpolordnungsabbildung sind, und daß (2) je zwei Drehgruppen mit demselben Bild unter der Bahnpolordnungsabbildung zueinander konjugiert sind. Wenn wir das alles gezeigt haben, so folgt, daß die Bahnpolordnungsabbildung eine Bijektion

$$\left\{ \begin{array}{c} \text{endliche Untergruppen} \\ \text{der Drehgruppe } \mathrm{SO}(3), \\ \text{bis auf Konjugation} \end{array} \right\} \tilde{\to} \left\{ \begin{array}{c} \emptyset,\ {}_\mu\{k,k\} \text{ und } {}_\mu\{2,2,k\} \text{ für } k \geq 2, \\ {}_\mu\{2,3,3\},\ {}_\mu\{2,3,4\},\ {}_\mu\{2,3,5\} \end{array} \right\}$$

liefert. Zusammen mit der beim Beweis erzeugten Anschauung zeigt das dann unseren Satz. Die Existenz endlicher Untergruppen der Drehgruppe mit derartigen Polbahnen und Polordnungen scheint mir anschaulich klar. Zum Beispiel hat die Würfelgruppe drei Polbahnen, als da sind: Eine Bahn aus den 8 Ecken zur Polordnung 3; eine Bahn aus den auf Länge Eins normierten 12 Mittelpunkten der Kanten, zur Polordnung 2; und eine Bahn aus den auf Länge Eins normierten 6 Mittelpunkten der Flächen, zur Polordnung 4. Diese Anschauung läßt sich auch leicht zu einem formalen Beweis präzisieren in allen Fällen mit Ausnahme des Ikosaeder-Falls $(2,3,5)$. In diesem Fall folgt die Existenz formal erst aus 4.4.12. Daß je zwei zyklische Gruppen derselben endlichen Ordnung und je zwei Diedergruppen derselben endlichen Ordnung in der Drehgruppe zueinander konjugiert sind, scheint mir offensichtlich. Die folgenden beiden Lemmata 4.4.10 und 4.4.11 zeigen, daß auch je zwei Gruppen mit gegebenen Bahnpolordnungen oder, wie wir von jetzt an abkürzend sagen werden, zu gegebenem **Typ** $(2,3,n)$ in der Drehgruppe zueinander konjugiert sind. Damit vervollständigen sie den Beweis unseres Satzes. □

4.4.9. Man mag eine Teilmenge eines dreidimensionalen euklidischen Raums eine **platonische Eckenmenge** nennen, wenn die Gruppe ihrer Symmetriebewegungen endlich ist und transitiv auf unserer Teilmenge operiert und jedes ihrer Elemente von mindestens drei Symmetriebewegungen festgehalten wird. Man mag einen **platonischen Körper** erklären als die konvexe Hülle einer platonischen Eckenmenge. Unsere Überlegungen zeigen dann, daß es bis auf Ähnlichkeit in unserem Raum genau fünf platonische Körper gibt.

Lemma 4.4.10. *1. Jede endliche Untergruppe einer Drehgruppe von einem der beiden Typen $(2,3,4)$ oder $(2,3,5)$ ist maximal unter allen endlichen Untergruppen der Drehgruppe;*

2. Eine endliche Drehgruppe von einem der Typen $(2,3,n)$ mit $n \geq 3$ kann beschrieben werden als der Stabilistor jeder ihrer beiden kleineren Bahnen von Polen.

Beweis. Nach unseren bisherigen Erkenntnissen kommen bei endlichen Drehgruppen für die Paare (Ordnung eines Pols, Kardinalität seiner Bahn) nur die Paare $(n,1)$, $(n,2)$, $(2,n)$, $(3,4)$, $(3,8)$, $(3,20)$, $(4,6)$ und $(5,12)$ in Frage. Für jeden Pol müssen sich bei Übergang zu einer echt größeren Gruppe nach der Bahnformel entweder seine Polordnung oder die Kardinalität seiner Bahn oder beide vervielfachen. Das ist aber bei $(4,6)$ und $(5,12)$ unmöglich und wir erhalten die erste Behauptung. In den drei Fällen der zweiten Behauptung enthält weiter jede Bahn von Polen mindestens drei Punkte, also auch zwei verschiedene sich nicht gegenüberliegende Punkte. Folglich operiert sogar der Stabilisator in $\mathrm{SO}(3)$ der Bahn P_i treu auf P_i und ist insbesondere endlich. Nun muß P_i auch unter diesem Stabilisator eine Bahn von Polen sein. Wenn die Symmetriegruppe von P_i größer sein will als die Drehgruppe, von der wir ausgegangen sind, muß sie also an den Polen aus P_i größere Polordnungen haben. Wieder ist das unmöglich bei $(3,4)$, $(3,8)$, $(3,20)$, $(4,6)$ und $(5,12)$. □

Lemma 4.4.11. *Sind zwei endliche Drehgruppen vom selben Typ $(2,3,n)$ mit $n \geq 3$ gegeben und sind P_3 und $\tilde{P}_3$ jeweils zugehörige Polbahnen kleinstmöglicher Kardinalität, so gibt es eine Drehung, die P_3 in $\tilde{P}_3$ überführt.*

Beweis. Für die Operation der Drehgruppe $\mathrm{SO}(3)$ auf Paaren von Vektoren (p,q) durch $g(p,q) := (gp, gq)$ ist klar, daß die Standgruppe jedes linear unabhängigen Paars trivial ist. Gegeben eine endliche Untergruppe $G \subset \mathrm{SO}(3)$ und eine Bahn von Polen P_i ist insbesondere die Standgruppe eines Paars (p,q) mit $p \neq \pm q$ trivial. Nach dieser Vorüberlegung betrachten wir die drei Fälle der Reihe nach.

Im Fall $(2,3,3)$ haben wir $|P_3| = 4$. Folglich gibt es in $P_3 \times P_3$ ein Paar mit trivialer Standgruppe, das also eine 12-elementige Bahn hat, die wegen $|P_3 \times P_3| = 16$ notwendig aus allen (p,q) mit $p \neq q$ bestehen muß. Je zwei verschiedene Punkte aus P_3 haben also denselben Abstand. Ich hoffe, daß damit sowohl die Aussage des Lemmas im Fall $n = 3$ klar wird als auch, daß die Punkte aus P_3 die Ecken eines Tetraeders bilden.

Im Fall $(2,3,4)$ haben wir $|P_3| = 6$. Folglich gibt es in $P_3 \times P_3$ ein Paar mit trivialer Standgruppe, das also eine 24-elementige Bahn hat, die wegen $|P_3 \times P_3| = 36$ notwendig aus allen (p,q) mit $p \neq \pm q$ bestehen muß. Die anderen Bahnen müssen

aus Paaren mit nichttrivialer Standgruppe bestehen, und da die Bahn der sechs Paare der Gestalt (p,p) noch nicht genug Elemente liefert, muß auch noch eine Bahn aus Paaren der Gestalt $(p,-p)$ vorkommen. Wir sehen so einerseits, daß P_3 stabil ist unter Punktspiegelung am Ursprung, und andererseits, daß je zwei voneinander verschiedene Pole aus P_3, die sich nicht gegenüberliegen, denselben Abstand haben. So erkennen wir hoffentlich sowohl die Aussage des Lemmas im Fall $n = 4$ als auch, daß die Elemente von P_3 die Ecken eines Oktaeders bilden müssen.

Im Fall $(2,3,5)$ haben wir $|P_3| = 12$ und $|P_3 \times P_3| = 144$. Wieder haben wir an Bahnen in $|P_3 \times P_3|$ die zwölfelementige Bahn aller Paare (p,p), möglicherweise noch eine zwölfelementige Bahn aller Paare $(p,-p)$, und daneben nur Bahnen mit 60 Elementen. Es folgt, daß $P_3 \times P_3$ in vier Bahnen zerfällt, und zwar die Bahn der Paare gleicher Pole, die Bahn der Paare von sich gegenüberliegenden Polen, und zwei weitere Bahnen von Polpaaren. Nehmen wir irgendeinen Pol $p \in P_3$, so bilden die Bilder von jedem Pol $q \in P_3$ mit $q \neq \pm p$ unter den Drehungen aus unserer Gruppe mit Fixpunkt p ein regelmäßiges Fünfeck, denn die Polordnung der Pole aus P_3 war ja 5. Für zwei verschiedene Ecken eines regelmäßigen Fünfecks gibt es zwei Möglichkeiten für ihren Abstand, deren Verhältnis nebenbei bemerkt nach **??** oder elementargeometrischen Überlegungen gerade der goldene Schnitt ist. Unsere beiden 60-elementigen Bahnen müssen sich also im Abstand zwischen den Polen ihrer Paare unterscheiden. Zu jedem Pol aus P_3 gibt es damit außer dem Pol selbst und dem gegenüberliegenden Pol noch 5 „nahe“ Pole und 5 „weite“ Pole. Nun bilden zwei sich gegenüberliegende Pole aus P_3 mit jedem weiteren Pol ein Dreieck, das nach dem Satz des Thales bei diesem weiteren Pol einen rechten Winkel hat, wobei dieser Pol notwendig zu einem von unseren beiden sich gegenüberliegenden Polen nah sein muß und zum anderen weit, da ja zu jedem unserer sich gegenüberliegenden Pole von den zehn verbleibenden Polen fünf nah und fünf weit sein müssen. Da unser Dreieck eine Hypothenuse der Länge 2 hat, wird dadurch der Abstand zwischen nahen Polen und der zwischen weiten Polen bereits vollständig beschrieben und hängt insbesondere nicht von unserer Gruppe ab. Damit erkennen wir, daß im Fall $(2,3,5)$ die Bahn P_3 bestehen muß aus (1) zwei gegenüberliegenden Punkten N und $S = -N$ sowie (2) zwei regelmäßigen Fünfecken der fünf zu N nahen Pole und der fünf zu S nahen Pole mit jeweils von der speziellen Gruppe unabhängigem Abstand der Ecken dieser Fünfecke zu den jeweiligen Polen. Jede Ecke des „nördlichen“ Fünfecks muß aber auch einer Ecke des „südlichen“ Fünfecks gegenüberliegen. Unser Lemma folgt unmittelbar. □

Lemma 4.4.12 (Existenz der Ikosaedergruppe). *Es gibt endliche Untergruppen der Drehgruppe* $\mathrm{SO}(3)$ *mit Elementen der Ordnungen drei und fünf.*

Beweis. Wir betrachten die Menge $\mathcal{D} \subset \mathcal{P}(S^2)$ aller gleichseitigen Dreiecke mit Ecken auf der Einheitssphäre, die nicht in einer Ebene mit dem Ursprung liegen,

formal also

$$\mathcal{D} = \left\{ \{a,b,c\} \;\middle|\; \begin{array}{c} a,b,c \in \mathbb{R}^3,\ \|a\| = \|b\| = \|c\| = 1, \\ \|a-b\| = \|b-c\| = \|c-a\|, \\ \langle a,b,c\rangle_{\mathbb{R}} = \mathbb{R}^3. \end{array} \right\}$$

Gegeben ein Dreieck $\Delta \in \mathcal{D}$ und eine Ecke $a \in \Delta$ definieren wir das **umgeklappte Dreieck** $\Delta^a \in \mathcal{D}$ als das eindeutig bestimmte gleichseitige Dreieck $\Delta^a \in \mathcal{D}$ mit $\Delta \cap \Delta^a = \{b,c\}$. Definieren wir zu einem Dreieck $\Delta \in \mathcal{D}$ die Menge

$$\mathcal{D}(\Delta)$$

als die kleinste Teilmenge $\mathcal{D}(\Delta) \subset \mathcal{D}$, die Δ enthält und stabil ist unter dem Umklappen von Dreiecken, so gilt offensichtlich $\mathcal{D}(\Delta) = \mathcal{D}(\Delta')$ für alle $\Delta' \in \mathcal{D}(\Delta)$. Ist $r \in \mathrm{O}(3)$ orthogonal, so gilt sicher $\{ra, rb, rc\}^{ra} = r(\{a,b,c\}^a)$ für jedes Dreieck $\{a,b,c\} \in \mathcal{D}$, das mit r gedrehte Dreieck am Bild $r(a)$ der Ecke a umklappen liefert also dasselbe wie das an der Ecke a umgeklappte Dreieck mit r drehen, und insbesondere gilt $r(\mathcal{D}(\Delta)) = \mathcal{D}(r\Delta)$. Haben wir nun zusätzlich $|(r\Delta) \cap \Delta| \geq 2$, so folgt $r\Delta \in \mathcal{D}(\Delta)$ und damit $\mathcal{D}(r\Delta) = \mathcal{D}(\Delta)$. Nach diesen Vorüberlegungen gehen wir nun aus von einem regelmäßigen Fünfeck, bilden darauf die Pyramide mit Spitze N und aufsteigenden Kanten von derselben Länge wie die Kanten des Fünfecks, und schrumpfen oder strecken diese Pyramide so, daß wir sie als „Polkappe“ in die Einheitssphäre legen können. Dann gehen offensichtlich die fünf gleichseitigen Dreiecke dieser Polkappe durch Umklappen auseinander hervor. Bezeichne $\mathcal{D}^* \subset \mathcal{D}$ die kleinste unter Umklappen stabile Menge von Dreiecken, die diese fünf Dreiecke umfaßt. Wir zeigen im folgenden, daß $\mathcal{D}^*$ endlich ist: Dann bilden alle Drehungen, die $\mathcal{D}^*$ in sich überführen, offensichtlich eine endliche Untergruppe der Drehgruppe mit Elementen der Ordnungen drei und fünf und wir sind fertig. Um zu zeigen, daß $\mathcal{D}^*$ endlich ist, bilden wir zu $\mathcal{D}^*$ einen Graphen im Sinne von 4.4.22 wie folgt: Als Graphenecken nehmen wir alle fünfelementigen Teilmengen von $\mathcal{D}^*$ vom Typ „Polkappe“, die also aus einem festen Dreieck mit ausgezeichneter Ecke durch wiederholtes Umklappen unter Festhalten dieser einen ausgezeichneten Ecke gewonnen werden können. Nun verbinden wir zwei verschiedene derartige Graphenecken durch eine Graphenkante genau dann, wenn sie mindestens ein Dreieck gemeinsam haben. So erhält man aus $\mathcal{D}^*$ einen zusammenhängenden Graphen mit den Eigenschaften aus Übung 4.4.22: Jede Graphenecke hat genau fünf Nachbarn, und je zwei benachbarte Graphenecken haben genau zwei gemeinsame Nachbarn. Nach Übung 4.4.22 ist ein zusammenhängender Graph mit diesen Eigenschaften jedoch endlich und damit muß auch unsere Menge von Dreiecken $\mathcal{D}^*$ endlich gewesen sein. □

Ergänzung 4.4.13. Die obigen Überlegungen kann man dahingehend zusammenfassen, daß gegeben ein gleichseitiges Dreieck $\Delta = \{a,b,c\}$, für das es eine Drehung r um die Ursprungsgerade durch a gibt mit $r^5 = \mathrm{id}$ und $r : b \mapsto c$, die

Menge $\mathcal{D}(\Delta)$ der daraus durch Umklappen entstehenden Dreiecke endlich ist. Die hier geforderte Eigenschaft hat sicher jedes Dreieck, das anschaulich gesprochen „Fläche eines Ikosaeders“ ist. Es gibt aber auch noch andere gleichseitige Dreiecke mit dieser Eigenschaft, nämlich diejenigen gleichseitigen Dreiecke, die anschaulich gesprochen die „Diagonale unseres Ausgangsfünfecks“ als Seitenlänge haben.

Ergänzung 4.4.14. Mit welchen platonischen Körpern kann man den Raum füllen? Ich vermute, das geht nur mit Würfeln: Die anderen sollten als Winkel zwischen an einer Kante angrenzenden Flächen nie einen Winkel der Gestalt $2\pi/n$ haben.

Ergänzung 4.4.15. Vielleicht ist es vernünftig, platonische Körper zu definieren über die Mengen ihrer Ecken, die man wohl wie folgt charakterisieren kann: Man definiere für eine endliche Teilmenge E des Raums ihre **Abständezahl** $A(E)$ als die Zahl der möglichen von Null verschiedenen verschiedenen Abstände zwischen ihren Elementen. Eine endliche Teilmenge E einer Sphäre heißt nun Tetraeder bei $|E| = 4$, $A(E) = 1$, Würfel bei $|E| = 8$, $A(E) = 3$, Oktaeder bei $|E| = 6$, $A(E) = 2$, Ikosaeder bei $|E| = 12$, $A(E) = 3$, Dodekaeder bei $|E| = 20$, $A(E) = 4$. Stimmt das eigentlich? Möglicherweise sollte man bei allen außer dem Tetraeder noch fordern, daß E stabil ist unter Punktspiegelung am Ursprung.

Übungen

Übung 4.4.16. Man berechne den Cosinus des Winkels zwischen zwei Seitenflächen eines Tetraeders. Hinweis: Man argumentiere, daß die Normalenvektoren auf die Flächen eines Tetraeders die Ecken eines Tetraeders bilden. Man bemerke, daß die Standardbasisvektoren im $\mathbb{R}^4$ einen Tetraeder bilden. Wieviele Tetraeder kann man längs einer gemeinsamen Kante zusammenlegen? Bleibt dann noch Luft? Hier mag ein Taschenrechner helfen.

Weiterführende Übung 4.4.17. Gegeben ein zusammenhängender ebener Graph, bei dem an jeder Ecke drei Kanten ankommen, leite man aus der Eulerschen Formel $E - K + F = 2$ her, daß es eine Fläche mit höchstens fünf Kanten geben muß. Hier haben wir die unbeschränkte Fläche mitgezählt.

Ergänzende Übung 4.4.18 (**Kristallgitter des Diamants**). Seien $v_1, \ldots, v_4$ Richtungsvektoren des dreidimensionalen Anschauungsraums, die vom Schwerpunkt eines Tetraeders zu seinen vier Ecken zeigen. Wir betrachten alle Linearkombinationen $\sum_{i=1}^4 n_i v_i$ mit $\sum_{i=1}^4 n_i \in \{0, 1\}$ und behaupten, daß diese Linearkombinationen gerade die Punkte beschreiben, an denen in einem Diamant die Kohlenstoffatome sitzen. In der Tat sind unsere Linearkombinationen paarweise verschieden, die „einzige“ Relation $v_1 + v_2 + v_3 + v_4 = 0$ unserer Vektoren führt aufgrund unserer Einschränkungen nicht zu Mehrdeutigkeiten, und unsere Linearkombinationen lassen sich auch beschreiben als die Elemente des von den

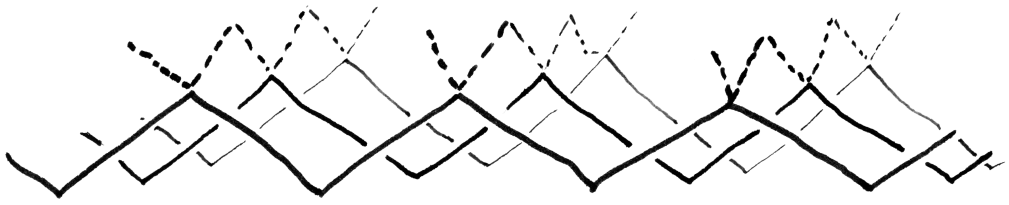
Richtungsvektoren $v_1 - v_2, v_1 - v_3$ und $v_1 - v_4$ erzeugten Gitters mitsamt dem um v_1 verschobenen Gitter. Jeder Punkt hat vier nächste Nachbarn, der Nullpunkt etwa $v_1, \ldots, v_4$, und zu diesen ist er gebunden im Diamantkristall. Anschaulich mag man sich eine Lage von parallelen horizontalen Zick-Zack-Linien denken, die Zick-Zacks darin nach oben und unten, dann eine weitere horizontale Lage senkrecht dazu, bei denen die Tiefpunkte immer gerade die Hochpunkte der Lage darunter berühren, und so weiter, und schließlich an jedem dieser Berührungspunkte ein Kohlenstoffatom.

Ergänzende Übung 4.4.19. Man konstruiere einen surjektiven Gruppenhomomorphismus $\mathcal{S}_4 \twoheadrightarrow \mathcal{S}_3$. Hinweis: Geometrisch mag man sich die $\mathcal{S}_4$ nach 4.4.8 als die Gruppe der Symmetriebewegungen eines Würfels denken und den fraglichen Gruppenhomomorphismus konstruieren über die Operation dieser Gruppe auf der Menge der drei Mittelsenkrechten auf den Flächen des Würfels. Später werden wir verstehen, daß dieser Homomorphismus etwas ganz besonderers ist: Surjektive nicht bijektive Gruppenhomomorphismen $\mathcal{S}_n \twoheadrightarrow G$ einer symmetrischen Gruppe auf irgendeine andere Gruppe gibt es unter der Annahme $n \geq 5$ nur für $|G| = 2$ und dann jeweils nur genau Einen, vergleiche 5.6.9.

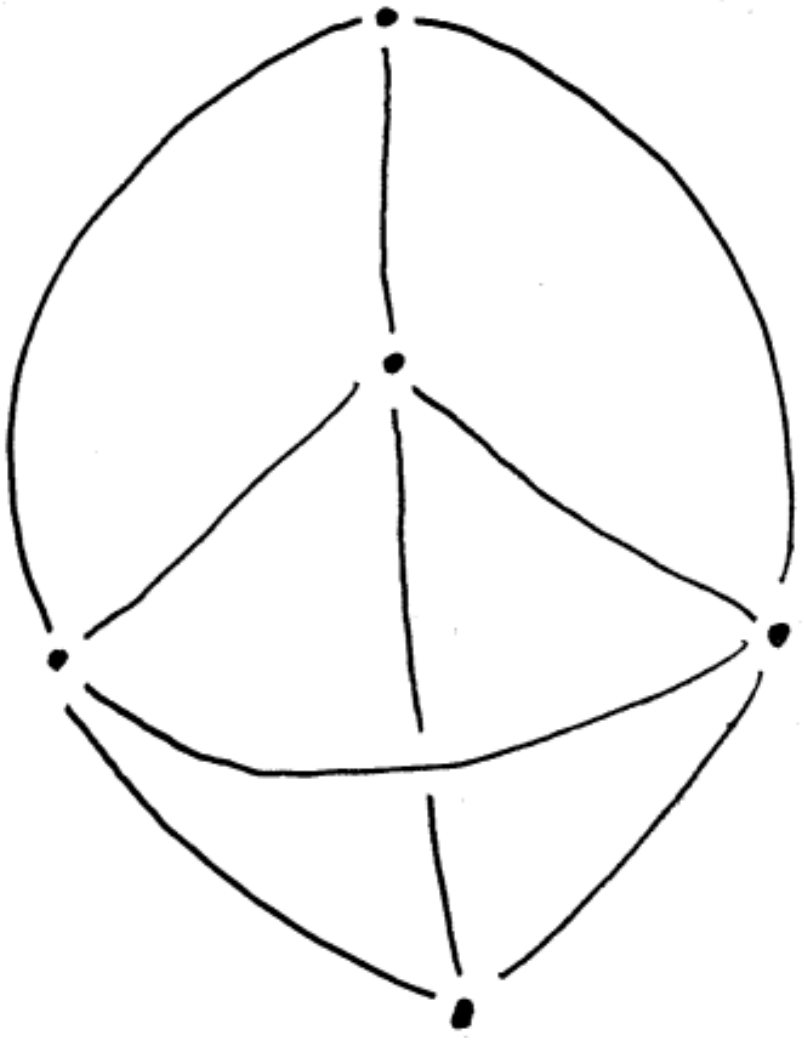
Ergänzende Übung 4.4.20. Die Multiplikation definiert einen Isomorphismus zwischen der Gruppe aller Symmetrien aus $\mathrm{O}(3)$ eines Ikosaeders und dem Produkt der Gruppe seiner Symmetriebewegungen mit der zweielementigen Gruppe, die von der Punktspiegelung am Ursprung erzeugt wird. Insbesondere ist die „nichtorientierte Ikosaedergruppe“ keineswegs isomorph zur symmetrischen Gruppe $\mathcal{S}_5$.

4.4.21. Unter einem **Graphen** oder genauer einem **kombinatorischen Graphen** (ungerichtet, ohne mehrfache Kanten, ohne Schleifen) verstehen wir ein Paar (E, K) bestehend aus einer Menge E und einem System $K \subset \mathcal{P}(E)$ von zweielementigen Teilmengen von E. Die Elemente von E heißen die **Ecken** unseres Graphen, die Elemente von K seine **Kanten**. Zwei verschiedene Ecken, die zu einer gemeinsamen Kante gehören, heißen **benachbart**. Ein **Isomorphismus** zwischen zwei Graphen ist eine Bijektion zwischen ihren Eckenmengen, die eine Bijektion zwischen ihren Kantenmengen induziert. Zwei Graphen heißen **isomorph**, wenn es zwischen ihnen einen Isomorphismus gibt. Die Äquivalenzklassen der kleinsten Äquivalenrelation auf der Eckenmenge eines Graphen, unter der benachbarte Elemente äquivalent sind, heißen die **Zusammenhangskomponenten** unseres Graphen. Ein Graph heißt **zusammenhängend**, wenn er aus einer einzigen Zusammenhangskomponente besteht.

Übung 4.4.22. Man zeige: Ein zusammenhängender Graph, in dem jede Ecke genau fünf (vier, drei) Nachbarn besitzt und je zwei benachbarte Ecken genau zwei gemeinsame Nachbarn, ist notwendig endlich und sogar isomorph zu jedem weiteren Graphen mit diesen beiden Eigenschaften. Den so charakterisierten Graphen



Versuch einer graphischen Darstellung der räumlichen Struktur des Diamantkristalls. Die durchgezogenen und gestrichelten Linien sind nur der Transparenz halber verschiedenartig gezeichnet und bedeuten die Bindungen zwischen den Kohlenstoffatomen, die jeweils an den Ecken der Zick-Zack-Linien sitzen. Die hier gezeichnete Struktur gilt es nun übereinanderzuschichten, so daß sich jeweils die Ecken treffen.



Ein zusammenhängender Graph mit fünf Punkten, von denen drei vier Nachbarn haben und zwei nur drei Nachbarn. Die beiden Punkte „auf halber Höhe auf dem Rand“ haben drei gemeinsame Nachbarn.

mag man den „Kantengraphen des Ikosaeders (Oktaeders, Tetraeders)“ nennen. Hinweis: Ausprobieren.

Übung 4.4.23 (**Endliche Untergruppen der** $\mathrm{SU}(2)$). Man zeige, daß die Gruppe $\mathrm{SU}(2)$ nur zwei Elemente g besitzt mit $g^2 = 1$, nämlich $g = \pm \mathrm{id}$. Man zeige, daß jede endliche Untergruppe ungerader Kardinalität n von $\mathrm{SU}(2)$ konjugiert ist zur Untergruppe $\{\mathrm{diag}(\zeta^r, \zeta^{-r}) | 1 \leq r \leq n\}$ für $\zeta = \exp(2\pi\mathrm{i}/n)$. Man zeige, daß die endlichen Untergruppen gerader Kardinalität von $\mathrm{SU}(2)$ genau die Urbilder von endlichen Untergruppen von $\mathrm{SO}(3)$ unter unserer Surjektion $\mathrm{SU}(2) \twoheadrightarrow \mathrm{SO}(3)$ aus **??** sind, die wir nach 4.4.2 bereits kennen. Das benötigt den Satz von Cauchy 4.1.35.

Übung 4.4.24 (**Ikosaeder**). Es gibt in der Einheitssphäre zwölfelementige Teilmengen, die stabil sind unter der Drehung mit den Winkeln $\pm 2\pi/5$ um die Ursprungsgeraden durch jeden ihrer Punkte, und je zwei derartige Teilmengen lassen sich durch eine Drehung ineinander überführen.

Übung 4.4.25 (**Endliche Untergruppen der Isometriegruppe des Raums**). Jede Wahl eines von Null verschiedenen Richtungsvektors versieht den Anschauungsraum mit einer Metrik. Alle diese Metriken unterscheiden sich nur um eine positive reelle Konstante und liefern folglich dieselben Isometrien. Die Gruppe aller Isometrien des Anschauungsraums ist damit wohldefiniert. Sie kann im übrigen auch beschrieben werden als die von allen Bewegungen und allen Punktspiegelungen erzeugte Gruppe von Selbstabbildungen. Diejenigen Isometrien des Anschauungsraums, die eine gegebene Teilmenge festhalten, nenne ich ihre **Isometriesymmetrien** oder im folgenden auch kurz **Symmetrien**. Man zeige, daß jede endliche Untergruppe der Gruppe der Isometrien alias abstandserhaltenden Selbstabbildungen des Anschauungsraums konjugiert ist zu genau einer Untergruppe der folgenden Liste:

1. Der Gruppe aller Symmetrien beziehungsweise Symmetriebewegungen eines Tetraeders, Würfels, oder Ikosaeders, insgesamt 6 Fälle mit den Kardinalitäten 24, 12, 48, 24, 120, 60;

2. Der Gruppe aller Symmetrien bzw. Symmetriebewegungen eines regelmäßigen k-eckigen Bierdeckels, $k \geq 3$, also 2 Fälle für jedes k von Gruppen der Kardinalitäten $4k$ und $2k$;

3. Der Gruppe aller Symmetrien beziehungsweise Symmetriebewegungen einer regelmäßigen k-eckigen Schale, $k \geq 3$, also 2 Fälle für jedes k von Gruppen der Kardinalitäten $2k$ und k;

4. Der Gruppe aller Symmetrien beziehungsweise Symmetriebewegungen, die von einem Tripel bestehend aus drei durch einen gemeinsamen Punkt laufenden paarweise orthogonalen Geraden jede der drei Geraden stabilisieren

und eine beziehungsweise zwei dieser Geraden punktweise festhalten. In Formeln übersetzt und nach den entsprechenden Identifikationen also einer der Untergruppen $\mathrm{diag}(\pm 1, 1, 1)$, $\mathrm{diag}(\pm 1, \pm 1, 1)$, $\mathrm{diag}(\pm 1, \pm 1 \pm 1)$ oder ihrer Schnitte mit der Drehgruppe $\mathrm{SO}(3)$, insgesamt 6 Fälle mit den Kardinalitäten 2, 1, 4, 2, 8, 4;

Übung 4.4.26 (**Existenz des Ikosaeders, Alternative**). Die Würfelgruppe ist isomorph zur Gruppe $\mathcal{S}_4$ aller Permutationen seiner Raumdiagonalen. Die Drehungen an Raumdiagonalen erzeugen darin die Untergruppe A_4 aller geraden Permutationen seiner Raumdiagonalen. Es gibt zwei Möglichkeiten, jeder Fläche des Würfels ein Paar von parallelen Kanten derselben Fläche so zuzuordnen, daß diese Wahl stabil ist unter A_4. Jetzt sollen einige der Kanten des Ikosaeders in der Mitte der Flächen unseres Würfels liegen, parallel zu den jeweils ausgewählten beiden Kanten, und nun muß man nur noch ihre Länge so bestimmen, daß die Abstände zwischen „benachbarten Kantenenden“ gleich der Kantenlängen sind. Man muß dann allerdings noch etwas argumentieren, um zu zeigen, daß die so gewonnene Menge von „Ecken des Ikosaeders“ Symmetrien der Ordnung fünf hat.

4.5 Diskussion der Eulerformel*

4.5.1. Indem man bei unseren platonischen Körpern die Zahlen E, K, F der Ecken, Kanten und Flächen bestimmt, prüft man unmittelbar in allen fünf Fällen die **Eulerformel**

$$E - K + F = 2$$

Diese Beziehung gilt allgemeiner für jede „kompakten konvexen dreidimensionalen Polyeder“, nur habe ich gar nicht definiert, was das eigentlich sein soll, und habe selbst bei den platonischen Körpern nur definiert, was für Teilmengen des Raums nun diesen Namen verdienen sollen, und nicht, wie denn nun die „Kanten“ oder „Flächen“ dieser Gebilde definiert werden sollen, die wir bereits so unbekümmert gezählt haben. Eine Formalisierung des Begriffs eines „dreidimensionalen konvexen Polyeders“ und seiner „Ecken, Kanten und Flächen“ wird in **??** ausgeführt, aber das schien mir hier unangemessen und sogar irreführend, da unsere Eulerformel anderer Natur ist. Im folgenden formuliere ich sehr präzise eine sehr allgemeine Fassung dieser Formel, gebe jedoch statt eines Beweises nur einige sehr unvollkommene heuristische Argumente.

4.5.2. Ich erinnere den Begriff eines Homöomorphismus aus **??**. Man bemerke, daß $\mathbb{R}^2$ nicht homöomorph ist zu $\mathbb{R}^1$. In $\mathbb{R}^2$ ist nämlich das Komplement jedes Punktes zusammenhängend, in $\mathbb{R}^1$ dahingegen ist das Komplement jedes Punktes unzusammenhängend.

Satz 4.5.3 (**Topologische Eulerformel**). *Sei* $S^2 = A_1 \sqcup \ldots \sqcup A_n$ *eine Zerlegung der Einheitssphäre* $S^2 := \{x \in \mathbb{R}^3 \mid \|x\| = 1\}$ *in endlich viele paarweise disjunkte Teilmengen* A_i*, die die beiden folgenden Eigenschaften hat:*

1. *Für jeden Index* i *ist* $A_1 \sqcup \ldots \sqcup A_i$ *abgeschlossen in* S^2*;*
2. *Jedes* A_i *ist homöomorph zu* $\mathbb{R}^2$ *oder* $\mathbb{R}^1$ *oder* $\mathbb{R}^0$ *alias einem Punkt.*

So gilt die **Euler-Formel** $E - K + F = 2$ *für* E, F *und* K *die Zahl der jeweils zu* $\mathbb{R}^0, \mathbb{R}^1$ *und* $\mathbb{R}^2$ *homöomorphen* A_i*.*

4.5.4. Die Bezeichnungen E, K und F stehen für „Ecken, Kanten und Flächen“. Man prüft die Formel leicht explizit für die durch die Zentralprojektion eines platonischen Körpers auf die Einheitssphäre gegebene Zerlegung derselben in die Bilder seiner Ecken, Kanten und Flächen. Besitzt allgemeiner ein lokal kompakter Hausdorffraum X eine Zerlegung

$$X = A_1 \sqcup \ldots \sqcup A_n$$

in endlich viele paarweise disjunkte Teilmengen derart, daß für jeden Index i gilt $A_1 \sqcup \ldots \sqcup A_i \not\subset X$ und daß jedes A_i homöomorph ist zu $\mathbb{R}^{d(i)}$ für ein $d(i) \geq 0$, so ist $\sum_i (-1)^{d(i)}$ unabhängig von der Wahl einer derartigen Zerlegung. Den Beweis der topologischen Euler-Formel 4.5.3 und auch dieser allgemeineren Aussage für beliebige lokal kompakte Hausdorffräume können Sie in **??** finden. Er benötigt vertiefte Kenntnisse in Topologie.

4.5.5 (**Diskussion einiger nicht erlaubter Zerlegungen**). Um die Aussage des Satzes herauszuarbeiten, will ich einige nicht erlaubte Zerlegungen angeben. Betrachten wir die ganze Einheitssphäre als eine einzige Fläche, so gilt unsere Formel sicher nicht. Die Einheitssphäre ist aber auch nicht homöomorph zu $\mathbb{R}^2$, zum Beispiel, da sie kompakt ist. Zerlegen wir die Einheitssphäre in den Äquator und die beiden Hemisphären, so gilt unsere Formel ebensowenig. Der Äquator ist aber auch nicht homöomorph zu $\mathbb{R}^1$, zum Beispiel, da er kompakt ist. Zerlegen wir den Äquator in einen Punkt und eine Kante, so gelten unserer Annahmen und unsere Formel. Malen wir noch einen zweiten in derselben Weise zerlegten Äquator daneben, so wird sie wieder falsch. Das liegt daran, daß die „ringförmige Fläche“ zwischen unseren beiden Äquatoren nicht homöomorph ist zu $\mathbb{R}^2$, was hier nicht formal gezeigt werden soll. Verbinden wir aber die beiden ausgewählten Punkte auf unseren beiden Äquatoren noch durch eine Kante, so wir unsere Formel wieder richtig und die Bedingungen des Satzes sind auch wieder erfüllt.

4.5.6 (**Heuristische Begründung der Eulerformel**). Wir gehen aus von der Zerlegung der Einheitssphäre in einen Punkt und sein Komplement. In diesem Fall gilt die Eulerformel. Jetzt argumentieren wir induktiv und gehen von einer Zerlegung der Einheitssphäre in Ecken, Kanten und Flächen aus, in der wir die Eulerformel bereits geprüft haben.

1. Ergänzen wir eine Ecke, indem wir eine bereits existierende Kante in zwei Kanten zerteilen, so entsteht eine neue Zerlegung mit einer zusätzlichen Ecke und einer zusätzlichen Kante.

2. Ergänzen wir eine Kante, indem wir zwei Ecken auf dem Rand einer bereits vorhandenen Fläche innerhalb dieser Fläche durch eine Kante verbinden, so entsteht eine neue Zerlegung mit einer zusätzlichen Kante und einer zusätzlichen Fläche, da ja unsere Fläche von unserer neuen Kante in zwei Teile geschnitten wird.

Induktiv folgt so die Eulerformel für alle Zerlegungen der Einheitssphäre in Ecken, Kanten und Flächen, die wir auf diese Weise induktiv konstruieren können. Die Schwäche der vorhergehenden Argumentation ist zusätzlich zur allgemeinen Unschärfe der darin verwendeten Begriffe, daß nicht klar ist, welche Zerlegungen der Einheitssphäre in Ecken, Kanten und Flächen wir denn mit dem im Beweis beschriebenen Verfahren induktiv erreichen können. Da aber diese Fragen nur mit dem Aufbau eines entsprechend starken Begriffsapparats befriedigend geklärt werden können, will ich sie hier nicht weiter verfolgen.

4.6 Bruhatzerlegung*

Satz 4.6.1 (Bruhatzerlegung). *Gegeben ein Kring R und eine natürliche Zahl $n \geq 1$ zerfällt die Gruppe $\mathrm{GL}(n;R)$ unter der beidseitigen Operation der Untergruppe der invertierbaren oberen Dreiecksmatrizen $B \subset \mathrm{GL}(n;R)$ in die disjunkte Vereinigung*

$$\mathrm{GL}(n;R) = \bigsqcup_{w \in \mathcal{S}_n} BwB$$

der Doppelnebenklassen der Permutationsmatrizen.

Beweis. Multiplikation mit oberen Dreicksmatrizen von rechts bedeutet solche Spaltenoperationen, bei denen eine Spalte mit einem invertierbaren Skalar multipliziert oder ein Vielfaches einer Spalte zu einer Spalte weiter rechts addiert wird. Ähnlich bedeutet die Multiplikation mit oberen Dreicksmatrizen von links solche Zeilenoperationen, bei denen eine Zeile mit einem invertierbaren Skalar multipliziert oder ein Vielfaches einer Zeile zu einer Zeile weiter oben addiert wird. Also besteht für jede Permutationsmatrix w die Nebenklasse Bw aus gewissen „Zahnlückenmatrizen“ und die Nebenklasse wB aus gewissen „Regaleinräummatrizen“, wie nebenstehendes Bild andeuten mag. Man erkennt so einerseits, daß aus $Bw \cap vB \neq \emptyset$ folgt $v(i) \leq w(i)$ für $1 \leq i \leq n$, wobei wir unsere Permutationsmatrizen nun als echte Permutationen aufgefaßt haben. Das zeigt $v = w$ und wir erkennen, daß die Doppelnebenklassen BwB für $w \in \mathcal{S}_n$ paarweise disjunkt sind. Andererseits können wir eine beliebige invertierbare Matrix g durch

Davormultiplizieren von $b \in B$ stets in eine Regaleinräummatrix transformieren: Wir beginnen dazu mit der ersten Spalte, nehmen darin den tiefsten von Null verschiedenen Eintrag, und benutzen Zeilenoperationen „nach oben“, um alle Einträge darüber auch auszuräumen. Dann streichen wir die Zeile dieses Eintrags und machen immer so weiter. Das zeigt, daß die Doppelnebenklassen BwB auch die ganze Gruppe überdecken. □

4.6.2. Für die meisten Matrizen g wird der tiefste von Null verschiedene Eintrag jedesmal in der untersten noch nicht gestrichenen Zeile auftauchen. Dann liegt die Matrix in der Doppelnebenklasse $Bw_\circ B$ der Permutationsmatrix mit Einsen in der Nebendiagonalen und Nullen sonst. Die zugehörige Permutation $w_\circ \in \mathcal{S}_n$ ist die Permutation, die „die Reihenfolge umdreht“. Diese Doppelnebenklasse heißt die **dicke Zelle**.

Ergänzung 4.6.3. Sei weiter $w_\circ$ die Permutationsmatrix mit Einsen in der Nebendiagonalen und Nullen sonst, der also die Permutation $w_\circ \in \mathcal{S}_n$ entspricht, die „die Reihenfolge umdreht“. Dann besteht $L := w_\circ B w_\circ$ genau aus allen invertierbaren unteren Dreiecksmatrizen. Die mit $w_\circ$ verschobene dicke Zelle kann also auch beschrieben werden als

$$w_\circ B w_\circ B = LB$$

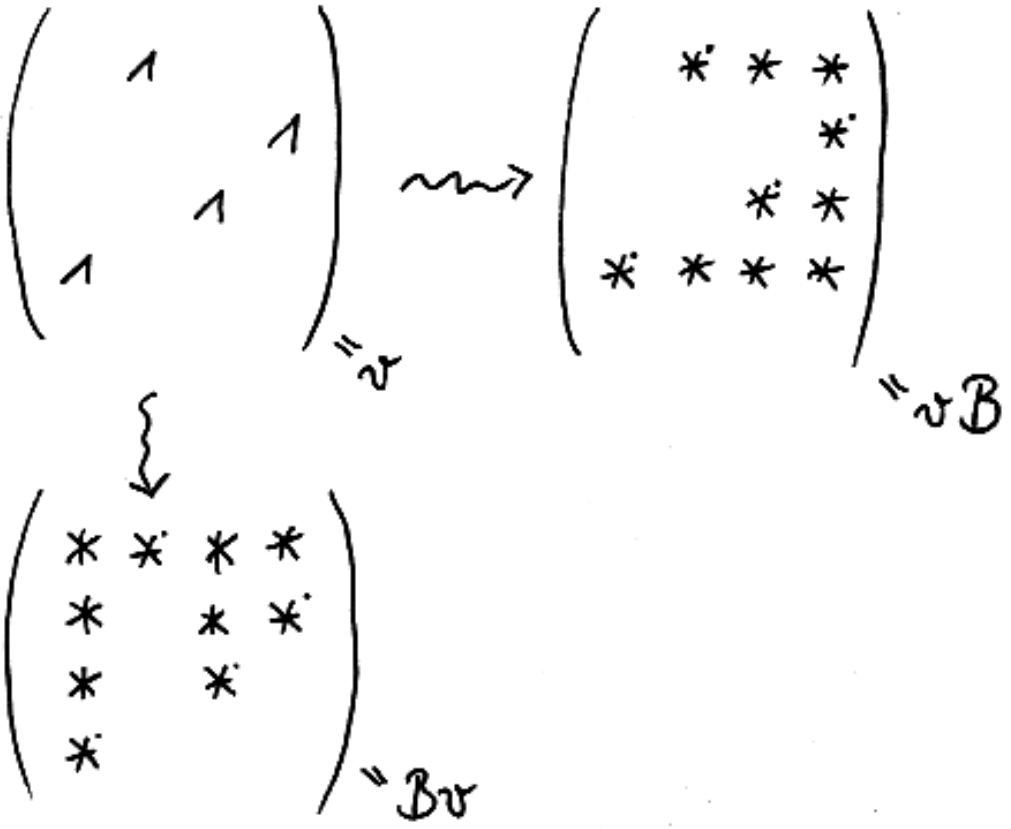
Bezeichnet $U := \mathrm{U}(n; R)$ die Menge aller oberen Dreiecksmatrizen mit Einsen auf der Diagonale, so besteht $L \cap U$ nur aus der Einheitsmatrix und wir haben $LU = LB$. Mithin liefert die Multiplikation eine Bijektion

$$L \times U \xrightarrow{\sim} LB$$

auf die mit $w_\circ$ verschobene dicke Zelle. In der Numerik nennt man diese Darstellung einer Matrix aus der verschobenen dicken Zelle LB als Produkt einer unteren mit einer oberen Dreiecksmatrix die **LR-Zerlegung** für „Links-Rechts“ oder **LU-Zerlegung** für „lower-upper“. Allgemeiner zeigt man, daß für eine beliebige Permutation $w \in \mathcal{S}_n$ die Abbildung $(a, u) \mapsto awu$ eine Bijektion

$$L \times (U \cap w^{-1}Uw) \xrightarrow{\sim} LwB$$

liefert. Die Surjektivität folgt hierbei in den Notationen von 3.1.12 aus der Erkenntnis, daß das Aufmultiplizieren in einer beliebigen aber festen Reihenfolge eine Bijektion $\prod_{i<j,\, w(i)>w(j)} U_{ij} \times (U \cap w^{-1}Uw) \xrightarrow{\sim} U$ liefert und daß gilt $wU_{ij} = U_{w(i)w(j)}w \in Lw$ für alle Faktoren des großen Produkts.



Die Nebenklassen einer Permutationsmatrix unter der Operation der oberen Dreiecksmatrizen. Das Symbol $*$ steht für einen beliebigen Matrixeintrag, das Symbol $*\cdot$ für einen invertierbaren Matrixeintrag.

4.6.1 Übungen

Übung 4.6.4. Seien R ein Ring. Wir betrachten in $\mathrm{GL}(n;R)$ die Untergruppen B, U und $U^- := w_\circ U w_\circ$ der obereren Dreiecksmatrizen, oberen Dreiecksmatrizen mit Einsen auf der Diagonale und unteren Dreiecksmatrizen mit Einsen auf der Diagonale. Man zeige, daß für jedes $w \in \mathcal{S}_n$ die Abbildung $(b,u) \mapsto bwu$ eine Bijektion

$$B \times (U \cap w^{-1}U^- w) \tilde{\to} BwB$$

induziert. Man zeige: Für je zwei Permutationen $v, w \in \mathcal{S}_n$ mit $l(vw) = l(v) + l(w)$ für $l(\sigma)$ wie in **??** die Zahl der Fehlstände einer Permutation σ liefert die Multiplikation eine Bijektion

$$BvB \times_{/B} BwB \tilde{\to} BvwB$$

des balancierten Produkts nach 4.2.6 unserer Doppelnebenklassen mit einer weiteren Doppelnebenklasse. Ist dahingegen $s \in \mathcal{S}_n$ eine Permutation mit nur einem Fehlstand und $w \in \mathcal{S}_n$ beliebig und gilt $l(sw) \leq l(w)$, so haben wir $l(sw) = l(w) - 1$ und

$$BsBwB = BswB \sqcup BwB$$

Übung 4.6.5. Genau dann besitzt eine invertierbare quadratische Matrix mit Koeffizienten in einem Kring eine LU-Zerlegung, wenn alle Untermatrizen, die durch Streichen von hinteren Spalten und gleichviel unteren Zeilen entstehen, alle auch invertierbar sind.

5 Mehr zu Gruppen

5.1 Die Frage nach der Klassifikation

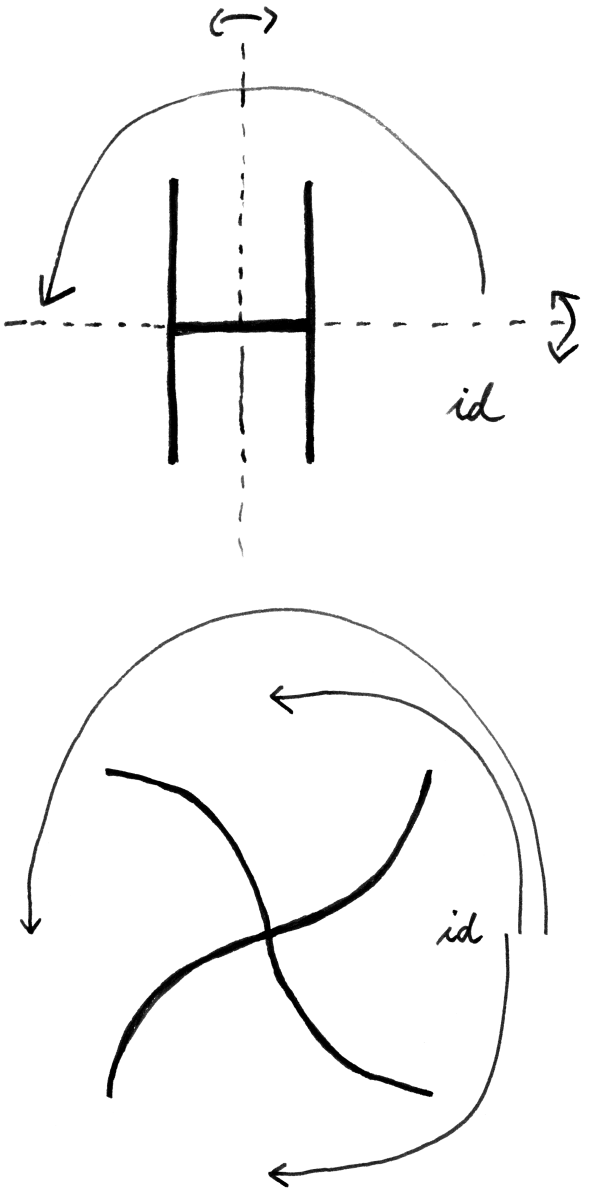
5.1.1. Ich erinnere an die Definition **??**. Eine **Gruppe** ist eine Menge G mit einer Verknüpfung $G \times G \to G$, $(a, b) \mapsto ab$ derart, daß für alle $a, b, c \in G$ gilt $(ab)c = a(bc)$, daß es ein Element $1 \in G$ gibt mit $1a = a1 = a\ \forall a \in G$, und daß es für alle $a, b \in G$ ein Element $c \in G$ gibt mit $ac = b$. Gegeben eine weitere Gruppe H ist ein **Gruppenhomomorphismus** $\varphi : G \to H$ eine Abbildung von G nach H mit $\varphi(ab) = \varphi(a)\varphi(b)$ für alle $a, b \in G$. Die Menge aller Gruppen homomorphismen von G nach H notiere ich $\mathrm{Grp}(G, H)$.

5.1.2. Wir wollen im folgenden der Frage nachgehen, welche endlichen Gruppen „es überhaupt gibt“. Wir nennen zwei Gruppen **isomorph**, wenn es zwischen ihnen einen Isomorphismus als da heißt einen bijektiven Homomorphismus gibt. Die Frage, welche endlichen Gruppen es überhaupt gibt, können wir dann konkret fassen als die folgende Aufgabe: Man gebe eine Liste von endlichen Gruppen an derart, daß jede beliebige endliche Gruppe isomorph ist zu genau einer Gruppe dieser Liste. In mathematischer Terminologie ist das die Frage nach der **Klassifikation der endlichen Gruppen**.

Beispiel 5.1.3. Für Gruppen mit höchstens 4 Elementen können wir diese Aufgabe noch ohne alle Theorie auf direktem Wege lösen. Eine endliche Menge mit Verknüpfung beschreiben wir dazu durch ihre Verknüpfungstabelle, die im Fall einer Gruppe auch **Gruppentafel** heißt. Zum Beispiel bilden die dritten Einheitswurzeln 1, $\zeta = \exp(2\pi\,\mathrm{i}\,/3)$ und $\eta = \exp(4\pi\,\mathrm{i}\,/3)$ in $\mathbb{C}$ unter der Multiplikation eine Gruppe mit der Gruppentafel

	1	ζ	η
1	1	ζ	η
ζ	ζ	η	1
η	η	1	ζ

Bei einer Gruppentafel muß nach der Kürzungsregel **??** in jeder Spalte und in jeder Zeile jedes Element genau einmal vorkommen. Man sieht so recht leicht, daß es bis auf Isomorphismus nur eine Gruppe G gibt mit $|G|$ Elementen für $|G| = 1, 2, 3$. Man sieht so auch, daß es für $|G| = 4$ bis auf Isomorphismus genau zwei Möglichkeiten gibt, die sich dadurch unterscheiden, ob jedes Element sein eigenes Inverses ist oder nicht: Je nachdem haben wir, bis auf Isomorphismus, die sogenannte **Klein'sche Vierergruppe** $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ oder die zyklische Gruppe $\mathbb{Z}/4\mathbb{Z}$ vor uns.



Die vier Symmetrien des Buchstabens H und des Sonnenrads, das wohl nicht zuletzt auch wegen seiner Symmetriegruppe so unvermittelt an furchtbare Zeiten der deutschen Geschichte erinnert.

5.1.4. Warum interessieren wir uns überhaupt für Gruppen? Stellen wir uns doch einmal eine ebene Figur vor, zum Beispiel eine stilisierte Blüte, einen Buchstaben, oder allgemein eine beliebige Teilmenge der Ebene $A \subset \mathbb{R}^2$. Unter einer „Symmetriebewegung“ oder kurz **Symmetrie** unserer Figur verstehen wir eine abstandserhaltende Selbstabbildung g der Ebene, die unsere Figur in sich selber überführt, in Formeln $gA = A$. Alle Symmetrien unserer Figur bilden unter der Hintereinanderausführung als Verknüpfung eine Gruppe, die **Symmetriegruppe** der Figur. Bei den meisten Figuren besteht die Symmetriegruppe nur aus einem Element, der Identität, aber ein Herz hat schon zwei Symmetrien, die Identität und eine Spiegelung. Der Buchstabe H hat sogar 4 Symmetrien, ebensoviele wie das Sonnenrad, aber die Symmetriegruppen dieser beiden Figuren sind nicht isomorph. In diesem Sinne kann man das Konzept einer Gruppe interpretieren als eine Formalisierung der Idee eines „abstrakten Symmetrietyps“.

5.2 Kompositionsreihen

5.2.1. Ich erinnere an Restklassen 3.1, Normalteiler 3.2, Gruppenwirkungen 4.1.1, Bahnformel 4.2 und Konjugationsklassen 4.3.

Definition 5.2.2. Eine Gruppe heißt **einfach**, wenn sie nicht nur aus dem neutralen Element besteht, aber außer dem neutralen Element und der ganzen Gruppe keine weiteren Normalteiler hat.

Beispiele 5.2.3. Beispiele einfacher Gruppen sind die zyklischen Gruppen von Primzahlordnung und die sogenannten **alternierenden Gruppen**

$$A_r := \ker(\operatorname{sgn} : \mathcal{S}_r \to \{\pm 1\})$$

aller geraden Permuationen von r Objekten unter der Annahme $r \geq 5$, wie wir als Satz 5.6.2 zeigen werden. Nicht zeigen werden wir, daß die alternierende Gruppe A_5 die kleinste nichtabelsche einfache Gruppe ist. Diese Gruppe ist übrigends genau unsere Ikosaedergruppe aus 4.4.2 aller Drehsymmetrien eines Ikosaeders, was wir im anschließenden Satz 5.2.5 zeigen.

Ergänzung 5.2.4. Alle endlichen einfachen Gruppen sind seit etwa 1980 bekannt, ihre Klassifikation ist jedoch schwierig und man kann nur hoffen, daß zukünftige Forschungen noch substantielle Vereinfachungen der Argumente erlauben. Eine wesentliche Zutat ist ein berühmter Satz von **Feit-Thompson**, nach dem jede endliche einfache nicht abelsche Gruppe eine gerade Ordnung haben muß.

Satz 5.2.5. *Die Ikosaedergruppe ist einfach und isomorph zur alternierenden Gruppe A_5.*

Beweis. Ein Ikosaeder hat 12 Ecken, 20 Flächen und 30 Kanten. Jedes Paar von gegenüberliegenden Ecken liefert vier Elemente der Ordnung 5 in I, macht 24 Elemente der Ordnung 5. Jedes Paar von gegenüberliegenden Flächen liefert zwei Elemente der Ordnung 3 in I, macht 20 Elemente der Ordnung 3. Jedes Paar von gegenüberliegenden Kanten liefert ein Element der Ordnung 2 in I, macht 15 Elemente der Ordnung 2. Zusammen mit dem neutralen Element haben wir damit alle Gruppenelemente aufgelistet, denn es gilt

$$60 = 1 + 15 + 20 + 24$$

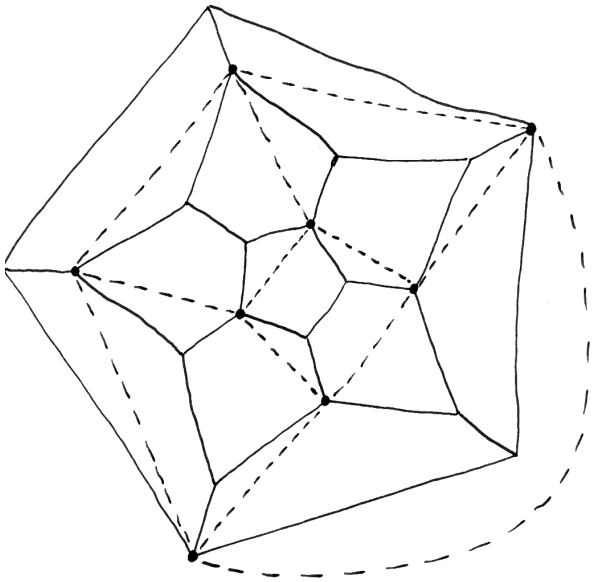
Da je zwei Kanten des Ikosaeders durch eine Drehsymmetrie des Ikosaeders ineinander überführt werden können, bilden die 15 Elemente der Ordnung 2 eine Konjugationsklasse: Sind in der Tat K und L Kanten und d_k, d_L die nichttrivialen Drehsymmetrien, die sie jeweils in sich selbst überführen, und ist g eine Drehsymmetrie mit $g(K) = L$, so gilt $d_K = g^{-1} d_L g$. Ähnlich sieht man, daß alle 20 Elemente der Ordnung 3 eine Konjugationsklasse bilden. Für die Elemente der Ordnung 5 kann das nicht gelten, denn 24 ist kein Teiler von 60. Mit ähnlichen Überlegungen erkennt man jedoch, daß die 24 Elemente der Ordnung 5 zerfallen in zwei Konjugationsklassen von je 12 Elementen, bestehend aus Drehungen einmal um Winkel $\pm\frac{2\pi}{5}$ und ein andermal $\pm\frac{4\pi}{5}$. Die Kardinalitäten der Konjugationsklassen sind also genau die Summanden auf der rechten Seite der Gleichung

$$60 = 1 + 15 + 20 + 12 + 12$$

Gäbe es nun in I einen echten Normalteiler N, so müßte die Ordnung von N ein Teiler sein von 60 und eine Summe von Kardinalitäten von Konjugationsklassen, darunter die Konjugationsklasse des neutralen Elements. Die einzigen solchen Zahlen sind aber 1 und 60, folglich ist die Ikosaedergruppe I einfach. Man überlegt sich nun anhand der nebenstehenden Zeichnung, daß es genau fünf Möglichkeiten gibt, aus den 20 Ecken eines Dodekaeders, die ja gerade die Flächenmitten eines Ikosaeders bilden, 8 Ecken so auszusuchen, daß sie die Ecken eines Würfels bilden: Auf der Menge dieser 5 einbeschriebenen Würfel operiert unsere Gruppe dann natürlich auch. Wir erhalten so einen Gruppenhomomorphismus

$$\varphi : I \to \mathcal{S}_5$$

Der Kern von $\operatorname{sgn} \circ \varphi : I \to \{+1, -1\}$ ist ein von 1 verschiedener Normalteiler von I, es folgt $\ker(\operatorname{sgn} \circ \varphi) = I$ und φ induziert einen Gruppenhomomorphismus nach $A_5 = \ker(\operatorname{sgn}) \subset \mathcal{S}_5$. Der Kern von $\varphi : I \to \mathcal{S}_5$ ist ein von I verschiedener Normalteiler von I, es folgt $\ker \varphi = 1$, und durch Abzählen folgt dann, daß φ einen Isomorphismus $\varphi : I \xrightarrow{\sim} A_5$ induziert. $\square$



Einer der fünf eingeschriebenen Würfel eines Dodekaeders, mit gestrichelt eingezeichneten Kanten. Diese Würfel entsprechen im übrigen auch eineindeutig den 2-Sylows unserer Ikosaedergruppe: Diese sind genau die vierelementigen Diedergruppen, die von den drei durch die Flächenmitten eines festen Würfels stechenden Geraden jede in sich überführen. Wenn Sie dieser Anschauung nicht so recht trauen, wofür ich durchaus Sympathie hätte, können Sie auch abstrakt die „Symmetriegruppe des Graphen mit den durchgezogenen Kanten“ betrachten. Sie würde den „Dreh- und Spiegelsymmetrien“ eines Ikosaeders entsprechen, aber wenn Sie zusätzlich an jeder Ecke auf der Menge der von ihr ausgehenden Kanten in der Terminologie **??** die zyklische Anordnung „im Uhrzeigersinn“ festlegen, so wird die Gruppe derjenigen Symmetrien unseres Graphen, die diese zyklischen Anordnungen respektieren, genau die Ikosaedergruppe werden.

Definition 5.2.6. Eine **Kompositionsreihe** einer Gruppe G ist eine Folge von Untergruppen

$$G = G_r \supset G_{r-1} \supset \ldots \supset G_0 = 1$$

derart, daß jede Gruppe unserer Folge ein Normalteiler in der nächstgrößeren Gruppe ist und daß die sukzessiven Quotienten einfach sind, daß also in Formeln G_i/G_{i-1} einfach ist für $1 \leq \mathrm{i} \leq r$. Die Gruppen G_i/G_{i-1} heißen die **Subquotienten** der Kompositionsreihe.

Satz 5.2.7 (**Jordan-Hölder**). *Je zwei Kompositionsreihen einer endlichen Gruppe haben dieselbe Länge und bis auf Reihenfolge isomorphe Subquotienten, die man die* **Kompositionsfaktoren** *unserer Gruppe nennt. Ist genauer G eine endliche Gruppe und sind $G = M_r \supset \ldots \supset M_0 = 1$ und $G = N_s \supset \ldots \supset N_0 = 1$ Kompositionsreihen von G, so haben wir $r = s$ und es gibt eine Permutation $\sigma \in \mathcal{S}_r$ mit $N_i/N_{i-1} \cong M_{\sigma(i)}/M_{\sigma(i)-1}$ für alle i.*

Beispiel 5.2.8. Jede abelsche Gruppe mit n Elementen hat als Kompositionsfaktoren die zyklischen Gruppen $\mathbb{Z}/p_i\mathbb{Z}$ für $n = p_1 \ldots p_r$ die Primfaktorzerlegung von n. Jeder endlichdimensionale Vektorraum V über $\mathbb{F}_p$ für eine Primzahl p hat insbesondere als Kompositionsfaktoren $\dim V$ Kopien von $\mathbb{F}_p$. Die Kompositionsfaktoren der symmetrischen Gruppen $\mathcal{S}_r$ werden wird in 5.6.2 und 5.6.3 diskutieren: Ab $r = 5$ ist der Kern des Signums ein einfacher Normalteiler und unsere Gruppe hat folglich nur zwei Kompositionsfaktoren: Diesen Normalteiler und $\mathbb{Z}/2\mathbb{Z}$.

Beweis. Wir zeigen das durch Induktion über die Gruppenordnung. Seien

$$\begin{array}{ccccccc} G & \supset & M & \supset & \ldots & \supset & 1 \\ G & \supset & N & \supset & \ldots & \supset & 1 \end{array}$$

zwei Kompositionsreihen. Gilt $M = N$, so folgt der Satz per Induktion. Sonst ist das Bild von M in G/N ein von 1 verschiedener Normalteiler, und da G/N einfach ist, liefert die offensichtliche Abbildung notwendig eine Surjektion $M \twoheadrightarrow G/N$ und einen Isomorphismus $M/(M \cap N) \xrightarrow{\sim} G/N$. Ebenso erhalten wir auch $N/(M \cap N) \xrightarrow{\sim} G/M$. Deuten wir mit $(M \cap N) \supset \ldots \supset 1$ eine Kompositionsreihe des Schnitts an, so hat die Gruppe G also Kompositionsreihen

$$\begin{array}{ccccccccc} G & \supset & M & \supset & & & \ldots & \supset & 1 \\ G & \supset & M & \supset & (M \cap N) & \supset & \ldots & \supset & 1 \\ G & \supset & N & \supset & (M \cap N) & \supset & \ldots & \supset & 1 \\ G & \supset & N & \supset & & & \ldots & \supset & 1 \end{array}$$

Je zwei in dieser Liste benachbarte Kompositionsreihen haben aber nun nach Induktionsvoraussetzung und den oben erwähnten Isomorphismen bis auf Reihenfolge dieselben Subquotienten. □

Übungen

Ergänzende Übung 5.2.9. Man zeige die Aussage des Satzes von Jordan-Hölder 5.2.7, ohne die Endlichkeit der Gruppe vorauszusetzen. Man zeige auch, daß in einer Gruppe mit Kompositionsreihe eine absteigende Folge von Untergruppen, die jeweils echte Normalteiler in der nächstgrößeren Untergruppe sind, höchstens so lang sein kann wie besagte Kompositionsreihe.

Ergänzende Übung 5.2.10 (**Semidirektes Produkt**). Seien $\varphi : G \twoheadrightarrow B$ ein surjektiver Gruppenhomomorphismus mit Kern $N := \ker \varphi$ und $\sigma : B \hookrightarrow G$ eine Spaltung von φ, also ein Gruppenhomomorphismus mit $\sigma \circ \varphi = \mathrm{id}_B$. Man zeige, daß dann die Abbildung $(n, b) \mapsto n\sigma(b)$ eine Bijektion $N \times B \xrightarrow{\sim} G$ liefert und daß die Verknüpfung von G unter dieser Bijektion derjenigen Verknüpfung auf $N \times B$ entspricht, die gegeben wird durch

$$(m, a)(n, b) = (m \,\mathrm{int}_{\sigma(a)}(n), ab) \quad \forall m, n \in N \text{ und } a, b \in B.$$

Sind umgekehrt N, B Gruppen und $\tau : B \to \mathrm{Grp}^{\times} N, a \mapsto \tau_a$ ein Gruppenhomomorphismus von B in die Automorphismengruppe von N, so wird $N \times B$ mit der Verknüpfung

$$(m, a)(n, b) := (m\tau_a(n), ab) \quad \forall m, n \in N \text{ und } a, b \in B$$

zu einer Gruppe. Diese Gruppe heißt das **semidirekte Produkt von** N **mit** B **über** τ und wird notiert als

$$N \rtimes B = N \rtimes_\tau B$$

Ergänzung 5.2.11. Ist speziell eine Gruppe N ein Produkt von n Kopien einer festen Gruppe $N = A^n = A \times \ldots \times A$ und operiert eine weitere Gruppe B darauf durch Vertauschung der Faktoren, also in hoffentlich offensichtlicher Weise vermittels eines Gruppenhomomorphismus $B \to \mathcal{S}_n$, so bezeichnet man das zugehörige semidirekte Produkt als **Kranzprodukt** und notiert es $N \rtimes B =: A \wr B$.

Ergänzende Übung 5.2.12. Man zeige, daß die symmetrische Gruppe $\mathcal{S}_4$ isomorph ist zum semidirekten Produkt der $\mathcal{S}_3$ mit der Klein'schen Vierergruppe $\mathbb{F}_2^2$ in Bezug auf einen und jeden Isomorphismus $\mathcal{S}_3 \xrightarrow{\sim} \mathrm{GL}(2; \mathbb{F}_2)$.

5.3 p-Gruppen

Definition 5.3.1. Das **Zentrum** einer Gruppe G ist die Menge

$$\mathrm{Z}(G) := \{x \in G \mid xg = gx \quad \forall g \in G\}$$

derjenigen Gruppenelemente, die mit allen anderen Gruppenelementen kommutieren.

5.3.2. Offensichtlich ist das Zentrum ein Normalteiler, was im Übrigen auch die alternative Beschreibung $\mathrm{Z}(G) = \ker(\mathrm{int} : G \to \mathrm{Grp}^\times(G))$ als Kern eines Gruppenhomomorphismus in den Notationen aus 4.3 sofort zeigt.

Definition 5.3.3. Die Standgruppe von $g \in G$ unter der Operation von G auf sich selbst durch Konjugation heißt der **Zentralisator** $\mathrm{Z}_G(g)$ von g, in Formeln

$$\mathrm{Z}_G(g) = \{x \in G \mid xgx^{-1} = g\}$$

5.3.4. Ist G eine endliche Gruppe, $G = C_1 \sqcup \ldots \sqcup C_r$ ihre Zerlegung in Konjugationsklassen und $g_i \in C_i$ jeweils ein Element, so liefert die Bahnformel 4.2.2 die sogenannte **Klassengleichung**

$$\begin{aligned} |G| &= |C_1| + \ldots + |C_r| \\ &= |G|/|\mathrm{Z}_G(g_1)| + \ldots + |G|/|\mathrm{Z}_G(g_r)| \end{aligned}$$

Die einelementigen Konjugationsklassen sind dabei genau die Konjugationsklassen der Elemente des Zentrums.

Definition 5.3.5. Sei p eine Primzahl. Eine **p-Gruppe** ist eine endliche Gruppe, deren Ordnung eine Potenz von p ist. Die triviale Gruppe hat p^0 Elemente und ist damit nach unserer Konvention 3.4.3 eine p-Gruppe für jede Primzahl p.

Proposition 5.3.6. *Jede nichttriviale p-Gruppe hat nichttriviales Zentrum.*

Beweis. Wir zerlegen unsere Gruppe in Konjugationsklassen $G = C_1 \sqcup \ldots \sqcup C_r$. Nach der Bahnformel sind alle Kardinalitäten von Konjugationsklassen $|C_i|$ Teiler von $|G|$, also p-Potenzen. Die einelementigen Konjugationsklassen gehören dabei genau zu den Elementen des Zentrums von G und wir folgern

$$|G| \equiv |\mathrm{Z}(G)| \pmod{p}$$

Da nun das Zentrum stets mindestens ein Element hat, nämlich das neutrale Element, muß es im Fall einer nichttrivialen p-Gruppe sogar mindestens p Elemente haben. □

Korollar 5.3.7. *Ist die Ordnung einer Gruppe das Quadrat einer Primzahl p, so ist die besagte Gruppe abelsch, in Formeln:*

$$|G| = p^2 \;\Rightarrow\; \mathrm{Z}(G) = G$$

Beweis. Nach der vorhergehenden Proposition 5.3.6 hat das Zentrum unserer Gruppe mindestens p Elemente. Gäbe es nun außerhalb des Zentrums noch ein Element unserer Gruppe, so müßte dieses Element zusammen mit dem Zentrum eine kommutative Untergruppe mit mehr als p Elementen erzeugen, und diese wäre dann nach dem Satz von Lagrange 3.1.5 bereits die ganze Gruppe. □

Satz 5.3.8 (Struktur von p-Gruppen). *Ist G eine p-Gruppe, so gibt es in G eine Kette $G = G_r \supset G_{r-1} \supset \ldots \supset G_0 = 1$ von Normalteilern von G mit $|G_i/G_{i-1}| = p$ für alle i. Zusätzlich können wir sogar erreichen, daß G_i/G_{i-1} jeweils im Zentrum von G/G_{i-1} liegt.*

Beweis. Wir führen den Beweis durch Induktion über die Gruppenordnung. Ist G nicht trivial, in Formeln $G \neq 1$, so hat G nach 5.3.6 nichttrivales Zentrum $\mathrm{Z}(G) \neq 1$. Indem wir von irgendeinem nichttrivialen Element des Zentrums eine geeignete Potenz nehmen, finden wir im Zentrum sogar ein Element x der Ordnung p. Die von x erzeugte Untergruppe $G_1 = \langle x \rangle$ ist also isomorph zu $\mathbb{Z}/p\mathbb{Z}$, und da x im Zentrum liegt, ist G_1 ein Normalteiler in G. Nach Induktion finden wir nun im Quotienten $\bar{G} := G/G_1$ eine Kette $\bar{G} = \bar{G}_l \supset \ldots \supset \bar{G}_1 \supset \bar{G}_0 = 1$ wie gewünscht. Dann nehmen wir $G_i := \mathrm{can}^{-1}(\bar{G}_{i-1})$ für $\mathrm{can} : G \twoheadrightarrow \bar{G}$ die Projektion. Wegen 3.2.20 erhalten wir so eine Kette von Normalteilern von G. Wegen 3.1.6 haben wir $|G_i| = p|\bar{G}_{i-1}| = p^i$. Damit hat G_i/G_{i-1} genau p Elemente. □

5.3.9. Eine Gruppe G heißt **auflösbar**, wenn es eine Folge von Untergruppen $G = G_r \supset G_{r-1} \supset G_{r-2} \supset \ldots \supset G_0 = 1$ gibt mit G_{i-1} normal in G_i und G_i/G_{i-1} abelsch für $1 \leq i \leq r$. Aus 5.3.16 wird folgen, daß wir dann sogar solch eine Folge finden können, bei der jedes G_i bereits in ganz G normal ist. Die Terminologie „auflösbar“ kommt von der Beziehung dieses Begriffs zum Auflösen von Gleichungen her und wird erst im Licht von Satz 8.6.22 verständlich. Bemerkung 5.6.3 zeigt, daß die symmetrische Gruppe $\mathcal{S}_4$ auflösbar ist. Eine nichtabelsche einfache Gruppe kann nie auflösbar sein. Alle Gruppen mit weniger als 60 Elementen sind auflösbar, und die Ikosaedergruppe alias die Gruppe der geraden Permutationen von 5 Elementen ist bis auf Isomorphsmus die einzige nichtauflösbare Gruppe mit 60 Elementen. Beides werden wir aber hier nicht zeigen.

Übungen

Übung 5.3.10. Eine Gruppe G heißt **nilpotent**, wenn es eine Folge $G = G_r \supset G_{r-1} \supset G_{r-2} \supset \ldots \supset G_0 = 1$ von Untergruppen von G gibt derart, daß G_i/G_{i-1} für $1 \leq i \leq r$ im Zentrum von G/G_{i-1} liegt. Jede endliche p-Gruppe ist nilpotent nach 5.3.8. Natürlich können wir zu jeder Gruppe G die Gruppe $G/\mathrm{Z}(G)$ konstruieren. Man zeige: Eine Gruppe ist nilpotent genau dann, wenn wiederholtes Anwenden dieser Konstruktion in endlich vielen Schritten von unserer Gruppe zur trivialen Gruppe führt.

Ergänzende Übung 5.3.11. Diese Übung soll die Herkunft der Bezeichnung „nilpotent“ erklären. Gegeben Elemente a, b einer Gruppe G setzt man $(a, b) := aba^{-1}b^{-1}$ und nennt dies Element den **Kommutator von a und b**. Gegeben Teilmengen A, B einer Gruppe bezeichnen wir mit $\langle (A, B) \rangle$ die von den Kommutatoren erzeugte Untergruppe. Vielfach wird sie auch vereinfacht (A, B) notiert. Jetzt

definiert man induktiv die **absteigende Zentralreihe** einer Gruppe G durch

$$G^0 := G, G^1 := \langle (G,G) \rangle, \ldots, G^{i+1} := \langle (G^i, G) \rangle, \ldots$$

Man zeige, daß eine Gruppe genau dann nilpotent ist, wenn ihre absteigende Zentralreihe nach endlich vielen Schritten bei der trivialen Gruppe landet, wenn also in Formeln gilt $G^i = 1$ für $i \gg 0$.

Übung 5.3.12. Eine Gruppe G heißt **überauflösbar**, wenn es eine Folge $G = G_r \supset G_{r-1} \supset G_{r-2} \supset \ldots \supset G_0 = 1$ von Normalteilern von G gibt mit G_i/G_{i-1} zyklisch für $1 \leq i \leq r$. Man zeige: Jede endliche nilpotente Gruppe ist überauflösbar.

Ergänzende Übung 5.3.13. Jede Untergruppe einer nilpotenten Gruppe ist nilpotent. Für jedes n ist die Gruppe der oberen $(n \times n)$-Dreiecksmatrizen mit Einsen auf der Diagonale und Einträgen in irgendeinem Ring nilpotent.

Ergänzende Übung 5.3.14. Man bestimme das Zentrum der Gruppe $\mathrm{GL}(n;k)$ für $n \in \mathbb{N}$ und k ein Körper. Man bestimme das Zentrum der Symmetriegruppe eines Quadrats.

Übung 5.3.15. Jede Untergruppe einer auflösbaren Gruppe ist auflösbar. Gegeben $G \supset N$ eine Gruppe mit Normalteiler ist die ganze Gruppe G auflösbar genau dann, wenn N und G/N auflösbar sind. Hinweis: 3.2.19.

Ergänzende Übung 5.3.16. Gegeben eine Gruppe G erklärt man ihre **derivierte Gruppe** als $\mathcal{D}G := \langle (G,G) \rangle$ und setzt induktiv $\mathcal{D}^{i+1}G := \mathcal{D}(\mathcal{D}^i G)$. Man zeige, daß eine Gruppe genau dann auflösbar ist, wenn ihre höheren derivierten Gruppen irgendwann trivial werden, wenn also in Formeln gilt $\mathcal{D}^i G = 1$ für $i \gg 0$. Man zeige weiter, daß alle höheren derivierten Gruppen $\mathcal{D}^i G$ Normalteiler von G sind.

5.4 Sylowsätze

Definition 5.4.1. Seien G eine endliche Gruppe und p eine Primzahl. Eine Untergruppe $P \subset G$ heißt eine **p-Sylowuntergruppe** oder kurz **p-Sylow von** G, wenn ihre Kardinalität $|P|$ die höchste p-Potenz ist, die die Gruppenordnung $|G|$ teilt.

Beispiel 5.4.2. Eine 2-Sylow in der Gruppe der 24 Drehsymmetrien eines Würfels ist per definitionem eine Untergruppe mit 8 Elementen. Zum Beispiel wäre jede Untergruppe, die die Achse durch die Mittelpunkte zweier gegenüberliegender Flächen stabilisiert, eine solche 2-Sylow. Die einzige 5-Sylow in derselben Gruppe wäre in unserer Terminologie die einelementige Untergruppe. Viele Autoren verstehen aber auch abweichend unter Sylowuntergruppen nur diejenigen Untergruppen, die wir in unserer Terminologie als „nichttriviale Sylowuntergruppen“ ansprechen würden.

5.4.3. Die Operation durch Konjugation einer Gruppe G auf sich selber induziert eine Operation unserer Gruppe auf ihrer Potenzmenge $\mathcal{P}(G)$, die wir auch als „Konjugation“ ansprechen. Im folgenden verwenden wir oft die davon auf der Teilmenge $\mathcal{U}(G) \subset \mathcal{P}(G)$ aller Untergruppen induzierte Operation. Insbesondere heißen also zwei Untergruppen $H, K \subset G$ **zueinander konjugiert**, wenn es $g \in G$ gibt mit $H = gKg^{-1}$.

Satz 5.4.4 (Sätze von Sylow). *Seien G eine endliche Gruppe, p eine Primzahl und p^r die größte p-Potenz, die die Gruppenordnung $|G|$ teilt. So gilt:*

1. *Unsere Gruppe G besitzt Untergruppen der Ordnung p^r alias p-Sylows;*
2. *Je zwei p-Sylows von G sind zueinander konjugiert;*
3. *Jede Untergruppe von G, deren Ordnung eine p-Potenz ist, liegt in einer p-Sylow von G;*
4. *Die Zahl der p-Sylows von G ist ein Teiler von $|G|/p^r$ und kongruent zu 1 modulo p.*

Beispiel 5.4.5. Ist G eine endliche abelsche Gruppe, so gibt es insbesondere genau eine p-Sylow für alle p. Wir kennen diese Untergruppe schon aus Proposition 3.3.17: Es ist die Untergruppe $G(p)$ aller Elemente von G, deren Ordnung eine p-Potenz ist.

Beispiel 5.4.6. Im Fall der Gruppe der 24 Drehsymmetrien eines Würfels liefern die drei Paare gegenüberliegender Flächen drei paarweise verschiedene 2-Sylows, bestehend aus allen Drehsymmetrien, die das jeweilige Paar in sich überführen. Das müssen dann auch bereits alle 2-Sylows alias alle 8-elementigen Untergruppen dieser Gruppe sein, wie man unschwer aus Teil 2 oder auch aus Teil 4 des vorhergehenden Satzes folgern kann.

Beweis. 1. Wir argumentieren durch Induktion über $|G|$. Ohne Beschränkung der Allgemeinheit dürfen wir annehmen, daß p die Ordnung unserer Gruppe teilt. Ist $G = C_1 \sqcup \ldots \sqcup C_s$ die Zerlegung in Konjugationsklassen und $g_i \in C_i$ für $1 \leq i \leq t$ jeweils ein Element aus jeder Konjugationsklasse mit mehr als einem Element, so liefert die Bahnformel nach 5.3.4 die Klassengleichung

$$|G| = |G|/|\mathrm{Z}_G(g_1)| + \ldots + |G|/|\mathrm{Z}_G(g_t)| + |\mathrm{Z}(G)|$$

Teilt p die Ordnung $|\mathrm{Z}(G)|$ des Zentrums von G, so gibt es nach 3.3.18 in $\mathrm{Z}(G)$ ein Element g der Ordnung p. Nach der Induktionsannahme finden wir nun eine p-Sylow von $G/\langle g\rangle$, und deren Urbild in G ist notwendig eine p-Sylow von G. Gilt sonst $p \nmid |\mathrm{Z}(G)|$, so finden wir auch ein i mit $p \nmid |G|/|\mathrm{Z}_G(g_i)|$ und dann folgt

die Behauptung direkt aus der Induktionsannahme angewendet auf die Gruppe $\mathrm{Z}_G(g_i)$.

5. Vor dem weiteren Fortgang des Beweises ergänzen wir nun unseren Satz um einen technischeren Teil 5, der dann als nächstes bewiesen wird. Bezeichne $\mathcal{S}$ die Menge aller p-Sylows von G. Sicher operiert G auf $\mathcal{S}$ durch Konjugation. Wir vereinbaren als Notation für den weiteren Verlauf des Beweises die folgenden Konventionen: Bezeichnen wir eine Sylow durch einen kleinen Buchstaben, so fassen wir sie primär als ein Element $x \in \mathcal{S}$ auf und notieren die mit $g \in G$ konjugierte Sylow gx. Bezeichnen wir eine Sylow jedoch durch einen großen Buchstaben, so fassen wir sie primär als eine Teilmenge $P \subset G$ auf und notieren die mit $g \in G$ konjugierte Sylow gPg^{-1}. Ich ergänze nun mit diesen Notationen den Satz um die folgende technische Aussage:

5. *Ist $H \subset G$ eine p-Gruppe und $y = Q \in \mathcal{S}$ ein Fixpunkt von H in der Menge aller p-Sylows von G, so gilt $H \subset Q$.*

In der Tat besagt die Fixpunkteigenschaft $hQh^{-1} = Q \ \forall h \in H$. Mithin ist $HQ = QH$ eine Untergruppe von G. Ihre Ordnung ist $|QH| = |QH/H| \cdot |H|$. Nun ist QH/H unter der Operation von Q durch Linksmultiplikation eine einzige Q-Bahn und damit ist $|QH/H|$ eine p-Potenz. Da auch $|H|$ eine p-Potenz ist, muß QH eine p-Gruppe sein. Es folgt $QH = Q$, also $H \subset Q$. Nun beweisen wir die restlichen Teile des Satzes.

2&3. Sei eine p-Sylow $P = x$ gegeben. Für ihre Standgruppe G_x gilt $G_x \supset P$, also ist nach der Bahnformel 4.2.2 die Kardinalität $|Gx|$ der Bahn $Gx \subset \mathcal{S}$ von x teilerfremd zu p. Sei weiter $H \subset G$ eine Untergruppe von p-Potenzordnung. Sicher zerfällt Gx in Bahnen unter H, und die Ordnung jeder solchen Bahn muß eine p-Potenz sein. Folglich gibt es in Gx einen Fixpunkt y von H. Nach dem eben bewiesenen Teil 5 ist dieser Fixpunkt $y = Q$ eine p-Sylow Q mit $Q \supset H$, und wegen $y \in Gx$ gibt es $g \in G$ mit $gPg^{-1} = Q$.

4. Nach Teil 5 gibt es nur einen Fixpunkt unserer Sylow P auf der Menge aller p-Sylows $\mathcal{S}$, nämlich den Punkt $x = P$ selber. Alle anderen P-Bahnen in $\mathcal{S}$ haben als Kardinalität eine echte p-Potenz, und das zeigt $|\mathcal{S}| \equiv 1 \pmod p$. Die Standgruppe G_x von $x \in \mathcal{S}$ umfaßt schließlich unsere Sylow $P = x$. Da nun je zwei p-Sylows konjugiert sind alias ganz $\mathcal{S}$ ein homogener G-Raum ist, folgt auch, daß $|\mathcal{S}| = |G/G_x|$ ein Teiler ist von $|G/P|$. □

Ergänzung 5.4.7. Ein alternativer Beweis des ersten Teils geht so: Man betrachtet das System $\mathcal{M} \subset \mathcal{P}(G)$ aller Teilmengen unserer Gruppe mit p^r Elementen. Die Gruppe G operiert auf $\mathcal{M}$ durch Konjugation. Hat der Stabilisator von einem $M \in \mathcal{M}$ genau p^r Elemente, so ist er eine p-Sylow. Sonst haben alle Stabilisatoren

weniger Elemente und damit alle Bahnen eine durch p teilbare Kardinalität: Widerspruch dazu, daß nach expliziter Rechnung die Kardinalität von $\mathcal{M}$ teilerfremd ist zu p, vergleiche **??**.

Satz 5.4.8 (**von Cauchy über Gruppenelelemente von Primzahlordnung**). *Jeder Primfaktor der Ordung einer endlichen Gruppe tritt auch als Ordnung eines Elements besagter Gruppe auf.*

5.4.9. Man beachte, daß wir diese Aussage im Fall abelscher Gruppen bereits in 3.3.18 bewiesen hatten, und daß wir sie in diesem Fall ihrerseits beim Beweis der Sylowsätze verwendet haben. Einen alternativen Beweis konnten Sie als Übung 4.1.35 ausarbeiten. Allgemeinere Teiler der Ordung einer endlichen Gruppe müssen keineswegs als Ordnung eines Elements besagter Gruppe auftreten. So gibt es etwa in der symmetrischen Gruppe $\mathcal{S}_5$ keine Untergruppe mit 15 Elementen, was Sie als Übung gleich zeigen können. Ebenso sieht man leicht ein, daß die alternierende Gruppe A_4 keine Untergruppe der Ordnung 6 hat. Teilt jedoch eine Primzahlpotenz die Ordnung einer Gruppe, so gibt es eine Untergruppe mit besagter Primzahlpotenz als Ordnung: Das folgt ähnlich wie im anschließenden Beweis leicht aus den Sylowsätzen zusammen mit unseren Erkenntnissen zur Struktur von p-Gruppen 5.3.8.

Beweis. Sei p unser Primfaktor. Man findet zunächst nach 5.4.4 in unserer Gruppe eine p-Sylow. Darin findet man ein Element, das nicht das neutrale Element ist. Dieses erzeugt eine zyklische Untergruppe, die isomorph ist zu $\mathbb{Z}/p^r\mathbb{Z}$ für $r \geq 1$. Darin ist dann die Nebenklasse von p^{r-1} das gesuchte Element der Ordnung p. □

Proposition 5.4.10. *Jede Gruppe mit genau sechs Elementen ist entweder zyklisch oder isomorph zur symmetrischen Gruppe $\mathcal{S}_3$.*

Beweis. Sei G unsere Gruppe der Ordnung $|G| = 6$. Wir finden nach dem Satz von Cauchy 5.4.8 Elemente $a, b \in G$ der Ordnungen 2 und 3. Nach Übung 1.3.8 zum Satz von Lagrange gilt $\langle a\rangle \cap \langle b\rangle = 1$, also liefert die Multiplikation eine Bijektion

$$\langle a\rangle \times \langle b\rangle \xrightarrow{\sim} G$$

Sicher kann unter diesen Umständen ba weder eine Potenz von a noch eine Potenz von b sein. Gilt $ba = ab$, so ist unsere Gruppe kommutativ und folglich isomorph zu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}$. Gilt $ba = ab^2$, so legt diese Gleichung schon die ganze Gruppenstruktur fest und wir haben die $\mathcal{S}_3$ vor uns. □

Korollar 5.4.11. *Jede Gruppe der Ordnung 15 ist zyklisch.*

Beweis. Die Zahl der 3-Sylows teilt 5 und ist kongruent zu 1 modulo 3. Es gibt also genau eine 3-Sylow und damit genau zwei Elemente der Ordnung 3. Ähnlich

gibt es genau eine 5-Sylow und damit genau 4 Elemente der Ordnung 5. Zusammen mit dem neutralen Element sind das nur 7 Elemente. Die übrigen 8 Elemente haben notwendig die Ordnung 15. □

Ergänzung 5.4.12 (**Gruppen mit höchstens** 15 **Elementen**). Mit den folgenden Übungen können Sie die Klassifikation der Gruppen mit höchstens 15 Elementen zu Ende bringen. Gruppen mit $2, 3, 5, 7, 11$ oder 13 Elementen sind ja zyklisch nach 3.3.5. Gruppen mit 4 oder 9 Elementen sind abelsch nach 5.3.7 und werden damit durch 3.4.5 klassifiziert. Gruppen mit 6 Elementen hatten wir in 5.4.10 diskutiert. Für Gruppen mit 10 oder 14 Elementen funktioniert dieselbe Argumentation, wie Sie als Übung 5.4.15 ausarbeiten dürfen. Gruppen mit 8 Elementen klassifizieren wir in 5.4.13, Gruppen mit 12 Elementen klassifizieren Sie in 5.4.19, und jede Gruppe mit 15 Elementen ist zyklisch nach 5.4.11. Bei Gruppen mit 16 Elementen fängt es aber an, unübersichtlich zu werden, es gibt von ihnen bereits 14 Isomorphieklassen.

Ergänzung 5.4.13 (**Gruppen mit** 8 **Elementen**). Es gibt 5 Isomorphieklassen von Gruppen der Ordnung acht, als da wären die drei abelschen Gruppen $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ und $(\mathbb{Z}/2\mathbb{Z})^3$, die Diedergruppe der Ordnung acht sowie die **Quaternionengruppe** der acht Quaternionen $\{\pm 1, \pm \mathrm{i}, \pm \mathrm{j}, \pm \mathrm{k}\}$ nach 2.6.4. Um das einzusehen, kann man argumentieren wie folgt: Jede nichtabelsche Gruppe der Ordnung acht besitzt nach **??** Elemente der Ordnung vier, also nach 3.2.21 einen zyklischen Normalteiler der Ordnung vier. Gibt es eine Involution außerhalb dieses Normalteilers, so sehen wir schnell, daß unsere Gruppe ein semidirektes Produkt $(\mathbb{Z}/4\mathbb{Z}) \rtimes (\mathbb{Z}/2\mathbb{Z})$ sein muß für die einzige nichttriviale Operation, so daß wir eine Diedergruppe vor uns haben. Sonst haben alle Elemente außerhalb unseres Normalteilers die Ordnung vier und in unserer Gruppe bleibt nur noch Platz für ein einziges Element der Ordnung zwei. Unsere Gruppe ist also die Vereinigung von drei zyklischen Gruppen der Ordnung vier, und der Schnitt dieser Gruppen ist auch der Schnitt von je zweien unter ihnen und ist zyklisch von der Ordnung zwei und zentral. Bezeichne 1 das neutrale Element und -1 das andere Element dieses Schnitts. Wählen wir i und j Erzeuger von zwei verschiedenen zyklischen Untergruppen der Ordnung vier, so müssen $\mathrm{i}\,\mathrm{j}$ und auch $\mathrm{k} := (-1)\,\mathrm{i}\,\mathrm{j}$ die dritte zyklische Untergruppe der Ordnung vier erzeugen, denn diese Elemente sind weder eine Potenz von i noch eine Potenz von j. Von hier aus ist leicht zu sehen, daß wir gerade die Quaternionengruppe vor uns haben.

Ergänzung 5.4.14. Jede Gruppe der Ordnung 18 ist auflösbar. In der Tat gibt es nur eine 3-Sylow, die ist notwendig normal, und wir sind fertig.

Übungen

Ergänzende Übung 5.4.15. Für jede Primzahl p gibt es bis auf Isomorphismus genau zwei Gruppen der Ordnung $2p$, eine zyklische Gruppe und eine Diedergruppe. Hinweis: Man erinnere die Argumentation im Fall $p = 3$ und interessiere sich für die Anzahl der 2-Sylows.

Ergänzende Übung 5.4.16. Sind $p > q$ Primzahlen und ist q kein Teiler von $p-1$, so ist jede Gruppe der Ordnung pq zyklisch. Hinweis: 5.4.11.

Ergänzende Übung 5.4.17 (**Struktur endlicher nilpotenter Gruppen**). Man zeige: In einer endlichen nilpotenten Gruppe ist jede Sylow ein Normalteiler. Insbesondere gibt es zu jeder Primzahl p nur eine Sylow, die aus allen Elementen von p-Potenzordnung besteht. Hinweis: Vollständige Induktion über die Gruppenordnung. Man zeige weiter, daß in einer endlichen nilpotenten Gruppe Elemente aus verschiedenen Sylowuntergruppen kommutieren und daß unsere Gruppe isomorph ist zum Produkt ihrer nichttrivialen Sylowuntergruppen.

Ergänzende Übung 5.4.18 (**Funktorialität semidirekter Produkte**). Seien A, M, B, N Gruppen und $\kappa : A \to \mathrm{Grp}^\times M$ sowie $\tau : B \to \mathrm{Grp}^\times N$ Gruppenhomomorphismen. Wie bei der Definition semidirekter Produkte in 5.2.10 schreiben wir $(\kappa(a))(m) =: ({}^a m)$ und $(\tau(b))(n) =: ({}^b n)$. Seien weiter $\psi : A \to B$ und $\varphi : M \to N$ Gruppenhomomorphismen mit ${}^{\psi(a)}\varphi(m) = \varphi({}^a m)$ für alle $a \in A$ und alle $m \in M$ alias $\tau(\psi(a)) \circ \varphi = \varphi \circ \kappa(a)$ für alle $a \in A$. So ist $\varphi \times \psi$ ein Homomorphismus der semidirekten Produkte

$$(\varphi \times \psi) : M \rtimes A \to N \rtimes B$$

Speziell haben wir$N \rtimes_\tau B \cong N \rtimes_\kappa B$ im Fall $\kappa = (\mathrm{int}\,\varphi) \circ \tau$ für einen Automorphismus $\varphi \in \mathrm{Grp}^\times N$ der Gruppe N.

Ergänzende Übung 5.4.19 (**Gruppen mit** 12 **Elementen**). In dieser Übung sollen Sie zeigen, daß es bis auf Isomorphismus genau 5 Gruppen der Ordnung 12 gibt: Die beiden abelschen Gruppen $(\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/3\mathbb{Z}$ und $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, die Diedergruppe D_6, die alternierende Gruppe A_4 und ein semidirektes Produkt $\mathbb{Z}/4\mathbb{Z} \ltimes \mathbb{Z}/3\mathbb{Z}$, für das mir keine konkrete Interpretation eingefallen ist. Ich rate, der Reihe nach folgendes zu zeigen:

1. In einer Gruppe mit 12 Elementen gibt es entweder nur eine 2-Sylow oder nur eine 3-Sylow. Hinweis: Mehr Platz ist nicht vorhanden.

2. Schreiben wir im folgenden $\rtimes$ nur für semidirekte Produkte, die nicht gewöhnliche Produkte sind, so gehört jede Gruppe mit 12 Elementen zu einer der sechs Typen

$$\begin{array}{lll} (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/3\mathbb{Z} & (\mathbb{Z}/2\mathbb{Z})^2 \ltimes \mathbb{Z}/3\mathbb{Z} & (\mathbb{Z}/2\mathbb{Z})^2 \rtimes \mathbb{Z}/3\mathbb{Z} \\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} & \mathbb{Z}/4\mathbb{Z} \ltimes \mathbb{Z}/3\mathbb{Z} & \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z} \end{array}$$

3. Vom letzten dieser Typen existiert keine Gruppe, von jedem anderen Typ existiert bis auf Isomorphismus genau eine, und diese fünf Gruppen sind paarweise nicht isomorph. Hinweis: Man beachte 5.4.18 und beachte auch, daß für den Fall, in dem es von beiden Typen von Sylow nur eine gibt, die Gruppe kommutativ sein muß: Sind H, K die beiden Sylows, so gilt dann ja $hkh^{-1}k^{-1} \in H \cap K$ für alle $h \in H, k \in K$.

Ergänzende Übung 5.4.20. Man zeige, daß die 2-Sylow in der symmetrischen Gruppe $\mathcal{S}_4$ der Drehsymmetrien eines Würfels isomorph ist zur Diedergruppe der Ordnung 8.

Ergänzende Übung 5.4.21. Gegeben in einer endlichen Gruppe G zwei Sylow-Untergruppen P, Q gilt stets $\{p \in P \mid pQp^{-1} = Q\} = P \cap Q$. Hinweis: Die Lösung ist im Beweis der Sylowsätze versteckt.

Übung 5.4.22. Seien $G \supset N$ eine endliche Gruppe mit einem Normalteiler und sei p prim. Man zeige: Genau dann ist eine Untergruppe $P \subset G$ eine p-Sylow von G, wenn $P \cap N$ eine p-Sylow von N ist und das Bild von P in G/N eine p-Sylow von G/N.

Übung 5.4.23. Eine Gruppe mit 30 Elementen kann nie einfach sein. Hinweis: Entweder besitzt sie nur eine 3-Sylow oder nur eine 5-Sylow.

5.5 Symmetrische Gruppen

Definition 5.5.1. Eine **Partition λ einer natürlichen Zahl** $n \in \mathbb{N}$ ist eine monoton fallende Folge von natürlichen Zahlen $\lambda_1 \geq \lambda_2 \geq \ldots$ derart, daß fast alle Folgenglieder verschwinden und die von Null verschiedenen Folgenglieder sich zu n aufsummieren. Die Menge aller Partitionen von n notieren wir $\mathcal{P}_n$.

Beispiel 5.5.2. Die Zahl 5 hat genau sieben Partitionen. Salopp können wir sie beschreiben als die Zerlegungen

$$\begin{aligned}
5 &= 5\\
5 &= 4+1\\
5 &= 3+2\\
5 &= 3+1+1\\
5 &= 2+2+1\\
5 &= 2+1+1+1\\
5 &= 1+1+1+1+1
\end{aligned}$$

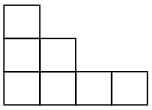
Hier haben wir nur die von Null verschiedenen Folgenglieder aufgeschrieben und sie durch $+$ getrennt. Formal meinen wir zum Beispiel im vierten Fall die Folge $3, 1, 1, 0, 0, \ldots$. Zur Abkürzung verwendet man auch oft die sogenannte **exponentielle Schreibweise**, in der unsere Partitionen von 5 der Reihe nach als 5, 41, 32,

31^2, 2^21, 21^3 und 1^5 geschrieben würden. Sie ist allerdings nur für Partitionen von Zahlen ≤ 9 geschickt.

Ergänzung 5.5.3. Eine in vielen Zusammenhängen geschickte Art, sich Partitionen zu veranschaulichen, sind die sogenannten Youngdiagramme. Unter einem **Youngdiagramm** verstehen wir eine endliche Teilmenge $Y \subset \mathbb{N} \times \mathbb{N}$ mit der Eigenschaft

$$((i,j) \in Y \text{ und } i' \leq i \text{ und } j' \leq j) \quad \Rightarrow \quad (i',j') \in Y$$

Die Elemente von Y nennen wir die **Kästchen** unseres Youngdiagramms und stellen uns ein Element (i,j) vor als das Kästchen auf einem Rechenpapier, bei dem die Koordinaten der linken unteren Ecke gerade (i,j) sind. Zum Beispiel stellt das Bild

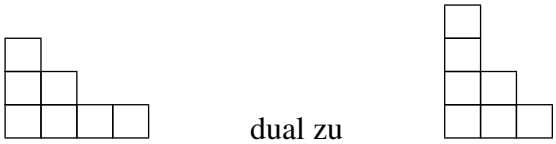


die Menge $\{(0,0),(0,1),(0,2),(1,0),(1,1),(2,0),(3,0)\}$ dar. In der Praxis denke ich bei Youngdiagrammen stets an Bilder dieser Art.

Ergänzung 5.5.4. Jedes Youngdiagramm Y mit n Kästchen im Sinne von 5.5.3 liefert zwei Partitionen der Zahl n, die Partition durch die Zeilenlängen $z(Y)$ und die Partition durch die Spaltenlängen $s(Y)$. Bezeichnet $\mathcal{Y}_n$ die Menge aller Youngdiagramme mit n Kästchen und $\mathcal{P}_n$ die Menge aller Partitionen der Zahl n, so erhalten wir auf diese Weise zwei Bijektionen

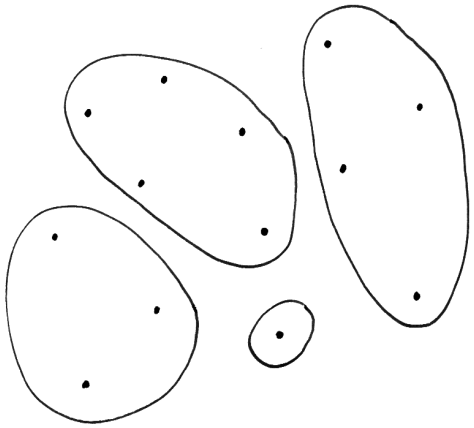
$$\mathcal{P}_n \overset{z}{\xleftarrow{\sim}} \mathcal{Y}_n \overset{s}{\xrightarrow{\sim}} \mathcal{P}_n$$

die zusammen eine selbstinverse Bijektion $\mathcal{P}_n \xrightarrow{\sim} \mathcal{P}_n$ liefern. Diese Bijektion notieren wir $\lambda \mapsto \lambda'$ und nennen λ' die **duale Partition zu** λ. Zum Beispiel ist die duale Partition zu $3,2$ die Partition $2,2,1$ und die duale Partition zu $3,2,1,1$ ist $4,2,1$, im Bild also ist



5.5.5. Unter einer **Partition einer Menge** X verstehen wir wie in 4.1.15 ein System $\mathcal{U} \subset \mathcal{P}(X)$ von paarweise disjunkten nichtleeren Teilmengen, deren Vereinigung ganz X ist. Die Menge aller Partitionen einer gegebenen Menge X notieren wir $\mathcal{P}_X$. Hat X genau n Elemente, so erhalten wir, indem wir die Kardinalitäten der Teilmengen unserer Mengensysteme der Größe nach aufführen und danach Nullen anhängen, eine offensichtliche Surjektion

$$\mathcal{P}_X \twoheadrightarrow \mathcal{P}_n$$



Eine Partition einer Menge mit dreizehn Elementen durch vier Teilmengen. Die im Sinne von 5.5.5 zugehörige Partition der Zahl 13 wäre $13 = 5 + 4 + 3 + 1$.

Eine Permutation $\sigma \in \mathcal{S}_7$, unter der die Bilder der Zahlen $1, 2, 3, 4, 5, 6, 7$ der Reihe nach gerade $2, 5, 3, 4, 1, 7, 6$ sind. Die zugehörige Partition der Menge $\{1, 2, 3, 4, 5, 6, 7\}$ ist durch die gestrichelten Linien angedeutet und wäre in Formeln die Zerlegung $\{1, 2, 3, 4, 5, 6, 7\} = \{1, 2, 5\} \cup \{6, 7\} \cup \{3\} \cup \{4\}$. Die zugehörige Partition der Zahl 7 ist $7 = 3 + 2 + 1 + 1$.

5.5.6. Jede Permutation $\sigma \in \mathrm{Ens}^\times(X)$ einer Menge X liefert eine Partition von X, nämlich die Partition in die Bahnen der von σ erzeugten Untergruppe $\langle\sigma\rangle = \{\sigma^r \mid r \in \mathbb{Z}\}$. Im Fall $|X| = n < \infty$ erhalten wir durch Verknüpfung dieser Abbildung $\mathrm{Ens}^\times(X) \to \mathcal{P}_X$ mit der in 5.5.5 diskutierten Abbildung $\mathcal{P}_X \twoheadrightarrow \mathcal{P}_n$ die sogenannte **Zykellängenabbildung** $\mathrm{Ens}^\times(X) \to \mathcal{P}_n$. Im Fall $X = \{1, \ldots, n\}$ ist das eine Abbildung $\mathcal{S}_n \to \mathcal{P}_n$.

5.5.7. Ich erinnere an die Operation durch Konjugation einer Gruppe auf sich selber aus 4.3.1 und an ihre Bahnen, die Konjugationsklassen.

Satz 5.5.8 (Konjugationsklassen in den symmetrischen Gruppen). *Ist X eine endliche Menge mit $|X| = n$ Elementen, so sind die Fasern der Zykellängenabbildung*

$$\mathrm{Ens}^\times(X) \to \mathcal{P}_n$$

genau die Konjugationsklassen in der Permutationsgruppe $\mathrm{Ens}^\times(X)$.

Ergänzung 5.5.9. Eine analoge Aussage gilt mit demselben Beweis auch für eine beliebige Menge X.

Beweis. Seien Permutationen $\sigma, \tau \in \mathrm{Ens}^\times(X)$ gegeben. Ist $X = X_1 \cup \ldots \cup X_r$ die Partition von X in die Bahnen von $\langle\sigma\rangle$, so ist

$$X = \tau(X_1) \cup \ldots \cup \tau(X_r)$$

die Partition in die Bahnen von $\langle\tau\sigma\tau^{-1}\rangle$, folglich ist die Zykellängenabbildung konstant auf Konjugationsklassen. Die Zykellängenabbildung ist auch offensichtlich surjektiv. Um schließlich zu zeigen, daß je zwei Permutationen mit denselben Zykellängen konjugiert sind, seien etwa $\sigma, \kappa \in \mathrm{Ens}^\times(X)$ unsere beiden Permutationen und

$$\begin{aligned} X &= X_1 \cup \ldots \cup X_r \\ X &= Y_1 \cup \ldots \cup Y_r \end{aligned}$$

die Zerlegungen in Bahnen unter $\langle\sigma\rangle$ und $\langle\kappa\rangle$ mit $|X_i| = |Y_i| = r_i$. Gegeben $z \in X_i$ und $u \in Y_i$ haben wir dann

$$\begin{aligned} X_i &= \{z, \sigma(z), \sigma^2(z), \ldots, \sigma^{r_i}(z) = z\} \\ Y_i &= \{u, \kappa(u), \kappa^2(u), \ldots, \kappa^{r_i}(u) = u\} \end{aligned}$$

Definieren wir also $\tau : X_i \xrightarrow{\sim} Y_i$ durch $\tau(\sigma^\nu(z)) = \kappa^\nu(u)$, so kommutiert das Diagramm

$$\begin{array}{ccc} X_i & \xrightarrow{\sigma} & X_i \\ {\scriptstyle\tau}\downarrow & & \downarrow{\scriptstyle\tau} \\ Y_i & \xrightarrow{\kappa} & Y_i \end{array}$$

Setzen wir dann alle diese $\tau : X_i \xrightarrow{\sim} Y_i$ zusammen zu $\tau : X \xrightarrow{\sim} X$, so gilt ebenso $\kappa\tau = \tau\sigma$ alias $\kappa = \tau\sigma\tau^{-1}$. □

Definition 5.5.10. Hat $\langle\sigma\rangle$ außer einer p-elementigen Bahn nur einelementige Bahnen, so nennt man σ einen **p-Zykel**. Die Zweizykel heißen auch **Transpositionen**.

5.5.11 (**Zykelschreibweise für Permutationen**). Eine Möglichkeit, Permutationen zu notieren, besteht darin, unter jedes Element sein Bild zu schreiben, also etwa

$$\tau \quad = \quad \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 2 & 3 & 5 & 1 \end{bmatrix}$$

Eine andere Möglichkeit ist die Notation als Produkt paarweise disjunkter Zykel. Ein p-Zykel σ wird notiert in der Form $\sigma = (z, \sigma(z), \sigma^2(z), \ldots, \sigma^{p-1}(z))$ wobei $\sigma^p(z) = z$ zu verstehen ist. In **Zykelschreibweise** hätten wir für unsere Permutation τ von eben etwa

$$\tau = (1,6)(2,4,3)(5)$$

und das ist so zu verstehen, daß jedes Element auf das dahinterstehende abgebildet wird, außer wenn es direkt vor einer Klammer steht: Dann wird es auf das erste Element innerhalb seiner Klammer abgebildet. Oft werden Fixpunkte nicht mit notiert, so daß wir also auch schreiben könnten

$$\tau = (1,6)(2,4,3)$$

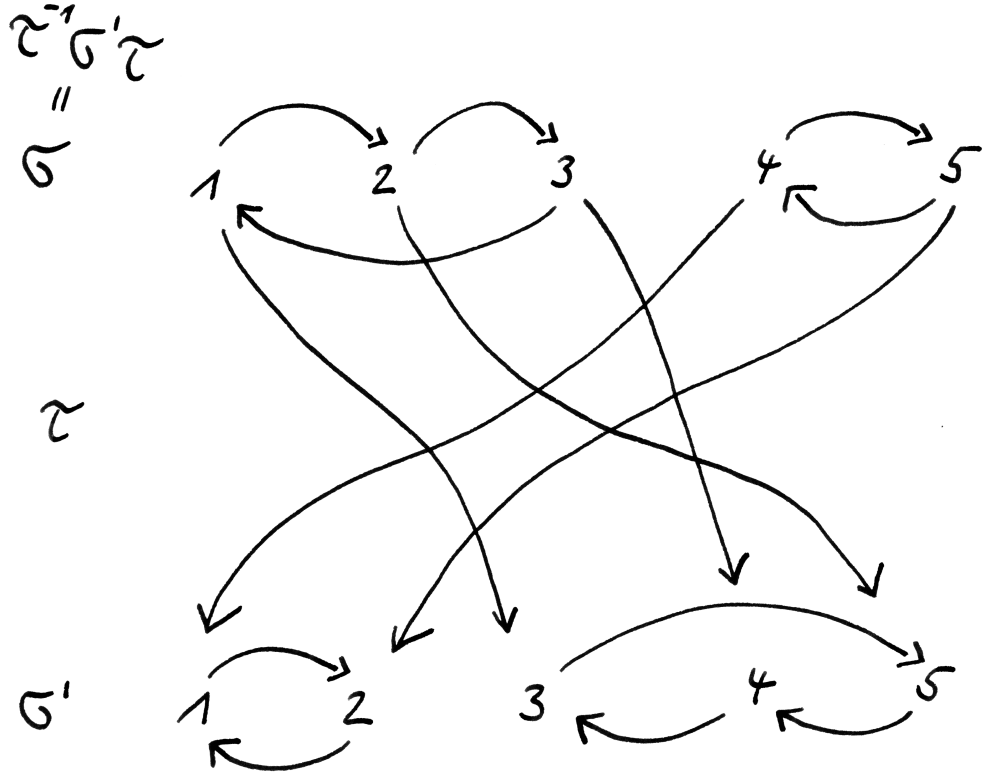
Das ist übrigends auch das Produkt der Transposition $\kappa = (1,6)$ mit den Dreizykel $\rho = (2,4,3)$ und wir haben $\tau = \kappa\rho = \rho\kappa$, was die Sinnhaftigkeit unserer Notation zeigt. Zwei Zykel heißen **disjunkt** genau dann, wenn jedes Element von einem der beiden festgehalten wird. Ganz allgemein kommutieren disjunkte Zykel, so gilt etwa $(1,6)(2,3,4) = (2,3,4)(1,6)$ in $\mathcal{S}_6$.

Übungen

Ergänzende Übung 5.5.12 (**Partitionen und nilpotente Matrizen**). Gegeben ein n-dimensionaler Vektorraum V bildet für jeden nilpotenten Endomorphismus $N \in \operatorname{End} V$ die Folge der Dimensionen $\dim(\operatorname{im} N^r / \operatorname{im} N^{r+1})$ eine Partition von n, und die Fasern der so konstruierten Abbildung

$$\{N \in \operatorname{End} V \mid N \text{ nilpotent}\} \to \mathcal{P}_n$$

sind genau die Bahnen der Operation von $\mathrm{GL}(V)$ durch Konjugation auf der Menge der nilpotenten Endomorphismen von V.



Zwei Permutationen $\sigma, \sigma' \in \mathcal{S}_5$, die dieselbe Partition $5 = 3 + 2$ liefern, und eine Permutation τ, die sie ineinander konjugiert.

Übung 5.5.13. Die symmetrische Gruppe $\mathcal{S}_5$ besitzt genau sieben Konjugationsklassen.

Ergänzende Übung 5.5.14. Das Signum eines p-Zykels ist stets $(-1)^{p+1}$.

Übung 5.5.15. Man zeige unabhängig von unseren geometrischen Betrachtungen zur Ikosaedergruppe 5.2.5, daß es in der alternierenden Gruppe A_5 genau 5 Konjugationsklassen gibt, die die Kardinalitäten 20, 15, 12, 12 und 1 haben. Man folgere, daß die alternierende Gruppe A_5 einfach ist.

Ergänzende Übung 5.5.16 (**Zentralisatoren in symmetrischen Gruppen**). Seien X eine endliche Menge und $\sigma \in \mathcal{S} := \mathrm{Ens}^\times X$ eine Permutation von X. Ihr Zentralisator $\mathrm{Z}_\mathcal{S}(\sigma)$ nach 5.3.3 operiert auf dem Bahnenraum von $\langle\sigma\rangle$ und jede Permutation des Bahnenraums $X/\langle\sigma\rangle$, die die Kardinalitäten von Bahnen erhält, kann durch ein Element unseres Zentralisators realisiert werden. Hat unser σ jeweils $n(i)$ Zykel der Länge i und keinen Zykel einer Länge $> r$, so hat das Bild von $\mathrm{Z}_\mathcal{S}(\sigma) \to \mathrm{Ens}^\times(X/\langle\sigma\rangle)$ also genau $n(1)!n(2)!\ldots n(r)!$ Elemente. Der Kern hinwiederum besteht aus denjenigen Elementen des Zentralisators, die jede Bahn von $\langle\sigma\rangle$ auf sich selber abbilden, und davon gibt es offensichtlich $1^{n(1)}\ldots r^{n(r)}$ Stück. Zusammen erhalten wir mit 1.3.11 so

$$|\mathrm{Z}_\mathcal{S}(\sigma)| = \prod_{i=1}^{r} n(i)!i^{n(i)}$$

5.6 Alternierende Gruppen*

5.6.1. Die Abbildung sgn, die jeder Permutation $\tau \in \mathcal{S}_r$ ihr Signum zuordnet, ist ein Gruppenhomomorphismus $\mathrm{sgn} : \mathcal{S}_r \to \{1, -1\}$. Der Kern dieses Gruppenhomomorphismus, d.h. die Gruppe aller geraden Permutationen von r Objekten, heißt die r-te **alternierende Gruppe** und wird notiert als

$$A_r = \ker(\mathrm{sgn} : \mathcal{S}_r \to \{1, -1\})$$

Satz 5.6.2. *Die alternierenden Gruppen A_r sind einfach für $r \geq 5$.*

5.6.3. In der alternierenden Gruppe A_4 bilden die drei Doppeltranspositionen zusammen mit dem neutralen Element einen Normalteiler, der isomorph ist zur Klein'schen Vierergruppe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Insbesondere ist A_4 nicht einfach. Die Gruppen A_1 und A_2 sind trivial, $A_3 \cong \mathbb{Z}/3\mathbb{Z}$ ist jedoch auch noch einfach. Daß A_5 einfach ist, kann man wie beim Beweis der Einfachkeit der Ikosaedergruppe unmittelbar einsehen, indem man die Kardinalitäten der Konjugationsklassen berechnet. Dem Beweis des Satzes im allgemeinen schicken wir zwei Lemmata voraus.

5.6.4. Hat das Erzeugnis $\langle\sigma\rangle$ einer Permutation σ genau zwei zweielementige und sonst nur einelementige Bahnen, so heißt σ eine **Doppeltransposition**. Hat $\langle\sigma\rangle$ genau zwei dreielementige und sonst nur einelementige Bahnen, so nennen wir σ einen **Doppeldreizykel**.

Lemma 5.6.5. *Die symmetrischen Gruppen $\mathcal{S}_r$ werden von den Transpositionen erzeugt, die alternierenden Gruppen A_r von den Dreizykeln.*

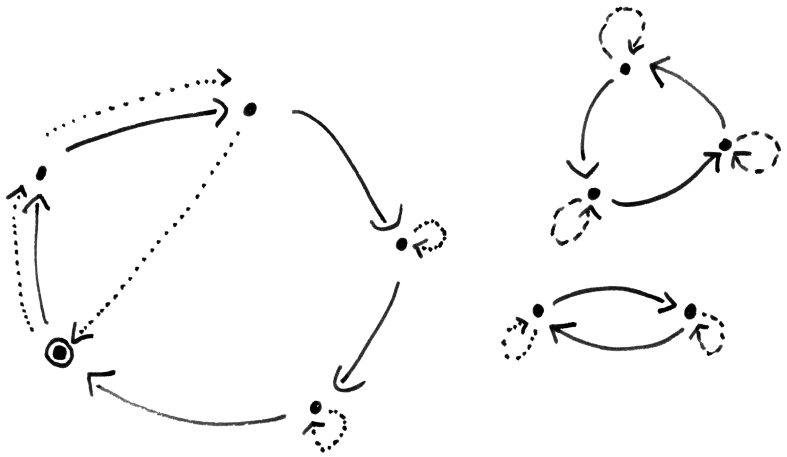
Beweis. Die erste Aussage war Übung **??**. Die Zweite folgt daraus, daß man jede Doppeltransposition als Produkt von zwei Dreizykeln schreiben kann, $(ab)(cd) = (abc)(bcd)$, und daß das Produkt von zwei nicht kommutierenden Transpositionen ein Dreizykel ist, $(ab)(ac) = (acb)$. Jedes Produkt einer geraden Zahl von Transpositionen läßt sich demnach auch als ein Produkt von Dreizykeln darstellen. □

Lemma 5.6.6. *Für $r \geq 5$ wird die alternierende Gruppe A_r nicht nur erzeugt von den Dreizykeln, sondern auch von den Doppeltranspositionen. Des weiteren sind für $r \geq 5$ je zwei Doppeltranspositionen und je zwei Dreizykel auch schon in A_r konjugiert.*

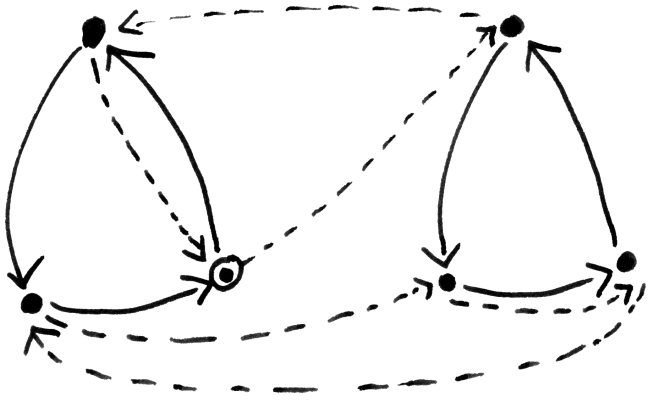
Beweis. Jeder Dreizykel kann als Verknüpfung von zwei Transpositionen seiner drei Elemente dargestellt werden. Haben wir noch zwei weitere Elemente zur Verfügung, so können wir diese beiden Transpositionen durch das Verknüpfen mit der Vertauschung dieser beiden Elemente zu Doppeltranspositionen machen. Das zeigt die erste Aussage. Zwei Doppeltranspositionen $(ab)(cd)$ und $(a'b')(c'd')$ sind konjugiert unter jeder Permutation τ mit $a \mapsto a', \ldots, d \mapsto d'$ und auch unter $\tau \circ (ab)$. Entweder τ oder $\tau \circ (ab)$ ist aber stets gerade. Zwei Dreizykel (abc) und $(a'b'c')$ sind konjugiert unter jeder Permutation τ mit $a \mapsto a', \ldots, c \mapsto c'$ und insbesondere auch unter $\tau \circ (de)$ für (de) disjunkt von (abc). Entweder τ oder $\tau \circ (de)$ ist aber stets gerade. Das zeigt die zweite Aussage. □

Beweis von 5.6.2. Sei ab jetzt r beliebig und $N \subset A_r$ ein nichttrivialer Normalteiler. Nach dem vorhergehenden Lemma 5.6.6 reicht es zu zeigen, daß es in N entweder eine Doppeltransposition oder einen Dreizykel gibt. Dazu zeigen wir, wie man zu jedem nichttrivialen Element $g \in N$, das weder eine Doppeltransposition noch ein Dreizykel ist, ein anderes nichttriviales Element $\tilde{g} \in N$ mit noch mehr Fixpunkten konstruieren kann. Indem wir zu Potenzen von g übergehen, können wir g von Primzahlordnung annehmen.

Ist $\operatorname{ord} g \geq 5$, so wählen wir einen Zykel von g und betrachten einen Dreizykel h, der von einem festen Ausgangspunkt auf dem Zykel von g zwei Schritte mitläuft um dann wieder zum Ausgangspunkt zurückzukehren. Dann ist unser Ausgangspunkt ein Fixpunkt von $\tilde{g} = h^{-1}g^{-1}hg$ und wir haben ein nichttriviales $\tilde{g} \in N$ gefunden, das mehr Fixpunkte hat als g.



Die durchgezogenen Pfeile stellen eine Permutation g der Ordnung ≥ 5 auf der Menge der fetten Punkte dar, die gestrichelten Pfeile den im Beweis beschriebenen Dreizykel h, der umrandete Punkt unseren „Ausgangspunkt“.



Die durchgezogenen Pfeile stellen einen Doppeldreizykel g auf der Menge der fetten Punkte dar, die gestrichelten Pfeile den im Beweis beschriebenen dazu konjugierten Doppeldreizykel h, der umrandete Punkt einen Fixpunkt von hg.

Ist $\operatorname{ord} g = 3$ und ist g kein Dreizykel, so muß g ein Produkt sein von mindestens zwei disjunkten Dreizykeln. Dann stimmen die Konjugationsklassen von g in A_r und in $\mathcal{S}_r$ überein, da es nämlich eine ungerade Permutation gibt, die mit g kommutiert, zum Beispiel eine geeignete „Dreifachtransposition zwischen zwei Dreizykeln von g“. Es ist nun ein Leichtes, in $\mathcal{S}_6$ zwei Doppeldreizykel zu finden derart, daß ihr Produkt nicht trivial ist und dennoch einen Fixpunkt hat. Wenn wir also einen Doppeldreizykel von g auf der zugehörigen 6-elementigen Menge konjugieren zu einem geeigneten anderen Doppeldreizykel, so erhalten wir ein $h \in N$ derart, daß hg nicht trivial ist und mehr Fixpunkte hat als g.

Ist schließlich $\operatorname{ord} g = 2$ und g keine Doppeltransposition, so muß g ein Produkt sein von mindestens zwei disjunkten Doppeltranspositionen. Wieder stimmen dann die Konjugationsklassen von g in A_r und in $\mathcal{S}_r$ überein, da es eine ungerade Permutation gibt, die mit g kommutiert, zum Beispiel eine „Transposition aus einer Doppeltransposition von g“. Wir finden also $h \in N$ derart, daß h auf einer vierelementigen Teilmenge eine andere Doppeltransposition ist als g und außerhalb dieser vierelementigen Teilmenge mit g übereinstimmt. Dann ist hg die dritte Doppeltransposition auf unserer vierelementigen Teilmenge und die Identität außerhalb, ist also einerseits nicht trivial und hat andererseits mehr Fixpunkte als g. □

Übungen

Übung 5.6.7. Man zeige, daß die Gruppe aller jeweils nur endlich viele Elemente bewegenden geraden Permutationen einer unendlichen Menge eine einfache aber nicht endlich erzeugte Gruppe ist.

Ergänzende Übung 5.6.8. Man zeige für $r \geq 5$, daß A_r der einzige nichttriviale echte Normalteiler von $\mathcal{S}_r$ ist. Man bestimme alle Kompositionsreihen aller symmetrischen Gruppen.

5.6.9. Nach der vorhergehenden Übung ist für $r \geq 5$ jeder Gruppenhomomorphismus von der symmetrischen Gruppe $\mathcal{S}_r$ in eine weitere Gruppe entweder injektiv oder konstant oder hat denselben Kern wie das Signum. Salopp gesprochen kann es also kein „verbessertes Signum“ geben.

Ergänzende Übung 5.6.10. In dieser Übung sollen Sie zeigen, daß die Gruppe $\mathrm{SL}(2;\mathbb{F}_5)$ genau fünf 2-Sylows besitzt und daß die Operation dieser Gruppe auf der Menge ihrer 2-Sylows einen Isomorphismus

$$\mathrm{SL}(2;\mathbb{F}_5)/\{\pm \mathrm{id}\} \;\tilde{\to}\; A_5$$

mit der sogenannten „alternierenden Gruppe“ aller geraden Permutationen einer fünfelementigen Menge induziert. Den Quotienten auf der linken Seite notiert man auch $\mathrm{PSL}(2;\mathbb{F}_5)$, er liegt als Untergruppe vom Index 2 in der Gruppe

$\mathrm{PGL}(2;\mathbb{F}_5)$ aller von invertierbaren Matrizen induzierten Automorphismen der projektiven Gerade alias dem Quotienten von $\mathrm{GL}(2;\mathbb{F}_5)$ nach der Gruppe der vier darin enthaltenen Diagonalmatrizen. Ich rate, der Reihe nach folgendes zu zeigen:

1. Jedes Element der Ordnung 4 in $\mathrm{SL}(2;\mathbb{F}_5)$ ist diagonalisierbar und der Normalisator seines Erzeugnisses ist eine 2-Sylow. Jede 2-Sylow enthält 6 Elemente der Ordnung 4.

2. Es gibt in $\mathrm{SL}(2;\mathbb{F}_5)$ genau dreißig Elemente der Ordnung 4 und fünf 2-Sylows, und der Schnitt von je zwei verschiedenen 2-Sylows besteht nur aus $\pm\mathrm{id}$.

3. Jede 2-Sylow von $\mathrm{PSL}(2;\mathbb{F}_5)$ ist eine Klein'sche Vierergruppe und operiert nach 5.4.21 frei auf der Menge der vier anderen 2-Sylows. Vom Bild unseres Homomorphismus $\mathrm{PSL}(2;\mathbb{F}_5) \to \mathcal{S}_5$ wissen wir damit, daß es alle Doppeltranspositionen enthält und aus höchstens 60 Elementen besteht. Nach 5.6.6 muß dieses Bild folglich die A_5 sein.

Ergänzung 5.6.11. Genau dann ist jede gerade Permutation von n Objekten ein Produkt von zwei l-Zykeln, falls gilt $3n/4 \leq l$. Edward Bertram: Even permutations as a product of two conjugate cycles. J. Combinatorial Theory Ser. A, 12: S. 368-380, 1972.

6 Mehr zu Ringen

6.1 Quotientenringe

6.1.1. Wir erinnern die grundlegenden Definitionen zu Ringen aus 2.1. Unter einem **Ring** versteht man eine Menge mit zwei Verknüpfungen $(R, +, \cdot)$ derart, daß $(R, +)$ eine abelsche Gruppe ist und $(R, \cdot)$ ein Monoid und daß für alle $a, b, c \in R$ die Distributivgesetze $a(b + c) = ab + ac$ sowie $(a + b)c = ac + bc$ gelten.

6.1.2. Das neutrale Element des multiplikativen Monoids eines Rings notiert man meist $1_R = 1$. Ein typisches Beispiel ist der Ring $\mathbb{Z}$ der ganzen Zahlen mit der üblichen Addition und Multiplikation als Verknüpfung. Ebenfall typisch ist der Ring $\mathrm{Mat}(n; R)$ der $(n \times n)$-Matrizen mit Einträgen aus einem beliebigen Ring R mit der Addition und Multiplikation von Matrizen als Verknüpfung.

6.1.3. Eine Abbildung $\varphi : R \to S$ von einem Ring in einen anderen heißt ein **Ringhomomorphismus**, wenn sie sowohl ein Gruppenhomomorphismus ist für die zugrundeliegenden additiven Gruppen als auch ein Monoidhomomorphismus ist für die zugrundeliegenden multiplikativen Monoide.

6.1.4. Wir fordern von einem Monoidhomomorphismus stets, daß er das neutrale Element auf das neutrale Element abbildet. Insbesondere fordern wir damit von einem Ringhomomorphismus stets $\varphi(1_R) = 1_S$. Die Menge aller Ringhomomorphismen von einem Ring R in einen Ring S notieren wir $\mathrm{Ring}(R, S)$.

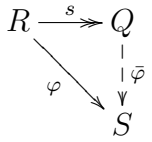
6.1.5. Die Stärke der Ringtheorie liegt unter anderem darin, daß es sehr viele Vefahren gibt, die zu einem gegebenen Ring einen weiteren Ring konstruieren, und daß man auf diese neuen Ringe dann wieder alle bereits bekannten Sätze anwenden kann. Beispiele sind das Bilden von Polynomringen, Potenzreihenringen 2.3.42 und Matrizenringen. Wir besprechen im folgenden zusätzlich das Bilden von Restklassenringen.

Satz 6.1.6 (Universelle Eigenschaft surjektiver Ringhomomorphismen). *Seien $s : R \twoheadrightarrow Q$ ein surjektiver Ringhomomorphismus und $\varphi : R \to S$ ein beliebiger Ringhomomorphismus. Genau dann existiert ein Ringhomomorphismus $\bar{\varphi} : Q \to S$ mit $\varphi = \bar{\varphi} \circ s$, wenn gilt $\ker(\varphi) \supset \ker(s)$.*

6.1.7. Dieser Homomorphismus $\bar{\varphi}$ ist dann natürlich eindeutig bestimmt. In diesem Sinne kann man diesen Satz auch dahingehend zusammenfassen, daß das Vorschalten eines surjektiven Homomorphismus $s : R \twoheadrightarrow Q$ für jeden weiteren Ring S eine Bijektion

$$(\circ s) : \mathrm{Ring}(Q, S) \xrightarrow{\sim} \{\varphi \in \mathrm{Ring}(R, S) \mid \ker(\varphi) \supset \ker(s)\}$$

liefert. Der Übersichtlichkeit halber stelle ich die in diesem Satz auftauchenden Ringe und Morphismen auch noch wieder anders in einem Diagramm dar:



Man formuliert diesen Satz auch mit den Worten, φ **faktorisiere in eindeutiger Weise über** s.

Beweis. Offensichtlich ist φ konstant auf den Fasern von s. Damit, oder auch indem wir die universelle Eigenschaft von surjektiven Gruppenhomomorphismen 3.2.1 zitieren, finden wir schon mal eine Abbildung $\bar{\varphi}$ wie behauptet. Man prüft leicht, daß sie ein Ringhomomorphismus ist. □

6.1.8 (**Surjektive Ringhomomorphismen mit gleichem Kern**). Gegeben ein Ring R und zwei surjektive Ringhomomorphismen $s : R \twoheadrightarrow Q$ und $t : R \twoheadrightarrow P$ mit demselben Kern $\ker(s) = \ker(t)$ sind die Ringhomomorphismen $\bar{t} : Q \to P$ mit $\bar{t} \circ s = t$ und $\bar{s} : P \to Q$ mit $\bar{s} \circ t = s$ nach 6.1.6 offensichtlich zueinander inverse Isomorphismen $Q \xrightarrow{\sim} P \xrightarrow{\sim} Q$. Salopp gesprochen wird also bei einem surjektiven Ringhomomorphismus „das Ziel bereits durch den Ausgangsraum und den Kern festgelegt bis auf eindeutigen Isomorphismus“.

Definition 6.1.9. Sei R ein Ring. Ein **Ideal von** R ist eine Teilmenge $I \subset R$ mit der Eigenschaft, daß I eine Untergruppe ist von $(R, +)$ und daß zusätzlich gilt $RI \subset I$ und $IR \subset I$.

6.1.10. Anders gesagt ist also Teilmenge $I \subset R$ eines Rings ein Ideal genau dann wenn gilt $0 \in I$, $a, b \in I \Rightarrow a + b \in I$, $a \in I \Rightarrow (-a) \in I$ sowie $r \in R, a \in I \Rightarrow ra, ar \in I$. Die Bedingung $(-a) \in I$ ist dabei sogar überflüssig, weil ja eh gilt $(-a) = (-1)a$ für alle $a \in R$. Weiter kann die Bedingung $0 \in I$ durch die Bedingung $I \neq \emptyset$ ersetzt werden, da ja gilt $0 = 0b$ für alle $b \in R$.

Beispiele 6.1.11. Ein Ideal von $\mathbb{Z}$ ist dasselbe wie eine Untergruppe von $\mathbb{Z}$, die Ideale von $\mathbb{Z}$ sind also nach 1.3.4 genau die Teilmengen der Gestalt $\mathbb{Z}m$ für $m \in \mathbb{N}$. Für ein beliebiges Element a in einem kommutativen Ring R ist die Menge Ra aller Vielfachen von a ein Ideal. Der ganze Ring R und $\{0\}$ sind stets Ideale.

6.1.12. Ist $\varphi : R \to S$ ein Ringhomomorphismus, so ist $\ker \varphi := \varphi^{-1}(0)$ ein Ideal von R. Man versteht bei Ringhomomorphismen den Kern stets in Bezug auf die additive Struktur. Allgemeiner ist das Urbild von einem Ideal unter einem Ringhomomorphismus stets wieder ein Ideal, und desgleichen das Bild eines Ideals unter einem *surjektiven* Ringhomomorphismus.

Proposition 6.1.13. *Seien R ein Ring und $I \subset R$ ein Ideal. So gibt es einen von R ausgehenden surjektiven Ringhomomorphismus mit I als Kern.*

6.1.14. Nach 6.1.8 ist ein surjektiver Ringhomomorphismus mit Kern I eindeutig bis auf das Nachschalten eines eindeutigen Isomorphismus. Wir notieren ihn

$$\mathrm{can} = \mathrm{can}_{\mathrm{q}} : R \twoheadrightarrow R/I$$

Vorsichtig veranlagte Leser mögen unter R/I alternativ das im folgenden Beweis konstruierte explizite Beispiel für solch einen Ringhomomorphismus verstehen. Das Bild in R/I von $a \in R$ bezeichnet man auch oft mit $\mathrm{can}(a) = \bar{a}$. Man nennt R/I einen **Restklassenring** oder **Quotientenring** oder abkürzend **Quotienten** oder auch einen **Faktorring**. Er darf nicht verwechselt werden mit dem Quotientenkörper eines kommutativen Integritätsbereichs, wie er in 2.5.2 eingeführt wurde.

Beispiel 6.1.15. Den Spezialfall der Restklassenringe $\mathbb{Z}/m\mathbb{Z}$ kennen wir bereits aus 2.2.4. Ich ziehe im allgemeinen die Bezeichnung als Quotientenring vor.

Beweis. Wir gehen aus von der Surjektion $q : R \twoheadrightarrow R/I$ auf die Quotientengruppe in Bezug auf die additive Struktur. Dann gibt es genau eine bilineare Abbildung $\bar{m} : R/I \times R/I \to R/I$ derart, daß mit der Multiplikation m in der oberen Horizontale das Diagramm

$$\begin{array}{ccc} R \times R & \xrightarrow{\ m\ } & R \\ {\scriptstyle q\times q}\downarrow & & \downarrow{\scriptstyle q} \\ R/I \times R/I & \xrightarrow{\ \bar{m}\ } & R/I \end{array}$$

kommutiert, denn $q \circ m$ ist konstant auf den Fasern von $q \times q$. In der Tat haben wir $(r+i)(s+j) = rs+is+rj+ij \in rs+I$ für alle $i, j \in I$ und $r, s \in R$. In größerer Allgemeinheit haben Sie das möglicherweise bereits als Übung 3.2.27 geprüft. Es ist dann leicht zu sehen, daß $\bar{m}$ als Multiplikation die Nebenklassengruppe R/I zu einem Ring macht. □

6.1.16. Ganz allgemein ist ein Schnitt von Idealen eines Rings R stets wieder ein Ideal. Gegeben eine Teilmenge $T \subset R$ bezeichen wir mit $\langle T \rangle \subset R$ das kleinste Ideal von R, das T umfaßt, und nennen es das **von T erzeugte Ideal**. Wir können $\langle T \rangle$ entweder beschreiben als den Schnitt aller Ideale, die T umfassen, oder als die Menge aller endlichen Ausdrücke

$$\langle T \rangle = \{a_1 t_1 b_1 + \ldots + a_n t_n b_n \mid n \geq 0,\ a_i, b_i \in R,\ t_i \in T\}$$

Hierbei ist der leere Ausdruck mit $n = 0$ wie üblich als die Null von R zu verstehen. Ist $T = \{t_1, \ldots, t_r\}$ eine endliche Menge, so schreiben wir auch $\langle T \rangle =$

$\langle t_1, \ldots, t_r \rangle$. Insbesondere gilt für einen kommutativen Ring R zum Beispiel $\langle a \rangle = Ra$ für alle $a \in R$. Wollen wir betonen, daß das Symbol zwischen den Spitzklammern für eine Menge von Erzeugern und nicht für einen einzigen Erzeuger steht, so schreiben wir $\langle T \rangle = \langle {}_!T \rangle$. Ideale, die von einem einzigen Element erzeugt werden können, heißen **Hauptideale**. Insbesondere ist nach 1.3.4 jedes Ideal in $\mathbb{Z}$ ein Hauptideal.

Ergänzung 6.1.17. Sei R ein Ring und $T \subset R$ eine Teilmenge. Wenn wir betonen wollen, daß $\langle T \rangle$ das von T erzeugte Ideal und nicht etwa die von T erzeugte Untergruppe meint, schreiben wir auch ${}_R\langle T \rangle_R$ oder $\langle RTR \rangle$ und im Fall eines kommutativen Rings $\langle T \rangle_R$ oder $\langle TR \rangle$. Im Fall eines nichtkommutativen Rings dahingegen meint $\langle T \rangle_R = \langle TR \rangle$ das von T erzeugte Rechtsideal, wie es in **??** eingeführt wird.

Ergänzung 6.1.18 (**Herkunft der Bezeichnung „Ideal“**). Die Bezeichnung als „Ideal“ ist abgeleitet von Kummer's Begriff einer „idealen Zahl“. Diese „idealen Zahlen“ führte Kummer ein, um Schwierigkeiten im Zusammenhang mit der Nichtexistenz eindeutiger Primfaktorzerlegungen in sogenannten „Ganzheitsringen von Zahlkörpern“ zu umgehen. Das einfachste Beispiel $\mathfrak{o} = \mathbb{Z}[\sqrt{-5}]$ für dieses Phänomen besprechen wir in 6.4.8. Erklären wir auf der Menge aller von Null verschiedenen Ideale eines solchen Ganzheitsrings $\mathfrak{o}$ eine Verknüpfung, in dem wir IJ als das von allen Produkten ab mit $a \in I$ und $b \in J$ erzeugte Ideal alias die von allen solchen Produkten erzeugte Untergruppe verstehen, die wir eigentlich $\langle IJ \rangle$ notieren müßten, so gilt in dieser Menge aller Ideale nämlich das Analogon der eindeutigen Primfaktorzerlegung, vergleiche etwa **??**. Ordnen wir nun jeder Zahl $a \in \mathfrak{o}$ das von a erzeugte Hauptideal $\langle a \rangle$ zu, so erhalten wir eine Einbettung

$$\mathfrak{o}/\mathfrak{o}^\times \hookrightarrow \{I \subset \mathfrak{o} \mid I \text{ ist Ideal}\}$$

des Monoids aller „bis auf Einheiten wohlbestimmten Elemente von $\mathfrak{o}$“, in dem das Analogon der eindeutigen Primfaktorzerlegung nicht immer gilt, in das Monoid aller von Null verschiedenen Ideale, in dem es im Fall des Ganzheitsrings eines Zahlkörpers eben doch immer gilt. Kummer konnte das in einigen Fällen bereits selbst zeigen und bezeichnete deshalb die Elemente dieses größeren Monoids, das er selbst auf recht verschlungenen Wegen konstruierte, als „ideale Zahlen“.

6.1.19 (**Ideale und Teilerbeziehung**). Gegeben ein Kring R und Elemente $a, b \in R$ ist a ein Teiler von b genau dann, wenn gilt $\langle a \rangle \ni b$ oder gleichbedeutend $\langle a \rangle \supset \langle b \rangle$, in Formelsprache

$$a|b \Leftrightarrow b \in \langle a \rangle \Leftrightarrow \langle b \rangle \subset \langle a \rangle$$

Gegeben ein Kring R und ein Element $u \in R$ ist u eine Einheit genau dann, wenn gilt $\langle u \rangle = R$. Gegeben ein kommutativer Integritätsbereich folgt aus $\langle a \rangle = \langle b \rangle$, daß es eine Einheit $u \in R^\times$ gibt mit $au = b$.

Beispiel 6.1.20 (**Quotienten von Polynomringen**). Gegeben ein Körper k und ein von Null verschiedenes Polynom $P \in k[X]\backslash 0$ haben wir

$$\dim_k k[X]/\langle P\rangle = \operatorname{grad} P$$

Genauer bilden für $\operatorname{grad} P = d$ die Nebenklassen der Monome $1, X, \ldots, X^{d-1}$ eine k-Basis des Restklassenrings $k[X]/\langle P\rangle$. Noch etwas allgemeiner liefert Polynomdivision mit Rest 2.3.15 für jeden Kring k und jedes normierte Polynom $P \in k[X]$, daß die Polynome von einem Grad $\leq (\operatorname{grad} P) - 1$ ein Repräsentantensystem für die Menge $k[X]/\langle P\rangle$ der Nebenklassen nach dem von P erzeugten Hauptideal bilden. Bezeichnet also $k[X]^{\leq n} \subset k[X]$ die Menge aller Polynome vom Grad $\leq n$, so liefert für jedes normierte Polynom P die kanonische Projektion einen Gruppenisomorphismus

$$k[X]^{\leq (\operatorname{grad} P)-1} \xrightarrow{\sim} k[X]/\langle P\rangle$$

Beispiel 6.1.21 (**Die komplexen Zahlen als Quotient**). Wir erinnern die komplexen Zahlen $\mathbb{C}$ mit ihrem ausgezeichneten Element $\mathrm{i} \in \mathbb{C}$. Das Einsetzen von i für X im Sinne von 2.3.5 liefert mithilfe der universellen Eigenschaft des Quotienten 6.1.13 Isomorphismen von Ringen

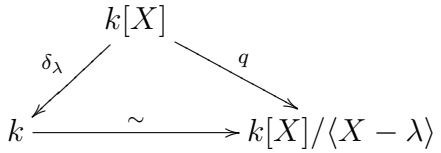
$$\mathbb{R}[X]/\langle X^2 + 1\rangle \xrightarrow{\sim} \mathbb{C}$$

und $\mathbb{Z}[X]/\langle X^2 + 1\rangle \xrightarrow{\sim} \mathbb{Z}[\mathrm{i}]$. Hier ist $\mathbb{Z}[\mathrm{i}]$ im Sinne von 6.2.1 zu verstehen als der Ring aller komplexen Zahlen mit ganzzahligem Real- und Imaginärteil. Ich mache die Nebenrechnung $(X - (2+\mathrm{i}))(X - \overline{(2+\mathrm{i})}) = X^2 - 4X + 3$. Das Einsetzen von $2 + \mathrm{i}$ für X liefert also auch einen Isomorphismus

$$\mathbb{R}[X]/\langle X^2 - 4X + 2\rangle \xrightarrow{\sim} \mathbb{C}$$

Allgemeiner könnten wir hier den Quotienten nach jedem Polynom vom Grad Zwei ohne reelle Nullstelle nehmen.

6.1.22. Gegeben ein Kring k und ein Element $\lambda \in k$ kommutiert das Diagramm



mit der Auswertungsabbildung δ_λ und der von der Einbettung $k \hookrightarrow k[X]$ induzierten unteren Horizontalen.

6.1.23 (**Polynomringe über Restklassenringen**). Gegeben sei ein Ring R mit einem Ideal I. Bezeichnet $I[X] \subset R[X]$ das von unserem Ideal I im Polynomring erzeugte Ideal, so induziert der offensichtliche Ringhomomorphismus $R[X] \twoheadrightarrow (R/I)[X]$ aus 2.3.11 offensichtlich einen Isomorphismus

$$R[X]/I[X] \xrightarrow{\sim} (R/I)[X]$$

Übungen

Ergänzende Übung 6.1.24. Man zeige: Gegeben ein surjektiver Ringhomomorphismus $\varphi : R \twoheadrightarrow S$ liefert das Bilden des Urbilds eine Bijektion zwischen der Menge der Ideale von S und der Menge derjenigen Ideale von R, die $\ker \varphi$ umfassen.

Übung 6.1.25. Gegeben ein normiertes Polynom P mit Koeffizienten in einem Körper k ist das P bis auf ein Vorzeichen genau das charakteristsche Polynom der Multiplikation mit X als Endomorphismus des k-Vektorraums $k[X]/\langle P\rangle$.

6.2 Teilringe

Definition 6.2.1. Eine Teilmenge eines Rings heißt ein **Teilring**, wenn sie so mit der Struktur eines Rings versehen werden kann, daß die Einbettung ein Ringhomomorphismus wird. Gleichbedeutend und expliziter ist das eine Teilmenge eines Rings, die sein Einselement enthält, die abgeschlossen ist unter Addition und Multiplikation, und die mit diesen Verknüpfungen zu einem Ring wird.

Ergänzung 6.2.2. Die in 2.1.5 bereits angesprochene Begriffsverwirrung setzt sich hier fort: Autoren, deren Ringe kein Einselement zu enthalten brauchen, fordern von ihren Teilringen zwar dem Wortlaut nach dasselbe wie wir im ersten Satz der Definition 6.2.1. Es bedeutet dann aber in unserer Terminologie nur noch, daß unsere Teilmenge unter Addition und Multiplikation abgeschlossen ist und mit diesen Verknüpfungen zu einem Rng wird. Wir nennen eine derartige Teilmenge eine **$\mathbb{Z}$-Unteralgebra**. Jedes Ideal eines Rings ist eine $\mathbb{Z}$-Unteralgebra, aber das einzige Ideal, das ein Teilring ist, ist der ganze Ring selber. Es ist im übrigen auch durchaus möglich, daß eine $\mathbb{Z}$-Unteralgebra eine Rings selbst wieder ein Ring ist, ohne aber in unserem Sinne ein Teilring zu sein: Der Nullring etwa ist eine $\mathbb{Z}$-Unteralgebra aber kein Teilring von $\mathbb{Q}$, und der Ring $\mathbb{Z} \times 0$ ist eine $\mathbb{Z}$-Unteralgebra aber kein Teilring von $\mathbb{Z} \times \mathbb{Z}$.

6.2.3. Jeder Schnitt von Teilringen ist selbst ein Teilring. Den kleinsten Teilring eines Ringes R, der eine gegebene Teilmenge $T \subset R$ umfaßt, heißt der **von** T **erzeugte Teilring**. Gegeben $S \supset R$ ein Kring mit einem Teilring und Elemente $a_1, \ldots, a_n \in S$ bezeichnet man mit

$$R[a_1, \ldots, a_n] \subset S$$

den Teilring von S, der von R und den a_i erzeugt wird, in anderen Worten den kleinsten Teilring von S, der R umfaßt und alle a_i enthält.

6.2.4. Die Notation aus 6.2.1 führt leicht zu Verwechslungen mit Polynomringen. Viele Autoren verwenden die Konvention, nach der die „freien“ oder „unabhängigen“ Variablen in Polynomringen mit großen Buchstaben vom Ende des Alphabets geschrieben werden, die „abhängigen“ Erzeuger eines Teilrings in einem bereits gegebenen Ring dahingegen mit kleinen Buchstaben. Nebenbei bemerkt kann man $R[a_1, \ldots, a_n]$ auch beschreiben als das Bild des Einsetzungshomomorphismus $R[X_1, \ldots, X_n] \to S$ mit $X_i \mapsto a_i$. Ist dieser Einsetzungshomomorphismus injektiv, also ein Isomorphismus auf sein Bild, so heißen die Elemente a_i **algebraisch unabhängig über** R. Wollen wir besonders betonen, daß wir mit freien Veränderlichen arbeiten, so setzen wir ein kleines „Freiheitsstrichlein“ vorne in die Klammer und schreiben $R[{}'X_1, \ldots, X_n]$. Diese Notation gibt es jedoch meines Wissens bisher nur in diesem Skriptum.

6.2.5 (**Isomorphiesatz für Ringe**). Gegeben ein Ringhomomorphismus $\varphi : R \to S$ ist nach 6.1.12 der Kern $\ker \varphi$ ein Ideal von R und das Bild $\operatorname{im} \varphi$ offensichtlich ein Teilring von S. Nach 6.1.13 und dem Isomorphiesatz 3.2.12 faktorisiert φ dann über einen Ringisomorphismus

$$R \twoheadrightarrow R/(\ker \varphi) \xrightarrow{\sim} \operatorname{im} \varphi \hookrightarrow S$$

Übungen

Ergänzende Übung 6.2.6. Seien $K \subset L$ Körper, $I \subset K[X_1, \ldots, X_n]$ ein Ideal. Bezeichne $\langle IL[X_1, \ldots, X_n]\rangle$ das von I im Polynomring über L erzeugte Ideal. So gilt

$$I = K[X_1, \ldots, X_n] \cap \langle IL[X_1, \ldots, X_n]\rangle$$

Hinweis: Jedes Element von $\langle IL[X_1, \ldots, X_n]\rangle$ hat die Gestalt $c_1 f_1 + \ldots + c_r f_r$ mit $f_\nu \in I$ und $c_\nu \in L$ linear unabhängig über K.

Übung 6.2.7. Man zeige, daß der Teilring $\mathbb{Q}[\sqrt{2}] \subset \mathbb{R}$ ein Körper ist.

Übung 6.2.8. Man zeige, daß $\mathbb{Z}$ der einzige Teilring von $\mathbb{Q}$ ist, der endlich erzeugt ist als abelsche Gruppe.

6.3 Abstrakter chinesischer Restsatz

6.3.1. Gegeben Ringe $R_1, \ldots, R_s$ bilden wir den **Produktring** $R_1 \times \ldots \times R_s$ mit komponentenweiser Addition und Multiplikation. Gegeben ein weiterer Ring R und Ringhomomorphismen $f_i : R \to R_i$ erhalten wir natürlich einen Ringhomomorphismus

$$\begin{array}{rccc} (f_1, \ldots, f_s): & R & \to & R_1 \times \ldots \times R_s \\ & r & \mapsto & (f_1(r), \ldots, f_s(r)) \end{array}$$

Genauer sind die Projektionen Ringhomomorphismen $\mathrm{pr}_i : R_1 \times \ldots \times R_s \to R_i$ und das Nachschalten der Projektionen liefert für jeden weiteren Ring R eine Bijektion

$$\mathrm{Ring}(R, R_1 \times \ldots \times R_s) \xrightarrow{\sim} \mathrm{Ring}(R, R_1) \times \ldots \times \mathrm{Ring}(R, R_s)$$

In der Terminologie **??** liefert unsere Konstruktion also ein Produkt in der Kategorie der Ringe.

Definition 6.3.2. Gegeben Ideale $\mathfrak{a}, \mathfrak{b}$ in einem Ring R ist auch ihre **Summe** $\mathfrak{a} + \mathfrak{b} := \{a+b \mid a \in \mathfrak{a},\ b \in \mathfrak{b}\}$ ein Ideal, und wir nennen ihr **Produkt** und bezeichnen mit $\langle \mathfrak{a}\mathfrak{b} \rangle$ dasjenige Ideal oder gleichbedeutend diejenige additive Untergruppe von R, das beziehungsweise die von allen Produkten ab mit $a \in \mathfrak{a}$ und $b \in \mathfrak{b}$ erzeugt wird. Analog notieren wir auch Produkte von mehr als zwei Idealen.

6.3.3. Für das Produkt zweier Ideale ist die Notation $\mathfrak{a}\mathfrak{b}$ gebräuchlicher, die wir aber bereits für die von der Multiplikation eines Rings auf seiner Potenzmenge induzierte Verknüpfung vergeben haben. Dennoch werden wir später meist diese abkürzende Notation für das Produkt von Idealen verwenden.

Satz 6.3.4 (Abstrakter chinesischer Restsatz). *Seien $\mathfrak{a}_1, \ldots, \mathfrak{a}_s$ endlich viele Ideale eines Rings R. Gilt $\mathfrak{a}_i + \mathfrak{a}_j = R$ für $i \neq j$, so ist die offensichtliche Abbildung eine Surjektion*

$$\kappa : R \twoheadrightarrow R/\mathfrak{a}_1 \times \ldots \times R/\mathfrak{a}_s$$

mit Kern $(\ker \kappa) = \bigcap_i \mathfrak{a}_i$ dem Schnitt unserer Ideale. Für einen kommutativen Ring alias Kring R fällt dieser Schnitt auch mit dem Produktideal $\langle \mathfrak{a}_1 \ldots \mathfrak{a}_s \rangle$ zusammen und wir erhalten einen Ringisomorphismus

$$R/\langle \mathfrak{a}_1 \ldots \mathfrak{a}_s \rangle \quad \xrightarrow{\sim} \quad R/\mathfrak{a}_1 \times \ldots \times R/\mathfrak{a}_s$$

Beispiel 6.3.5. Der Name dieses Satzes rührt von seiner Bedeutung im Ring der ganzen Zahlen her, die wir bereits in 3.3.11 folgende besprochen hatten.

Beispiel 6.3.6. Wir finden etwa

$$\mathbb{R}[X]/\langle X^2 - 1\rangle \xrightarrow{\sim} \mathbb{R}[X]/\langle X + 1\rangle \times \mathbb{R}[X]/\langle X - 1\rangle \xrightarrow{\sim} \mathbb{R} \times \mathbb{R}$$

und ähnlich für den Quotienten $\mathbb{R}[X]/\langle P\rangle$ nach dem Hauptideal eines beliebigen quadratischen Polynoms P mit zwei reellen Nullstellen im Gegensatz zum Fall 6.1.21 eines reellen quadratischen Polynoms ohne reelle Nullstelle.

Beweis. Für die Surjektivität reicht es nachzuweisen, daß alle nur in einem Eintrag von Null verschiedenen Tupel im Bild liegen. Ohne Beschränkung der Allgemeinheit reicht es also zu zeigen, daß für alle $r \in R$ das Tupel $(\bar{r}, 0, \ldots, 0)$ im Bild

liegt. Es reicht sogar, wenn wir das für $r = 1$ zeigen, denn aus $\kappa(x) = (\bar{1}, 0, \ldots, 0)$ folgt $\kappa(rx) = \kappa(r)\kappa(x) = (\bar{r}, 0, \ldots, 0)$. Nach Annahme gilt für $i \neq 1$ jedoch $\mathfrak{a}_i + \mathfrak{a}_1 = R$, wir finden für $i \neq 1$ also eine Darstellung $a_i + b_i = 1$ mit $a_i \in \mathfrak{a}_i$ und $b_i \in \mathfrak{a}_1$. Für das Ringelement $a_i = 1 - b_i$ hat $\kappa(a_i)$ dann natürlich die Gestalt

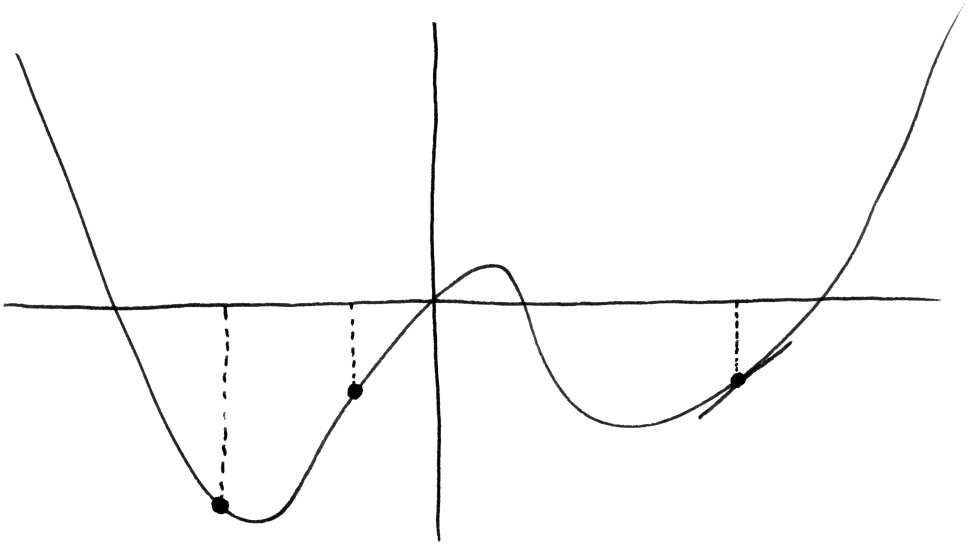
$$\kappa(a_i) = (1, *, \ldots, *, 0, *, \ldots *)$$

mit einer Null an der i-ten Stelle. Für das Bild des Produkts der a_i folgt dann $\kappa(a_2 a_3 \ldots a_s) = (1, 0, \ldots, 0)$ und die Surjektivität ist gezeigt. Der Kern dieser Surjektion ist offensichtlich genau der Schnitt der $\mathfrak{a}_i$, und wir müssen nur noch zeigen, daß er für kommutatives R mit dem Produktideal zusammenfällt. Im Fall $s = 2$ impliziert $\mathfrak{a} + \mathfrak{b} = R$ schon mal $\mathfrak{a} \cap \mathfrak{b} = \langle \mathfrak{a}\mathfrak{b} \rangle$, denn schreiben wir $1 = a + b$ mit $a \in \mathfrak{a}$ und $b \in \mathfrak{b}$, so gilt $x = xa + xb$ auch für alle $x \in \mathfrak{a} \cap \mathfrak{b}$. Im allgemeinen beachten wir, daß das Aufmultiplizieren unserer Identitäten $a_i + b_i = 1$ von eben für $2 \leq i \leq n$ sogar zeigt $\mathfrak{a}_1 + \langle \mathfrak{a}_2 \ldots \mathfrak{a}_s \rangle = R$. Mit vollständiger Induktion erhalten wir dann $\mathfrak{a}_1 \cap (\mathfrak{a}_2 \cap \ldots \cap \mathfrak{a}_s) = \mathfrak{a}_1 \cap \langle \mathfrak{a}_2 \ldots \mathfrak{a}_s \rangle = \langle \mathfrak{a}_1 \langle \mathfrak{a}_2 \ldots \mathfrak{a}_s \rangle \rangle = \langle \mathfrak{a}_1 \mathfrak{a}_2 \ldots \mathfrak{a}_s \rangle$. □

6.3.7. Wir schreiben auch $\langle I^n \rangle$ für das n-fache Produkt eines Ideals mit sich selbst. Betrachten wir zum Beispiel $R = k[X, Y]$ für einen Körper k und darin das Ideal $I = \langle X, Y \rangle$, so gilt $\langle I^2 \rangle = \langle X^2, XY, Y^2 \rangle$, $\langle I^3 \rangle = \langle X^3, X^2Y, XY^2, Y^3 \rangle$ und so weiter.

Korollar 6.3.8 (Polynominterpolation). *Seien k ein Körper und $n \in \mathbb{N}$. Wir finden stets ein Polynom $P \in k[X_1, \ldots, X_n]$, das an endlich vielen vorgegebenen Stellen des k^n vorgegebene Werte annimmt und sogar eine beliebig vorgegebene Taylorentwicklung bis zu einem festen endlichen Grad hat.*

Beweis. Für einen Punkt $p \in k^n$ bezeichne $I(p)$ das Ideal aller Polynome, die bei p verschwinden. Mit der vagen Formulierung „die Taylorentwicklung bei p eines Polynoms $P \in k[X_1, \ldots, X_n]$ bis zum Grad $m - 1$ vorzugeben“ meinen wir, seine Nebenklasse in $k[X_1, \ldots, X_n]/\langle I(p)^m \rangle$ vorzugeben. Damit wir den abstrakten chinesischen Restsatz anwenden können, müssen wir nur noch zeigen $\langle I(p)^m \rangle + \langle I(q)^m \rangle = \langle 1 \rangle$ falls $p \neq q$. Offensichtlich gilt $I(p) + I(q) = \langle 1 \rangle$, denn p und q unterscheiden sich in mindestens einer Koordinate, sagen wir $p_i \neq q_i$, und dann ist $(X_i - p_i) + (q_i - X_i)$ eine Einheit im Polynomring. Schreiben wir nun $1 = a + b$ mit $a \in I(p)$ und $b \in I(q)$ und nehmen von dieser Gleichung die $2m$-te Potenz, so folgt $1 \in \langle I(p)^m \rangle + \langle I(q)^m \rangle$ wie gewünscht. □



Eine Interpolation in einer Variablen mit vorgegebenen Werten an zwei Punkten und vorgegebenem Wert und Wert der Ableitung an einem weiteren Punkt.

6.4 Euklidische Ringe und Primfaktorzerlegung

6.4.1. Die folgende schematische Übersicht soll die Struktur dieses Abschnitts und die Beziehungen der darin neu eingeführten Begriffe untereinander verdeutlichen:

Interessante Ringe, etwa $\mathbb{Z}$, $\mathbb{Z}[\mathrm{i}]$, oder der Ring $k[X]$ für einen Körper k;
$\cap$
Euklidische Ringe, in denen es eine „Division mit Rest“ gibt;
$\cap$
Hauptidealringe, in denen jedes Ideal von einem Element erzeugt wird;
$\cap$
Faktorielle Ringe, alias Ringe mit „eindeutiger Primfaktorzerlegung“.

Wir arbeiten nun unser Schema von unten nach oben ab und beginnen mit faktoriellen Ringen.

Definition 6.4.2. Ein Element a eines Krings R heißt **irreduzibel** oder genauer **irreduzibel in** R, wenn es weder eine Einheit ist noch sich als ein Produkt von zwei Nichteinheiten darstellen läßt. In Formeln fordern wir also $a \notin R^\times$ und $a = bc \Rightarrow (b \in R^\times \text{ oder } c \in R^\times)$.

Beispiele 6.4.3. Die Null ist nie irreduzibel, denn im Nullring ist sie eine Einheit und in anderen Kringen das Produkt der zwei Nichteinheiten $0 = 0 \cdot 0$. Eine ganze Zahl $n \in \mathbb{Z}$ ist irreduzibel in $\mathbb{Z}$ genau dann, wenn ihr Betrag $|n|$ eine Primzahl ist. In einem Körper gibt es überhaupt keine irreduziblen Elemente, insbesondere ist auch keine ganze Zahl n irreduzibel in $\mathbb{Q}$.

6.4.4. Ich erinnere daran, daß man unter einem **Integritätsbereich** oder **Integritätsring** einen von Null verschiedenen Ring versteht, bei dem das Produkt je zweier von Null verschiedener Elemente stets auch wieder von Null verschieden ist.

Definition 6.4.5. Ein Ring R heißt **faktoriell**, wenn er ein kommutativer Integritätsbereich ist und wenn zusätzlich gilt:

1. Jedes $a \in R \backslash (R^\times \sqcup \{0\})$ läßt sich darstellen als ein Produkt von irreduziblen Elementen, in Formeln $a = p_1 \ldots p_n$ mit p_i irreduzibel und $n \geq 1$.

2. Diese Darstellung ist eindeutig bis auf Einheiten und die Reihenfolge der Faktoren. Ist genauer $a = q_1 \ldots q_m$ eine zweite Darstellung wie eben, so gilt $n = m$ und es gibt eine Permutation $\tau \in \mathcal{S}_n$ von n sowie Einheiten $u_i \in R^\times$ mit $q_i = u_i p_{\tau(i)}$ für $1 \leq i \leq n$.

6.4.6. Unsere einzigen Beispiele für faktorielle Ringe sind bisher nur $\mathbb{Z}$ und alle Körper. Im folgenden werden wir viele weitere Beispiele für faktorielle Ringe kennenlernen und insbesondere zeigen, daß Polynomringe über Körpern, ja Polynomringe über faktoriellen Ringen stets faktoriell sind.

Ergänzung 6.4.7. Gegeben ein Integritätsbereich bilden die von Null verschiedenen Elemente ein Monoid und unser Integritätsbereich ist faktoriell genau dann, wenn dieses Monoid isomorph ist zum Produkt einer abelschen Gruppe, eben der Einheitengruppe unseres Integritätsbereichs, mit einem freien Abmonoid. Ein freies Abmonoid ist hierbei zu verstehen als ein „freies Objekt“ im Sinne von **??** oder explizit als ein Monoid, das isomorph ist zum Monoid aller fast überall verschwindenden Abbildungen von einer Menge in das additive Monoid $\mathbb{N}$.

Beispiele 6.4.8 (**Ein Integritätsbereich, der nicht faktoriell ist**). Als Beispiel für einen nicht faktoriellen kommutativen Integritätsbereich betrachten wir den Teilring $\mathbb{Z}[\sqrt{-5}]$ der komplexen Zahlen, der gegeben wird durch

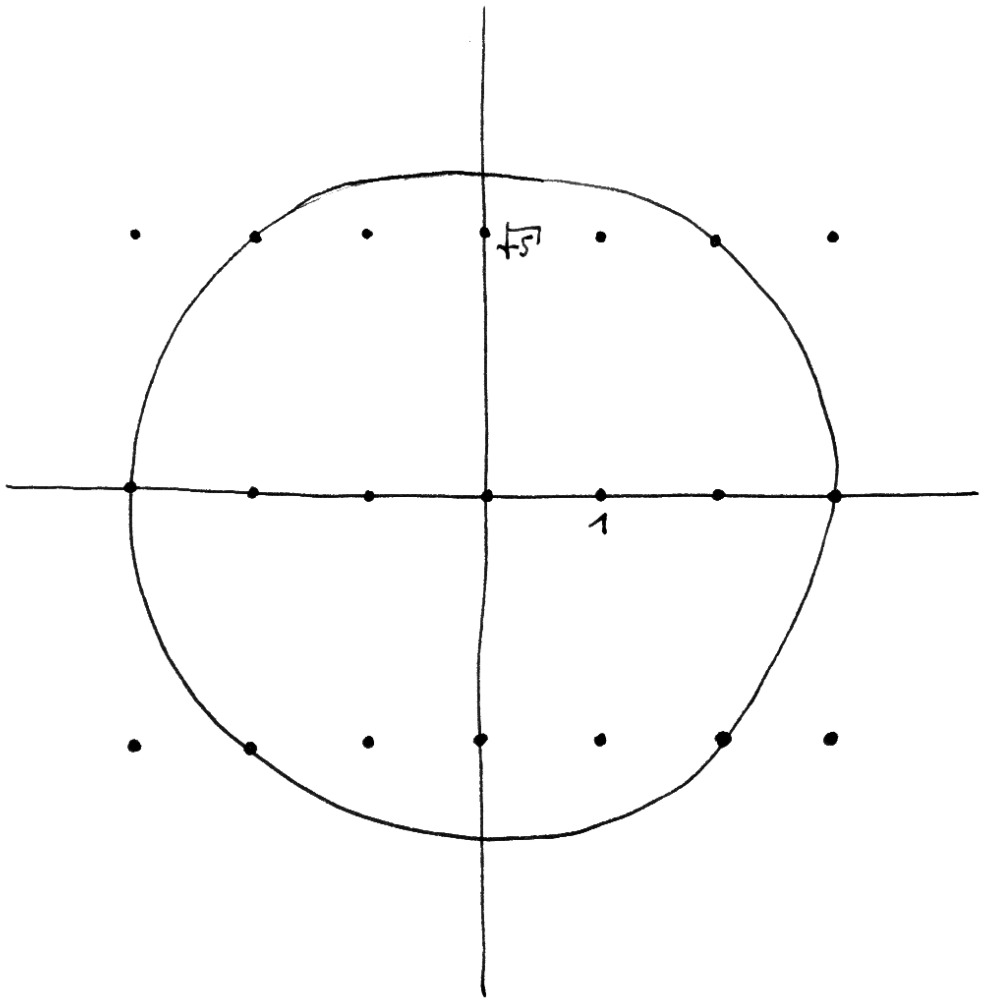
$$\mathbb{Z}[\sqrt{-5}] := \{a + b\,\mathrm{i}\,\sqrt{5} \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$$

Ich behaupte, daß $6 = 2\cdot 3 = (1+\sqrt{-5})\cdot(1-\sqrt{-5})$ zwei Zerlegungen in irreduzible Faktoren sind, die sich nicht nur um Einheiten und Reihenfolge unterscheiden. Das folgt leicht unter Verwendung der Multiplikativität der Norm $|zw| = |z||w|$ für $z, w \in \mathbb{C}$ aus der anschließenden Tabelle, in der alle Elemente $z \in \mathbb{Z}[\sqrt{-5}]$ der Quadratlänge $|z|^2 \leq 9$ aufgelistet sind.

$\lvert z\rvert^2$	mögliche $z \in \mathbb{Z}[\sqrt{-5}]$
0	0
1	± 1
4	± 2
5	$\pm\sqrt{-5}$
6	$(\pm 1) + (\pm\sqrt{-5})$
9	± 3, $(\pm 2) + (\pm\sqrt{-5})$

Definition 6.4.9. Ein Ring R heißt ein **Hauptidealring**, wenn R ein kommutativer Integritätsbereich ist aber kein Körper und jedes Ideal von R ein Hauptideal ist, also von einem einzigen Element erzeugt wird.

Beispiel 6.4.10. Nach 1.3.4 ist der Ring $\mathbb{Z}$ der ganzen Zahlen ein Hauptidealring. Der Polynomring in zwei Variablen $\mathbb{C}[X, Y]$ ist kein Hauptidealring, denn das Ideal aller beim Ursprung von $\mathbb{C}^2$ verschwindenden Polynome ist kein Hauptideal: Jedes Polynom, das am Ursprung verschwindet, verschwindet auch sonst noch irgendwo, und dasselbe gilt für alle Polynome des von ihm erzeugten Hauptideals.



Einige Elemente des Rings $\mathbb{Z}[\sqrt{-5}]$ als Punkte in der Gauß'schen Zahlenebene

Satz 6.4.11. *Jeder Hauptidealring ist faktoriell.*

Ergänzung 6.4.12. In diesem Beweis verwenden wir implizit das Auswahlaxiom, um die Existenz einer Faktorisierung in Irreduzible zu zeigen. Will man das Zorn'sche Lemma an dieser Stelle vermeiden, mag man sich auf den Fall euklidischer Ringe beschränken, für den wir in 6.4.18 einen Beweis ohne Auswahlaxiom geben.

Beweis. Wir zeigen als erstes, daß in einem Hauptidealring jedes Element $a \in R\backslash(R^\times \sqcup \{0\})$ ein Produkt von endlich vielen irreduziblen Elementen ist. Wir argumentieren durch Widerspruch. Gäbe es ein Element $a \in R\backslash(R^\times \sqcup \{0\})$, das kein Produkt von Irreduziblen ist, so wäre insbesondere a selbst nicht irreduzibel, also von der Gestalt $a = a_1 b_1$ mit $a_1, b_1 \notin R^\times$. Hier können nicht sowohl a_1 als auch b_1 Produkte von Irreduziblen sein. Wir dürfen ohne Beschränkung der Allgemeinheit annehmen, a_1 sei kein Produkt von Irreduziblen, und können schreiben $a_1 = a_2 b_2$ mit $a_2, b_2 \notin R^\times$ und a_2 keinem Produkt von Irreduziblen. Wir bemerken nun, daß in einem Integritätsbereich R die Gleichheit $\langle a\rangle = \langle b\rangle$ von Hauptidealen zu $a, b \in R\backslash 0$ äquivalent ist zu $a = ub$ mit einer Einheit $u \in R^\times$. Indem wir wie oben immer weitermachen, finden wir also in R eine unendliche echt aufsteigende Folge von Hauptidealen

$$\langle a\rangle \subsetneq \langle a_1\rangle \subsetneq \langle a_2\rangle \subsetneq \dots$$

Die Vereinigung über alle diese Hauptideale ist auch ein Ideal, also ein Hauptideal $\langle h\rangle$. Diese Vereinigung ist aber aber auch das Erzeugnis $\langle h\rangle = \langle a_1, a_2, \dots\rangle$ der a_i. Es folgt eine Relation der Gestalt $h = r_1 a_1 + \dots + r_n a_n$ und damit $\langle h\rangle = \langle a_n\rangle$ im Widerspruch zu $\langle a_n\rangle \neq \langle a_{n+1}\rangle$. Dieser Widerspruch zeigt, daß jedes Element, das weder Null ist noch eine Einheit, ein Produkt von Irreduziblen sein muß. Jetzt zeigen wir die Eindeutigkeit. Es reicht dazu, ähnlich wie wir das im Fall der ganzen Zahlen bereits gesehen hatten, wenn wir für jedes irreduzible Element p zeigen

$$p|ab \;\Rightarrow\; p|a \text{ oder } p|b$$

Wir wiederholen dafür unseren Beweis des Lemmas von Euklid 1.4.15. Gleichbedeutend dürfen wir zeigen, daß aus $p \nmid a$ und $p|ab$ folgt $p|b$. Weil wir in einem Hauptidealring sind, gibt es aber c mit $\langle a, p\rangle = \langle c\rangle$ und wegen $c|p$ und p irreduzibel haben wir entweder $c \in R^\times p$ oder $c \in R^\times$. Der erste Fall $c \in R^\times p$ wird durch $p \nmid a$ ausgeschlossen, also haben wir $c \in R^\times$ alias $\langle a, p\rangle = R$ alias $1 = ax + py$ für geeignete $x, y \in R$. Multiplikation mit b liefert dann $b = abx + bpy$ und zusammen mit $p|ab$ folgt $p|b$ wie gewünscht. □

Definition 6.4.13. Ein **euklidischer Ring** ist ein kommutativer Integritätsbereich mit einer Abbildung $\sigma : R\backslash 0 \to \mathbb{N}$ derart, daß man für alle $a, b \in R$ mit $a \neq 0$ Elemente $q, r \in R$ finden kann mit $b = aq + r$ und $r = 0$ oder $\sigma(r) < \sigma(a)$.

6.4.14. Salopp gesprochen ist also ein euklidischer Ring ein Integritätsbereich, in dem man „teilen kann mit Rest“, wobei der Rest in einer präzisen, durch σ spezifizierten Weise „kleiner“ sein soll als der Teiler. Alle unsere Argumente funktionieren auch noch, wenn σ allgemeiner Werte in einer beliebigen „wohlgeordneten“ Menge annimmt, als da heißt einer angeordneten Menge, in der jede nichtleere Teilmenge ein kleinstes Element besitzt.

Beispiele 6.4.15.

1. $R = \mathbb{Z}$ mit $\sigma(n) = |n|$;
2. $R = k[X]$ für einen Körper k und $\sigma(P) = \operatorname{grad} P$, siehe 2.3.15;
3. $R = \mathbb{Z}[\mathrm{i}] = \{x + y\,\mathrm{i} \mid x, y \in \mathbb{Z}\}$, $\sigma(x + y\,\mathrm{i}) = x^2 + y^2$. Dieser Ring der sogenannten **Gauß'schen Zahlen** ist als Teilring von $\mathbb{C}$ zu verstehen. Wir werden dies Beispiel in 6.6 noch ausführlich besprechen.

Satz 6.4.16. *Jeder euklidische Ring ist ein Körper oder ein Hauptidealring und damit insbesondere faktoriell.*

Ergänzung 6.4.17. Dieser Satz verallgemeinert unseren Satz 1.3.4, mit dem wir alle Untergruppen der Gruppe $\mathbb{Z}$ der ganzen Zahlen beschrieben hatten. Der Beweis ist auch im wesentlichen derselbe.

Beweis. Sei $I \subset R$ ein Ideal. Ist $I = 0$, so ist $I = \langle 0 \rangle$ ein Hauptideal. Sonst finden wir $a \in I \backslash 0$ mit $\sigma(a)$ kleinstmöglich. Wir behaupten $I = \langle a \rangle$. Gäbe es nämlich $b \in I \backslash \langle a \rangle$, so könnten wir schreiben $b = aq + r$ mit $r \neq 0$ und $\sigma(r) < \sigma(a)$. Dann gilt aber auch $r = b - aq \in I$, und das steht im Widerspruch zur Wahl von a. $\square$

Ergänzung 6.4.18 (**Faktorialität ohne Zorn**). Für die Beweise der zentralen Resultate dieser Vorlesung müssen wir nur wissen, daß euklidische Ringe faktoriell sind. In diesem Fall können wir die Existenz einer Faktorisierung in Irreduzible auch ohne Auswahlaxiom einsehen. Dazu brauchen wir nur die Erkenntnis aus dem vorhergehenden Beweis, nach der jedes von Null verschiedene Ideal von jedem seiner von Null verschiedenen Elemente mit kleinstmöglichem σ-Wert erzeugt wird. Gäbe es nun von Null verschiedene Elemente ohne Faktorisierung in Irreduzible, so auch ein derartiges Element a mit kleinstmöglichem σ-Wert. Es hätte dann eine Faktorisierung in ein Produkt von zwei Nichteinheiten $a = bc$, und die Hauptideale $\langle b \rangle$ und $\langle c \rangle$ wären echt größer als $\langle a \rangle$. Das Minimum von σ auf $\langle b \rangle \backslash 0$ müßte also echt kleiner sein als das Minimum von σ auf $\langle a \rangle \backslash 0$, denn wir haben $b = aq + r$ mit $r \neq 0$ und $\sigma(r) < \sigma(a)$. Wird das Minimum von σ auf $\langle b \rangle \backslash 0$ bei β angenommen, so folgt weiter $\beta | b$ und damit $\beta \in R^\times b$. Genauso finden wir $\gamma \in R^\times c$ mit $\sigma(\gamma) < \sigma(a)$. Dann aber müßten β und γ und damit auch b und c Faktorisierungen in Irreduzible besitzen und damit auch a selbst. Dieser Widerspruch zeigt die Behauptung.

Korollar 6.4.19. *Der Polynomring in einer Veränderlichen mit Koeffizienten in einem Körper ist stets ein Hauptidealring und ist insbesondere stets faktoriell.*

Beweis. Wie in 6.4.15 ausgeführt wird, ist unser Polynomring ein euklidischer Ring. Das Korollar folgt damit aus 6.4.16. □

6.4.20. Die irreduziblen Elemente des Polynomrings $k[X]$ mit Koeffizienten in einem Körper k nennt man **irreduzible Polynome**. Wenn wir mit mehreren Körpern gleichzeitig arbeiten, werden wir auch von k**-irreduziblen Polynomen** reden, da dieser Begriff ganz entscheidend von k abhängt: Zum Beispiel ist das Polynom $X^2 + 1$ zwar $\mathbb{R}$-irreduzibel, aber keineswegs $\mathbb{C}$-irreduzibel.

Beispiel 6.4.21. Die irreduziblen Polynome in $\mathbb{C}[X]$ sind nach 2.3.26 genau die Polynome vom Grad Eins. Die irreduziblen Polynome in $\mathbb{R}[X]$ sind nach 2.3.28 genau die Polynome vom Grad Eins sowie die Polynome vom Grad Zwei ohne reelle Nullstelle. Die irreduziblen Polynome in $\mathbb{Q}[X]$ lassen sich nicht so leicht aufzählen.

Satz 6.4.22 (Quotienten von Hauptidealringen). *Gegeben ein von Null verschiedenes Element a eines Hauptidealrings R sind gleichbedeutend:*

1. *Der Quotient $R/\langle a\rangle$ ist ein Körper;*
2. *Der Quotient $R/\langle a\rangle$ ist ein Integritätsbereich;*
3. *Unser Element a ist irreduzibel.*

Beweis. (1)⇒(2) ist klar. Wir zeigen nun (2)⇒(3) alias (nicht 3)⇒(nicht 2). Ist $a \in R$ nicht irreduzibel, so haben wir $a \in R^\times$ oder $a = bc$ mit $b, c \notin R^\times$. Im ersten Fall ist der Quotient der Nullring und mithin kein Integritätsbereich. Im zweiten Fall folgt, da R ein Integritätsbereich ist, schon mal $b, c \notin \langle a\rangle$. Für die Nebenklassen in $R/\langle a\rangle$ gilt also $\bar b \neq 0$ und $\bar c \neq 0$ aber $\bar b\bar c = 0$. Deshalb kann für a nicht irreduzibel der Quotient $R/\langle a\rangle$ kein Integritätsbereich sein, und das gilt sogar für einen beliebigen kommutativen Integritätsbereich R. Schließlich zeigen wir noch (3)⇒(1). Gegeben $a, b \in R$ gibt es $c \in R$ mit $\langle a, b\rangle = \langle c\rangle$. Insbesondere ist c ein Teiler von a, und ist a irreduzibel, so folgt $\langle c\rangle = \langle a\rangle$ oder $\langle c\rangle = R$. Gilt zusätzlich $b \notin \langle a\rangle$, so folgt $\langle a, b\rangle = R$ und folglich gibt es $x, y \in R$ mit $1 = ax + by$. Dann aber ist $\bar y$ ein multiplikatives Inverses zu $\bar b$ in $R/\langle a\rangle$. □

Beispiel 6.4.23. Gegeben $p \in \mathbb{Z}$ ist $\mathbb{Z}/p\mathbb{Z}$ ist genau dann ein Körper, wenn p oder $-p$ eine Primzahl ist.

Beispiel 6.4.24. $\mathbb{R}[X]/\langle X^2 + 1\rangle$ ist ein Körper, genauer induziert das Einsetzen von i für X einen Isomorphismus dieses Körpers mit $\mathbb{C}$.

Beispiel 6.4.25. $\mathbb{R}[X]/\langle X^2+2\rangle$ ist ein Körper, genauer induziert das Einsetzen von $\mathrm{i}\sqrt{2}$ für X einen Isomorphismus dieses Körpers mit $\mathbb{C}$.

Beispiel 6.4.26. $\mathbb{R}[X]/\langle X+1\rangle$ ist ein Körper, genauer induziert das Einsetzen von -1 für X einen Isomorphismus dieses Körpers mit $\mathbb{R}$.

Beispiel 6.4.27. $\mathbb{R}[X]/\langle X^2-1\rangle$ ist *kein* Körper. Vielmehr liefert der chinesische Restsatz in Verbindung mit dem vorhergehenden Beispiel einen Ringisomorphismus $\mathbb{R}[X]/\langle X^2-1\rangle \xrightarrow{\sim} \mathbb{R}\times\mathbb{R}$, und $\mathbb{R}\times\mathbb{R}$ ist kein Köper, es gilt darin ja etwa $(1,0)\cdot(0,1)=(0,0)$.

Übungen

Übung 6.4.28. Man zeige, daß $\mathbb{Z}[X]$ kein Hauptidealring ist.

Übung 6.4.29. Sei k ein Körper. Man zeige: (1) Alle Polynome vom Grad 1 sind irreduzibel in $k[X]$. (2) Ist $P\in k[X]$ irreduzibel und $\operatorname{grad} P>1$, so hat P keine Nullstelle in k. (3) Ist $P\in k[X]\setminus k$ vom Grad $\operatorname{grad} P\leq 3$ und hat P keine Nullstelle in k, so ist P irreduzibel in $k[X]$. (4) Ist k algebraisch abgeschlossen, so sind die irreduziblen Polynome in $k[X]$ genau die Polynome vom Grad 1. Man gebe auch (5) ein Polynom positiven Grades in $\mathbb{R}[X]$ an, das keine Nullstelle hat, aber dennoch nicht irreduzibel ist.

Ergänzende Übung 6.4.30. In einem Polynomring in mindestens einer Variablen über einem Körper gibt es stets unendlich viele normierte irreduzible Polynome. Hinweis: Man multipliziere sonst alle zusammen und ziehe 1 ab.

Ergänzende Übung 6.4.31. Man zeige: Gegeben ein Körper k ist der Ring $k[\![X]\!]$ der formalen Potenzreihen mit Koeffizienten aus k aus 2.3.42 ein Hauptidealring, und die Ideale dieses Rings sind das Nullideal sowie die Ideale $X^n k[\![X]\!]$ für $n\in\mathbb{N}$. Man bespreche die Primfaktorzerlegung in diesem Hauptidealring.

Übung 6.4.32. Seien R ein faktorieller Ring und $q\in\operatorname{Quot}(R)$ ein Element seines Quotientenkörpers und $n\geq 1$ mit $q^n\in R$. Man zeige $q\in R$.

Übung 6.4.33 (**Eindeutigkeitsaussagen für teilerfremde Polynome**). Seien k ein Körper und $f,g\in k[T]$ teilerfremde Polynome. Man zeige, daß es dann für jedes Polynom h Polynome a,b gibt mit $h=af+bg$. Man zeige, daß man unter der zusätzlichen Annahme $g\neq 0$ hier (a,b) sogar so wählen kann, daß gilt $\operatorname{grad} a<\operatorname{grad} g$, und daß im Fall $\operatorname{grad}(h)\leq\operatorname{grad}(f)+\operatorname{grad}(g)-1$ unser Paar (a,b) dadurch dann eindeutig bestimmt ist. Hinweis: Dimensionsabschätzung. Die analoge Aussage gilt nicht für $k=\mathbb{Z}$, selbst wenn wir f und g normiert annehmen.

Übung 6.4.34. Der Quotient eines faktoriellen Rings R nach einem Hauptideal $\langle a\rangle$ ist genau dann ein Integritätsbereich, wenn gilt $a=0$ oder a irreduzibel.

Übung 6.4.35. Im Quotienten eines faktoriellen Rings R nach dem Hauptideal zu einem Element $a \neq 0$ ist das Bild von $b \in R$ genau dann kürzbar, wenn a und b teilerfremd sind.

Übung 6.4.36. Seien k ein Körper und R eine Ringalgebra über k. Ein Element $\alpha \in R$ heißt **algebraisch über** k, wenn es ein von Null verschiedenes Polynom $P \in k[X]\backslash 0$ gibt mit $P(\alpha) = 0$. Man zeige, daß es in diesem Fall genau ein normiertes Polynom $Q \in k[X]$ kleinstmöglichen Grades gibt mit $Q(\alpha) = 0$. Es heißt dann das **Minimalpolynom von** α.

6.5 Primelemente und maximale Ideale*

Definition 6.5.1. Sei R ein kommutativer Ring. Ein Element $p \in R$ heißt ein **euklidisches Element** oder üblicher **Primelement**, falls es (1) weder Null noch eine Einheit ist und falls (2) aus $p|ab$ folgt $p|a$ oder $p|b$. Wir sagen auch abkürzend, so ein Element sei **euklidisch** alias **prim**.

6.5.2 (**Diskussion der Terminologie**). Mir scheint die Bezeichnung als Primelement eine unglückliche Wahl, aber sie ist nun einmal historisch gewachsen. Einerseits sind nun zwar die positiven Primelemente des Rings der ganzen Zahlen $\mathbb{Z}$ genau unsere Primzahlen, aber das ist bereits ein nichttrivialer Satz, den wir in 1.4.15 als „Lemma von Euklid“ bewiesen hatten. Von ihrer ursprünglichen Definition her versteht man unter Primzahlen ja viel eher die positiven irreduziblen Elemente des Rings der ganzen Zahlen. Andererseits wäre es auch eine vernünftige Terminologie, in einem beliebigen kommutativen Ring diejenigen Elemente als Primelemente zu bezeichnen, die im Sinne von **??** „ein Primideal erzeugen“, aber dann müßten wir in unserer Definition auch die Null als Primelement zulassen. So gesehen sitzt man mit der obigen und allgemein gebräuchlichen Definition eines Primelements leider zwischen allen Stühlen.

6.5.3 (**Primelemente und irreduzible Elemente**). Euklidische Elemente p alias Primelemente in Integritätsbereichen sind stets irreduzibel, denn aus $p = ab$ folgt $p|a$ oder $p|b$, also ohne Beschränkung der Allgemeinheit $a = p\alpha$ und dann $p = ab = p\alpha b$ und so $1 = \alpha b$ und b ist eine Einheit. Irreduzible Elemente müssen auch in Integritätsbereichen im allgemeinen keineswegs euklidisch alias prim sein, wie das Beispiel 6.4.8 des Rings $\mathbb{Z}[\sqrt{-5}]$ mit den Zerlegungen $6 = 2\cdot 3 = (1+\sqrt{-5})\cdot (1-\sqrt{-5})$. Wir hatten uns ja überlegt, daß hier alle Faktoren irreduzibel sind, sich aber nicht gegenseitig teilen. Also teilt $(1+\sqrt{-5})$ das Produkt $2\cdot 3$, teilt aber keinen der Faktoren. In einem faktoriellen Ring sind die euklidischen Elemente alias Primelemente aber offensichtlich genau die irreduziblen Elemente.

Definition 6.5.4. Ein Ideal in einem Ring heißt ein **echtes Ideal**, wenn es nicht der ganze Ring ist. Ein Ideal in einem Ring heißt ein **maximales echtes Ideal**, wenn

es ein maximales Element der durch Inklusion teilgeordneten Menge aller *echten* Ideale unseres Ringes ist. Es ist eine allgemeine Konvention, unsere maximalen echten Ideale abkürzend als **maximale Ideale** zu bezeichnen, obwohl sie natürlich nicht die maximalen Elemente der Menge aller Ideale unseres Ringes sind: Diese Menge hat nämlich nur genau ein maximales Element, den Ring selbst. Ich werde dieser allgemeinen Konvention folgen.

Beispiele 6.5.5. Die maximalen Ideale eines Hauptidealrings sind genau die von den irreduziblen Elementen erzeugten Hauptideale. Jeder Körper besitzt nur genau ein maximales Ideal, nämlich das Nullideal. Ist umgekehrt in einem Kring R das Nullideal ein maximales Ideal, so muß unser Kring offensichtlich ein Körper sein, denn wir haben $R \neq 0$ und für $a \in R\backslash 0$ gilt $Ra = \langle a\rangle = R \ni 1$. Der Nullring besitzt überhaupt kein maximales Ideal. In **??** zeigen wir, daß er der einzige Ring ohne maximales Ideal ist.

Proposition 6.5.6 (Quotienten nach maximalen Idealen). *Ein Ideal in einem Kring ist maximal genau dann, wenn der Quotientenring nach besagtem Ideal ein Körper ist.*

Erster Beweis. Sei R unser Kring und $\mathfrak{m} \subset R$ unser Ideal. Ist $R/\mathfrak{m}$ ein Körper, so gilt $\mathfrak{m} \neq R$ und es gibt für jedes $a \notin \mathfrak{m}$ ein $b \in R$ mit $ab \in 1 + \mathfrak{m}$. Folglich gilt $\langle a, \mathfrak{m}\rangle = R$ für jedes $a \notin \mathfrak{m}$ und damit ist $\mathfrak{m}$ ein maximales Ideal von R. Ist umgekehrt $\mathfrak{m}$ ein maximales Ideal von R, so ist $R/\mathfrak{m}$ nicht der Nullring und für jedes $a \notin \mathfrak{m}$ gilt $\langle a, \mathfrak{m}\rangle = R$ und folglich gibt es $b \in R$ und $m \in \mathfrak{m}$ mit $ab+m = 1$. Dann aber folgt $\bar{a}\bar{b} = 1$ in $R/\mathfrak{m}$ und dieser Quotient ist ein Körper. □

Zweiter Beweis. Nach 6.5.5 ist ein Kring genau dann ein Körper, wenn er genau zwei Ideale besitzt, das Nullideal und den ganzen Kring. Nach 6.1.24 entsprechen die Ideale von $R/\mathfrak{m}$ eindeutig den Idealen von R, die $\mathfrak{m}$ umfassen. Die Proposition folgt. □

6.5.7. Für unseren Satz 6.4.22, nach dem ein Quotient von einem Hauptidealring nach einem Hauptideal $\langle a\rangle$ genau dann ein Körper ist, wenn a ein irreduzibles Element ist, können wir damit einen neuen Beweis geben: Beide Eigenschaften von a sind nach 6.5.5 beziehungsweise 6.5.6 gleichbedeutend zur Forderung, daß $\langle a\rangle$ ein maximales Ideal ist. Bei genauerer Betrachtung ist dieser neue Beweis aber doch nur der alte in neuen Worten.

Übungen

Übung 6.5.8. Ein kommutativer Integritätsbereich ist faktoriell genau dann, wenn (1) jedes von Null verschiedene Element als Produkt von einer Einheit mit einigen Irreduziblen dargestellt werden kann und (2) jedes irreduzible Element prim ist.

6.6 Irreduzible im Ring der Gauß'schen Zahlen

Lemma 6.6.1. *Der Ring $\mathbb{Z}[\mathrm{i}]$ der Gauß'schen Zahlen ist euklidisch und mithin faktoriell.*

Beweis. Die Elemente des von einem festen von Null verschiedenen Element $0 \neq a = x + \mathrm{i}y \in \mathbb{Z}[\mathrm{i}]$ im Ring $\mathbb{Z}[\mathrm{i}]$ der Gauß'schen Zahlen erzeugten Hauptideals bilden die Ecken eines quadratischen Rasters auf der komplexen Zahlenebene, mit $|a| = \sqrt{x^2+y^2}$ der Seitenlänge der Quadrate. Jedes $b \in \mathbb{Z}[\mathrm{i}]$ liegt in einem dieser Quadrate und hat von einer der Ecken einen Abstand $\leq \sqrt{2}|a|/2 < |a|$. Folglich ist unser Ring euklidisch mit $\sigma(a) = |a|^2$. □

6.6.2. Von nun an wird in diesem Abschnitt der Begriff „Quadrat" nicht mehr in seiner geometrischen Bedeutung verwendet, sondern in seiner algebraischen Bedeutung als Abkürzung für „Quadratzahl". Die ersten Quadrate in $\mathbb{Z}$ sind also $0, 1, 4, 9, 16, 25, \ldots$

Lemma 6.6.3 (Irreduzible im Ring der Gauß'schen Zahlen).

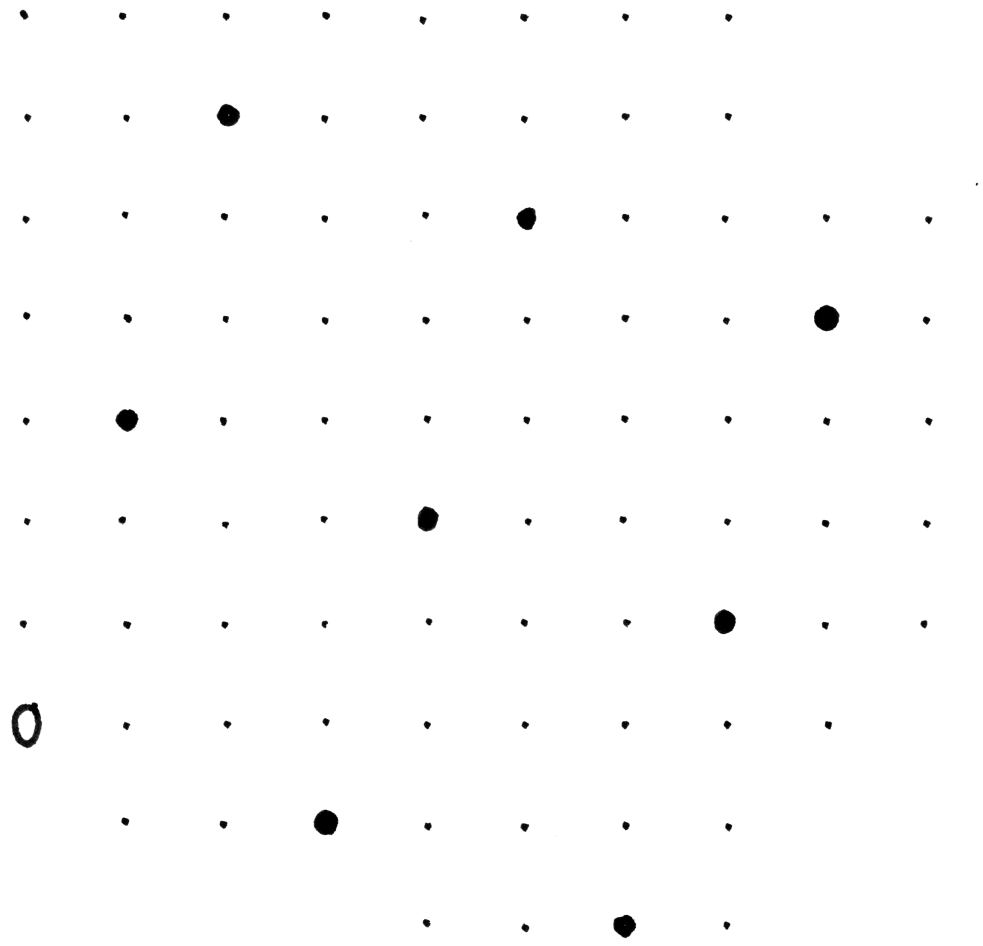
1. *Jedes irreduzible Element $\pi \in \mathbb{Z}[\mathrm{i}]$ teilt genau eine Primzahl $p \in \mathbb{N}$;*
2. *Jede Primzahl $p \in \mathbb{N}$ bleibt entweder irreduzibel in $\mathbb{Z}[\mathrm{i}]$ oder zerfällt dort in ein Produkt aus zwei irreduziblen Elementen, die dann notwendig zueinander komplex konjugiert sind und nur im Fall $p = 2 = (1+\mathrm{i})(1-\mathrm{i})$ durch Multiplikation mit einer Einheit auseinander hervorgehen.*

6.6.4. Gleich im Anschluß in 6.6.5 zeigen wir, daß eine Primzahl genau dann im Ring der Gauß'schen Zahlen irreduzibel bleibt, wenn sie beim Teilen durch Vier den Rest Drei läßt.

Beweis. Aus $\pi|\pi\bar{\pi}$ folgt $\pi|p$ für mindestens einen Primteiler p von $\pi\bar{\pi}$, also teilt π mindestens eine Primzahl. Aus $\pi|p$ und $\pi|q$ für Primzahlen p und q folgt umgekehrt $\pi\bar{\pi}|p^2$ und $\pi\bar{\pi}|q^2$ und so $p = q$. Das zeigt Teil 1. Gegeben eine Primzahl p würde jede Zerlegung $p = \alpha\beta\gamma$ in Nichteinheiten von $\mathbb{Z}[\mathrm{i}]$ eine Zerlegung in Nichteinheiten $p^2 = (\alpha\bar{\alpha})(\beta\bar{\beta})(\gamma\bar{\gamma})$ in $\mathbb{Z}$ liefern, was unmöglich ist. Folglich ist p entweder irreduzibel in $\mathbb{Z}[\mathrm{i}]$ oder zerfällt in ein Produkt von Irreduziblen als $p = \alpha\beta$. Dann folgt sofort $p^2 = (\alpha\bar{\alpha})(\beta\bar{\beta})$ und damit $p = \alpha\bar{\alpha} = \beta\bar{\beta}$ alias $\beta = \bar{\alpha}$. Gibt es nun eine Einheit ε mit $\bar{\alpha} = \varepsilon\alpha$, so haben wir notwendig $\varepsilon = \pm\mathrm{i}$, da sonst p keine Primzahl gewesen wäre. Bis auf eine eventuelle Vertauschung der Faktoren dürfen wir also $\bar{\alpha} = -\mathrm{i}\alpha$ annehmen, und das impliziert offensichtlich $\alpha \in \mathbb{Z}(1+\mathrm{i})$ und, wenn α auch noch irreduzibel sein soll, $\alpha = \pm(1+\mathrm{i})$. □

Proposition 6.6.5. *Für eine Primzahl $p \in \mathbb{N}$ sind gleichbedeutend:*

1. *p bleibt nicht prim im Ring $\mathbb{Z}[\mathrm{i}]$ der Gauß'schen Zahlen;*



Die Elemente des von $1 + 3\,\mathrm{i}$ im Ring der Gauß'schen Zahlen erzeugten Hauptideals habe ich in diesem Bild als fette Punkte dargestellt, die anderen Elemente des Rings der Gauß'schen Zahlen durch kleine Punkte.

2. *p ist Summe von zwei Quadraten, in Formeln $p = x^2 + y^2$;*

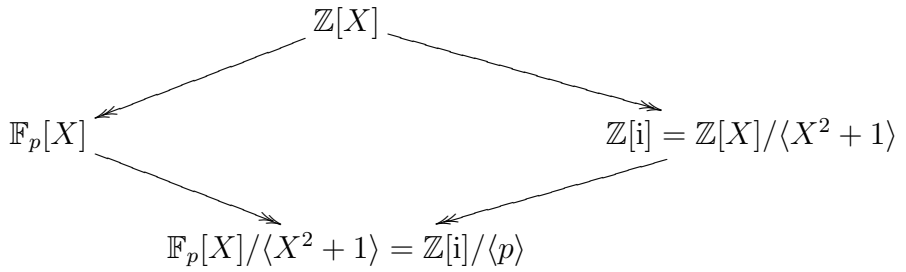
3. *p läßt beim Teilen durch Vier den Rest Eins oder Zwei, in Formeln $p \equiv 1 \pmod 4$ oder $p = 2$;*

4. *Das Polynom $(X^2 + 1)$ ist nicht irreduzibel in $\mathbb{F}_p[X]$;*

5. *(-1) ist ein Quadrat in $\mathbb{F}_p$.*

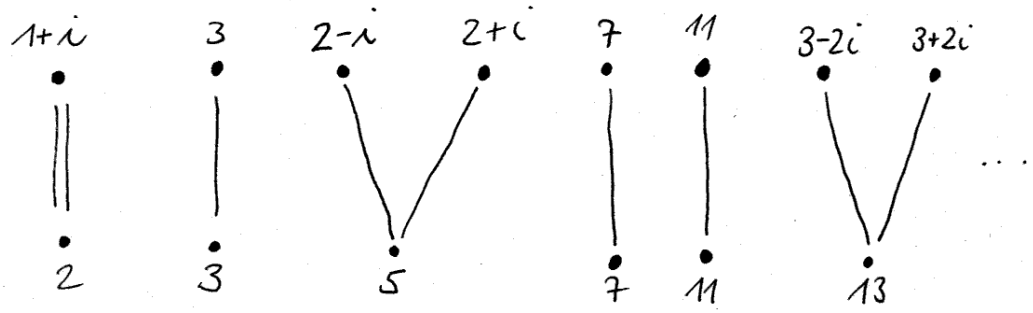
Beispiele 6.6.6. $2 = 1^2 + 1^2$, $5 = 1^2 + 2^2$, $13 = 2^2 + 3^2$, $17 = 1^2 + 4^2$, ...

Beweis. Ist $\pi = x + \mathrm{i}y$ ein irreduzibler Faktor echt kleinerer Länge von p, so ist $\pi\bar{\pi} = x^2 + y^2$ ein Primfaktor echt kleinerer Länge von p^2, also $x^2 + y^2 = p$. Das zeigt 1⇒2. Aus $p = x^2 + y^2$ folgt umgekehrt $p = (x + \mathrm{i}y)(x - \mathrm{i}y)$, also haben wir auch 2⇒1. Die Implikation 2⇒3 folgt daraus, daß jedes Quadrat kongruent ist zu Null oder Eins modulo Vier, da nämlich gilt $\{x^2 \mid x \in \mathbb{Z}/4\mathbb{Z}\} = \{\bar{0}, \bar{1}\}$. Eine Summe von zwei Quadraten kann also modulo 4 nie zu 3 kongruent sein. 1⇔4 folgert man durch die Betrachtung des Diagramms von Ringen



Alle vier Morphismen sind hierbei Surjektionen mit einem Hauptideal als Kern. Nach 6.4.22 sind also sowohl 1 als auch 4 gleichbedeutend dazu, daß der Ring $\mathbb{F}_p[X]/\langle X^2+1\rangle$ kein Körper ist, und damit sind sie auch untereinander äquivalent. 4⇔5 ist evident. Schließlich zeigen wir noch 3⇒5. Sicher ist nämlich -1 ein Quadrat in $\mathbb{F}_2$. Unter der Vorausetzung $p \equiv 1 \pmod 4$ gilt dasselbe in $\mathbb{F}_p$. Wir wissen nämlich aus 3.4.17, daß $\mathbb{F}_p^\times$ als endliche Untergruppe der multiplikativen Gruppe eines Körpers zyklisch ist, und in einer zyklischen Gruppe von durch Vier teilbarer Ordnung gibt es offensichtlich Elemente der Ordnung Vier. So ein Element der Ordnung Vier löst dann die Gleichung $x^2 = -1$ in $\mathbb{F}_p^\times$. □

6.6.7. Man beachte, daß jede Gauß'sche Zahl ungleich Null durch Multiplikation mit einer Einheit auf genau eine Gauß'sche Zahl $x + \mathrm{i}y$ mit $x \geq y > -x$, also auf genau eine Gauß'sche Zahl im „um $45°$ im Uhrzeigersinn verdrehten offenen ersten Quadranten mitsamt seiner oberen Kante ohne den Ursprung“ abgebildet werden kann. Die im wesentlichen eindeutige Zerlegung einer Primzahl $p \in \mathbb{N}$



Versuch einer graphischen Darstellung des Zerfallens der gewöhnlichen Primzahlen im Ring der Gauß'schen Zahlen. Die Zwei ist ein Sonderfall, weil bei ihr ein irreduzibles Element des Rings der Gauß'schen Zahlen als zweifacher Faktor auftritt.

in ein Produkt irreduzibler Elemente von $\mathbb{Z}[\mathrm{i}]$ hat nach unserem Satz folgende Gestalt:

$$\begin{array}{lll} p \equiv 3 \pmod 4 & p = p; \\ p \not\equiv 3 \pmod 4 & p = (x + \mathrm{i}y)(x - \mathrm{i}y) \text{ für } x^2 + y^2 = p. \end{array}$$

Beschränken wir uns auf die irreduziblen Elemente $x + \mathrm{i}y$ mit $x \geq y > -x$, so ist das die eindeutige Faktorisierung von p in eine Einheit und irreduzible Elemente dieser Art in allen Fällen mit Ausnahme des Falls $p = 2$, in dem diese eindeutige Faktorisierung die Gestalt $2 = -\mathrm{i}(1 + \mathrm{i})^2$ hat.

Ergänzung 6.6.8. Es gibt auch einen sehr elementaren Beweis „durch Zauberei“ nach Zagier für die Tatsache, daß jede Primzahl p, die bei Teilen durch Vier den Rest Eins läßt, eine Summe von zwei Quadraten ist: Man betrachtet die endliche Menge $S := \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$ und definiert darauf eine Involution durch die Vorschrift

$$(x, y, z) \mapsto \begin{cases} (x + 2z, z, y - x - z) & \text{falls } x < y - z; \\ (2y - x, y, x - y + z) & \text{falls } y - z < x < 2y; \\ (x - 2y, x - y + z, y) & \text{falls } x > 2y. \end{cases}$$

Diese Involution hat genau einen Fixpunkt, also ist die Zahl der Elemente von S ungerade und die Involution $(x, y, z) \mapsto (x, z, y)$ von S muß auch einen Fixpunkt haben. Für den aber gilt $x^2 + (2y)^2 = p$. Bei diesem Beweis sind noch einige implizit enthaltene Behauptungen zu prüfen, das geht alles mit Schulstoff. Aber man muß die Zauberformel auswendig hersagen können!

Korollar 6.6.9 (**Summen von zwei Quadraten**). *Eine positive natürliche Zahl ist Summe von zwei Quadratzahlen genau dann, wenn in ihrer Primfaktorzerlegung alle diejenigen Primfaktoren, die modulo Vier kongruent sind zu Drei, in geraden Potenzen auftreten.*

Beweis. Genau dann ist $n \in \mathbb{Z}$ Summe von zwei Quadratzahlen, wenn es $a \in \mathbb{Z}[\mathrm{i}]$ gibt mit $n = a\bar{a}$. Ist $n \neq 0$ und $a = \varepsilon\pi_1\pi_2 \ldots \pi_r$ eine Darstellung als Produkt einer Einheit ε mit Primelementen, von denen wir $\pi_1, \ldots, \pi_s$ weder reell noch rein imaginär annehmen und $\pi_{s+1}, \ldots, \pi_r$ aus $\mathbb{N}$, so muß

$$n = (\varepsilon\bar{\varepsilon})(\pi_1\bar{\pi}_1) \ldots (\pi_s\bar{\pi}_s)\pi_{s+1}\pi_{s+1} \ldots \pi_r\pi_r$$

die Primfaktorzerlegung in $\mathbb{N}$ sein. Damit folgt das Korollar aus unserer Beschreibung 6.6.7 der Primelemente im Ring der Gauß'schen Zahlen. □

6.6.10. Um aus einer Primfaktorzerlegung einer natürlichen Zahl $n \geq 1$ im Ring der Gauß'schen Zahlen alle möglichen Darstellungen als Summe zweier Quadrate

zu erhalten, muß man alle Zerlegungen $n = (x+\mathrm{i}y)(x-\mathrm{i}y)$ finden, also alle Zerlegungen $n = a\bar{a}$, wobei der Übergang von a zu εa mit einer Einheit $\varepsilon \in \mathbb{Z}[\mathrm{i}]^\times$ und der Übergang von a zu $\bar{a}$ bis auf Reihenfolge dieselbe Zerlegung liefert. Dafür ist es besonders übersichtlich, mit dem in 6.6.7 beschriebenen Repräsentantensystem modulo Einheiten aller irreduziblen Elemente zu arbeiten, das stabil wird unter der komplexen Konjugation, sobald wir die Ausnahmestelle $1+\mathrm{i}$ entfernen.

6.6.11. Gegeben ein faktorieller Ring R bezeichne $\mathrm{irk}(R)$ die Menge **Irreduziblenklassen**, als da heißt der Bahnen unter der Einheitengruppe $R^\times$ in der Menge der irreduziblen Elemente von R. Gegeben ein irreduzibles $r \in R$ bezeichne $[r] \in \mathrm{irk}(R)$ seine Klasse.

Proposition* 6.6.12 (Irreduziblenklassen in Invariantenringen). *Seien R ein faktorieller Ring und Γ eine endliche Gruppe von Automorphismen von R und es sei auch der Ring R^Γ der Γ-Invarianten faktoriell. So gilt:*

1. *Wir erhalten eine Bijektion*

$$\mathrm{irk}(R^\Gamma) \xrightarrow{\sim} \mathrm{irk}(R)/\Gamma$$

   durch die Abbildung, die jedem R^Γ-irreduziblen Element p die Menge der Klassen seiner R-irreduziblen Faktoren π zuordnet;

2. *Die Vielfachheit von π in p teilt die Ordnung $|\Gamma_{[\pi]}|$ der Isotropiegruppe der Irreduziblenklasse $[\pi]$.*

6.6.13. Diese Proposition systematisiert unsere obigen Betrachtungen zu irreduziblen Gauß'schen Zahlen. Betrachten wir genauer $R = \mathbb{Z}[\mathrm{i}]$ mit der Operation der zweielementigen Gruppe Γ, deren nichttriviales Element als die komplexe Konjugation operiert, so erhalten wir $R^\Gamma = \mathbb{Z}$ und sehen ein weiteres Mal, daß jede irreduzible Gauß'schen Zahl π nur genau eine Primzahl p teilt und daß die Abbildung, die ihr diese Primzahl zuordnet, surjektiv ist mit bis auf Einheiten höchstens zweielementigen Fasern. Teil 2 zeigt dann weiter, daß die Vielfachheit von π in p höchstens Zwei ist und nur dann genau Zwei sein kann, wenn gilt $\bar{\pi} \in \mathbb{Z}[\mathrm{i}]^\times \pi$. Davon ausgehend analysiert man wie oben erklärt, daß $2 = -\mathrm{i}(1+\mathrm{i})^2$ bis auf Einheiten die einzige Möglichkeit für Vielfachkeit Zwei ist.

Beweis. Für $\pi \in R$ gehört das Produkt $b(\pi) := \prod_{\gamma\in\Gamma} \gamma(\pi)$ zu R^Γ. Mithin ist jedes R-irreduzible Element ein Teiler mindestens eines R^Γ-irreduziblen Elements und unsere Abbildung ist surjektiv. Teilt andererseits ein R-irreduzibles Element π zwei R^Γ-Irreduzible p und q, so teilt $b(\pi)$ sowohl $b(p) = p^{|\Gamma|}$ als auch $b(q) = q^{|\Gamma|}$, und da $b(\pi)$ keine Einheit sein kann, können sich p und q höchstens um eine Einheit unterscheiden und unsere Abbildung ist auch injektiv. Wir finden sogar

genauer $b(\pi) = \varepsilon p^n$ für $\varepsilon \in R^\Gamma$ eine Einheit. Wenn r die Vielfachheit von π in p ist und $\Gamma_{[\pi]}$ die Standgruppe der Irreduziblenklasse $[\pi]$, so haben wir weiter

$$p = \eta \prod_{\bar{\gamma} \in \Gamma/\Gamma_{[\pi]}} \gamma(\pi)^r$$

mit einer Einheit $\eta \in R^\times$, die von der Wahl der Repräsentanten γ unserer Nebenklassen $\bar{\gamma}$ abhängt, und für $d = |\Gamma_{[\pi]}|$ gilt folglich $p^d \in b(\pi)^r R^\times = (p^n)^r R^\times$ und folglich $d = rn$. □

Übungen

Übung 6.6.14. Man bestimme sämtliche Zerlegungen von 1000000 in eine Summe von zwei Quadratzahlen.

6.7 Primfaktorzerlegung in Polynomringen

6.7.1. Gegeben ein faktorieller Ring R und ein irreduzibles Element $p \in R$ erklären wir

$$v_p : \mathrm{Quot} R \to \mathbb{Z} \sqcup \{\infty\}$$

als die eindeutig bestimmte Abbildung mit $v_p\left(p^n a/b\right) = n$ für $a, b \in R \backslash 0$ teilerfremd zu p und mit $v_p(0) = \infty$. Diese Abbildung v_p heißt die p**-Bewertung** oder englisch p**-valuation**. Offensichtlich gilt $v_p(fg) = v_p(f) + v_p(g)$ für alle Elemente $f, g \in \mathrm{Quot}\, R$.

Beispiele 6.7.2. Wir haben $v_2(16/6) = 3$, $v_3(16/6) = -1$, $v_5(16/6) = 0$. Ist k ein Körper und $R = k[t]$ der Polynomring, so ist per definitionem $\mathrm{Quot} R = k(t)$ der Funktionenkörper und für $f \in k(t)$ und $\lambda \in k$ ist $v_{(t-\lambda)}(f)$ die Nullstellenordnung beziehungsweise das Negative der Polstellenordnung der gebrochen rationalen Funktion f an der Stelle λ.

6.7.3 (**Bewertung von Polynomen**). Gegeben ein faktorieller Ring R mit einem irreduziblen Element p sowie ein Polynom $A = a_n X^n + \ldots + a_1 X + a_0 \in (\mathrm{Quot} R)[X]$ erklären wir die p**-Bewertung des Polynoms** A durch

$$v_p(A) := \min(v_p(a_i))$$

Insbesondere ist das Nullpolynom das einzige Polynom A mit $v_p(A) = \infty$.

Beispiele 6.7.4. Im Fall $R = \mathbb{Z}$ haben wir etwa $v_2(10X^2 + 6X + 8) = 1$.

Proposition 6.7.5 (Lemma von Gauß). *Gegeben ein faktorieller Ring R und ein irreduzibles Element $p \in R$ und Polynome $A, B \in (\mathrm{Quot} R)[X]$ gilt*

$$v_p(AB) = v_p(A) + v_p(B)$$

Beweis. Ist eines unserer Polynome konstant, so gilt die Gleichung offensichtlich. Mit dieser Erkenntnis können wir uns auf den Fall zurückziehen, daß A und B Koeffizienten in R haben und daß gilt $v_p(A) = v_p(B) = 0$. Es bleibt, aus diesen Annahmen $v_p(AB) = 0$ zu folgern. Für ein Polynom $A \in R[X]$ ist $v_p(A) = 0$ nun gleichbedeutend dazu, daß sein Bild $\bar{A} \in (R/\langle p\rangle)[X]$ nicht das Nullpolynom ist. Wir haben also

$$\begin{aligned} v_p(A) = 0 = v_p(B) &\Rightarrow \bar{A} \neq 0 \neq \bar{B} \\ &\Rightarrow \bar{A}\bar{B} \neq 0 \\ &\Rightarrow \overline{AB} \neq 0 \\ &\Rightarrow v_p(AB) = 0 \end{aligned}$$

mit der zweiten Implikation, da $R/\langle p\rangle$ nach 6.4.34 und dann auch $(R/\langle p\rangle)[X]$ Integritätsbereiche sind. □

Definition 6.7.6. Sei R ein faktorieller Ring. Ein Polynom $\sum_{i=0}^{r} a_i X^i$ aus dem Polynomring $R[X]$ heißt **primitiv**, wenn es kein irreduzibles Element von R gibt, das alle seine Koeffizienten teilt. Ein Polynom mit Koeffizienten im Quotientenkörper $P \in (\mathrm{Quot}R)[X]$ nennen wir **primitiv** oder genauer **R-primitiv**, wenn es bereits in $R[X]$ liegt und dort primitiv ist.

6.7.7 (**Diskussion der Terminologie**). Ich bin nicht glücklich darüber, daß mit dieser Definition auch alle Einheiten von R primitive Polynome in $R[X]$ sind. An primitive Polynome aber noch zusätzliche Bedingungen zu stellen, schien mir ein größeres Übel.

6.7.8. Offensichtlich ist ein Polynom $A \in (\mathrm{Quot}R)[X]$ primitiv genau dann, wenn gilt $v_p(A) = 0$ für alle irreduziblen Elemente p von R. Offensichtlich gibt es für jedes von Null verschiedene Polynom $A \in (\mathrm{Quot}R)[X]\backslash 0$ ein Element $c \in \mathrm{Quot}R$ mit cA primitiv.

6.7.9 (**Lemma von Gauß, ursprüngliche Form**). In seiner ursprünglichen Form sagt das Lemma von Gauß, daß das Produkt zweier primitiver Polynome mit ganzzahligen Koeffizienten auch selbst wieder primitiv ist. Das folgt sofort aus 6.7.5 und ist auch im wesentlichen die Aussage, auf die wir uns dort beim Beweis zurückgezogen haben.

Beispiele 6.7.10. Die Polynome $X^2+2X+10$ und $3X^2+20X+150$ sind primitiv in $\mathbb{Z}[X]$. Das Polynom $10X^2 + 6X + 8$ ist nicht primitiv in $\mathbb{Z}[X]$.

Satz 6.7.11 (Polynomringe über faktoriellen Ringen). *Ist R ein faktorieller Ring, so ist auch der Polynomring $R[X]$ ein faktorieller Ring und die irreduziblen Elemente von $R[X]$ sind genau:*

1. *Alle irreduziblen Elemente von R;*

2. *Alle primitiven Polynome aus $R[X]$, die irreduzibel sind in $(\mathrm{Quot}R)[X]$.*

Beweis. Man sieht leicht, daß die unter 1 und 2 aufgeführten Elemente irreduzibel sind. Wir nennen sie für den Moment kurz die 1&2-Irreduziblen von $R[X]$. Wir vereinbaren für das weitere die Notation $\mathrm{Quot}R = K$. Gegeben $A \in R[X]$ zerlegen wir $A = P_1 \dots P_n$ als Produkt von irreduziblen Polynomen in $K[X]$ und schreiben $P_i = c_i \tilde{P}_i$ mit $c_i \in K^\times$ und $\tilde{P}_i$ primitiv. So erhalten wir eine Zerlegung $A = c\tilde{P}_1 \dots \tilde{P}_n$ mit $\tilde{P}_i$ primitiv und irreduzibel in $K[X]$ sowie $c \in K^\times$. Nach dem Lemma von Gauß 6.7.5 folgt $v_p(c) = v_p(A) \geq 0$ für alle Irreduziblen p von R und damit $c \in R$. Wir können also c faktorisieren in $c = up_1 \dots p_r$ mit $u \in R^\times$ und $p_i \in R$ irreduzibel und folgern so die Existenz einer Zerlegung von A in ein Produkt einer Einheit mit 1&2-Irreduziblen. Das zeigt insbesondere, daß wir unter 1 und 2 in der Tat alle irreduziblen Elemente von R aufgelistet haben. Sind

$$A = up_1 \dots p_r P_1 \dots P_m = vq_1 \dots q_s Q_1 \dots Q_n$$

zwei Zerlegungen von A in ein Produkt einer Einheit mit irreduziblen Elementen, sagen wir $u, v \in R^\times$, $p_i, q_j \in R$ irreduzibel und $P_k, Q_l \in R[X]$ irreduzibel in $K[X]$ und R-primitiv, so liefert die Eindeutigkeit der Primfaktorzerlegung in $K[X]$ zunächst $n = m$ und $P_i = a_i Q_{\sigma(i)}$ für geeignetes $\sigma \in \mathcal{S}_n$ und $a_i \in K^\times$. Aus der Primitivität folgt dann $a_i \in R^\times$ und aus der Faktorialität von R schließlich die Gleichheit $r = s$ sowie die Existenz einer Permutation $\tau \in \mathcal{S}_r$ mit $q_i \in p_{\tau(i)} R^\times$. □

Ergänzung 6.7.12. Die Zerlegung eines Polynoms aus $\mathbb{Z}[X]$ in irreduzible Faktoren kann im Prinzip durch Ausprobieren in endlicher Zeit bestimmt werden. Ein Polynoms vom Grad n muß ja, wenn es nicht irreduzibel ist, einen Faktor haben von höchstens dem halben Grad, sagen wir höchstens Grad m. Nehmen wir dann $m + 1$ ganzzahlige Stellen, so müssen die Werte unseres Faktors die Werte des ursprünglichen Polynoms teilen. Wir müssen also nur für alle Wahlen von Teilern der Werte des ursprünglichen Polynoms an besagten Stellen das Interpolationspolynom bilden und prüfen, ob es unser ursprüngliches Polynom teilt.

Korollar 6.7.13. *Sei R ein faktorieller Ring. Ist ein von Null verschiedenes Polynom $P \in R[X]\backslash 0$ nicht irreduzibel als Element des Polynomrings über dem Quotientenkörper $P \in (\mathrm{Quot}R)[X]$, so gibt es bereits in $R[X]$ Polynome A, B positiven Grades mit $AB = P$.*

Erster Beweis. Ist P primitiv, so folgt das unmittelbar aus unserem Satz. Andernfalls schreiben wir $P = c\tilde{P}$ mit $c \in R$ und $\tilde{P}$ primitiv und argumentieren genauso. □

Beispiel 6.7.14. Ich will auch noch an einem Beispiel erklären, wie man dies Korollar direkt aus dem Gauß'schen Lemma folgern kann. Nehmen wir an, wir hätten für $7X^2 - 7$ in $\mathbb{Q}[X]$ die Faktorisierung

$$7X^2 - 7 = (3X/7 + 3/7)(49X/3 - 49/3)$$

gefunden. Dann gilt $v_7(3X/7 + 3/7) + v_7(49X/3 - 49/3) = 1 \geq 0$ nach dem Gauß'schen Lemma und wir können folglich so Primfaktoren 7 zwischen den Faktoren unserer Faktorisierung austauschen, daß beide Faktoren dadurch eine positive 7-Bewertung kriegen. Diese Möglichkeiten wären hier $7X^2 - 7 = (3X + 3)(7X/3 - 7/3)$ und $7X^2 - 7 = (21X + 21)(X/3 - 1/3)$. Ebenso können wir für den Primfaktor 3 vorgehen und erhalten so die beiden Zerlegungen $7X^2 - 7 = (X + 1)(7X - 7)$ und $7X^2 - 7 = (7X + 7)(X - 1)$ in $\mathbb{Z}[X]$.

Korollar 6.7.15. *Für jeden Körper k ist der Polynomring $k[X_1, \ldots, X_n]$ faktoriell. Sogar $\mathbb{Z}[X_1, \ldots, X_n]$ ist ein faktorieller Ring.*

Korollar 6.7.16. *Ist k ein Körper und sind $f, g \in k[X, Y]$ teilerfremde Polynome, so haben f und g höchstens endlich viele gemeinsame Nullstellen in k^2.*

Vorschau 6.7.17. In 6.10.2 werden wir genauer die „Schranke von Bézout" für die maximal mögliche Zahl gemeinsamer Nullstellen herleiten.

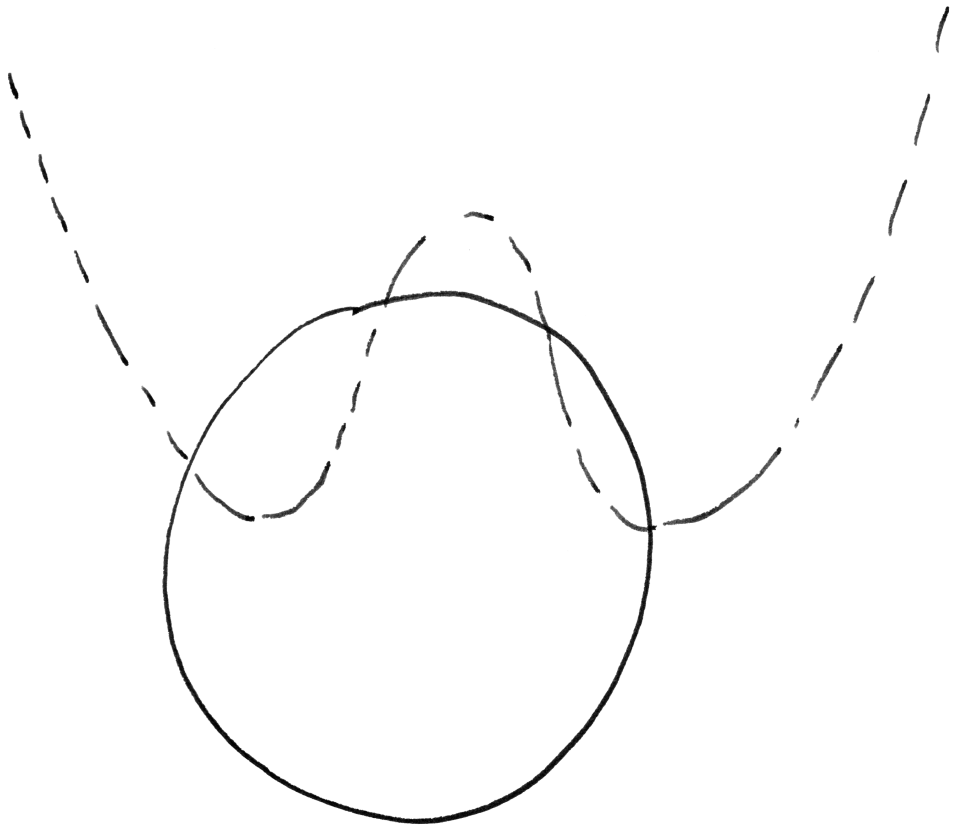
Beweis. Unsere Polynome haben nach der Beschreibung 6.7.11 der irreduziblen Elemente in Polynomringen über faktoriellen Ringen außer Einheiten erst recht keine gemeinsamen Teiler im Ring $k(X)[Y]$. Da dieser Ring nach 6.4.19 ein Hauptidealring ist, und da jeder Erzeuger des von unseren beiden Polynomen darin erzeugten Ideals ein gemeinsamer Teiler ist, gibt es notwendig $p, q \in k(X)[Y]$ mit $1 = pf + qg$. Nach Multiplikation mit so einer Art Hauptnenner h von p und q erhalten wir eine Identität der Gestalt

$$h = \tilde{p}f + \tilde{q}g$$

mit $0 \neq h \in k[X]$ und $\tilde{p}, \tilde{q} \in k[X, Y]$. Die endlich vielen Nullstellen von h sind dann die einzigen x-Koordinaten, die für gemeinsame Nullstellen von f und g in Frage kommen. Ebenso kommen auch nur endlich viele y-Koordinaten für gemeinsame Nullstellen in Frage. Das Korollar folgt. □

Übungen

Übung 6.7.18. Ist R ein faktorieller Ring mit Quotientenkörper K und sind $P, Q \in K[X]$ normierte Polynome mit $PQ \in R[X]$, so folgt bereits $P, Q \in R[X]$.



Die Nullstellenmengen zweier Polynome $f, g \in \mathbb{R}[X, Y]$ ohne gemeinsamen nichtkonstanten Teiler als durchgezogener Kreis und gestrichelter Umriß eines auf dem Rücken liegenden Kamels. Hierfür ist die Papierebene vermittels eines Koordinatensystems mit dem $\mathbb{R}^2$ zu identifizieren. Legen wir etwa den Ursprung ins Zentrum des durgezogenen Kreises, so würden wir $f(X, Y) = X^2 + Y^2 - 1$ und $g(X, Y) = X^4 - 2X^2 + \frac{3}{2} - Y$ in etwa die skizzierten Nullstellenmengen besitzen.

Übung 6.7.19. Sei k ein Körper. Gibt es für ein Polynom P aus dem Polynomring $P \in k[X_1, \ldots, X_n]$ ein Element $Q \in k(X_1, \ldots, X_n)$ aus dem Quotientenkörper mit $Q^2 = P$, so ist Q bereits selbst ein Polynom, in Formeln $Q \in k[X_1, \ldots, X_n]$. Hinweis: 6.4.32.

Übung 6.7.20. Seien k ein Körper und $0 < n(1) < n(2) < \ldots < n(r) < n$ natürliche Zahlen, $r \geq 0$. Man zeige, daß das Polynom

$$T^n + a_r T^{n(r)} + \ldots + a_1 T^{n(1)} + a_0$$

irreduzibel ist in $K[T]$, für $K = \operatorname{Quot} k[{}'a_0, \ldots, a_r]$ der Funktionenkörper. Hinweis: Jede Zerlegung käme nach 6.7.18 und 6.7.11 notwendig von einer Zerlegung im Polynomring $k[{}'a_0, \ldots, a_r, T]$ her und müßte unter dem Einsetzen $a_1 = \ldots = a_r = 0$ zu einer Zerlegung von $T^n + a_0$ in $k[{}'a_0, T]$ führen.

Übung 6.7.21. Sei K ein Körper und $K(X)$ sein Funktionenkörper. Man zeige, daß jedes K-irreduzible Polynom in $K[T]$ auch $K(X)$-irreduzibel ist. Hinweis: 6.7.18.

Übung 6.7.22 (**Satz über rationale Nullstellen**). Man zeige: Gegeben ein Polynom

$$a_n T^n + \ldots + a_1 T + a_0$$

mit ganzzahligen Koeffizienten und eine rationale Wurzel p/q mit p, q teilerfremden ganzen Zahlen ist p ein Teiler von a_0 und q ein Teiler von a_n.

6.8 Kreisteilungspolynome

6.8.1. Wir interessieren uns in dieser Vorlesung besonders für uns die Zerlegung der Polynome $X^n - 1$ in irreduzible Faktoren in $\mathbb{Z}[X]$. Die komplexen Nullstellen von $X^n - 1$ heißen die **komplexen n-ten Einheitswurzeln**. Sie bilden in der komplexen Zahlenebene die Ecken eines in den Einheitskreis eingeschriebenen regelmäßigen n-Ecks. In $\mathbb{C}[X]$ gilt natürlich

$$X^n - 1 = \prod_{\zeta^n = 1} (X - \zeta)$$

Nun bilden wir in $\mathbb{C}[X]$ die Polynome

$$\Phi_d(X) = \prod_{\operatorname{ord} \zeta = d} (X - \zeta)$$

Dann gilt offensichtlich

$$X^n - 1 = \prod_{d|n} \Phi_d(X)$$

Sicher sind alle unsere Polynome Φ_d normiert. Daraus folgt durch Teilen mit Rest 2.3.15 und Induktion $\Phi_n(X) \in \mathbb{Z}[X]$ für alle $n \geq 1$. Dies Polynom Φ_n heißt das n**-te Kreisteilungspolynom** oder bei griechisch Gebildeten das n**-te zyklotomische Polynom**. Natürlich gilt $\mathrm{grad}(\Phi_n) = \varphi(n)$, der Grad des n-ten Kreisteilungspolynoms ist also genau der Wert der Euler'schen φ-Funktion an der Stelle n, und das macht auch die Notation plausibel. Wir werden in 8.4.2 zeigen, daß alle Kreisteilungspolynome irreduzibel sind in $\mathbb{Q}[X]$, so daß wir das n-te Kreisteilungspolynom auch und vielleicht eher noch besser charakterisieren können als das eindeutig bestimmte normierte in $\mathbb{Q}[X]$ irreduzible Polynom, das die n-te Einheitswurzel $\exp(2\pi\mathrm{i}/n)$ als Nullstelle hat. Natürlich haben wir für $p > 1$ stets die Zerlegung $X^p - 1 = (X-1)(X^{p-1} + X^{p-2} + \ldots + X + 1)$, also ist für p prim der zweite Faktor das p-te Kreisteilungspolynom Φ_p. In diesem Fall können wir die Irreduzibilität mithilfe des gleich folgenden „Eisensteinkriteriums" bereits hier zeigen.

Satz 6.8.2 (**Eisensteinkriterium**). *Sei $P = a_nX^n + \ldots + a_1X + a_0 \in \mathbb{Z}[X]$ ein Polynom mit ganzzahligen Koeffizienten und p eine Primzahl. Gilt $p \nmid a_n$, $p|a_{n-1}$, $\ldots$, $p|a_0$ und $p^2 \nmid a_0$, so ist P irreduzibel in $\mathbb{Q}[X]$.*

6.8.3. Eine analoge Aussage gilt mit demselben Beweis auch für Polynome mit Koeffizienten in einem beliebigen faktoriellen Ring.

Beweis. Ist P nicht irreduzibel in $\mathbb{Q}[X]$, so besitzt es nach 6.7.13 bereits eine Faktorisierung $P = QR$ in $\mathbb{Z}[X]$ mit Q, R von positiven Graden $r, s > 0$ und $r + s = n$. Wir reduzieren nun die Koeffizienten modulo p und folgern in $\mathbb{F}_p[X]$ eine Faktorisierung

$$\bar{P} = \bar{Q}\,\bar{R}$$

Nach Annahme haben wir aber $\bar{P} = \bar{a}_nX^n$ mit $\bar{a}_n \neq 0$. Es folgt $\bar{Q} = bX^r$ und $\bar{R} = cX^s$ für geeignete $b, c \in \mathbb{F}_p^\times$ und denselben positiven $r, s > 0$, denn das sind die einzig möglichen Faktorisierungen von $\bar{a}_nX^n$ als Produkt von Nichteinheiten im faktoriellen Ring $\mathbb{F}_p[X]$. Daraus folgt hinwiederum, daß die konstanten Terme von Q und R durch p teilbar sind, und dann muß der konstante Term von $QR = P$ teilbar sein durch p^2 im Widerspruch zur Annahme. □

Korollar 6.8.4. *Für jede Primzahl p ist das p-te Kreisteilungspolynom $\Phi_p(X) = X^{p-1} + X^{p-2} + \ldots + X + 1$ irreduzibel in $\mathbb{Q}[X]$.*

Beweis. Wir haben $X^p - 1 = (X-1)\Phi_p(X)$. Reduzieren wir diese Gleichung modulo p und beachten die Gleichung $X^p - 1 = (X-1)^p$ in $\mathbb{F}_p[X]$, so folgt $\bar{\Phi}_p(X) = (X-1)^{p-1}$ in $\mathbb{F}_p[X]$ und nach der Substitution $X = Y + 1$ haben wir $\bar{\Phi}_p(Y+1) = Y^{p-1}$ in $\mathbb{F}_p[Y]$, als da heißt, alle Koeffizienten von $\Phi_p(Y+1)$ bis auf den Leitkoeffizienten sind durch p teilbar. Jetzt prüfen wir einfach explizit, daß

der konstante Term von $\Phi_p(Y+1)$ genau p ist, und haben gewonnen nach dem Eisensteinkriterium 6.8.2. □

Ergänzung 6.8.5. Nach ersten Rechnungen mag man vermuten, daß als Koeffizienten von Kreisteilungspolynomen nur 1, 0 und -1 in Frage kommen. Das erste Gegenbeispiel für diese Vermutung liefert das 105-te Kreisteilungspolynom, in dem X^7 mit dem Koeffizienten 2 auftritt. Man kann allgemeiner sogar zeigen [Suz87, SDAT00], daß jede ganze Zahl als Koeffizient mindestens eines Kreisteilungspolynoms auftritt.

Übungen

Übung 6.8.6 (**Kreisteilungspolynome zu Primzahlpotenzen**). Man zeige die Formel $\Phi_9(X) = X^6 + X^3 + 1$ für das neunte Kreisteilungspolynom. Man zeige allgemeiner $\Phi_{p^r}(X) = \Phi_p(X^{p^{r-1}})$ für p prim und $r \geq 1$. Man gebe auch explizite Formeln für alle kleineren Kreisteilungspolynome $\Phi_1, \ldots, \Phi_8$.

Übung 6.8.7. Man zeige, daß das neunte Kreisteilungspolynom $\Phi_9(X) = X^6 + X^3 + 1$ in $\mathbb{Q}[X]$ irreduzibel ist. Hinweis: Man substituiere $X = Y + 1$ und wende das Eisensteinkriterium an. Mit einem bereits weiter oben verwendeten Trick kann die Rechnung stark vereinfacht werden. Dasselbe Argument zeigt, daß alle Kreisteilungspolynome $\Phi_{p^r}(X)$ für eine Primzahl p in $\mathbb{Q}[X]$ irreduzibel sind.

Übung 6.8.8. Man zeige, daß $X^7 - 9$ ein irreduzibles Polynom in $\mathbb{Z}[X]$ ist. Hinweis: Man betrachte die Einbettung $\mathbb{Z}[X] \hookrightarrow \mathbb{Z}[Y]$ mit $X \mapsto Y^2$.

Ergänzende Übung 6.8.9. Man zerlege $(X^n - Y^n)$ in $\mathbb{C}[X, Y]$ in ein Produkt irreduzibler Faktoren.

Ergänzende Übung 6.8.10 (**Quantisierte Binomialkoeffizienten**). Ist $\mathbb{F}$ ein endlicher Körper mit q Elementen, so ist die Zahl der k-dimensionalen Teilräume von $\mathbb{F}^n$ genau

$$\frac{(q^n-1)(q^n-q)\ldots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\ldots(q^k-q^{k-1})}$$

Setzen wir $[n]_q := q^{n-1} + q^{n-1} + \ldots + 1 = (q^n - 1)/(q - 1)$, so können wir unser Ergebnis auch darstellen als

$$\frac{[n]_q[n-1]_q\ldots[n-k+1]_q}{[k]_q[k-1]_q\ldots[1]_q}$$

Für diese **quantisierten Binomialkoeffizienten** ist auch eine Notation wie für die gewöhnlichen Binomialkoeffizienten mit eckigen statt runden Klammern üblich. Man zeige, daß unsere quantisierten Binomialkoeffizienten, wenn wir sie als Element des Quotientenkörpers $\mathbb{Q}('q)$ lesen, für alle k, n mit $0 \leq k \leq n$ bereits im Polynomring $\mathbb{Z}['q] \subset \mathbb{Q}('q)$ liegen. Hinweis: Man finde eine induktive Beschreibung der Art, wie sie dem Pascal'schen Dreieck zugrunde liegt.

6.9 Symmetrische Polynome

Definition 6.9.1. Sei k ein Ring. Für jede Permutation $\sigma \in \mathcal{S}_n$ setzen wir die Identität auf k fort zu einem Ringhomomorphismus

$$\begin{array}{rccc} \sigma: & k[X_1,\ldots,X_n] & \to & k[X_1,\ldots,X_n] \\ & X_i & \mapsto & X_{\sigma(i)} \end{array}$$

Ein Polynom $f \in k[X_1,\ldots,X_n]$ heißt **symmetrisch**, wenn gilt $f = \sigma f \quad \forall \sigma \in \mathcal{S}_n$. Die Menge aller symmetrischen Polynome ist ein Teilring des Polynomrings $k[X_1,\ldots,X_n]$. Wir notieren ihn $k[X_1,\ldots X_n]^{\mathcal{S}_n}$.

6.9.2. Operiert ganz allgemein eine Gruppe G auf einem Ring R durch Ringhomomorphismen, so bilden die G-Invarianten stets einen Teilring R^G, den sogenannten **Invariantenring**.

6.9.3. Operiert eine Gruppe G auf einem Ring R durch Ringhomomorphismen, so operiert unsere Gruppe natürlich auch auf dem Polynomring über R in einer oder sogar in mehreren Veränderlichen. Die Invarianten des Polynomrings fallen dann mit dem Polynomring über dem Invariantenring zusammen, in Formeln $R[T]^G = R^G[T]$.

Beispiele 6.9.4. Das Produkt $X_1 \ldots X_n$ und die Summe $X_1 + \ldots + X_n$ sind symmetrische Polynome. Allgemeiner definieren wir die **elementarsymmetrischen Polynome** in n Veränderlichen $s_i(X_1,\ldots,X_n) \in \mathbb{Z}[X_1,\ldots,X_n]^{\mathcal{S}_n}$ durch die Identität

$$(T+X_1)(T+X_2)\ldots(T+X_n) = T^n + s_1T^{n-1} + s_2T^{n-2} + \ldots + s_n$$

im Ring $\mathbb{Z}[X_1,\ldots,X_n][T]^{\mathcal{S}_n} = \mathbb{Z}[X_1,\ldots,X_n]^{\mathcal{S}_n}[T]$, so daß wir also haben

$$s_i = \sum_{|I|=i} \left(\prod_{j\in I} X_j \right)$$

Die Summe läuft über alle i-elementigen Teilmengen $I \subset \{1,\ldots,n\}$. Speziell ergibt sich $s_1 = X_1 + \ldots + X_n$ und $s_2 = X_1X_2 + X_1X_3 + \ldots + X_1X_n + X_2X_3 + \ldots + X_2X_n + \ldots + X_{n-1}X_n$ und $s_n = X_1 \ldots X_n$.

6.9.5. Gegeben ein kommutativer Ring k sind für beliebige $\zeta_1,\ldots,\zeta_n \in k$ die Koeffizienten des Polynoms $\prod_{i=1}^n (T-\zeta_i) \in k[T]$ per definitionem die elementarsymmetrischen Polynome in den $(-\zeta_i)$. Grob gesprochen sind also „die Koeffizienten eines Polynoms bis auf Vorzeichen die elementarsymmetrischen Polynome in seinen Nullstellen“.

Satz 6.9.6 (über symmetrische Polynome). *Alle symmetrischen Polynome sind polynomiale Ausdrücke in den elementarsymmetrischen Polynomen, und die elementarsymmetrischen Polynome s_i sind algebraisch unabhängig. Für einen beliebigen Ring k haben wir also in Formeln*

$$k[X_1, \ldots, X_n]^{\mathcal{S}_n} = k['s_1, \ldots, s_n]$$

mit einem „Freiheitsstrichlein“ an der eröffnenden Klammer im Sinne unserer Notation 6.2.4.

Beispiel 6.9.7. Wir haben $X_1^3 + X_2^3 + X_3^3 = s_1^3 - 3s_1s_2 + 3s_3$.

Beispiel 6.9.8. Die Darstellung von $(X_1 - X_2)^2$ durch elementarsymmetrische Polynome ist

$$\begin{aligned}(X_1 - X_2)^2 &= (X_1 + X_2)^2 - 4X_1X_2 \\ &= s_1^2 - 4s_2\end{aligned}$$

Ein quadratisches Polynom $T^2 - pT + q = (T - \zeta)(T - \xi)$ mit Koeffizienten p, q und Nullstellen ζ, ξ in einem Integritätsbereich k hat also genau dann eine doppelte Nullstelle $\zeta = \xi$, wenn gilt

$$0 = p^2 - 4q$$

In diesem Spezialfall läuft unsere Argumentation darauf hinaus, für unsere p, q die Identität $(\zeta - \xi)^2 = (\zeta + \xi)^2 - 4\zeta\xi = p^2 - 4q$ zu zeigen, was nicht schwer nachzurechnen ist.

Beweis. Da die symmetrischen Polynome einen Ring bilden, folgt aus s_1, …, $s_n \in k[X_1, \ldots, X_n]^{\mathcal{S}_n}$ sofort $k[X_1, \ldots, X_n]^{\mathcal{S}_n} \supset k[s_1, \ldots, s_n]$. Für das weitere verwenden wir die Multiindexnotation wie in **??** und vereinbaren für einen Multiindex $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ die Abkürzung

$$X^\alpha := X_1^{\alpha_1} \ldots X_n^{\alpha_n}$$

Um nun die umgekehrte Inklusion $\subset$ zu zeigen, betrachten wir auf $\mathbb{N}^n$ die **lexikographische Ordnung**, also etwa $(5, 1, 3) \geq (4, 7, 1) \geq (4, 7, 0) \geq (4, 6, 114)$ im Fall $n = 3$. In Formeln ist sie induktiv definiert durch

$$\begin{aligned}(\alpha_1, \ldots, \alpha_n) \geq (\beta_1, \ldots, \beta_n) \quad \Leftrightarrow \quad & \alpha_1 > \beta_1 \\ & \text{oder} \\ & \alpha_1 = \beta_1 \text{ und } (\alpha_2, \ldots, \alpha_n) \geq (\beta_2, \ldots, \beta_n).\end{aligned}$$

Bezüglich dieser Ordnung besitzt jede nichtleere Teilmenge von $\mathbb{N}^n$ ein kleinstes Element. Für ein von Null verschiedenes Polynom $0 \neq f = \sum c_\alpha X^\alpha$ nennen wir

das größte $\alpha \in \mathbb{N}^n$ mit $c_\alpha \neq 0$ seinen „Leitindex“. Zum Beispiel hat das i-te elementarsymmetrische Polynom s_i den Leitindex $(1, \ldots, 1, 0, \ldots, 0)$ mit i Einsen vorneweg und dann nur noch Nullen. Gälte unsere Inklusion $\subset$ nicht, so könnten wir unter allen symmetrischen Polynomen außerhalb von $k[s_1, \ldots, s_n]$ ein f mit kleinstmöglichem Leitindex α wählen. Wegen $f = \sum c_\alpha X^\alpha$ symmetrisch gilt $c_\alpha = c_\beta$, falls sich die Multiindizes α und β nur in der Reihenfolge unterscheiden. Der Leitindex von f hat folglich die Gestalt

$$\alpha = (\alpha_1, \ldots, \alpha_n) \text{ mit } \alpha_1 \geq \ldots \geq \alpha_n$$

Dann hat das Produkt

$$g := s_1^{\alpha_1 - \alpha_2} s_2^{\alpha_2 - \alpha_3} \ldots s_{n-1}^{\alpha_{n-1} - \alpha_n} s_n^{\alpha_n}$$

denselben Leitindex wie f und den Koeffizienten Eins vor dem entsprechenden Monom. Die Differenz $f - c_\alpha g$ ist folglich entweder Null oder hat zumindest einen echt kleineren Leitindex, gehört also zu $k[s_1, \ldots, s_n]$. Dann gehört aber auch f selbst zu $k[s_1, \ldots, s_n]$ im Widerspruch zu unseren Annahmen. Um schließlich die lineare Unabhängigkeit der Monome $s_1^{\gamma_1} \ldots s_n^{\gamma_n}$ in den elementarsymmetrischen Funktionen zu zeigen beachten wir, daß diese Monome paarweise verschiedene Leitindizes haben. Ist nun eine Linearkombination mit Koeffizienten in k unserer Monome null, so notwendig auch der Koeffizient des Monoms mit dem größten Leitindex, und dann induktiv alle Koeffizienten aller Monome. □

Definition 6.9.9. Gegeben ein Multiindex $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ verwenden wir wie in **??** die Notation

$$|\alpha| := \alpha_1 + \ldots + \alpha_n$$

Ein Polynom in mehreren Veränderlichen mit Koeffizienten in einem beliebigen Ring heißt **homogen vom Grad** d, wenn es eine Linearkombination von Monomen X^α ist mit $|\alpha| = d$, in Formeln

$$f = \sum_{|\alpha|=d} c_\alpha X^\alpha$$

Nennt man ein Polynom einfach nur **homogen**, so ist gemeint, daß es einen Grad d gibt derart, daß unser Polynom homogen ist vom Grad d. Das Nullpolynom ist homogen von jedem Grad, aber jedes von Null verschiedene homogene Polynom ist homogen von nur genau einem Grad. Das Produkt zweier homogener Polynome ist homogen vom Grad der Summe der Grade der Faktoren. Gegeben ein nicht notwendig homogenes Polynom $g = \sum_\alpha c_\alpha X^\alpha$ heißt $\sum_{|\alpha|=d} c_\alpha X^\alpha$ seine **homogene Komponente vom Grad** d. Jedes Polynom ist mithin die Summe seiner homogenen Komponenten, und fast alle dieser homogenen Komponenten sind Null.

6.9.10 (**Diskussion der Terminologie**). Das Nullpolynom hat in unserer Terminologie einerseits den Grad $-\infty$ und ist andererseits homogen von jedem Grad $d \in \mathbb{N}$. Diese terminologische Schwierigkeit gilt es auszuhalten.

Beispiel 6.9.11. Das Polynom $X^3Y^3Z + X^2Z^5 - 98X^4YZ^2$ ist homogen vom Grad 7. Das elementarsymmetrische Polynom s_d ist homogen vom Grad d.

Beispiel 6.9.12. Wir versuchen, das symmetrische Polynom $\Delta := (X-Y)^2(Y-Z)^2(Z-X)^2$ durch elementarsymmetrische Funktionen auszudrücken, wo ich statt X_1, X_2, X_3 die Notation X, Y, Z verwendet habe. Unser Polynom ist homogen vom Grad 6 und das i-te elementarsymmetrische Polynom s_i ist homogen vom Grad i. Wir machen also den Ansatz

$$\Delta = As_1^6 + Bs_1^4s_2 + Cs_1^3s_3 + Ds_1^2s_2^2 + Es_1s_2s_3 + Fs_2^3 + Gs_3^2$$

Hier haben wir die Summanden nach ihren Leitindizes geordnet. Da in Δ keine Monome X^6 oder X^5Y vorkommen, gilt $A = B = 0$. Setzen wir $Z = 0$, so folgt

$$(XY)^2(X^2 - 2XY + Y^2) = D(X+Y)^2(XY)^2 + F(XY)^3$$

und damit $D = 1$ und $F = -4$. Wir kommen so zu einer Darstellung der Form

$$\Delta = Cs_1^3s_3 + s_1^2s_2^2 + Es_1s_2s_3 - 4s_2^3 + Gs_3^2$$

Zählen wir die Monome X^4YZ auf beiden Seiten, so folgt $C = -4$. Setzen wir jetzt für (X, Y, Z) speziell die Werte $(1, 1, -1)$ und $(2, -1, -1)$ ein, so erhalten für (s_1, s_2, s_3) die Werte $(1, -1, -1)$ und $(0, -3, 2)$ und finden

$$4 + 1 + E + G + 4 = 0 = 4G + 4 \cdot 27$$

Daraus folgt sofort $G = -27$, $E = 18$, und dann als Endresultat

$$\Delta = s_1^2s_2^2 - 4s_1^3s_3 + 18s_1s_2s_3 - 4s_2^3 - 27s_3^2$$

Ein kubisches Polynom $T^3 + aT^2 + bT + c = (T+\alpha)(T+\beta)(T+\gamma)$ mit Koeffizienten a, b, c und Nullstellen $-\alpha, -\beta, -\gamma$ in einem Integritätsbereich k hat also mehrfache Nullstellen genau dann, wenn gilt

$$0 = a^2b^2 - 4a^3c + 18abc - 4b^3 - 27c^2$$

Das Negative $\mathrm{Disk}_3 := -\Delta$ dieses Ausdrucks in den Koeffizienten werden wir gleich in 6.9.13 für normierte Polynome beliebigen Grades als deren „Diskriminante“ einführen.

Satz 6.9.13. *Es gibt für jedes $n \in \mathbb{N}$ genau ein Polynom in n Variablen, genannt die n-te* **Diskriminante** $\mathrm{Disk}_n \in \mathbb{Z}['a_1, \ldots, a_n]$*, mit der Eigenschaft, daß beim Einsetzen derjenigen Polynome $a_i \in \mathbb{Z}['\zeta_1, \ldots, \zeta_n]$ in die Variablen, die durch die Identität $T^n + a_1T^{n-1} + \ldots + a_n = (T + \zeta_1) \ldots (T + \zeta_n)$ gegeben werden, im Polynomring $\mathbb{Z}['\zeta_1, \ldots, \zeta_n]$ gilt*

$$\mathrm{Disk}_n(a_1, \ldots, a_n) = \prod_{i \neq j} (\zeta_i - \zeta_j)$$

6.9.14 (**Ursprung der Terminologie**). Die Bezeichnung „Diskriminante“ wird verständlich, wenn man mehrfache Nullstellen ansieht als „eigentlich verschiedene“ Nullstellen, die nur unglücklicherweise zusammenfallen und deshalb nicht mehr voneinander unterschieden oder lateinisierend „diskriminiert“ werden können.

Beweis. Unser Produkt ist offensichtlich symmetrisch und läßt sich nach 6.9.6 folglich eindeutig schreiben als Polynom in den elementarsymmetrischen Polynomen. □

6.9.15. Für jeden kommutativen Integritätsbereich k und jedes normierte Polynom $T^n + a_1T^{n-1} + \ldots + a_n$ im Polynomring $k[T]$, das in $k[T]$ vollständig in Linearfaktoren zerfällt, sind für die eben definierte Diskriminante Disk_n offensichtlich gleichbedeutend:

1. $\mathrm{Disk}_n(a_1, \ldots, a_n) = 0$;
2. Das Polynom $T^n + a_1T^{n-1} + \ldots + a_n$ hat mehrfache Nullstellen.

Man nennt das Element $\mathrm{Disk}_n(a_1, \ldots, a_n) \in k$ auch die **Diskriminante des normierten Polynoms** $T^n + a_1T^{n-1} + \ldots + a_n$. Eine explizite Formel für die Diskriminante geben wir in 7.9.27. Manche Quellen definieren die Diskriminate abweichend als $\prod_{i<j}(\zeta_i - \zeta_j)^2 = (-1)^{n(n-1)/2} \mathrm{Disk}_n$.

Beispiel 6.9.16. Gilt speziell im Polynomring $k[T]$ über irgendeinem Kring k die Identität $T^2 - pT + q = (T - \zeta)(T - \xi)$ für $p, q, \alpha, \beta, \gamma \in k$, so erhalten wir in k die Identität $-(\zeta - \xi)^2 = -p^2 + 4q$. Das bedeutet

$$\mathrm{Disk}_2(p, q) = -p^2 + 4q$$

Beispiel 6.9.17. Gilt speziell im Polynomring $k[T]$ über irgendeinem Kring k die Identität $T^3 + pT + q = (T - \alpha)(T - \beta)(T - \gamma)$ für $p, q, \alpha, \beta, \gamma \in k$, so erhalten wir in k die Identität $-(\alpha - \beta)^2(\beta - \gamma)^2(\gamma - \alpha)^2 = 4p^3 + 27q^2$. Das bedeutet

$$\mathrm{Disk}_3(0, p, q) = 4p^3 + 27q^2$$

Übungen

Übung 6.9.18. Was ist die Summe der $\lambda_1^3+\lambda_2^3+\lambda_3^3+\lambda_4^3$ dritten Potenzen der vier komplexen Nullstellen $\lambda_1,\ldots,\lambda_4$ des Polynoms $X^4+3X^3-5X^2+X+1$?

Ergänzende Übung 6.9.19. Man zeige für symmetrische Polynome im Fall $n \geq k$ die Identität

$$s_{2k}(X_1,\ldots,X_n,-X_1,\ldots,-X_n) = (-1)^k s_k(X_1^2,\ldots,X_n^2)$$

Ergänzende Übung 6.9.20. Man zeige, daß die Polynome $P \in \mathbb{Z}[X,Y]$, die bei Vertauschung von X und Y in ihr Negatives übergehen, gerade die Produkte von $(X-Y)$ mit symmetrischen Polynomen sind.

Ergänzende Übung 6.9.21. Sei k ein Körper einer von Zwei verschiedenen Charakteristik. Ein Polynom $f \in k[X_1,\ldots,X_n]$ heißt **antisymmetrisch** genau dann, wenn gilt $\sigma f = \operatorname{sgn}(\sigma) f \quad \forall \sigma \in \mathcal{S}_n$. Man zeige, daß die antisymmetrischen Polynome genau die Produkte von $\prod_{i<j}(X_i - X_j)$ mit symmetrischen Polynomen sind. Hinweis: 2.4.5. Man zeige dasselbe auch allgemeiner im Fall eines faktoriellen Rings k einer von Zwei verschiedenen Charakteristik.

Ergänzende Übung 6.9.22. Ist der Koeffizientenring k ein unendlicher Integritätsbereich, so ist ein Polynom $f \in k[X_1,\ldots,X_n]$ homogen vom Grad d genau dann, wenn gilt

$$f(\lambda X_1,\ldots,\lambda X_n) = \lambda^d f(X_1,\ldots,X_n) \qquad \forall \lambda \in k$$

Übung 6.9.23. Man stelle $X^4+Y^4+Z^4+W^4$ als Polynom in den elementarsymmetrischen Polynomen dar.

Ergänzende Übung 6.9.24. Ist R ein Kring mit einer Primzahl p als Charakteristik, so bilden die Elemente $a \in R$ mit $a^p = a$ einen Teilring.

Übung 6.9.25. Man zeige: Die Darstellung eines symmetrischen Polynoms vom Grad d durch elementarsymmetrische Polynome ist dieselbe für jede Zahl von Variablen $\geq d$. Zum Beispiel impliziert unsere Formel $X_1^3+X_2^3+X_3^3 = s_1^3 - 3s_1s_2+3s_3$, daß auch in 14 Variablen gilt $X_1^3+X_2^3+\ldots+X_{14}^3 = s_1^3-3s_1s_2+3s_3$.

Ergänzende Übung 6.9.26. Der Ring der symmetrischen Funktionen in n Veränderlichen mit Koeffizienten aus $\mathbb{Q}$ wird auch als Ring erzeugt von $\mathbb{Q}$ und den Potenzsummen $X_1^k+\ldots+X_n^k$ für $1 \leq k \leq n$. Hinweis: Wir schreiben $X_1^n+\ldots+X_n^n = P(s_1,\ldots,s_n)$ und müssen zeigen, daß rechts der Summand s_n mit von Null verschiedenem Koeffizienten auftritt. Dann kommen wir mit 6.9.25 und Induktion zum Ziel. Spezialisieren wir aber die X_ν zu den Negativen der n-ten Einheitswurzeln $\exp(2\pi\mathrm{i}\nu/n)$ alias den Negativen der Nullstellen von X^n-1, so werden alle $s_{n-1} = \ldots = s_1$ zu Null. Eine $(n \times n)$-Matrix A über einem Körper der Charakteristik Null ist nilpotent genau dann, wenn für die Spuren ihrer Potenzen gilt

$$0 = \operatorname{tr}(A) = \operatorname{tr}(A^2) = \ldots = \operatorname{tr}(A^n)$$

Übung 6.9.27. Seien k ein Körper und $f, g \in k[X,Y]$ teilerfremde Polynome, die homogen sind von den Graden m und n. Man zeige, daß sich jedes homogene Polynom h vom Grad $m+n-1$ eindeutig schreiben läßt als $h = af + bg$ mit a homogen vom Grad $n-1$ und b homogen vom Grad $m-1$. Hinweis: 6.4.33.

6.10 Schranke von Bézout*

Definition 6.10.1. Sei k ein Körper. Ein Polynom in zwei Veränderlichen $f \in k[X,Y]$ können wir in eindeutiger Weise schreiben in der Gestalt $f = \sum c_{pq} X^p Y^q$ mit $c_{pq} \in k$. Wir definieren den **Grad** oder genauer **Totalgrad** von f durch die Vorschrift

$$\operatorname{grad} f := \sup\{p+q \mid c_{pq} \neq 0\}$$

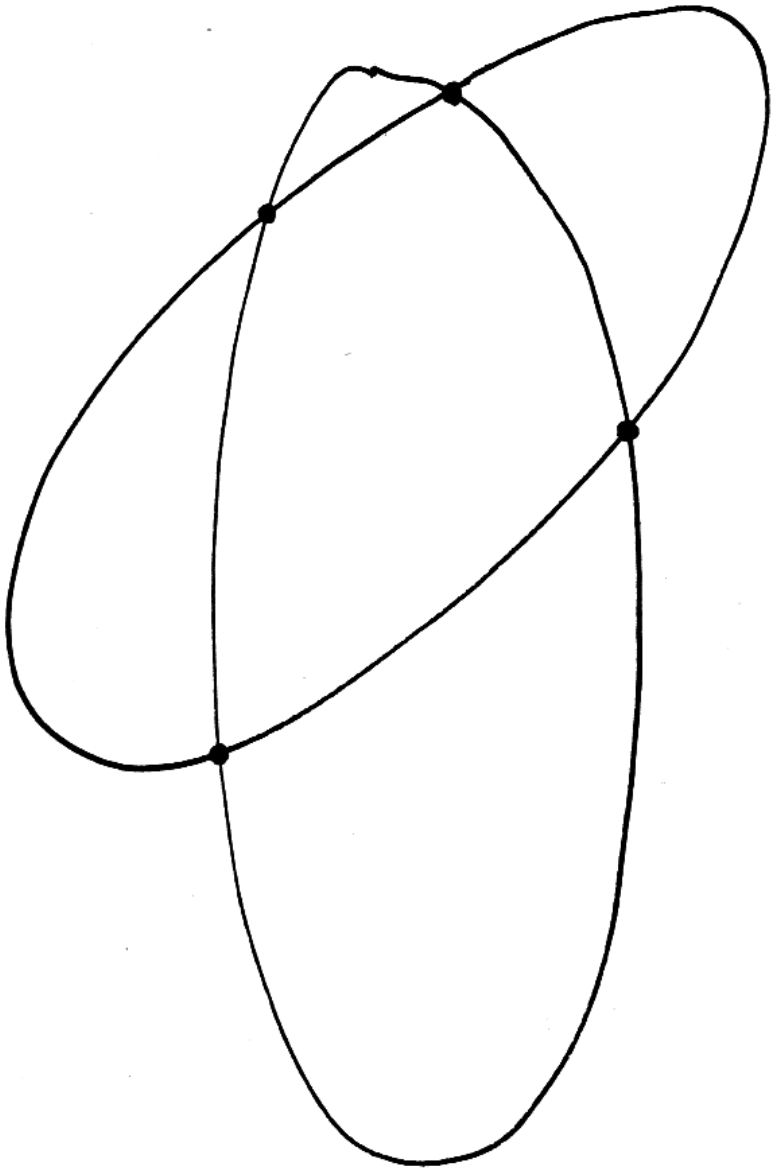
Speziell geben wir im Lichte von **??** dem Nullpolynom wie in einer Veränderlichen den Grad $-\infty$. Analog definieren wir auch den Grad eines Polynoms in beliebig vielen Veränderlichen.

Satz 6.10.2 (Schranke von Bézout). *Sei k ein Körper und seien im Polynomring $k[X,Y]$ in zwei Veränderlichen über k zwei von Null verschiedene teilerfremde Polynome f, g gegeben. So haben f und g in der Ebene k^2 höchstens $(\operatorname{grad} f)(\operatorname{grad} g)$ gemeinsame Nullstellen.*

Vorschau 6.10.3. Ist $k = \bar{k}$ algebraisch abgeschlossen und zählt man die gemeinsamen Nullstellen von f und g mit geeignet definierten Vielfachheiten und nimmt auch noch die „Nullstellen im Unendlichen“ mit dazu, so haben f und g in diesem verfeinerten Sinne sogar genau $(\operatorname{grad} f)(\operatorname{grad} g)$ gemeinsame Nullstellen. Mehr dazu können Sie in der algebraischen Geometrie **??** lernen.

Beispiel 6.10.4. Ist eines unserer Polynome von der Gestalt $a_n X^n + \ldots + a_1 X + a_0 - Y$ und seine Nullstellenmenge mithin der Graph des Polynoms $a_n X^n + \ldots + a_1 X + a_0$ in einer Veränderlichen, so kann man diese Schranke schnell einsehen: Man setzt einfach in das andere Polynom $Y = a_n X^n + \ldots + a_1 X + a_0$ ein und erhält ein Polynom in X, das eben nur höchstens so viele Nullstellen haben kann, wie sein Grad ist.

Beweis. Sicher reicht es, wenn wir unsere Schranke zeigen für geeignet transformierte Polynome $f \circ \varphi$, $g \circ \varphi$ mit $\varphi \in \mathrm{GL}(2;k)$ als da heißt $\varphi : k^2 \xrightarrow{\sim} k^2$ linear. Wir interessieren uns hier insbesondere für die Scherungen $\varphi_\lambda : k^2 \to k^2$, $(x,y) \mapsto (x + \lambda y, y)$ mit $\lambda \in k$. Gegeben $f \in k[X,Y]$ ein Polynom vom Totalgrad $\operatorname{grad} f = n$ enthält $f \circ \varphi_\lambda$ für alle $\lambda \in k$ mit höchstens endlich vielen Ausnahmen einen Term cY^n mit $c \neq 0$. Das ist formal leicht einzusehen und entspricht der anschaulichen Erkenntnis, daß „das Nullstellengebilde von f nur höchstens endlich viele Asymptoten besitzt“. Wir wissen nach 6.7.16 schon, daß



Zwei verschiedene Ellipsen schneiden sich in höchstens vier Punkten. In der Tat sind sie jeweils Nullstellenmengen von Polynomfunktionen vom Totalgrad Zwei, so daß wir das unmittelbar aus der Schranke von Bézout folgern können.

unsere beiden Polynome höchstens endlich viele gemeinsame Nullstellen haben können. Ist k unendlich, und jeder Körper k läßt sich notfalls in den unendlichen Körper $k(t)$ einbetten, so finden wir nun $\lambda \in k$ derart, daß unsere transformierten Polynome $f \circ \varphi_\lambda$ beziehungsweise $g \circ \varphi_\lambda$ beide Monome der Gestalt cY^n beziehungsweise dY^m mit $c \neq 0 \neq d$ enthalten, für $n = \operatorname{grad} f$, $m = \operatorname{grad} g$, und daß zusätzlich die gemeinsamen Nullstellen unserer transformierten Polynome paarweise verschiedene x-Koordinaten haben. Anschaulich gesprochen bedeutet das, daß wir die y-Achse so kippen, daß keine unserer Nullstellenmengen „einen in Richtung unserer gekippten y-Achse ins Unendliche gehenden Teil hat“ und daß jede Parallele zu unserer gekippten y-Achse höchstens eine gemeinsame Nullstelle unserer beiden Polynome trifft. Ohne Beschränkung der Allgemeinheit dürfen wir also annehmen, daß unsere Polynome f und g die Gestalt

$$\begin{aligned} f &= Y^n + a_1(X)Y^{n-1} + \ldots + a_n(X) \\ g &= Y^m + b_1(X)Y^{m-1} + \ldots + b_m(X) \end{aligned}$$

haben mit $a_i, b_j \in k[X]$, $\operatorname{grad} a_i \leq i$, $\operatorname{grad} b_j \leq j$, und daß darüber hinaus die gemeinsamen Nullstellen von f und g paarweise verschiedene x-Koordinaten haben. Die x-Koordinaten gemeinsamer Nullstellen sind aber genau die Nullstellen der im folgenden definierten „Resultante“ $\operatorname{Res}(f,g) \in k[X]$, und in 6.10.9 zeigen wir, daß diese Resultante als Polynom in X höchstens den Grad nm hat. Das beendet dann den Beweis. □

Satz 6.10.5 (über die Resultante). *Gegeben $m, n \geq 0$ gibt es genau ein Polynom $\operatorname{Res} = \operatorname{Res}_{n,m} \in \mathbb{Z}[' a_1, \ldots, a_n, b_1, \ldots, b_m]$ mit ganzzahligen Koeffizienten in $n+m$ Veränderlichen derart, daß unter der Substitution der a_i und b_j durch diejenigen Elemente von $\mathbb{Z}[' \zeta_1, \ldots, \zeta_n, \xi_1, \ldots, \xi_m]$, die erklärt sind durch die Gleichungen*

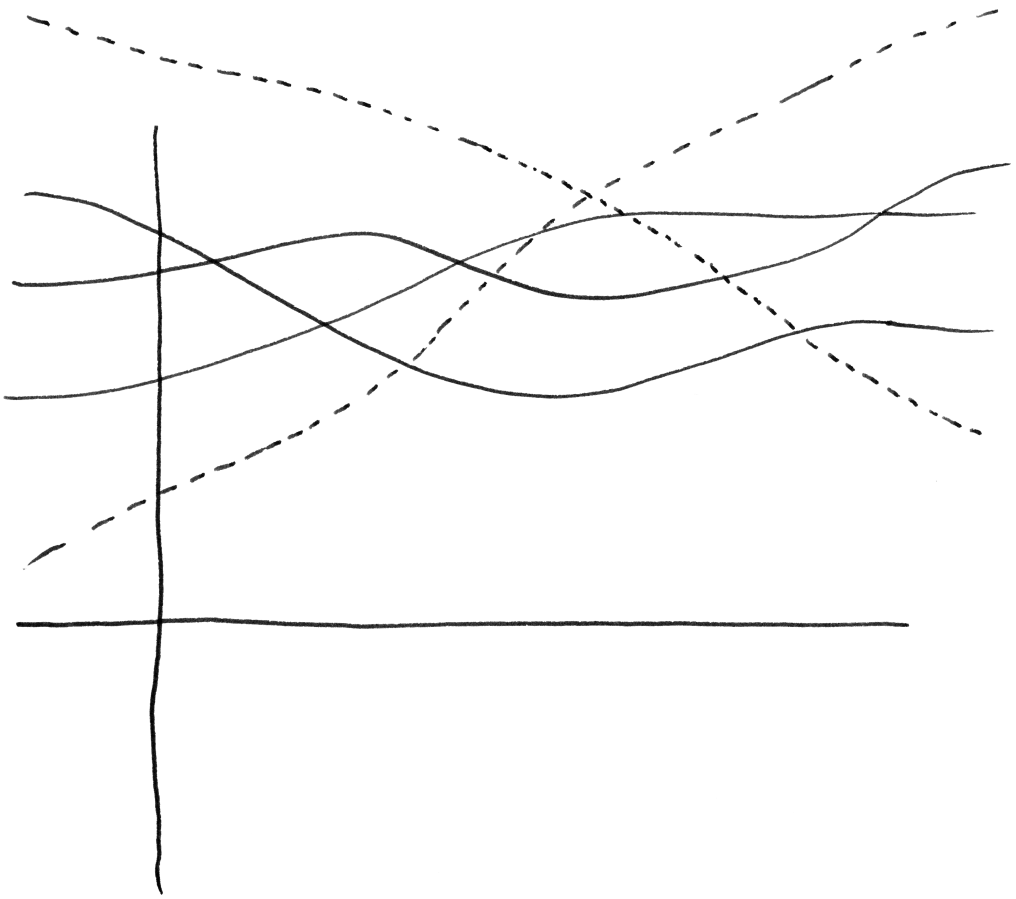
$$\begin{aligned} T^n + a_1T^{n-1} + \ldots + a_n &= (T+\zeta_1)\ldots(T+\zeta_n), \\ T^m + b_1T^{m-1} + \ldots + b_m &= (T+\xi_1)\ldots(T+\xi_m), \end{aligned}$$

im Polynomring in den ζ_i und ξ_j gilt

$$\operatorname{Res}(a_1, \ldots a_n, b_1, \ldots, b_m) = \prod_{i=1,j=1}^{n,m} (\zeta_i - \xi_j)$$

Definition 6.10.6. Gegeben normierte Polynome $f(T) = T^n + a_1T^{n-1} + \ldots + a_n$ und $g(T) = T^m + b_1T^{m-1} + \ldots + b_m$ mit Koeffizienten in einem Kring k benutzen wir die Abkürzung

$$\operatorname{Res}(a_1, \ldots, a_n, b_1, \ldots, b_m) = \operatorname{Res}(f,g)$$



Das Nullstellengebilde von $f = Y^3 + a_2(X)Y^2 + \ldots + a_0(X)$ als durchgezognene und von $g = Y^2 + b_1(X)Y + \ldots + b_0(X)$ als gestrichelte Linien. Über jedem Punkt der x-Achse liegen genau drei beziehungsweise zwei Lösungen von f beziehungsweise g.

und nennen dies Element von k die **Resultante von f und g**. Bei der Determinantenbeschreibung der Resultante erklären wir allgemeiner für jede zwei nicht notwendig normierte Polynome f, g der Grade $\leq n$ beziehungsweise $\leq m$ ihre Resultante $\mathrm{Res}_{n,m}(f,g)$.

6.10.7 (**Bedeutung der Resultante**). Ist $k = \bar{k}$ ein algebraisch abgeschlossener Körper, so verschwindet die Resultante von zwei normierten Polynomen mit Koeffizienten in k per definitionem genau dann, wenn die beiden Polynome eine gemeinsame Nullstelle haben. Im allgemeinen verschwindet die Resultante jedenfalls, wann immer die beiden Polynome eine gemeinsame Nullstelle haben.

Beispiel 6.10.8. Im Fall $m = n = 2$ folgt aus $T^2 + a_1T + a_2 = (T - \zeta_1)(T - \zeta_2)$ und $T^2 + b_1T + b_2 = (T - \xi_1)(T - \xi_2)$ unmittelbar

$$\begin{aligned} a_2 &= \zeta_1\zeta_2, \quad a_1 = \zeta_1 + \zeta_2, \\ b_2 &= \xi_1\xi_2, \quad b_1 = \xi_1 + \xi_2, \end{aligned}$$

Eine kurze Rechnung liefert dann

$$(\zeta_1 - \xi_1)(\zeta_2 - \xi_2)(\zeta_1 - \xi_2)(\zeta_2 - \xi_1) = (a_2 - b_2)^2 - (a_2 + b_2)a_1b_1 + a_2b_1^2 + b_2a_1^2$$

Der Ausdruck rechts in den Koeffizienten ist also die Resultante der Polynome $f(T) = T^2 + a_1T + a_2$ und $g(T) = T^2 + b_1T + b_2$. Zum Beispiel sehen wir, daß im Fall $a_1 = b_1$ unsere Polynome f und g in einem algebraisch abgeschlossenen Körper genau dann eine gemeinsame Nullstelle haben, wenn gilt $a_2 = b_2$. Das hätten wir natürlich auch so schon gewußt, aber es ist doch ganz beruhigend, unseren Argumenten mal in einem überschaubaren Spezialfall bei der Arbeit zugesehen zu haben.

Beweis. Das Polynom $\prod_{i=1,j=1}^{n,m}(\zeta_i - \xi_j) \in \mathbb{Z}[\zeta_1, \ldots, \zeta_n][\xi_1, \ldots, \xi_m]$ ist symmetrisch in den ξ_j und liegt nach 6.9.6 folglich in

$$\mathbb{Z}[\zeta_1, \ldots, \zeta_n][b_1, \ldots, b_m] = \mathbb{Z}[b_1, \ldots, b_m][\zeta_1, \ldots, \zeta_n]$$

Unser Polynom ist aber auch symmetrisch in den ζ_i, folglich liegt es wieder nach 6.9.6 sogar in $\mathbb{Z}[b_1, \ldots, b_m][a_1, \ldots, a_n]$. □

6.10.9 (**Grad der Resultante**). Wir zeigen nun noch die Behauptungen für den Grad der Resultante, die beim Beweis für die Schranke von Bézout benötigt wurden. Als Polynom in $\mathbb{Z}[\zeta_1, \ldots, \zeta_n, \xi_1, \ldots, \xi_m]$ ist die Resultante ja offensichtlich homogen vom Grad mn. Dahingegen sind die $a_i \in \mathbb{Z}[\zeta_1, \ldots, \zeta_n]$ homogen vom Grad i und die $b_j \in \mathbb{Z}[\xi_1, \ldots, \xi_m]$ homogen vom Grad j. Aus der algebraischen Unabhängigkeit der elementarsymmetrischen Polynome folgt, daß ein Monom

$a_1^{\lambda_1} \ldots a_n^{\lambda_n} b_1^{\mu_1} \ldots b_m^{\mu_m}$ nur dann mit von Null verschiedenem Koeffizienten in der Resultante auftauchen kann, wenn gilt

$$\lambda_1 + 2\lambda_2 + \ldots + n\lambda_n + \mu_1 + 2\mu_2 + \ldots + m\mu_m = nm$$

Setzen wir hier insbesondere für a_i gewisse $a_i(X) \in k[X]$ vom Grad $\leq i$ und für b_j gewisse $b_j(X) \in k[X]$ vom Grad $\leq j$ ein, so ist die Resultante ein Polynom in $k[X]$ vom Grad $\leq mn$.

Ergänzung 6.10.10 (**Die Resultante als Determinante**). Sei M die Matrix aus nebenstehendem Bild. Eine explizite Formel für die Resultante ist

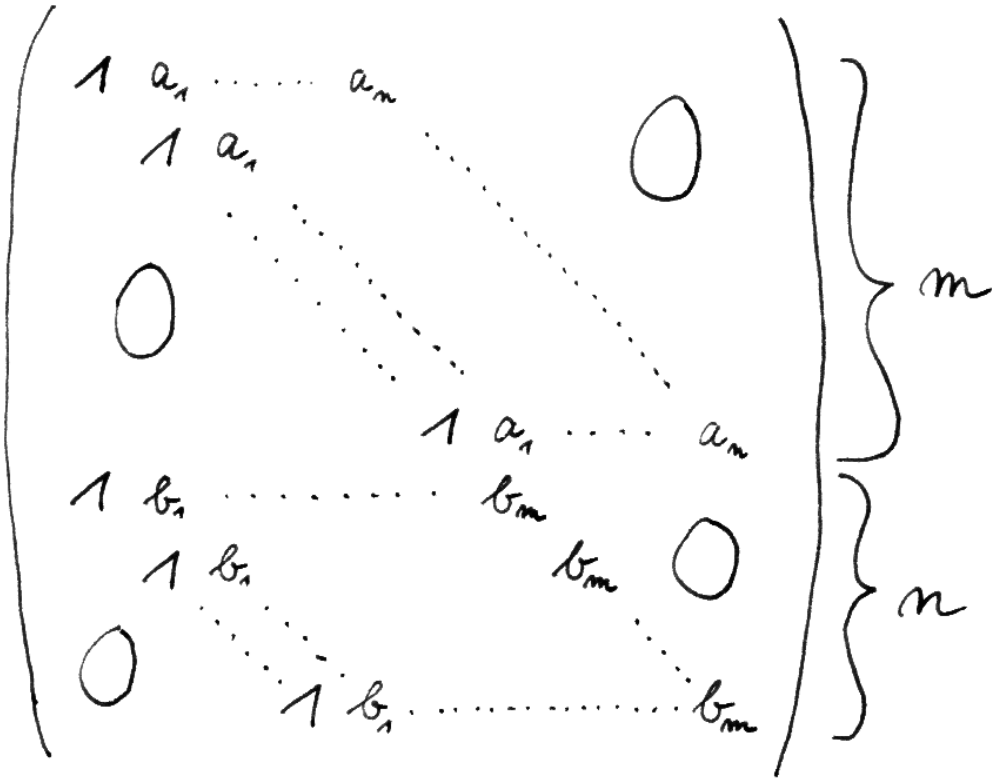
$$\mathrm{Res}(a_1, \ldots, a_n, b_1, \ldots, b_m) = \det M$$

Um das einzusehen, kann man wie folgt argumentieren: Gegeben zwei normierte nicht konstante Polynome $f, g \in k[T]$ mit Koeffizienten in einem Körper k sind ja gleichbedeutend:

(1) Unsere beiden Polynome sind teilerfremd in $k[T]$;

(2) Es gibt Polynome p, q mit $\deg p < \deg g$ und $\deg q < \deg f$, für die gilt $pf + qg = 1$.

In der Tat ist $(2) \Rightarrow (1)$ offensichtlich und $(1) \Rightarrow (2)$ folgt unmittelbar aus dem abstrakten chinesischen Restsatz 6.3.4, wenn wir etwa das Urbild kleinsten Grades von $(0, 1) \in k[T]/\langle f\rangle \times k[T]/\langle g\rangle$ in $k[T]$ aufsuchen. Insbesondere sehen wir so, daß p und q bereits eindeutig bestimmt sind, wenn es sie denn gibt. Nun können wir die Gleichung $pf + qg = 1$ als ein lineares Gleichungssystem für die Koeffizienten von p und q auffassen, und die Matrix dieses Systems ist dann genau die oben gegebene Matrix, wie der Leser leicht selbst einsehen wird. Genau dann ist also unser System eindeutig lösbar, wenn die Determinante der fraglichen Matrix nicht Null ist. Genau dann verschwindet also diese Determinante, wenn f und g nicht teilerfremd sind, und im Fall eines algebraisch abgeschlossenen Körpers k ist das gleichbedeutend dazu, daß f und g eine gemeinsame Nullstelle haben. Speziell erkennen wir so mit 2.4.5, daß das Polynom $\prod(\zeta_i - \xi_j)$ in $\mathbb{Q}[\zeta_i, \xi_j]$ unsere Determinante teilt, wenn wir sie zu den Polynomen aus 6.10.5 mit Koeffizienten in $\mathbb{Q}[\zeta_i, \xi_j]$ bilden. Wir erkennen sogar genauer, daß unsere Determinante bis auf eine von Null verschiedene Konstante ein Produkt von Faktoren $(\zeta_i - \xi_j)$ ist, wobei jeder Faktor mindestens einmal vorkommt. Daß hier keine Faktoren mehrfach auftreten und daß die besagte von Null verschiedene Konstante eine Eins ist, können wir unschwer prüfen, indem wir alle ζ_i Null setzen.



Die Matrix M, deren Determinante die Resultante liefert. Gegeben zwei nicht notwendig normierte Polynome vom Grad $\leq n$ und $\leq m$ der Gestalt $a_0T^n + a_1T^{n-1} + \ldots + a_n$ und $b_0T^m + b_1T^{m-1} + \ldots + b_m$ nehmen wir diese Determinante mit den Einsen ersetzt durch a_0 beziehungsweise b_0 von nun an als unsere Definition der Resultante $\mathrm{Res}_{n,m}$.

Übungen

Ergänzende Übung 6.10.11. Zwei beliebige homogene Polynome $f(X,Y) = a_0X^n+a_1X^{n-1}Y+\ldots+a_nY^n$ und $g(X,Y) = b_0X^m+b_1X^{m-1}Y+\ldots+b_mY^m$ mit Koeffizienten in einem algebraisch abgeschlossenen Körper k haben genau dann eine gemeinsame Nullstelle außerhalb des Ursprungs, wenn die Determinante derjenigen Variante der nebenstehenden Matrix verschwindet, die entsteht, wenn wir die erste Reihe von Einsen durch a_0 und die zweite Reihe von Einsen durch b_0 ersetzen. Diese Determinante heißt dann auch die **Sylvester-Determinante**.

7 Mehr zu Körpern

7.1 Grundlagen und Definitionen

Beispiele 7.1.1. Ein Körper ist nach 2.2.25 ein kommutativer von Null verschiedener Ring, in dem jedes Element ungleich Null eine Einheit ist. Aus den Grundvorlesungen bekannt sind die Körper $\mathbb{R}$ und $\mathbb{C}$ der reellen und komplexen Zahlen sowie der Körper $\mathbb{Q}$ der rationalen Zahlen. Allgemeiner haben wir in 2.5 zu jedem kommutativen Integritätsbereich R seinen Quotientenkörper $\operatorname{Quot} R$ konstruiert, zum Beispiel ist $\operatorname{Quot} \mathbb{Z} = \mathbb{Q}$ der Körper der rationalen Zahlen und $\operatorname{Quot} K[X] = K(X)$ der Funktionenkörper über einem gegebenen Körper K. Weiter ist nach 6.4.22 der Restklassenring R/pR von einem Hauptidealring nach dem von einem irreduziblen Element $p \in R$ erzeugten Ideal ein Körper. Insbesondere sind die Restklassenringe $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ für p eine Primzahl in $\mathbb{Z}$ Körper und ebenso die Quotienten $K[X]/\langle P\rangle$ des Polynomrings $K[X]$ über einem Körper K nach einem irreduziblen Polynom $P \in K[X]$.

Definition 7.1.2. Eine Teilmenge eines Körpers heißt ein **Unterkörper**, wenn sie so mit der Struktur eines Körpers versehen werden kann, daß die Einbettung ein Körperhomomorphismus ist. Gleichbedeutend ist die Forderung, daß unsere Teilmenge ein Teilring und mit der induzierten Ringstruktur ein Körper ist.

7.1.3. Sicher ist ein beliebiger Schnitt von Unterkörpern eines Körpers wieder ein Unterkörper. Ist K ein Körper und $T \subset K$ eine Teilmenge, so heißt der kleinste Unterkörper von K, der T enthält, der **von** T **erzeugte Unterkörper**. Den kleinsten Unterkörper von K, in anderen Worten den von der leeren Menge $T = \emptyset$ erzeugten Unterkörper, nennt man den **Primkörper von** K.

7.1.4. Für jeden Körper, ja jeden Ring K erinnern wir uns aus 2.2.30 an die Definition seiner **Charakteristik**, eines Elements $(\operatorname{char} K) \in \mathbb{N}$, durch die Identität

$$\ker(\mathbb{Z} \to K) = \mathbb{Z} \cdot (\operatorname{char} K)$$

Hier meint $\mathbb{Z} \to K$ den nach 2.1.10 eindeutig bestimmten Ringhomomorphismus von $\mathbb{Z}$ nach K.

7.1.5 (**Diskussion der Charakteristik**). Die Charakteristik ist also Null, wenn das neutrale Element der multiplikativen Gruppe $K^\times$ als Element der additiven Gruppe $(K, +)$ unendliche Ordnung hat, und ist sonst genau diese Ordnung. Gibt es demnach in noch anderen Worten eine natürliche Zahl $d > 0$ derart, daß in unserem Körper K gilt $1 + 1 + \ldots + 1 = 0$ (d Summanden), so ist das kleinstmögliche derartige $d > 0$ die Charakteristik $d = \operatorname{char} K$ von K, und gibt es kein derartiges d, so hat K die Charakteristik Null.

Lemma 7.1.6 (Kleinster Unterkörper eines Körpers). *Die Charakteristik eines Körpers ist entweder Null oder eine Primzahl und es gilt:*

$$\begin{array}{lcl} \operatorname{char} K = 0 & \Leftrightarrow & \textit{Der kleinste Unterkörper von } K \textit{ ist isomorph zu } \mathbb{Q};\\ \operatorname{char} K = p > 0 & \Leftrightarrow & \textit{Der kleinste Unterkörper von } K \textit{ ist isomorph zu } \mathbb{F}_p. \end{array}$$

Beweis. Sei $d = \operatorname{char} K$. Da wir eine Inklusion $\mathbb{Z}/d\mathbb{Z} \hookrightarrow K$ haben, muß $\mathbb{Z}/d\mathbb{Z}$ ein Integritätsring sein, also ist die Charakteristik eines Körpers nach 2.2.26 entweder null oder eine Primzahl. Im Fall $\operatorname{char} K = p > 0$ prim induziert $\mathbb{Z} \to K$ unter Verwendung der universellen Eigenschaft des Restklassenrings 6.1.13 oder spezieller 6.2.5 einen Isomorphismus von $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ auf einen Unterkörper von K. Im Fall $d = 0$ induziert $\mathbb{Z} \to K$ unter Verwendung der universellen Eigenschaft des Quotientenkörpers 2.5.5 einen Isomorphismus von $\mathbb{Q} = \operatorname{Quot} \mathbb{Z}$ auf einen Unterkörper von K. Man prüft leicht, daß die Bilder jeweils die kleinsten Unterkörper von K sind. □

7.2 Körpererweiterungen

Definition 7.2.1. Eine **Körpererweiterung** ist ein Paar $L \supset K$ bestehend aus einem Körper L mit einem Unterkörper K. So ein Paar $L \supset K$ nennt man dann auch eine **Körpererweiterung von** K. Man schreibt statt $L \supset K$ meist L/K und nennt K den **Grundkörper** und L den **Erweiterungskörper** oder **Oberkörper** der Körpererweiterung. Von einer **echten Körpererweiterung** fordern wir zusätzlich, daß der Erweiterungskörper nicht mit dem Grundkörper zusammenfällt.

Beispiele 7.2.2. Ein Grundbeispiel ist die Körpererweiterung $\mathbb{C} \supset \mathbb{R}$. Das Beispiel $\mathbb{C}(X) \supset \mathbb{C}(X^2)$ zeigt, daß es auch bei einer echten Körpererweiterung durchaus vorkommen kann, daß es einen Körperisomorphismus zwischen Grundkörper und Oberkörper gibt. In diesem Beispiel ist mit $\mathbb{C}(X^2)$ der Quotientenkörper des Rings der geraden Polynome $\mathbb{C}[X^2] \subset \mathbb{C}[X]$ gemeint.

Vorschau 7.2.3. In 7.8.7 werden wir unsere Definition abändern und eine Körpererweiterung als Synonym für einen Körperhomomorphismus erklären. Zum jetzigen Zeitpunkt führt dieser Standpunkt jedoch noch nicht zu mehr Klarheit, sondern vielmehr nur zu einer unnötig aufgeblähten Notation, unter der das Verständnis, so fürchte ich, mehr leidet als unter einer späteren Umwidmung des Begriffs einer Körpererweiterung.

Definition 7.2.4 (Erzeugung von Körpererweiterungen). Gegeben eine Körpererweiterung L/K und Elemente des Erweiterungskörpers $\alpha_1, \ldots, \alpha_n \in L$ bezeichnet man mit $K(\alpha_1, \ldots, \alpha_n) \subset L$ den von K und den α_i erzeugten Unterkörper von L. Er ist im allgemeinen verschieden von dem von K und den α_i erzeugten Teilring $K[\alpha_1, \ldots, \alpha_n] \subset L$. Eine Körpererweiterung L/K heiße

körperendlich, wenn der Erweiterungskörper über dem Grundkörper als Körper endlich erzeugt ist, wenn es also in Formeln endlich viele Elemente $\alpha_1, \ldots, \alpha_n \in L$ gibt mit

$$L = K(\alpha_1, \ldots, \alpha_n)$$

7.2.5 (**Diskussion der Notation**). Das Symbol $K(X)$ kann nun leider auf zweierlei Weisen interpretiert werden: Einerseits als der Quotientenkörper des Polynomrings $K[X]$ über K in einer Veränderlichen X, andererseits als der von K und einem weiteren Element X in einem größeren Körper L erzeugte Unterkörper. Wie viele Autoren benutzen wir nach Möglichkeit große Buchstaben vom Ende des Alphabets für die „algebraisch unabhängigen“ Variablen in einem Funktionenkörper, also im ersten Fall, und kleine Buchstaben für Elemente einer bereits gegebenen Körpererweiterung, also im zweiten Fall. Wollen wir die Freiheit unserer Veränderlichen besonders betonen, so setzen wir wie in 6.2.4 ein „Freiheitsstrichlein“ oben an die eröffnende Klammer und schreiben $K(\,'X)$ für den Funktionenkörper in einer Variablen X.

Ergänzung 7.2.6. Gegeben Körper $K \subset L$ und eine Teilmenge $T \subset L$ bezeichnen wir mit $K(T) \subset L$ auch den von K und T in L erzeugten Teilkörper und nennen ihn den **über** K **von** T **erzeugten Teilkörper von** L. Wenn wir besonders betonen wollen, daß hier T eine Teilmenge von L ist und nicht etwa ein Element von L, schreiben wir auch ausführlicher $K(\,!T)$. Gegeben Körper $K \subset L$ und eine Teilmenge $T \subset L$ kann der von K und T erzeugte Teilkörper $K(\,!T) \subset L$ von L beschrieben werden als die Vereinigung aller von endlichen Teilmengen von T über K erzeugten Teilköper, in Formeln

$$K(\,!T) = \bigcup_{\substack{n \geq 0 \\ \alpha_1, \ldots, \alpha_n \in T}} K(\alpha_1, \ldots, \alpha_n)$$

Beispiele 7.2.7. Wir haben $\mathbb{R}(\mathrm{i}) = \mathbb{R}[\mathrm{i}] = \mathbb{C}$ und $\mathbb{Q}[\sqrt{2}] = \mathbb{Q}(\sqrt{2})$, aber $K[\,'X] \neq K(\,'X)$, der Polynomring ist nämlich verschieden von seinem Quotientenkörper.

Übungen

Übung 7.2.8. Alle Elemente von $\mathbb{Q}(\sqrt{2})$ lassen sich eindeutig schreiben in der Form $a + b\sqrt{2}$ mit $a, b \in \mathbb{Q}$, vergleiche **??**. Man schreibe das Inverse von $7 + \sqrt{2}$ in dieser Form.

Übung 7.2.9. Man zeige $\sqrt{5} \notin \mathbb{Q}(\sqrt{2})$.

Übung 7.2.10. Gegeben $a, b \in \mathbb{Q}^\times$ zeige man, daß gilt $\mathbb{Q}(\sqrt{a}) \in \mathbb{Q}(\sqrt{b})$ genau dann, wenn a/b in $\mathbb{Q}$ ein Quadrat ist. Gegeben allgemeiner Körper $K \subset L$ einer von zwei verschiedenen Charakteristik und $\alpha, \beta \in L^\times$ mit $\alpha^2, \beta^2 \in K$ zeige man, daß gilt $K(\alpha) = K(\beta)$ genau dann, wenn $\alpha/\beta \in K$.

Übung 7.2.11. Sei L/K eine Körpererweiterung und seien $P, Q \in K[X]$ teilerfremd in $K[X]$. So haben P und Q auch in L keine gemeinsame Nullstelle. Hinweis: Unser Polynomring ist ein Hauptidealring. Nun verwende man ein Analogon des Satzes von Bezout. Weitergehende Aussagen in Richtung dieser Übung faßt Proposition 7.9.11 zusammen.

Ergänzung 7.2.12. Sehr viel allgemeiner kann man für paarweise verschiedene Primzahlen $p, q, \ldots w$ und beliebige $n, m, \ldots, r \geq 2$ zeigen, daß gilt

$$\sqrt[n]{p} \notin \mathbb{Q}(\sqrt[m]{q}, \ldots, \sqrt[r]{w})$$

Das und vieles weitere in dieser Richtung lernt man in der algebraischen Zahlentheorie, die auf dieser Vorlesung aufbaut. Den Fall $n = m = \ldots = r = 2$ behandeln wir in 8.1.34. Noch allgemeiner zeigt Besicovich [Bes40], daß gegeben paarweise verschiedene Primzahlen $p_1, \ldots, p_s$ und positive natürliche durch keine dieser Primzahlen teilbare Zahlen $a_1, \ldots, a_s$ und beliebige positive natürliche Zahlen $n_1, \ldots, n_s$ stets gilt

$$[\mathbb{Q}(\sqrt[n_1]{p_1 a_1}, \ldots, \sqrt[n_s]{p_s a_s}) : \mathbb{Q}] = n_1 \ldots n_s$$

Die Wurzeln sind hierbei stets als die positiven Wurzeln in $\mathbb{R}$ zu verstehen.

Übung 7.2.13. Seien K ein Körper und $P \in K[X] \backslash K$ ein nichtkonstantes Polynom. So ist der Ringhomomorphismus $K[Y] \to K[X]$ mit $Y \mapsto P$ injektiv und die davon induzierte Körpererweiterung $K(Y) \hookrightarrow K(X)$ hat als Grad den Grad von P.

7.3 Elemente von Körpererweiterungen

Definition 7.3.1. Sei L/K eine Körpererweiterung und $\alpha \in L$. Gibt es ein vom Nullpolynom verschiedenes Polynom $0 \neq Q \in K[X]$ mit $Q(\alpha) = 0$, so heißt α **algebraisch über** K. Sonst heißt α **transzendent über** K. Unter einer **algebraischen** beziehungsweise **transzendenten Zahl** versteht man eine komplexe Zahl, die algebraisch beziehungsweise transzendent ist über dem Körper der rationalen Zahlen. Ein berühmter Satz von Lindemann besagt, daß die Kreiszahl $\pi \in \mathbb{R}$ transzendent ist über dem Körper $\mathbb{Q}$ der rationalen Zahlen, vergleiche **??**.

7.3.2. Gegeben eine Körpererweiterung L/K und ein Element $\alpha \in L$ betrachten wir die Auswertungsabbildung

$$\begin{array}{ccc} K[X] & \to & L \\ Q & \mapsto & Q(\alpha) \end{array}$$

Ist α transzendent, so ist diese Abbildung injektiv und induziert nach der universellen Eigenschaft des Quotientenkörpers 2.5.5 einen Isomorphismus $K(X) = \operatorname{Quot} K[X] \xrightarrow{\sim} K(\alpha) \subset L$. Den anderen Fall klärt der folgende Satz.

Satz 7.3.3 (über das Minimalpolynom). *Seien L/K eine Körpererweiterung und $\alpha \in L$ algebraisch über K. So gilt:*

1. *Es gibt in $K[X]$ unter allen normierten Polynomen P mit $P(\alpha) = 0$ genau eines von minimalem Grad. Es heißt das* **Minimalpolynom** $P = \operatorname{Irr}(\alpha, K)$ **von** α **über** K*;*

2. *Dies Minimalpolynom ist K-irreduzibel und jedes Polynom $Q \in K[X]$ mit einer Nullstelle bei α ist ein Vielfaches des Minimalpolynoms von α;*

3. *Gegeben ein normiertes K-irreduzibles Polynom $Q \in K[X]$ mit einer Nullstelle bei α ist Q bereits das Minimalpolynom von α;*

4. *Das Auswerten bei α liefert einen Isomorphismus*

$$K[X]/\langle \operatorname{Irr}(\alpha, K)\rangle \xrightarrow{\sim} K(\alpha)$$

5. *Ist $d = \operatorname{grad}(\operatorname{Irr}(\alpha, K))$ der Grad des Minimalpolynoms von α über K, so bilden die Potenzen $1, \alpha, \alpha^2, \ldots, \alpha^{d-1}$ eine Basis des K-Vektorraums $K(\alpha)$.*

Beispiel 7.3.4. Wir betrachten die Körpererweiterung $\mathbb{C}/\mathbb{R}$. Das Element $\mathrm{i} \in \mathbb{C}$ ist algebraisch über $\mathbb{R}$ mit Minimalpolynom $\operatorname{Irr}(\mathrm{i}, \mathbb{R}) = X^2 + 1$. Wir haben $\mathbb{R}(\mathrm{i}) = \mathbb{C}$ und die Abbildung $\mathbb{R}[X] \to \mathbb{C}$ mit $X \mapsto \mathrm{i}$ definiert einen Ringisomorphismus $\mathbb{R}[X]/\langle X^2 + 1\rangle \xrightarrow{\sim} \mathbb{C}$. Die beiden Elemente $1 = \mathrm{i}^0$ und $\mathrm{i} = \mathrm{i}^1$ bilden eine Basis von $\mathbb{C}$ über $\mathbb{R}$.

Beweis. Da $K[X]$ nach 6.4.19 ein Hauptidealring ist und da das Auswerten $\varphi_\alpha : K[X] \to L$ mit $Q \mapsto Q(\alpha)$ keine Injektion ist, wir hatten ja α algebraisch über K angenommen, gibt es ein von Null verschiedenes und dann natürlich auch ein normiertes Polynom $P \in K[X]$ mit $\ker(\varphi_\alpha) = \langle P\rangle$. Alle anderen normierten Polynome aus $\langle P\rangle$ haben offensichtlich einen Grad, der echt größer ist als der Grad von P, und das zeigt bereits den ersten Teil des Satzes. Für unser P haben wir nach 6.2.5 weiter eine Einbettung $K[X]/\langle P\rangle \hookrightarrow L$, folglich ist $K[X]/\langle P\rangle$ ein Integritätsbereich. Nach 6.4.22 ist also P irreduzibel und $K[X]/\langle P\rangle$ sogar ein Körper. Dann induziert aber offensichtlich die Einbettung einen Isomorphismus $K[X]/\langle P\rangle \xrightarrow{\sim} K(\alpha)$. Nach 6.1.20 bilden für $d = \operatorname{grad} P$ die Bilder der Potenzen $1, X, X^2, \ldots, X^{d-1}$ eine Basis von $K[X]/\langle P\rangle$ über K, und damit bilden dann auch $1, \alpha, \alpha^2, \ldots, \alpha^{d-1}$ eine Basis von $K(\alpha)$ über K. □

7.3.5. Ich will die Irreduzibilität des Minimalpolynoms auch noch einmal ganz explizit begründen. Wäre das Minimalpolynom P ein Produkt $P = QR$ von Polynomen positiven Grades, so gälte $Q(\alpha) \neq 0 \neq R(\alpha)$ wegen der Minimalität des Minimalpolynoms, und das würde sofort zum Widerspruch $P(\alpha) \neq 0$ führen.

7.3.6. Sei L/K ein Körpererweiterung und $\alpha \in L$. Das Minimalpolynom von α über K ist im allgemeinen nur in $K[X]$ irreduzibel, in $L[X]$ spaltet es zumindest einen Faktor $(X - \alpha)$ ab und ist also reduzibel, es sei denn, wir sind im Fall $\alpha \in K$. Zum Beispiel ist $X^3 - 2$, da es ja $\mathbb{Q}$-irreduzibel ist, das Minimalpolynom von $\sqrt[3]{2}$ über $\mathbb{Q}$ und es gilt

$$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \mid a, b, c \in \mathbb{Q}\}$$

7.3.7. Ist eine Körpererweiterung als Körpererweiterung erzeugt von einem einzigen Element über dem Grundkörper, so nennt man sie eine **einfache** oder auch eine **primitive Körpererweiterung** des Grundkörpers und das fragliche Element heißt ein **primitives Element** der Körpererweiterung. In dieser Terminologie geben die vorhergehenden Überlegungen einen Überblick über die primitiven Erweiterungen eines gegebenen Körpers: Bis auf den Funktionenkörper sind das genau die Quotienten des Polynomrings nach irreduziblen Polynomen. Dabei können allerdings verschiedene normierte irreduzible Polynome durchaus zu „derselben“ primitiven Körpererweiterung führen – und was hier genau mit „derselben“ Körpererweiterung gemeint ist, wird im weiteren noch ausführlich diskutiert werden müssen.

Übungen

Übung 7.3.8. Alle Elemente von $\mathbb{Q}(\sqrt[3]{2})$ lassen sich eindeutig schreiben in der Form $a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2$ mit $a, b, c \in \mathbb{Q}$. Man schreibe das Inverse von $7 + \sqrt[3]{2}$ in dieser Form.

Übung 7.3.9. Gegeben eine Körpererweiterung L/K und ein Element $a \in L$, das algebraisch ist über K, zeige man, daß das Minimalpolynom $\operatorname{Irr}(a; K)$ bis auf ein Vorzeichen mit dem charakteristischen Polynom nach **??** des durch Multiplikation mit a gegebenen Endomorphismus des K-Vektorraums $K(a)$ zusammenfällt. Hinweis: Cayley-Hamilton.

Übung 7.3.10. Man bestimme das Minimalpolynom der komplexen Zahl $1 + \mathrm{i}$ über $\mathbb{R}$.

Ergänzende Übung 7.3.11. Zeigen Sie, daß das Minimalpolynom von $\sqrt[3]{2}$ über $\mathbb{Q}$ in $\mathbb{Q}(\sqrt[3]{2})$ nicht in Linearfaktoren zerfällt. Zeigen Sie, daß für jede Einheitswurzel ζ das Minimalpolynom von ζ über $\mathbb{Q}$ in $\mathbb{Q}(\zeta)$ in Linearfaktoren zerfällt. Zeigen Sie, daß für ζ eine nichttriviale dritte Einheitswurzel und $K = \mathbb{Q}(\zeta)$ das Minimalpolynom von $\sqrt[3]{2}$ über K in $K(\sqrt[3]{2})$ in Linearfaktoren zerfällt.

Ergänzende Übung 7.3.12. Sei $K \supset \mathbb{C}$ eine Körpererweiterung von $\mathbb{C}$. Gilt $K \neq \mathbb{C}$, so kann der $\mathbb{C}$-Vektorraum K nicht von einer abzählbaren Teilmenge erzeugt werden, d.h. K hat „überabzählbare Dimension“ über $\mathbb{C}$. Hinweis: $\mathbb{C}$ ist algebraisch abgeschlossen nach **??** und abzählbar viele gebrochen rationale Funktionen aus $\mathbb{C}(X)$ können nur abzählbar viele Polstellen haben.

Übung 7.3.13. Seien $R \supset K$ ein Kring mit einem Teilring, der sogar ein Körper ist. Genau ist $\alpha \in R$ Nullstelle eines von Null verschiedenen Polynoms $P \in K[X]$, wenn $K[\alpha]$ endlichdimensional ist als K-Vektorraum.

Übung 7.3.14. Seien $R \supset K$ ein Kring mit einem Teilring, der sogar ein Körper ist. Ist R endlichdimensional als K-Vektorraum und ein Integritätsring, so ist R auch selbst bereits ein Körper.

Übung 7.3.15. Sei K ein Körper und $K(X)$ der Funktionenkörper über K. So sind die Elemente von K die einzigen Elemente von $K(X)$, die algebraisch sind über K.

7.4 Endliche Körpererweiterungen

Definition 7.4.1. Gegeben eine Körpererweiterung L/K ist der Oberkörper L in natürlicher Weise ein Vektorraum über dem Unterkörper K. Die Dimension von L als K-Vektorraum notieren wir

$$[L : K] := \dim_K L \in \mathbb{N} \cup \{\infty\}$$

und nennen sie den **Grad der Körpererweiterung**. Eine Körpererweiterung von endlichem Grad heißt eine **endliche Körpererweiterung**.

7.4.2 (**Diskussion der Terminologie**). Jede endliche Körpererweiterung ist körperendlich im Sinne unserer Definition 7.2.4, aber das Umgekehrte gilt nicht. Wenn wir einmal Moduln über Ringen eingeführt haben, werden wir unsere endlichen Körpererweiterungen manchmal auch ausführlicher **modulendlich** nennen, um diesen Unterschied zu betonen.

7.4.3 (**Grad einer primitiven Körpererweiterung**). Ist L/K eine Körpererweiterung und $\alpha \in L$ algebraisch über K, so stimmt nach dem letzten Teil des Satzes 7.3.3 über das Minimalpolynom der Grad $[K(\alpha) : K]$ der von α erzeugten Körpererweiterung überein mit dem Grad $\operatorname{grad}(\operatorname{Irr}(\alpha, K))$ des Minimalpolynoms von α über K. Daher rührt wohl auch die Begriffsbildung des „Grades einer Körpererweiterung“. Wir vereinbaren für diese Zahl die abkürzende Bezeichnung

$$\operatorname{grad}_K(\alpha) := \operatorname{grad}(\operatorname{Irr}(\alpha, K)) = [K(\alpha) : K]$$

und nennen sie den **Grad von α über K**.

Ergänzung 7.4.4 (**Diskussion der Notation**). Man kann sich fragen, warum man für den Grad einer Körpereweiterung L/K zusätzlich zu $\dim_K L$ noch eine eigene Notation einführen sollte. Meine Antwort auf diese Frage wäre, daß in der Notation $\dim_K L$ der Körper K unten im Index steht und dadurch weniger wichtig erscheint und schlecht selbst mit Indizes versehen werden kann. Diese Notation

ist deshalb nur für das Arbeiten über einem festen Körper K praktisch. Im Zusammenhang der Körpertheorie aber sind alle auftretenden Körper gleichermaßen Hauptdarsteller, und in derartigen Situationen ist eine Notation wie $[L : K]$ geschickter.

Beispiele 7.4.5. Es gilt $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, $[\mathbb{C} : \mathbb{R}] = 2$, $[\mathbb{R} : \mathbb{Q}] = \infty$.

Beispiel 7.4.6. Jede endliche Körpererweiterung L/K eines algebraisch abgeschlossenen Körpers ist trivial, als da heißt, es gilt $L = K$. In der Tat muß das Minimalpolynom jedes Elements von L den Grad Eins haben. Eine andere Formulierung eines sehr ähnlichen Arguments war Übung **??**.

Proposition 7.4.7. *Sei L/K eine Körpererweiterung. Für $\alpha \in L$ sind gleichbedeutend:*

1. *α ist algebraisch über K;*
2. *$[K(\alpha) : K] < \infty$;*
3. *Es gibt einen Zwischenkörper $K \subset L' \subset L$ mit $[L' : K] < \infty$ und $\alpha \in L'$.*

Beweis. $1 \Rightarrow 2$ folgt unmittelbar aus 7.3.3. Die Implikation $2 \Rightarrow 3$ ist offensichtlich. Aber falls gilt $\dim_K L' < \infty$, können die Potenzen α^ν von α für $\nu = 0, 1, 2, \ldots$ nicht K-linear unabhängig sein, also $3 \Rightarrow 1$. □

Definition 7.4.8. Eine Körpererweiterung vom Grad 2 heißt eine **quadratische Körpererweiterung**.

Proposition 7.4.9 (Quadratische Körpererweiterungen). *Für eine Körpererweiterung L/K mit $\operatorname{char} K \neq 2$ sind gleichbedeutend:*

1. *L/K ist eine quadratische Körpererweiterung, in Formeln $[L : K] = 2$.*
2. *L entsteht aus K durch Adjunktion einer Quadratwurzel, in Formeln $L = K(\alpha)$ für ein $\alpha \in L \backslash K$ mit $\alpha^2 \in K$.*

Beweis. $2 \Rightarrow 1$ ist klar. Für die andere Richtung $1 \Rightarrow 2$ beachte man, daß jedes $\beta \in L \backslash K$ ja notwendig ein Minimalpolynom $P(X) = X^2 + aX + b$ vom Grad zwei hat. Schreiben wir das um zu $P(X) = (X + \frac{a}{2})^2 + (b - \frac{a^2}{4})$, so finden wir $(\beta + \frac{a}{2})^2 = \frac{a^2}{4} - b$ und das gesuchte α ist $\alpha = \beta + \frac{a}{2}$. □

Ergänzung 7.4.10. Wir werden in 7.7.1 sehen, daß auch der Körper $\mathbb{F}_2$ eine Erweiterung vom Grad 2 besitzt. Diese Erweiterung entsteht jedoch sicher nicht durch Adjunktion einer Quadratwurzel, da jedes Element von $\mathbb{F}_2$ seine eigene Quadratwurzel ist.

Satz 7.4.11 (Multiplikativität des Grades). *Für Körper $M \supset L \supset K$ gilt*

$$[M : K] = [M : L][L : K]$$

Beweis. Wir betrachten nur den endlichen Fall. Sei $m_1, \ldots, m_r$ eine Basis von M über L und $l_1, \ldots, l_s$ eine Basis von L über K. Wir behaupten, daß dann die Produkte $l_i m_j$ eine Basis von M über K bilden. Natürlich sind sie ein Erzeugendensystem. Gilt andererseits $\sum_{i,j} k_{ij} l_i m_j = 0$ mit $k_{ij} \in K$, so folgt zunächst $\sum_i k_{ij} l_i = 0$ für alle j aufgrund der linearen Unabhängigkeit der m_j über L und dann $k_{ij} = 0$ für alle i, j aufgrund der linearen Unabhängigkeit der l_i über K. □

Korollar 7.4.12 (Grade von Elementen in Körpererweiterungen). *Gegeben eine endliche Körpererweiterung ist jedes Element des Oberkörpers algebraisch über dem Unterkörper und sein Grad über dem Unterkörper teilt den Grad unserer Körpererweiterung.*

Beweis. Sei L/K unsere Körpererweiterung und $\alpha \in L$ unser Element. Die Kette $L \supset K(\alpha) \supset K$ zeigt $[L : K] = [L : K(\alpha)][K(\alpha) : K]$. □

Beispiel 7.4.13. Es gilt $\sqrt{2} \notin \mathbb{Q}(\sqrt[3]{2})$. In der Tat sind nach 6.4.29 die Polynome $X^2 - 2$ und $X^3 - 2$ irreduzibel in $\mathbb{Q}[X]$, nach 7.3.6 sind sie also bereits die Minimalpolynome von $\sqrt{2}$ beziehungsweise $\sqrt[3]{2}$, und folglich hat $\sqrt{2}$ den Grad 2 über $\mathbb{Q}$ und $\sqrt[3]{2}$ den Grad 3.

Korollar 7.4.14. *Seien L/K eine Körpererweiterung und $\alpha_1, \ldots, \alpha_n \in L$ algebraisch über K. So ist $K(\alpha_1, \ldots, \alpha_n)$ endlich über K und insbesondere sind alle Elemente dieser Körpererweiterung auch algebraisch über K.*

Beweis. Im Körperturm $K \subset K(\alpha_1) \subset K(\alpha_1, \alpha_2) \subset \ldots \subset K(\alpha_1, \ldots, \alpha_n)$ sind alle Schritte endliche Körpererweiterungen. Nach 7.4.11 ist also auch die ganze Erweiterung endlich. □

Übungen

Ergänzende Übung 7.4.15. Ist $\sqrt{2} + \sqrt{3}$ algebraisch über $\mathbb{Q}$? Wenn ja, was ist sein Minimalpolynom über $\mathbb{Q}$? Liegt $\sqrt{2}$ in $\mathbb{Q}(\sqrt{2} + \sqrt{3})$?

Ergänzende Übung 7.4.16. Sei K ein Körper und seien $P, Q \in K[X]$ irreduzibel mit $\operatorname{grad} P$ und $\operatorname{grad} Q$ teilerfremd. Sei $L = K(\alpha)$ eine Körpererweiterung von K, wobei $\alpha \in L$ eine Nullstelle von P ist. Dann ist Q auch irreduzibel in $L[X]$. Hinweis: Wäre sonst β Nullstelle eines irreduziblen Faktors von Q in $L[X]$, so hätte $K(\alpha, \beta)$ zu kleinen Grad über K, denn es umfaßt $K(\alpha)$ und $K(\beta)$.

Übung 7.4.17. Die durch den Funktionenkörper $K(X)$ über einem vorgegebenen Körper K gegebene Körpererweiterung $K(X)/K$ ist stets körperendlich, aber nie endlich.

Übung 7.4.18. Man zeige für jede Körpererweiterung L/K, daß ihr Grad übereinstimmt mit dem Grad der auf den Funktionenkörpern induzierten Erweiterung, in Formeln $[L : K] = [L(X) : K(X)]$. Hinweis: Man ziehe sich auf den Fall primitiver Erweiterungen zurück und verwende 6.7.21 und 7.3.15.

7.5 Notationen für Erzeugung**

7.5.1. Im folgenden sollen die folgenden Konventionen befolgt werden:

$|\ \rangle$ Unsymmetrische Klammern verwenden wir, um **Erzeugung als Monoid** anzudeuten, manchmal in der Form $|\ ;\top\rangle$ im Fall der Verknüpfung $\top$;

$\langle\ \rangle$ Spitze Klammern verwenden wir, um **Erzeugung als Modul** oder **Erzeugung als Gruppe** anzudeuten, manchmal in der Form $\langle\ \rangle_k$ im Fall von Moduln über einem Ring k;

$[\ ]$ Eckige Klammern verwenden wir, um **Erzeugung als Kring** anzudeuten, allgemeiner auch Erzeugung als Ring über einem nicht notwendig kommutativen Ring, aber mit paarweise kommutierenden Erzeugern;

$\lfloor\ \rfloor$ Oben offene eckige Klammern verwenden wir, um **Erzeugung als Ring** anzudeuten, insbesondere im Fall von nicht kommutierenden Erzeugern;

$(\ )$ Runde Klammern verwenden wir, um **Erzeugung als Körper** anzudeuten;

$|_!\ \rangle, \langle_!\ \rangle, [_!\ ], \lfloor_!\ \rfloor, (_!\ )$ Steht zwischen den Klammern nur ein Symbol und meint dies Symbol eine Menge von Erzeugern und nicht einen einzigen Erzeuger, so kann das aber muß nicht durch ein Ausrufezeichen unten an der eröffnenden Klammer angezeigt werden, den **Mengenanzeiger**;

$|'\ \rangle, \langle'\ \rangle, ['\ ], \lfloor'\ \rfloor$ Freies Erzeugen als Monoid oder Modul oder Kring oder Kringerweiterung kann aber muß nicht durch ein kleines **Freiheitsstrichlein** oben an der eröffnenden Klammer angezeigt werden;

$('\ )$ Im Fall einer Körpererweiterung meint das **Freiheitsstrichlein**, daß zwischen den Klammer algebraisch unabhängige Erzeuger stehen.

Beispiele 7.5.2. Wir schreiben $k['x_1, \ldots, x_n] = k[x_1, \ldots, x_n]$ für Polynomring über k in den Variablen $x_1, \ldots, x_n$. Der freie k-Vektorraum über einer Menge X aus **??** kann bezeichnet werden mit $k\langle'_!X\rangle = k\langle X\rangle = kX$. Ist ein k-Vektorraum M bereits gegeben und $X \subset M$ eine Teilmenge, so schreiben wir $\langle_!X\rangle_k = \langle X\rangle_k = \langle kX\rangle \subset M$ für den von X erzeugten Untervektorraum. Wir kürzen $\langle\{x_1, \ldots, x_n\}\rangle_k = \langle x_1, \ldots, x_n\rangle_k = k\langle x_1, \ldots, x_n\rangle$ ab und lassen k ganz

weg, wenn wir hoffen, daß es aus dem Kontext hervorgeht oder wenn die Erzeugung als Untergruppe gemeint ist. Allerdings setzen wir nur dann ein Freiheitsstrichlein, wenn die Erzeuger linear unabhängig sind. Sind weiter $R \supset k$ ein Kring mit einem Teilring und sind $x_1, \ldots, x_n$ Elemente von R, so notieren wir $k[x_1, \ldots, x_n] \subset R$ den von den x_i über k in R erzeugten Teilring und erlauben uns das Freiheitsstrichlein nur, wenn die Erzeuger über k algebraisch unabhängig sind.

7.6 Konstruktionen mit Zirkel und Lineal

Definition 7.6.1. Sei $E \subset \mathbb{C}$ eine Teilmenge der komplexen Zahlenebene.

1. Eine reelle affine Gerade durch zwei verschiedene Punkte von E heißt eine „aus E elementar konstruierbare Gerade“;

2. Ein Kreis durch einen Punkt von E mit Mittelpunkt in einem anderen Punkt von E heißt ein „aus E elementar konstruierbarer Kreis“ ;

3. Alle aus E elementar konstruierbaren Geraden und Kreise fassen wir zusammen unter dem Oberbegriff der „aus E elementar konstruierbaren Figuren“;

4. Ein Punkt $z \in \mathbb{C}$ heißt **elementar konstruierbar aus** E, wenn er im Schnitt von zwei verschiedenen aus E elementar konstruierbaren Figuren liegt.

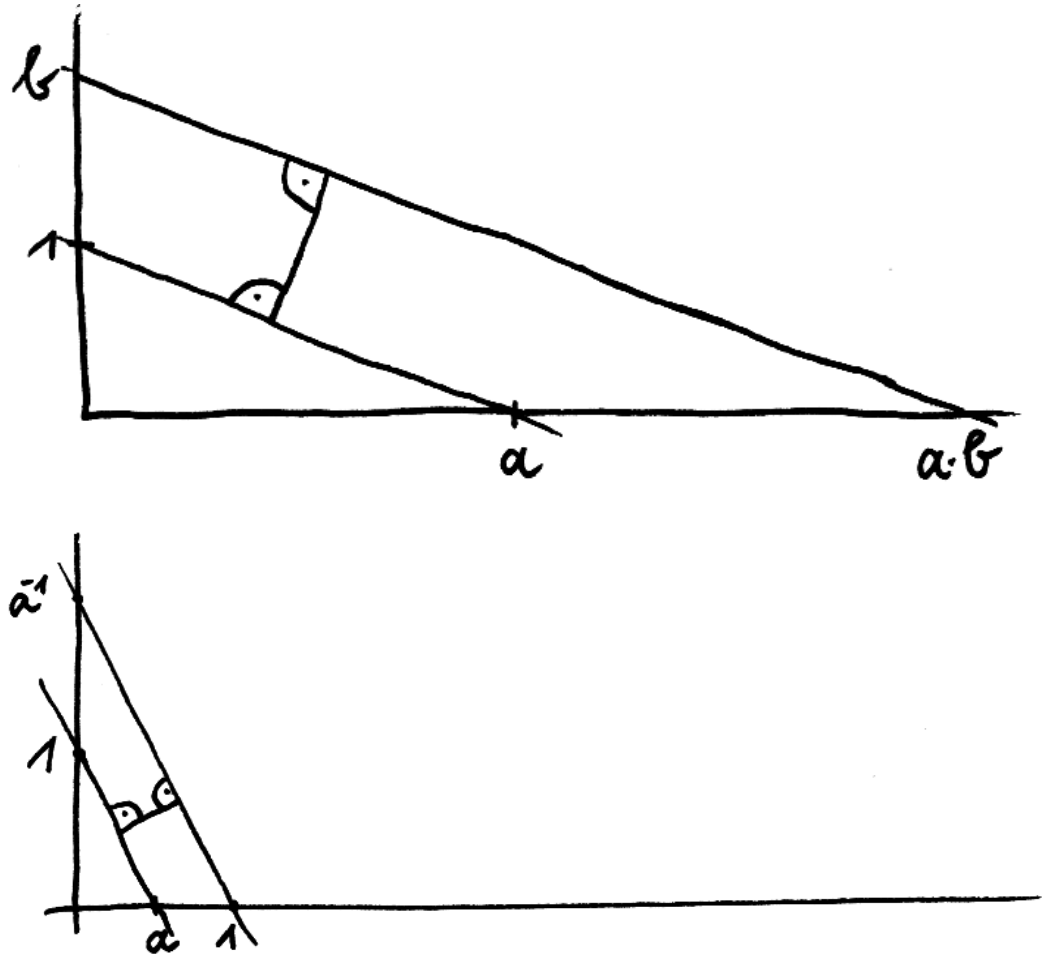
Satz 7.6.2 (**Konstruierbarkeit und quadratische Erweiterungen**)**.** *Die folgenden beiden Teilmengen K und Q von $\mathbb{C}$ stimmen überein:*

1. *Die kleinste Teilmenge $K \subset \mathbb{C}$, die 0 und 1 enthält und stabil ist unter elementaren Konstruktionen, also die Eigenschaft hat, daß jede aus K elementar konstruierbare komplexe Zahl wieder in K liegt. Wir nennen die Elemente von K die* **konstruierbaren Zahlen***;*

2. *Die kleinste Teilmenge $Q \subset \mathbb{C}$, die sowohl ein Teilkörper ist als auch stabil unter dem Bilden von Quadratwurzeln.*

7.6.3. Als allererstes und eigentlich noch vor der Formulierung des Satzes sollten wir uns hier überlegen, daß es solche kleinsten Teilmengen überhaupt gibt. Das ist aber klar: Wir können jeweils einfach den Schnitt aller Teilmengen mit besagter Eigenschaft nehmen, und der hat offensichtlich wieder besagte Eigenschaft.

Beweis. Wir beginnen mit der Inklusion $Q \subset K$. Dazu reicht es zu zeigen, daß die Menge $K \subset \mathbb{C}$ der konstruierbaren Zahlen ein Teilkörper ist und stabil unter



Zur Konstruktion von Produkten und Inversen reeller Zahlen mit Zirkel und Lineal

dem Bilden von Quadratwurzeln. Offensichtlich ist K stabil unter Addition. Um die Stabilität unter Multiplikation und Inversenbildung zu zeigen beachten wir, daß für $a \in \mathbb{C}^\times$ offensichtlich gleichbedeutend sind:

1. a liegt in K;
2. $|a|$ und $\frac{a}{|a|}$ liegen in K;
3. $\mathrm{Re}(a)$ und $\mathrm{Im}(a)$ liegen in K.

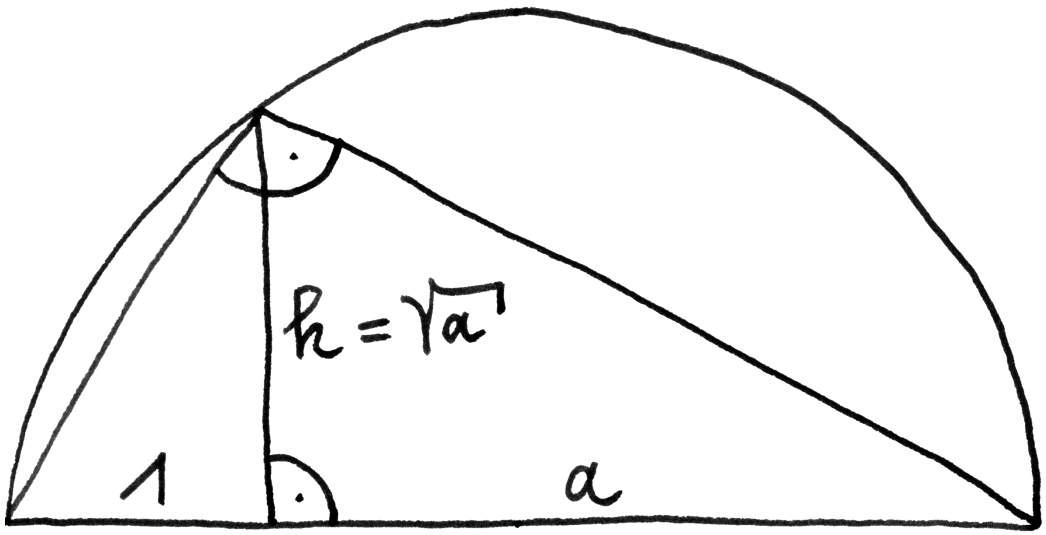
Nun ist es unproblematisch, Punkte auf dem Einheitskreis mithilfe von Zirkel und Lineal zu invertieren und zu multiplizieren. Daß das auch für reelle Zahlen möglich ist, zeigen die nebenstehenden Abbildungen. Also ist K ein Teilkörper von $\mathbb{C}$. Nun zeigen wir, daß er stabil ist unter dem Bilden von Quadratwurzeln. In der Tat ist klar, wie wir die Wurzeln von Punkten auf dem Einheitskreis mit Zirkel und Lineal bestimmen können, und daß das Wurzelziehen mit Zirkel und Lineal aus einer positiven reellen Zahl möglich ist, zeigt das nebenstehende Bild, in dem ja gilt $(h^2 + a^2) + (h^2 + 1^2) = (a + 1)^2$, also $h^2 = a$. Also ist $K \subset \mathbb{C}$ ein Teilkörper, der stabil ist unter dem Bilden von Quadratwurzeln, und wir haben $Q \subset K$ gezeigt. Wir zeigen nun umgekehrt $K \subset Q$. Dafür müssen wir nur zeigen, daß Q stabil ist unter elementaren Konstruktionen. Sicher ist Q stabil unter der komplexen Konjugation, denn mit Q ist auch $Q \cap \bar{Q}$ ein unter dem Bilden von Quadratwurzeln stabiler Unterkörper von $\mathbb{C}$. Eine komplexe Zahl z gehört folglich zu Q genau dann, wenn ihr Real- und Imaginärteil zu Q gehören. Mit $z = x + \mathrm{i}y$ werden unsere aus Q elementar konstruierbaren Figuren nun aber beschrieben durch Gleichungen der Gestalt

$$\begin{aligned} (x-a)^2 + (y-b)^2 &= c \\ ax + by &= c \end{aligned}$$

für geeignete $a, b, c \in Q \cap \mathbb{R}$, und simultane Lösungen zweier verschiedener derartiger Gleichungen sind in der Tat Lösungen von linearen oder quadratischen Gleichungen mit Koeffizienten aus Q, ja sogar aus $Q \cap \mathbb{R}$. Im kompliziertesten Fall des Schnitts zweier Kreise bildet man hierzu zunächst die Differenz beider Gleichungen und erhält so eine lineare Gleichung in x und y, die man anschließend nach einer Variable auflöst und in eine der Kreisgleichungen einsetzt. Das zeigt, daß $Q \subset \mathbb{C}$ stabil ist unter elementaren Konstruktionen. Da auch 0 und 1 zu Q gehören, folgt $K \subset Q$. □

Korollar 7.6.4 (**Eine notwendige Bedingung für Konstruierbarkeit**). *Jede konstruierbare Zahl ist algebraisch und ihr Grad über $\mathbb{Q}$ ist eine Zweierpotenz.*

Vorschau 7.6.5. Das Umgekehrte gilt nicht. Es gibt durchaus algebraische komplexe Zahlen, deren Grad über $\mathbb{Q}$ eine Zweierpotenz ist, die aber keineswegs



Zur Konstruktion der Wurzel aus einer positiven reellen Zahl mit Zirkel und Lineal

konstruierbar sind. Ein hinreichendes und notwendiges Kriterium können Sie in 8.4.15 kennenlernen: Eine algebraische komplexe Zahl ist konstruierbar genau dann, wenn der Grad des Zerfällungskörpers ihres Minimalpolynoms als Körpererweiterung von $\mathbb{Q}$ eine Zweierpotenz ist.

Beweis. Es scheint mir offensichtlich, daß Q auch beschrieben werden kann als die Vereinigung aller Teilkörper von $\mathbb{C}$ der Gestalt $\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_r)$ für Folgen $\alpha_1, \alpha_2, \ldots, \alpha_r$ komplexer Zahlen mit der Eigenschaft $\alpha_i^2 \in \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_{i-1})$ für alle i. In der Tat ist die Vereinigung aller derartigen Teilkörper offensichtlich selbst ein Teilkörper von $\mathbb{C}$ und damit sicher der Kleinste unter dem Ziehen von Quadratwurzeln stabile Teilkörper von $\mathbb{C}$. Sei nun z unsere konstruierbare Zahl. Nach dem Satz gibt es eine Kette von Körpererweiterungen

$$\mathbb{Q} = K_0 \subset K_1 \subset \ldots \subset K_r$$

mit $[K_i : K_{i-1}] = 2$ und $z \in K_r$. Es folgt $[K_r : \mathbb{Q}] = 2^r$ und der Grad von z über $\mathbb{Q}$ ist nach 7.4.12 ein Teiler von $[K_r : \mathbb{Q}]$. □

Korollar 7.6.6 (Klassische unlösbare Konstruktionsaufgaben).

1. *Das regelmäßige Siebeneck ist nicht konstruierbar mit Zirkel und Lineal;*
2. *Die Seitenlänge eines Würfels mit Volumen Zwei ist nicht konstruierbar mit Zirkel und Lineal;*
3. *Es gibt keine Konstruktion mit Zirkel und Lineal, die es erlaubt, einen beliebig vorgegebenen Winkel zu dritteln.*

Ergänzung 7.6.7. Wir werden in 8.4.7 allgemeiner zeigen, daß sich für $n \geq 3$ das regelmäßige n-Eck mit Zirkel und Lineal konstruieren läßt genau dann, wenn die Anzahl $\varphi(n) = |\{a \mid 1 \leq a \leq n,\ \langle a, n\rangle = 1\}|$ der zu n teilerfremden Zahlen unter n eine Zweierpotenz ist. Zum Beispiel ist das regelmäßige Dreieck konstruierbar, aber nicht das regelmäßige Neuneck. Das heißt, daß der Winkel $2\pi/3$ nicht mit Zirkel und Lineal gedrittelt werden kann. Hier geben wir für diese beiden Aussagen schon mal direkte Argumente.

Ergänzung 7.6.8. Die Griechen scheinen in der hellenistischen Hochkultur Konstruktionen mit Zirkel und Lineal auf Papyrus in derselben Weise eingesetzt zu haben, wie bei uns bis etwa 1960 Rechenschieber, dann Taschenrechner, und mittlerweile Laptops eingesetzt wurden und werden: Als unverzichtbare Hilfsmittel des Ingenieurs. Das Ziehen von Kubikwurzeln etwa war wichtig, um gemäß der Formel eines gewissen Philon die Dicke des Spannseils einer Wurfmaschine so zu berechnen, daß sie ein vorgegebenes Gewicht über eine vorgegebene Entfernung schleuderte. Mehr dazu findet man in [Rus05] in Abschnitt 2.3 und zu Ende des Abschnitts 4.3.

Ergänzung 7.6.9. Die Frage der **Würfelverdopplung**, also die Frage, mit Zirkel und Lineal aus einer gegebenen Strecke eine weitere Strecke zu konstruieren derart, daß das Längenverhältnis der beiden Strecken gerade $\sqrt[3]{2}$ ist, heißt das **Deli'sche Problem**. Diese Bezeichnung geht auf eine Geschichte zurück, nach der das Orakel in Delphi den Deliern aufgab, zur Abwehr einer Pest den würfelförmigen Altar ihres Tempels zu verdoppeln.

Beweis. 1. Nach der Bestimmung des siebten Kreisteilungspolynoms in 6.8.4 und der Gleichheit 7.3.6 vom Grad einer primitiven Körpererweiterung und dem Grad des Minimalpolynoms eines jeden Erzeugers hat $\exp(2\pi\mathrm{i}/7)$ den Grad 6 über $\mathbb{Q}$ und ist nach 7.6.4 also nicht konstruierbar.

2. Nach 7.3.6 hat die gesuchte Länge $\sqrt[3]{2}$ als algebraische Zahl den Grad 3 über $\mathbb{Q}$ und ist nach 7.6.4 also nicht konstruierbar.

3. Sicher gilt $\exp(2\pi\mathrm{i}/3) \in K$. Es reicht, $\exp(2\pi\mathrm{i}/9) \notin K$ zu zeigen. Sicher ist $\exp(2\pi\mathrm{i}/9) = \zeta$ eine Nullstelle des Polynoms $X^9 - 1$. Natürlich zerfällt dieses Polynom in

$$X^9 - 1 = (X^3 - 1)(X^6 + X^3 + 1)$$

und ζ ist Nullstelle des zweiten Faktors, unseres neunten Kreisteilungspolynom aus 6.8.6. Es reicht zu zeigen, daß dieses Polynom irreduzibel ist über $\mathbb{Q}$, denn dann hat ζ den Grad 6 über $\mathbb{Q}$ und kann nach 7.6.4 nicht konstruierbar sein. In 8.4.2 werden wir zeigen, daß alle Kreisteilungspolynome irreduzibel sind. Hier basteln wir nur ein schnelles Argument für unseren speziellen Fall zusammen, vergleiche auch 6.8.7. In $\mathbb{F}_3[X]$ gilt sicher $(X^9 - 1) = (X - 1)^9$ und $(X^3 - 1) = (X-1)^3$ und folglich $X^6+X^3+1 = (X-1)^6$. Substituieren wir in X^6+X^3+1 nun $X = Y+1$, so erhalten wir in $\mathbb{F}_3[Y]$ also das Polynom Y^6. Gehen wir wieder über zu $\mathbb{Q}[Y]$, so hat $(Y+1)^6 + (Y+1)^3 + 1$ den konstanten Term 3. Damit können wir aus dem Eisenstein-Kriterium 6.8.2 folgern, daß unser Polynom irreduzibel ist. □

Satz 7.6.10 (**Konstruierbarkeit, Variante**). *Gegeben eine Teilmenge $A \subset \mathbb{C}$ stimmen die folgenden beiden Teilmengen K_A und Q_A von $\mathbb{C}$ überein:*

1. *Die kleinste Teilmenge $K_A \subset \mathbb{C}$, die 0 und 1 enthält und A umfaßt und stabil ist unter elementaren Konstruktionen;*
2. *Der kleinste Teilkörper $Q_A \subset \mathbb{C}$, der A und $\bar{A}$ umfaßt und stabil ist unter dem Bilden von Quadratwurzeln.*

7.6.11. Gegeben eine Teilmenge $A \subset \mathbb{C}$ nennen wir die Elemente der Menge K_A aus 7.6.10 die **aus A konstruierbaren Zahlen**. Der Beweis unserer Variante ist vollständig analog zum Beweis von 7.6.2 und bleibe dem Leser überlassen. Durch

Anwendung auf die einelementige Menge $A = \{a\}$ und Beachtung der Formel $a\bar{a} = 1$ für Punkte auf dem Einheitskreis erkennt man daraus, daß ein Winkel genau dann mit Zirkel und Lineal gedrittelt werden kann, wenn für den zugehörigen Punkt a auf dem Einheitskreis das Polynom $X^3 - a$ über $\mathbb{Q}(a)$ nicht irreduzibel ist alias eine Nullstelle hat. Zum Beispiel lassen sich $360°$ und $180°$ mit Zirkel und Lineal dritteln, denn $X^3 - 1$ und $X^3 + 1$ haben rationale Nullstellen. Ebenso läßt sich $135° = 3 \times 45°$ mit Zirkel und Lineal dritteln, denn für die primitive achte Einheitswurzel $a = (\mathrm{i} - 1)/\sqrt{2}$ ist a^3 eine Nullstelle von $X^3 - a$. Andererseits läßt sich ein durch einen tranzendenten Punkt a auf dem Einheitskreis gegebener Winkel nie mit Zirkel und Lineal dritteln, denn im Funktionenkörper $\mathbb{Q}(X) \cong \mathbb{Q}(a)$ besitzt die Variable X offensichtlich keine dritte Wurzel.

7.7 Endliche Körper

Satz 7.7.1 (Klassifikation endlicher Körper). *Die Kardinalität eines endlichen Körpers ist stets eine echte Primzahlpotenz, und zu jeder echten Primzahlpotenz gibt es bis auf nichteindeutigen Isomorphismus genau einen endlichen Körper mit dieser Kardinalität.*

7.7.2. Gegeben eine echte Primzahlpotenz q notiert man „den“ Körper mit q Elementen meist $\mathbb{F}_q$. Ich weiß nicht, ob $\mathbb{F}$ in diesem Zusammenhang für „finite“ oder für „field“, die englische Bezeichnung für Körper, steht.

Vorschau 7.7.3. Man kann zeigen, daß jeder endliche Schiefkörper schon ein Körper ist, siehe zum Beispiel [Wei74], I, §1.

Beweis. Ein endlicher Körper $\mathbb{F}$ hat notwendig eine positive Charakteristik $p = \operatorname{char}\mathbb{F} > 0$. Nach 7.1.6 ist diese Charakteristik p eine Primzahl und wir haben eine Einbettung $\mathbb{F}_p \hookrightarrow \mathbb{F}$. Damit wird $\mathbb{F}$ ein endlichdimensionaler $\mathbb{F}_p$-Vektorraum. Für $r = \dim_{\mathbb{F}_p}\mathbb{F} = [\mathbb{F} : \mathbb{F}_p]$ gilt dann offensichtlich $|\mathbb{F}| = p^r$. Das zeigt, daß die Kardinalität eines endlichen Körpers stets eine Primzahlpotenz ist. Unser Satz behauptet darüber hinaus, daß die Kardinalität eine Bijektion

$$\{\text{endliche Körper}\}_{/\cong} \quad \tilde{\to} \quad \{\text{echte Primzahlpotenzen}\}$$

liefert. Wir unterbrechen nun den Beweis durch einen Satz und zwei Lemmata, um die nötigen Hilfsmittel bereitzustellen. □

Satz 7.7.4 (Zerfällung von Polynomen in Körpererweiterungen). *Gegeben ein Körper K und ein von Null verschiedenes Polynom $P \in K[X]$ gibt es eine endliche Körpererweiterung L von K derart, daß P als Element von $L[X]$ in Linearfaktoren zerfällt.*

Beweis. Das folgt mit Induktion aus dem anschließenden Lemma 7.7.6, wenn wir beachten, daß nach 2.2.43 jeder Körperhomomorphismus injektiv ist. □

Vorschau 7.7.5. Natürlich folgt obiger Satz auch unmittelbar aus der Existenz eines algebraischen Abschlusses 7.11.5. Diese Argumentation ist jedoch zumindest im Rahmen der hier gegebenen Darstellung unzulässig, da unser Satz selbst einen wesentlichen Baustein beim Beweis der Existenz algebraischer Abschlüsse darstellt. Zumindest um das folgende Lemma kommt meines Wissens kein Beweis für die Existenz algebraischer Abschlüsse herum.

Lemma 7.7.6 (Adjunktion von Nullstellen). *Seien ein Körper K und ein nichtkonstantes Polynom $P \in K[X]\backslash K$ gegeben. So gibt es einen Körperhomomorphismus $i : K \to L$ derart, daß das Bild $i(P)$ von P unter der von i auf den Polynomringen induzierten Abbildung $i = i_{[X]} : K[X] \to L[X]$ in L eine Nullstelle hat.*

7.7.7. Die Adjunktion von Quadratwurzeln haben Sie möglicherweise bereits sozusagen zu Fuß als Übung **??** ausgearbeitet, um die komplexen Zahlen aus den reellen Zahlen zu gewinnen. Das Verfahren aus dem Beweis unseres Lemmas wird in manchen Quellen als die **Kronecker-Konstruktion** bezeichnet. Es ist eine gute Übung, im Fall der Adjunktion einer Quadratwurzel einen expliziten Isomorphismus zwischen der hier konstruierten und der in **??** beschriebenen Körpererweiterung anzugeben.

Beweis. Sei ohne Beschränkung der Allgemeinheit P irreduzibel in $K[X]$. Dann ist $L := K[X]/\langle P\rangle$ nach 6.4.22 als Quotient eines Hauptidealrings nach einem von einem irreduziblen Element erzeugten Ideal ein Körper. Wir notieren $\bar{Q} \in L$ die Nebenklasse eines Polynoms $Q \in K[X]$. Jetzt betrachten wir den offensichtlichen Körperhomomorphismus

$$i : K \to L = K[X]/\langle P\rangle$$

mit $i(a) = \bar{a}$ und behaupten, daß die Nebenklasse $\bar{X} \in L$ von $X \in K[X]$ eine Nullstelle des Polynoms $i(P) \in L[X]$ ist. In der Tat finden wir für unser Polynom $P = a_nX^n + \ldots + a_1X + a_0$ mit Koeffizienten $a_\nu \in K$ sofort $i(P) = \bar{a}_nX^n + \ldots + \bar{a}_1X + \bar{a}_0$ und dann

$$(i(P))(\bar{X}) = \bar{a}_n\bar{X}^n + \ldots + \bar{a}_1\bar{X} + \bar{a}_0 = \overline{a_nX^n + \ldots + a_1X + a_0} = \bar{P} = 0 \quad \square$$

7.7.8. Gegeben ein Körper K und ein Polynom $P \in K[X]$ und eine Körpererweiterung $K \subset L$ und eine Nullstelle $\alpha \in L$ unseres Polynoms P sagen wir auch, der Körper $K(\alpha) \subset L$ entstehe aus K durch **Adjunktion einer Nullstelle**

von P. Ist $P \in K[X]$ irreduzibel, so induziert das Einsetzen von α für X einen Körperisomorphismus

$$K[X]/\langle P\rangle \xrightarrow{\sim} K(\alpha)$$

In diesem Sinne darf man also an die linke Seite denken, wenn von der „Adjunktion einer Nullstelle eines Polynoms zu einem Körper“ die Rede ist, sofern besagtes Polynom irreduzibel ist.

Beispiel 7.7.9. In $\mathbb{F}_5$ sind 0 und ± 1 die einzigen Quadrate. Wir erhalten also einen Körper mit 25 Elementen, indem wir zu $\mathbb{F}_5$ eine Wurzel aus 2 adjungieren, und können alle Elemente dieses Körpers dann eindeutig schreiben in der Form $a + b\sqrt{2}$ mit $a, b \in \mathbb{F}_5$.

Lemma 7.7.10. *Seien p eine Primzahl, $q = p^r$ mit $r \geq 1$ eine echte Potenz von p und L ein Körper der Charakteristik p. Zerfällt das Polynom $X^q - X$ über dem Körper L vollständig in Linearfaktoren, so bilden die Nullstellen unseres Polynoms in L einen Unterkörper der Kardinalität q.*

Beweis. Nach 2.2.37 ist die Abbildung $F : L \to L$, $a \mapsto a^q$ ein Körperhomomorphismus. Die Nullstellen unseres Polynoms sind nun genau die Fixpunkte dieses Körperautomorphismus, und als Fixpunkte eines Körperautomorphismus bilden sie damit einen Unterkörper $\mathbb{F}$ von L. Um zu zeigen, daß dieser Unterkörper $\mathbb{F}$ genau q Elemente hat, müssen wir nachweisen, daß das Polynom $X^q - X$ nur einfache Nullstellen hat. Ist aber a eine Nullstelle, so gilt im Polynomring $\mathbb{F}_p[X]$ die Gleichheit $X^q - X = (X-a)^q - (X-a) = ((X-a)^{q-1} - 1)\,(X-a)$. Also ist jede Nullstelle unseres Polynoms einfach. □

Beweis von 7.7.1, Fortsetzung. Jetzt können wir zeigen, daß es zu jeder echten Potenz q einer Primzahl p auch tatsächlich einen Körper mit genau q Elementen gibt. Wir finden ja nach 7.7.4 eine Körpererweiterung L von $\mathbb{F}_p$, in der das Polynom $X^q - X \in \mathbb{F}_p[X]$ vollständig in Linearfaktoren zerfällt, und nach 7.7.10 bilden die Nullstellen dieses Polynoms in L dann einen Unterkörper der Kardinalität q. Schließlich müssen wir, um unsere Klassifikation der endlichen Körper abzuschließen, noch zeigen, daß je zwei endliche Körper derselben Kardinalität isomorph sind. Ist $\mathbb{F}$ ein endlicher Körper mit $q = p^r$ Elementen, so gilt $a^{q-1} = 1$ für alle $a \in \mathbb{F}^\times$ nach 3.3.8, also haben wir $a^q - a = 0$ für alle $a \in \mathbb{F}$. Insbesondere sind die Minimalpolynome der Elemente von $\mathbb{F}$ über $\mathbb{F}_p$ genau die $\mathbb{F}_p$-irreduziblen Faktoren des Polynoms $X^q - X \in \mathbb{F}_p[X]$. Die Erzeuger der Körpererweiterung $\mathbb{F}$ sind damit genau die Nullstellen der $\mathbb{F}_p$-irreduziblen Faktoren P vom Grad r unseres Polynoms $X^q - X$. Nach 3.4.17 gibt es solche Erzeuger und damit auch solche Faktoren und mit 7.3.3 folgt

$$\mathbb{F} \cong \mathbb{F}_p[X]/\langle P\rangle$$

für einen und jeden $\mathbb{F}_p$-irreduziblen Faktor P vom Grad r des Polynoms $X^q - X$. Das zeigt, daß ein endlicher Körper durch die Zahl seiner Elemente bis auf Isomorphismus eindeutig bestimmt ist. Das Argument zeigt nebenbei bemerkt auch, wie man in endlichen Körpern explizit rechnen kann. □

7.7.11. Teile dieses Beweises lassen sich mithilfe der allgemeinen Theorie, sobald wir sie einmal entwickelt haben, auch schneller erledigen: Die Eindeutigkeit erhält man aus dem Satz 7.8.2 über die Eindeutigkeit von Zerfällungskörpern. Die Existenz folgt wie oben daraus, daß $X^q - X$ keine mehrfachen Nullstellen hat, aber das kann man nach 7.9.14 auch daraus folgern, daß die Ableitung dieses Polynoms keine Nullstellen hat.

Satz 7.7.12 (Endliche Erweiterungen endlicher Körper). *Gegeben ein endlicher Körper F liefert die Kardinalität eine Bijektion*

$$\begin{array}{ccc} \{\textit{Unterkörper } K \subset F\} & \xrightarrow{\sim} & \{q \in \mathbb{N} \mid \exists d \in \mathbb{N} \textit{ mit } q^d = |F|\} \\ K & \mapsto & |K| \end{array}$$

7.7.13. Gegeben zwei endliche Körper läßt sich insbesondere der eine in den anderen einbetten genau dann, wenn die Kardinalität des einen eine Potenz der Kardinalität des anderen ist. Mit den Methoden der Galois-Theorie werden wir dies Resultat in 8.3.3 sehr viel müheloser einsehen können als im folgenden Beweis.

Beweis. Für den Grad $d = [F : K]$ unserer Körpererweiterung gilt sicher $|F| = |K|^d$, also liefert die Kardinalität jedenfalls eine Abbildung zwischen den im Satz beschriebenen Mengen. Weiter muß unser Unterkörper K, wenn es ihn denn gibt, genau aus den $(|K| - 1)$-ten Einheitswurzeln von F mitsamt der Null bestehen, und das zeigt die Injektivität unserer Abbildung. Für den Nachweis ihrer Surjektivität überlegen wir uns zunächst, daß es in $\mathbb{F}_{q^r}$ stets genau $(q - 1)$ Elemente der Ordnung $q - 1$ gibt. Das ist klar, da $\mathbb{F}_{q^r}^\times$ eine zyklische Gruppe der Ordnung $q^r - 1$ ist und da gilt $(q-1)|(q^r-1)$, genauer ist der Quotient ja $q^{r-1} + q^{r-2} + \ldots + q + 1$. Also gibt es in $\mathbb{F}_{q^r}$ genau q Lösungen der Gleichung $X^q - X$ und nach 7.7.10 bilden diese einen Unterkörper von $\mathbb{F}_{q^r}$ mit q Elementen. □

Übungen

Übung 7.7.14. Ein endlicher Körper kann nie algebraisch abgeschlossen sein.

Übung 7.7.15. Geben Sie einen Körperisomorphismus $\mathbb{F}_5(\sqrt{2}) \xrightarrow{\sim} \mathbb{F}_5(\sqrt{3})$ an als $\mathbb{F}_5$-lineare Abbildung in Bezug auf die Basen $1, \sqrt{2}$ links und $1, \sqrt{3}$ rechts.

Ergänzende Übung 7.7.16 (**Partialbruchzerlegung**). Ist k ein Körper, so wird eine k-Basis des Funktionenkörpers $k(X)$ gebildet von erstens den $(X^n)_{n\geq 1}$ mitsamt zweitens den

$$(X^d P^{-n})_{n\geq 1,\, \operatorname{grad} P > d \geq 0}$$

für $P \in k[X]$ normiert und irreduzibel zuzüglich drittens der 1 aus $k(X)$. Für den Fall k algebraisch abgeschlossen vergleiche man 2.5.12. Sonst ziehe man sich für den Beweis der linearen Unabhängigkeit mit 7.7.4 auf den Fall von in Linearfaktoren zerfallenden Nennern zurück.

Ergänzende Übung 7.7.17. Man bestimme die Partialbruchzerlegung, also die Darstellung in der Basis aus 7.7.16, von $(1+x^4)^{-1}$ in $\mathbb{R}(X)$.

Übung 7.7.18. Man zeige, daß es im Polynomring über einem endlichen Körper irreduzible Polynome von jedem positiven Grad gibt.

Ergänzende Übung 7.7.19. Geben Sie Verknüpfungstafeln für die Addition und die Multiplikation eines Körpers mit vier Elementen an.

7.8 Zerfällungskörper

Definition 7.8.1. Sei K ein Körper und $P \in K[X]\backslash 0$ ein von Null verschiedenes Polynom. Unter einem **minimalen Zerfällungskörper** oder kurz **Zerfällungskörper von** P verstehen wir eine Körpererweiterung L/K derart, daß (1) das Polynom P in $L[X]$ vollständig in Linearfaktoren zerfällt und daß (2) der Körper L über K erzeugt wird von den Nullstellen von P. Mit einem Zerfällungskörper meint man also eigentlich eine Körpererweiterung und sollte deshalb besser von einer **Zerfällungserweiterung** reden, aber das tut kein Mensch.

Satz 7.8.2 (Existenz und Eindeutigkeit von Zerfällungskörpern). *Seien K ein Körper und $P \in K[X]\backslash 0$ ein von Null verschiedenes Polynom. So existieren Zerfällungskörper von P, und sind L/K und L'/K zwei Zerfällungskörper von P, so gibt es einen Körperisomorphismus $L \xrightarrow{\sim} L'$, der auf K die Identität induziert.*

7.8.3. Die Existenz eines Zerfällungskörpers folgt leicht aus Satz 7.7.4, nach dem es für jedes Polynom eine Körpererweiterung gibt, in der es in Linearfaktoren zerfällt: Wir müssen darin dann nur noch den von besagten Nullstellen erzeugten Teilkörper betrachten. Die Eindeutigkeit zeigen wir erst nach den Beweis von 7.8.13.

7.8.4 (**Fragen der Eindeutigkeit und Terminologie**). Da ein Zerfällungskörper für ein Polynom damit in gewisser Weise eindeutig ist, spricht man auch oft von *dem* Zerfällungskörper eines Polynoms. Das ist jedoch auch wieder irreführend: Im allgemeinen gibt es nämlich zwischen zwei Zerfällungskörpern L, L' desselben Polynoms durchaus verschiedene Isomorphismen $L \xrightarrow{\sim} L'$, und das auch dann noch, wenn wir die naheliegende Forderung stellen, daß unsere Isomorphismen auf K die Identität induzieren sollen. Zerfällungskörper eines vorgegebenen Polynoms sind in diesem Sinne „wohlbestimmt bis auf nicht eindeutigen Isomorphismus“. Sie sollten bereits einige Strukturen kennen, die wohlbestimmt sind bis

auf nicht eindeutigen Isomorphismus: Mengen mit zwei Elementen, Gruppen mit drei Elementen, eindimensionale Vektorräume über einem gegebenen Körper, etc. Beispiele für Strukturen, die wohlbestimmt sind bis auf eindeutigen Isomorphismus, wären dahingegen: Mengen mit einem Element, Gruppen mit zwei Elementen, der Ring der ganzen Zahlen, der Körper der rationalen Zahlen, der Körper der reellen Zahlen. Eigentlich bräuchte man eben zum Schreiben über Mathematik außer dem bestimmten und dem unbestimmten Artikel noch ein Zwischending für „wohlbestimmt bis auf nicht eindeutigen Isomorphismus“, aber es wäre wohl vermessen, die deutsche Grammatik dahingehend erweitern zu wollen. Wir sind mit unseren beiden Arten von Artikeln verglichen etwa mit dem Russischen sogar schon gut bedient. Sie werden das merken, sobald Sie mathematische Artikel lesen, die aus dieser Sprache übersetzt sind: Oft sind dann in der Übersetzung ohne Verstand bestimmte oder unbestimmte Artikel gewählt worden, was man dann beim Lesen erst im Geiste korrigieren muß, damit sich ein sinnvoller Text ergibt. Um diese Phänomene der „Wohlbestimmtheit bis auf nicht eindeutigen Isomorphismus“ im vorliegenden Fall begrifflich zu fassen, führen wir zunächst einmal eine geeignete Terminologie ein.

Definition 7.8.5. Sei K ein Kring. Unter einem **K-Kring** verstehen wir ein Paar (L, i) bestehend aus einem Kring L und einem Ringhomomorphismus $i : K \to L$. Ist (M, j) ein weiterer K-Kring, so verstehen wir unter einem **Homomorphismus von K-Kringen** $L \to M$ einen Kringhomomorphismus $\varphi : L \to M$ mit $\varphi \circ i = j$. Alternativ sprechen wir auch von einem **Homomorphismus über** K. Die Menge aller solchen Homomorphismen notieren wir

$$\mathrm{Kring}^K(L, M)$$

Einen bijektiven Ringhomomorphismus über K nennen wir auch einen **Isomorphismus von K-Kringen** oder einen **Isomorphismus über** K.

Beispiel 7.8.6. Unser Satz 2.3.5 über das Einsetzen in Polynome kann in dieser Terminologie dahingehend formuliert werden, daß für jeden Kring K und jeden K-Kring (R, i) das Auswerten $\varphi \mapsto \varphi(X)$ bei X eine Bijektion

$$\mathrm{Kring}^K(K[X], R) \;\tilde{\to}\; R$$

liefert. Die Umkehrabbildung ordnet jedem Element $b \in R$ den durch das Einsetzen von b nach 2.3.9 erklärten Ringhomomorphismus $K[X] \to R$ zu. Dasselbe gilt allgemeiner für jede K-Ringalgebra R.

Definition 7.8.7. Ist K ein Körper, so bezeichnen wir einen K-Kring, der seinerseits ein Körper ist, auch als eine **Körpererweiterung von** K. Das hatten wir bereits in 7.2.3 angedeutet. Wenn wir pedantisch sein wollen, sprechen wir von einer

„Körpererweiterung im verallgemeinerten Sinne“. Unsere Homomorphismen und Isomorphismen von K-Kringen nennen wir in diesem Kontext **Homomorphismen** beziehungsweise **Isomorphismen von Körpererweiterungen**. Fassen wir $i : K \hookrightarrow L$ auf als die Einbettung eines Unterkörpers $K \subset L$ und ist $j : K \to M$ ein weiterer Körperhomomorphismus, so nennen wir einen Körperhomomorphismus $L \to M$ über K auch eine **Ausdehnung** von j auf L und benutzen Notationen wie zum Beispiel $\tilde{j} : L \to M$.

Ergänzung 7.8.8. Ist K ein Körper, so ist jeder K-Kring im Sinne der vorhergehenden Definition 7.8.5 eine K-Kringalgebra im Sinne unserer Definition **??**, und jede K-Kringalgebra A wird umgekehrt durch den einzigen Homomorphismus $K \to A$ von K-Kringalgebren zu einem K-Kring. Diese beiden Konzepte sind also äquivalent.

Proposition 7.8.9 (**Ausdehnungen auf primitive Erweiterungen**). *Gegeben eine Körpererweiterung $j : K \hookrightarrow M$ und eine primitive algebraische Erweiterung $K(\alpha)$ von K werden die Ausdehnungen von j zu einer Einbettung $\tilde{j} : K(\alpha) \hookrightarrow M$ parametrisiert durch die Nullstellen in M des Minimalpolynoms von α über K. Genauer liefert das Auswerten an α eine Bijektion*

$$\begin{array}{ccc} \mathrm{Kring}^K(K(\alpha), M) & \tilde{\to} & \{\beta \in M \mid \mathrm{Irr}(\alpha, K)(\beta) = 0\} \\ \varphi & \mapsto & \varphi(\alpha) \end{array}$$

7.8.10. In der Formulierung dieser Proposition haben wir beim Auswerten des Polynoms $\mathrm{Irr}(\alpha, K) \in K[X]$ auf $\beta \in M$ stillschweigend die Elemente von K mit ihren Bildern in M unter j identifiziert. Die Proposition gilt unverändert und mit demselben Beweis auch allgemeiner für jeden K-Kring M, ja für jede Ringalgebra M über K.

Beispiel 7.8.11. Wir haben im Fall $K = \mathbb{Q}$, $M = \mathbb{C}$, $\alpha = \mathrm{i}$ etwa

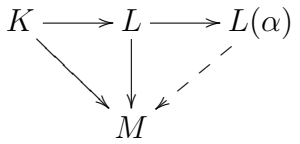
$$\begin{array}{ccc} \mathrm{Kring}^{\mathbb{Q}}(\mathbb{Q}(\mathrm{i}), \mathbb{C}) & \tilde{\to} & \{\beta \in \mathbb{C} \mid \beta^2 + 1 = 0\} \\ \varphi & \mapsto & \varphi(\mathrm{i}) \end{array}$$

Beweis. Wir setzen $P := \mathrm{Irr}(\alpha, K)$ und etablieren der Reihe nach die Bijektionen

$$\begin{array}{lcll} \mathrm{Kring}^K(K[X], M) & \tilde{\to} & M & \varphi \mapsto \varphi(X) \\ \mathrm{Kring}^K(K[X]/\langle P\rangle, M) & \tilde{\to} & \{\beta \in M \mid P(\beta) = 0\} & \varphi \mapsto \varphi(\bar{X}) \\ \mathrm{Kring}^K(K(\alpha), M) & \tilde{\to} & \{\beta \in M \mid P(\beta) = 0\} & \varphi \mapsto \varphi(\alpha) \end{array}$$

Die Erste in 7.8.6 und gilt für jeden Kring K und jeden K-Kring M. Die Zweite gilt für jeden Kring K und jeden K-Kring M und jedes Polynom $P \in K[X]$ und folgt aus der universellen Eigenschaft des Quotienten, da für φ gegeben durch $\varphi(X) = \beta$ eben $\varphi(P) = 0$ gleichbedeutend ist zu $P(\beta) = 0$. Die Dritte folgt, da unter den Annahmen der Proposition das Einsetzen von α einen Isomorphismus $K[X]/\langle P\rangle \tilde{\to} K(\alpha)$ induziert. □

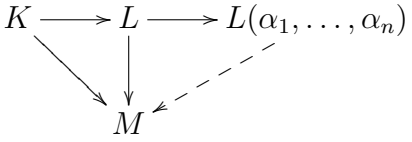
Lemma 7.8.12 (Primitives Ausdehnbarkeitskriterium). *Sei ein kommutatives Dreieck von Körperhomomorphismen gegeben wie in der rechten Hälfte des Diagramms*



und sei $L \subset L(\alpha)$ eine primitive Körpererweiterung von L mit α algebraisch über K derart, daß das Minimalpolynom $\operatorname{Irr}(\alpha, K)$ in $M[X]$ vollständig in Linearfaktoren zerfällt. So laßt sich der Körperhomomorphismus $L \to M$ wie durch den gestrichelten Pfeil angedeutet zu einem Körperhomomorphismus $L(\alpha) \to M$ ausdehnen.

Beweis. Das Minimalpolynom $\operatorname{Irr}(\alpha, L)$ ist ein Teiler von $\operatorname{Irr}(\alpha, K)$ und muß deshalb nach Annahme eine Nullstelle $\beta \in M$ haben. Nach 7.8.9 erhalten wir für jede solche Nullstelle eine Ausdehnung durch $\alpha \mapsto \beta$. □

Proposition 7.8.13 (Allgemeines Ausdehnbarkeitskriterium). *Sei ein kommutatives Dreieck von Körperhomomorphismen gegeben wie in der rechten Hälfte des Diagramms*



und seien $\alpha_1, \ldots, \alpha_n$ algebraisch über K derart, daß alle ihre Minimalpolynome $\operatorname{Irr}(\alpha_i, K)$ in $M[X]$ vollständig in Linearfaktoren zerfallen. So laßt sich der Körperhomomorphismus $L \to M$ wie durch den gestrichelten Pfeil angedeutet zu einem Körperhomomorphismus $L(\alpha_1, \ldots, \alpha_n) \to M$ ausdehnen.

Beweis. Das folgt induktiv aus dem Ausdehnbarkeitskriterium für primitive Erweiterungen 7.8.12. □

Vorschau 7.8.14. Diese Proposition wird auch unmittelbar aus der allgemeineren und vielleicht „glatteren“ Aussage 7.11.9 über Einbettungen in den algebraischen Abschluß folgen: Mit 7.11.3.2 dürfen wir M algebraisch über K annehmen. Nach 7.11.9 läßt sich M dann über K in einen algebraischen Abschluß $\bar{K}$ von K einbetten. Wieder nach 7.11.9 können wir auch $K(\alpha_1, \ldots, \alpha_n)$ über K in $\bar{K}$ einbetten, und nach Annahme liegt sein Bild dann notwendig im Bild von M.

Beweis der Eindeutigkeit von Zerfällungskörpern 7.8.2. Proposition 7.8.13 liefert uns Injektionen $L \hookrightarrow L'$ und $L' \hookrightarrow L$ über K. Da hier beide Seiten endlichdimensionale Vektorräume sind über K, und da unsere Injektionen beide K-linear sind, müssen sie beide Isomorphismen sein. □

Satz 7.8.15 (**Maximalzahl von Ausdehnungen**). *Gegeben eine Körpererweiterung ist die Zahl der Ausdehnungen auf den Erweiterungskörper eines Homomorphismus des Grundkörpers in irgendeinen weiteren Körper beschränkt durch den Grad unserer Körpererweiterung. Ist also in Formeln L/K eine endliche Körpererweiterung und $j : K \hookrightarrow M$ ein Körperhomomorphismus, so gilt*

$$|\operatorname{Kring}^K(L, M)| \leq [L : K]$$

Erster Beweis. Gibt es einen Zwischenkörper L' mit $K \subset L' \subset L$ aber $K \neq L' \neq L$, so folgt der Satz mit vollständiger Induktion über den Grad unserer Körpererweiterung. Sonst gilt $L = K(\alpha)$ für ein $\alpha \in L$, und die Erweiterungen von j zu einer Einbettung von $K(\alpha)$ in M werden nach 7.8.9 parametrisiert durch die Nullstellen in M des Minimalpolynoms von α über K. Dieses Polynom hat aber den Grad $[K(\alpha) : K]$ und höchstens ebensoviele Nullstellen in M. □

Zweiter Beweis. Seien $\sigma_1, \ldots, \sigma_r$ paarweise verschiedene K-lineare Körperhomomorphismen $L \to M$. Nach Satz 7.8.16 über die lineare Unabhängigkeit von Charakteren, den wir im Anschluß beweisen, sind sie linear unabhängig im M-Vektorraum $\operatorname{Ens}(L, M)$. Gegeben eine K-Basis $B \subset L$ von L bleiben ihre Restriktionen im M-Vektorraum $\operatorname{Ens}(B, M)$ offensichtlich linear unabhängig und es folgt $r \leq |B|$. □

Satz 7.8.16 (**Lineare Unabhängigkeit von Charakteren**). *Die Menge aller Homomorphismen von einer Gruppe in die multiplikative Gruppe eines Körpers ist stets linear unabhängig im Vektorraum aller Abbildungen von besagter Gruppe in besagten Körper.*

7.8.17. Dasselbe gilt mit demselben Beweis allgemeiner auch für die Menge aller Homomorphismen von einem Monoid in die multiplikative Gruppe eines Körpers.

Beweis. Bezeichnen wir unsere Gruppe mit G und unserem Körper mit M, so behaupten wir in Formeln, daß $\operatorname{Grp}(G, M^\times)$ eine linear unabhängige Teilmenge des M-Vektorraums $\operatorname{Ens}(G, M)$ ist. Sei in der Tat sonst

$$a_1\chi_1 + a_2\chi_2 + \ldots + a_n\chi_n = 0$$

eine nichttriviale lineare Relation kürzestmöglicher Länge mit $a_i \in M$ und $\chi_i : G \to M^\times$ paarweise verschiedenen Gruppenhomomorphismen. Wegen $\chi(1) = 1$ für alle Charaktere χ haben wir notwendig $n \geq 2$. Wegen $\chi_1 \neq \chi_2$ finden wir $g \in G$ mit $\chi_1(g) \neq \chi_2(g)$. Unsere Gleichung impliziert nun aber für jedes und insbesondere auch für dieses $g \in G$ durch Substituieren von gh für h beziehungsweise Multiplizieren mit $\chi_1(g)$ die Gleichungen

$$\begin{aligned} a_1\chi_1(g)\chi_1 + a_2\chi_2(g)\chi_2 + a_n\chi_n(g)\chi_n &= 0 \\ a_1\chi_1(g)\chi_1 + a_2\chi_1(g)\chi_2 + a_n\chi_1(g)\chi_n &= 0 \end{aligned}$$

Deren Differenz wäre dann eine kürzere und wegen $\chi_1(g) \neq \chi_2(g)$ nichttriviale Linearkombination im Widerspruch zu unserer Annahme. □

Definition 7.8.18. Eine Körpererweiterung heißt **algebraisch**, wenn alle Elemente der Erweiterung algebraisch sind über dem Grundkörper.

7.8.19. Jede endliche Körpererweiterung ist also nach 7.4.7 auch algebraisch. Genauer ist nach 7.4.7 eine Körpererweiterung algebraisch genau dann, wenn sie eine Vereinigung von Teilerweiterungen ist, die jeweils endlich sind über dem Grundkörper.

Definition 7.8.20. Eine Körpererweiterung L/K heißt **normal**, wenn sie algebraisch ist und wenn gilt: Jedes *irreduzible* Polynom mit Koeffizienten im Grundkörper $P \in K[X]$, das im Erweiterungskörper L eine Nullstelle hat, zerfällt im Polynomring $L[X]$ über dem Erweiterungskörper bereits vollständig in Linearfaktoren.

7.8.21 (**Diskussion der Terminologie**). In der älteren Literatur, zum Beispiel in [Art], wird der Begriff „normal“ manchmal auch abweichend definiert als diejenige Eigenschaft einer Körpererweiterung, die wir später mit „Galois“ bezeichnen werden. Ich finde die Begriffsbildung in beiden Varianten ungeschickt: Normalerweise ist eine Körpererweiterung nämlich keineswegs normal im mathematischen Sinne, oder um es anders auszudrücken: Normal zu sein ist für Körpererweiterungen etwas ganz Besonderes. Aber gut, ein Psychologe ist vermutlich durchaus auch der Ansicht, daß es für einen Menschen etwas ganz Besonderes ist, normal zu sein, und für eine Körpererweiterung erst recht: So fern vom umgangssprachlichen Wortsinn ist unsere mathematische Terminologie also auch wieder nicht.

Beispiele 7.8.22. $\mathbb{Q}(\sqrt{2})$ ist normal über $\mathbb{Q}$, aber $\mathbb{Q}(\sqrt[3]{2})$ ist nicht normal über $\mathbb{Q}$, denn wir können $\mathbb{Q}(\sqrt[3]{2})$ einbetten in $\mathbb{R}$ und die beiden anderen Wurzeln des in $\mathbb{Q}[X]$ irreduziblen Polynoms $X^3 - 2$ sind nicht reell.

Satz 7.8.23 (Charakterisierung normaler Erweiterungen). *Für eine endliche Körpererweiterung L/K sind gleichbedeutend:*

1. *L/K ist normal;*
2. *L ist der Zerfällungskörper eines Polynoms $P \in K[X]$.*

Beweis. 1⇒2. Ist L normal über K und erzeugt von $\alpha_1, \ldots, \alpha_r$, so ist L ein Zerfällungskörper für das Produkt der Minimalpolynome $\mathrm{Irr}(\alpha_i, K)$ der α_i über K. Für die andere Implikation machen wir einen Umweg und zeigen zusätzlich die Äquivalenz zu der folgenden technischen Aussage:

3. *Für jede Einbettung $j : K \hookrightarrow M$ von K in einen beliebigen weiteren Körper M haben alle Fortsetzungen von j zu Einbettungen $\varphi, \psi : L \hookrightarrow M$ dasselbe Bild, in Formeln*

$$\varphi(L) = \psi(L) \qquad \forall M,\ \forall j : K \hookrightarrow M,\ \forall \varphi, \psi \in \mathrm{Kring}^K(L, M)$$

Jetzt zeigen wir 2⇒3⇒1 und beginnen mit 2⇒3. Sowohl φ als auch ψ identifizieren die Nullstellen von P in L mit den Nullstellen von P in M, wenn auch nicht notwendig in derselben Weise. Da nun L erzeugt wird über K von den Nullstellen von P, ist sowohl $\varphi(L)$ als auch $\psi(L)$ der von allen Nullstellen von P in M über K erzeugte Teilkörper und es folgt $\varphi(L) = \psi(L)$. Schließlich zeigen wir noch 3⇒1. Sei $P \in K[X]$ irreduzibel mit einer Nullstelle $\alpha \in L$. Wir ergänzen α zu einem endlichen Erzeugendensystem von L über K, sagen wir $L = K(\alpha, \alpha_1, \ldots, \alpha_r)$. Dann wählen wir für M eine Körpererweiterung von L, in der sowohl das Minimalpolynom von α als auch die Minimalpolynome aller α_i vollständig in Linearfaktoren zerfallen. Für jede Nullstelle $\beta \in M$ von P können wir unsere Einbettung $K \hookrightarrow M$ zunächst nach 7.8.9 fortsetzen zu einer Einbettung $K(\alpha) \hookrightarrow M$ mit $\alpha \mapsto \beta$ und dann nach 7.8.13 weiter zu einer Einbettung $\varphi : L \hookrightarrow M$. Jede Nullstelle von P in M liegt also in $\varphi(L)$ für ein und damit jedes $\varphi \in \mathrm{Kring}^K(L, M)$. Also zerfällt unser Polynom P bereits in $\varphi(L)$ und a forteriori in L vollständig in Linearfaktoren. □

7.8.24. Unter formalen Gesichtspunkten ist es im vorhergehenden Beweis unschön um nicht zu sagen falsch, über alle Körper zu quantifizieren. Es reicht aber offensichtlich aus, Aussage 3 nur für die Zerfällungskörper M aller von Null verschiedenen Polynomen aus $K[X]$ zu fordern, um daraus wieder Aussage 1 zu folgern.

Proposition 7.8.25 (Vergrößern zu normaler Erweiterung). *Jede endliche Körpererweiterung läßt sich zu einer endlichen normalen Körpererweiterung vergrößern.*

Beweis. Gegeben eine endliche Körpererweiterung L/K behaupten wir in Formeln, daß es stets eine endliche Erweiterung N/L gibt, für die N/K normal ist. Um das zu zeigen, nehmen wir Erzeuger $\alpha_1, \ldots, \alpha_r$ von L über K und konstruieren N als einen Zerfällungskörper über L des Produkts ihrer Minimalpolynome. Dies N ist dann natürlich auch ein Zerfällungskörper des besagten Produkts über K und damit normal über K. □

Übungen

Übung 7.8.26. Man zeige, daß eine algebraische Körpererweiterung eines unendlichen Körpers stets dieselbe Kardinalität hat wie der Ausgangskörper. Diese Er-

kenntnis wird bei einer Konstrution des algebraischen Abschlusses benötigt werden.

Übung 7.8.27. Es sei K ein Körper, $P \in K[X]$ ein Polynom vom Grad n und L/K der Zerfällungskörper von P. Zeigen Sie die Abschätzung $[L{:}K] \leq n!$. Mutige zeigen stärker $[L{:}K]|n!$. Hinweise: Induktion über den Grad n von P. Man beachte $n!m!|(n+m)!$ nach der Formel für die Binomialkoeffizienten im Fall eines nicht irreduziblen Polynoms. Im Fall eines irreduziblen Polynoms entsteht durch Adjunktion einer Nullstelle eine Körpereweiterung vom Grad n.

Übung 7.8.28. Es seien M/L und L/K endliche oder allgemeiner algebraische Körpererweiterungen. Ist M/K normal, so ist auch M/L normal. Sind L_1 und L_2 normale Körpererweiterungen von K und $L_1, L_2 \subset M$, so ist $L_1 \cap L_2$ normal über K. Geben Sie ein Beispiel für Körper $M \supset L \supset K$ an, bei dem M/L und L/K jeweils normal sind, M/K jedoch nicht normal ist.

Übung 7.8.29. Man formuliere präzise und zeige, daß es bis auf nichteindeutigen Isomorphismus genau ein minimales N wie in Proposition 7.8.25 gibt. Dies N heißt die **normale Hülle von** L **über** K.

Übung 7.8.30. Jede endliche Körpererweiterung von $\mathbb{R}$ ist isomorph im Sinne von 7.8.5 zu $\mathbb{R}$ oder $\mathbb{C}$. Hinweis: $\mathbb{C}$ ist bekanntlich algebraisch abgeschlossen.

Ergänzende Übung 7.8.31. Sei k ein Körper und $a \in k^\times$ und $n \geq 1$. Man zeige, daß im Zerfällungskörper des Polynoms $X^n - a$ auch das Polynom $X^n - 1$ stets in Linearfaktoren zerfällt, daß aber umgekehrt im Zerfällungskörper des Polynoms $X^n - 1$ ein Polynom $X^n - a$ nicht notwendig in Linearfaktoren zerfallen muß.

Übung 7.8.32. Gegeben eine endliche Körpererweiterung $K \subset L$ zeige man, daß jedes Polynom aus dem Polynomring $L[X]$ Teiler eines Polynoms aus dem Polynomring $K[X]$ ist.

Übung 7.8.33. Gegeben eine Primzahl p und zwei primitive p-te Einheitswurzeln $\zeta, \xi \in \mathbb{C}$ gilt $\mathbb{Q}(\zeta) = \mathbb{Q}(\xi)$ und es gibt genau einen Körperhomomorphismus $\mathbb{Q}(\zeta) \to \mathbb{Q}(\zeta)$ mit $\zeta \mapsto \xi$. Hinweis: Irreduzibilität des p-ten Kreisteilungspolynoms 6.8.4.

7.9 Vielfachheit von Nullstellen

7.9.1. Unter einer **mehrfachen Nullstelle** eines Polynoms mit Koeffizienten in einem Körper oder allgemeiner einem kommutativen Integritätsbereich verstehen wir eine Nullstelle der Vielfachheit mindestens Zwei. Sagen wir, unser Polynom habe „mehrfache Nullstellen“, so ist gemeint, daß es mindestens eine mehrfache Nullstelle haben soll. Eigentlich wäre es gemäß unserer allgemeinen Konventionen **??** präziser, zu sagen, es habe „eine mehrfache Nullstelle“, aber das ist unüblich. Möglicherweise rührt das daher, daß man eine mehrfache Nullstelle

gerne denkt als „mehrere Nullstellen, die zusammenfallen“. Das Nullpolynom hat stets mehrfache Nullstellen, bei ihm haben ja sogar alle Nullstellen die Vielfachheit ∞.

Satz 7.9.2 (Mehrfache Nullstellen bei Irreduzibilität über Teilkörper). *Seien $K \subset L$ Körper. Gilt $\operatorname{char} K = 0$ oder ist K endlich, so hat ein K-irreduzibles Polynom $P \in K[X]$ keine mehrfachen Nullstellen in L.*

7.9.3. Wir werden in 7.9.17 und 7.9.24 sogar noch etwas allgemeinere Aussagen zeigen. Das braucht jedoch einige Vorbereitungen.

Beispiel 7.9.4 (**Ein K-irreduzibles Polynom mit mehrfachen L-Nullstellen**). In positiver Charakteristik können irreduzible Polynome über einem Körper durchaus mehrfache Nullstellen in einem Erweiterungskörper haben. Um ein Beispiel anzugeben, beachten wir zunächst, daß für K ein Körper positiver Charakteristik $\operatorname{char} K = p > 0$ jedes Element $a \in K$ höchstens eine p-te Wurzel in K hat. In der Tat folgt aus $b^p = a$ leicht $(X^p - a) = (X - b)^p$, mithin ist b die einzige Nullstelle des Polynoms $X^p - a$. Betrachten wir nun den Körper $K := \mathbb{F}_p(T)$, so besitzt das Element $a := T$ keine p-te Wurzel in K, denn die Menge der p-ten Potenzen von Elementen von $\mathbb{F}_p(T)$ kann explizit beschrieben werden als $\mathbb{F}_p(T^p)$ und enthält T nicht. Das Polynom $X^p - T$ ist nun sogar K-irreduzibel, da jeder seiner normierten K-irreduziblen Faktoren das Minimalpolynom $\operatorname{Irr}(\sqrt[p]{T}, K)$ sein muß, so daß unser Polynom, da es auch selbst normiert ist, eine Potenz dieses Minimalpolynoms sein muß. Das läßt aber wegen p prim nur die Möglichkeit $X^p - T = \operatorname{Irr}(\sqrt[p]{T}, K)$ offen. Dies Polynom ist also K-irreduzibel und hat in seinem Zerfällungskörper mehrfache Nullstellen, genauer eine einzige Nullstelle $\sqrt[p]{T}$ der Vielfachheit p.

Definition 7.9.5. Für ein Polynom $P = a_n X^n + \ldots + a_2 X^2 + a_1 X + a_0$ mit Koeffizienten in einem beliebigen Ring R erklären wir seine **Ableitung** oder genauer **formale Ableitung** $P' \in R[X]$ durch die Vorschrift

$$P' := n a_n X^{n-1} + \ldots + 2a_2 X + a_1$$

Lemma 7.9.6 (Ableitungsregeln). *Auch für unser formales Ableiten gelten die Summenregel $(P + Q)' = P' + Q'$ und die Produktregel $(PQ)' = P'Q + PQ'$.*

Beweis. Die Summenregel ist offensichtlich. Bei der Produktregel sind mithin beide Seiten additiv in P und Q und wir dürfen uns deshalb auf den Fall $P = aX^i$ und $Q = bX^j$ zurückziehen. In diesem Fall prüft man die Formel leicht explizit. □

Lemma 7.9.7 (Ableitung und mehrfache Nullstellen). *Gegeben K ein Körper, $g \in K[X]$ ein Polynom und $\alpha \in K$ eine Nullstelle von g ist α genau dann eine mehrfache Nullstelle von g, wenn auch die Ableitung g' von g bei α verschwindet.*

Beispiel 7.9.8. Sei p eine Primzahl. Unser Polynom $P := X^p - T$ mit Koeffizienten in $\mathbb{F}_p(T)$ hat nach 7.9.4 in seinem Zerfällungskörper $\mathbb{F}_p(\sqrt[p]{T})$ nur eine einzige Nullstelle $\alpha = \sqrt[p]{T}$ der Vielfachheit p. Nach unserem Lemma muß also gelten $P'(\alpha) = 0$. In unserem Fall ist sogar stärker $P' = 0$ selbst das Nullpolynom.

Beweis. Aus $g = (x-\alpha)^2 f$ folgt mit der Produktregel 7.9.6 leicht $g'(\alpha) = 0$. Gilt umgekehrt $g(\alpha) = g'(\alpha) = 0$ und schreiben wir $g = (x-\alpha)h$, so folgt wieder mit der Produktregel 7.9.6 aus $g'(\alpha) = 0$ unmittelbar $h(\alpha) = 0$. □

7.9.9. Gegeben ein Körper K und Polynome $f, g \in K[X]$, die nicht beide Null sind, gibt es genau ein normiertes Polynom $d \in K[X]$, das das von f und g erzeugte Ideal erzeugt, in Formeln

$$\langle f, g\rangle = \langle d\rangle$$

Per definitionem gilt $d|f$ und $d|g$ und es gibt $a, b \in K[X]$ mit $d = af + bg$. Insbesondere folgt für ein Polynom c aus $c|f$ und $c|g$ bereits $c|d$. Mithin ist d der eindeutig bestimmte normierte gemeinsame Teiler größtmöglichen Grades von f und g. Wir nennen d den **normierten größtgradigen gemeinsamen Teiler** von f und g. Man kann ihn, analog wie in 1.4.18 im Fall der ganzen Zahlen erklärt, mit dem euklidischen Algorithmus unschwer explizit berechnen.

Ergänzung 7.9.10. Analog finden wir, daß jede Menge von Polynomen in einer Veränderlichen mit Koeffizienten einem Körper, die mindestens ein von Null verschiedenes Polynom enthält, genau einen normierten größtgradigen gemeinsamen Teiler besitzt.

Proposition 7.9.11 (Körpererweiterungen und Polynomdivision). *Es seien $K \subset L$ Körper und $f, g \in K[X]$ Polynome mit $g \neq 0$. So gilt:*

1. *Das Teilen mit Rest von f durch g führt zum selben Resultat unabhängig davon, ob wir es in $K[X]$ oder in $L[X]$ durchführen;*
2. *Genau dann ist g ein Teiler von f in $L[X]$, wenn dasselbe gilt in $K[X]$;*
3. *Der normierte größtgradige gemeinsame Teiler von f und g in $K[X]$ ist auch der normierte größtgradige gemeinsame Teiler von f und g in $L[X]$.*

Beweis. 1. Schreiben wir $f = qg + r$ mit $\operatorname{grad} r < \operatorname{grad} g$, so sind q und r schon eindeutig bestimmt. Insbesondere ist die Lösung in $K[X]$ auch die einzig mögliche Lösung in $L[X]$.

2. Das ist der Spezialfall von Teil 1 mit Rest $r = 0$.

3. Seien dazu d_K beziehungsweise d_L der normierte größtgradige gemeinsame Teiler von f und g in $K[X]$ beziehungsweise in $L[X]$ nach 7.9.9. Natürlich ist d_K

auch ein gemeinsamer Teiler in $L[X]$, also gilt $d_K|d_L$ nach 7.9.9. Andererseits haben wir eine Darstellung $d_K = qf + pg$ mit $q, p \in K[X]$, also gilt auch umgekehrt $d_L|d_K$. Zusammen folgt $d_L = d_K$. □

7.9.12. Ich erinnere an unsere Definition 2.2.16: Zwei Elemente eines Krings oder allgemeiner die Elemente einer beliebigen Teilmenge eines Krings heißen **teilerfremd**, wenn sie außer Einheiten keine gemeinsamen Teiler haben. Im Fall eines Hauptidealrings ist das offensichtlich gleichbedeutend dazu, daß das von unseren Elementen erzeugte Ideal der ganze Ring ist.

7.9.13 (**Gemeinsame Nullstellen und gemeinsame Teiler**). Gegeben ein Körper K haben zwei Polynome $f, g \in K[X]$ genau dann eine gemeinsame Nullstelle in mindestens einem Erweiterungskörper L/K, wenn sie nicht teilerfremd sind. In der Tat dürfen wir annehmen, daß f und g nicht beide das Nullpolynom sind. Gibt es nun eine Körpererweiterung L/K und $\alpha \in L$ mit $f(\alpha) = g(\alpha) = 0$, so folgt $(X-\alpha)|f$ und $(X-\alpha)|g$ und f und g sind nicht teilerfremd in $L[X]$ und dann nach unserer Proposition 7.9.11 auch nicht in $K[X]$. Haben umgekehrt f und g einen gemeinsamen Teiler positiven Grades, so hat dieser Teiler in mindestens einer Körpererweiterung L/K eine Nullstelle, und diese ist dann auch eine Nullstelle von f und von g.

Lemma 7.9.14 (**Ableitung und Existenz mehrfacher Nullstellen**). *Für ein von Null verschiedenes Polynom mit Koeffizienten in einem Körper sind gleichbedeutend:*

1. *Das Polynom hat mehrfache Nullstellen in seinem Zerfällungskörper;*
2. *Das Polynom hat mehrfache Nullstellen in mindestens einer Erweiterung seines Koeffizientenkörpers;*
3. *Das Polynom und seine Ableitung sind nicht teilerfremd.*

7.9.15. Bei der Bedingung „teilerfremd“ kommt es wegen 7.9.11 nicht darauf an, ob wir sie in unserem ursprünglichen Polynomring oder im Polynomring mit Koeffizienten in einem beliebigen Erweiterungskörper verstehen.

Beweis. Seien K unser Körper und $P \in K[X]\backslash 0$ unser Polynom.

$1 \Rightarrow 2$. Das ist offensichtlich.

$2 \Rightarrow 3$. Ist α eine mehrfache Nullstelle des Polynoms P in einer Körpererweiterung L von K, so ist $(X - \alpha)$ ein Teiler sowohl von P als auch von P' in $L[X]$ und es folgt $\langle P, P' \rangle \neq \langle 1 \rangle$.

$3 \Rightarrow 1$. Es gibt eine Körpererweiterung M/K, in der P und falls $P' \neq 0$ auch P' in Linearfaktoren zerfallen. Gilt $\langle P, P' \rangle \neq \langle 1 \rangle$, so gibt es in M ein Element α derart,

daß $(X - \alpha)$ sowohl P als auch P' teilt. In anderen Worten ist α eine Nullstelle von P und P' und damit eine mehrfache Nullstelle von P nach 7.9.7. □

7.9.16. Ein Polynom, das in keinem Erweiterungskörper seines Koeffizientenkörpers mehrfache Nullstellen hat, heißt **separabel**. Gleichbedeutend ist die Bedingung, daß unser Polynom keine mehrfachen Nullstellen in seinem Zerfällungskörper hat.

Satz 7.9.17 (**Mehrfache Nullstellen bei Irreduzibilität über Teilkörper**). *Seien K ein Körper und $P \in K[X]$ ein K-irreduzibles Polynom. So sind gleichbedeutend:*

1. *Das Polynom P ist nicht separabel, hat also mindestens eine mehrfache Nullstelle in mindestens einer Erweiterung seines Koeffizientenkörpers;*
2. *Die Ableitung P' von P ist das Nullpolynom;*
3. *Es gilt $\operatorname{char} K = p > 0$ und es gibt $Q \in K[X]$ mit $P(X) = Q(X^p)$;*
4. *Jede Nullstelle unseres Polynoms in einer beliebigen Erweiterung seines Koeffizientenkörpers ist ein mehrfache Nullstelle.*

Beweis. $1 \Rightarrow 2$. Hat P mehrfache Nullstellen, so ist es nach 7.9.14 nicht teilerfremd zu seiner Ableitung. Wenn aber ein irreduzibles Polynom nicht teilerfremd ist zu einem weiteren Polynom echt kleineren Grades, muß dieses weitere Polynom das Nullpolynom sein.

$2 \Leftrightarrow 3$. Das scheint mir offensichtlich.

$2 \Rightarrow 4$. Ist die Ableitung das Nullpolynom, so ist jede Nullstelle unseres Polynoms auch eine Nullstelle seiner Ableitung, mithin nach 7.9.7 eine mehrfache Nullstelle unseres Polynoms.

$4 \Rightarrow 1$. Das scheint mir offensichtlich. □

Definition 7.9.18. Sei L/K eine Körpererweiterung. Ein Element $\alpha \in L$ heißt **separabel über** K, wenn es über K algebraisch und eine einfache Nullstelle seines Minimalpolynoms ist. Unsere Körpererweiterung heißt **separabel**, wenn jedes Element von L separabel ist über K.

7.9.19. Nach 7.9.17 ist ein Element eines Körpers separabel über einem Teilkörper genau dann, wenn es über diesem algebraisch ist mit separablem Minimalpolynom.

Beispiel 7.9.20. In Charakteristik Null ist jede algebraische Körpererweiterung separabel nach 7.9.17. Nicht separabel ist $\mathbb{F}_p(\sqrt[p]{T})$ über $\mathbb{F}_p(T)$ nach 7.9.4.

Definition 7.9.21. Ein Körper heißt **vollkommen**, wenn er entweder die Charakteristik Null hat oder aber für $p = \operatorname{char} K > 0$ die Abbildung $x \mapsto x^p$ eine Surjektion $K \twoheadrightarrow K$ ist.

Ergänzung 7.9.22. Für „vollkommen“ sagt man in diesem Zusammenhang auf Englisch **perfect** und auf Französisch **parfait**.

Beispiel 7.9.23 (**Endliche Körper sind vollkommen**). Jeder endliche Körper vollkommen, denn jeder Körperhomomorphismus und damit auch der Frobeniushomomorphismus ist injektiv und folglich im Fall eines endlichen Körpers auch surjektiv.

Satz 7.9.24 (Irreduzible Polynome über vollkommenen Körpern). *Jedes irreduzible Polynom über einem vollkommenen Körper ist separabel. Jede algebraische Erweiterung eines vollkommenen Körpers ist separabel.*

Beweis. Sei K unser vollkommener Körper. Den Fall $\operatorname{char} K = 0$ haben wir bereits durch 7.9.2 oder besser 7.9.17 erledigt. Sei also ohne Beschränkung der Allgemeinheit $\operatorname{char} K = p > 0$ und $P \in K[X]$ irreduzibel. Wäre P nicht separabel, so hätte P nach 7.9.17 die Form $P = b_n(X^p)^n + \ldots + b_1X^p + b_0$. Nehmen wir aber nun $a_n, \ldots, a_0 \in K$ mit $a_i^p = b_i$ und betrachten $Q = a_nX^n + \ldots + a_0$, so folgt $P = Q^p$ im Widerspruch zur Irreduzibilität von P. □

7.9.25 (**Algebraische Körpererweiterungen endlicher Körper sind separabel**). Jede algebraische Körpererweiterung eines endlichen Körpers ist separabel, da jeder endliche Körper vollkommen ist nach 7.9.23 und folglich jedes irreduzible Polynom darüber separabel nach 7.9.24.

Satz 7.9.26 (Charakterisierung separabler Erweiterungen). *Für eine Körpererweiterung L/K sind gleichbedeutend:*

1. *L/K ist separabel;*
2. *L wird erzeugt über K von Elementen, die separabel sind über K.*

Ist L/K endlich, so sind auch gleichbedeutend:

3. *Für jede Vergrößerung N/L von L zu einer normalen Erweiterung von K gilt $|\mathrm{Kring}^K(L, N)| = [L : K]$;*
4. *Es gibt mindestens eine Körpererweiterung N/K von K mit der Eigenschaft $|\mathrm{Kring}^K(L, N)| = [L : K]$.*

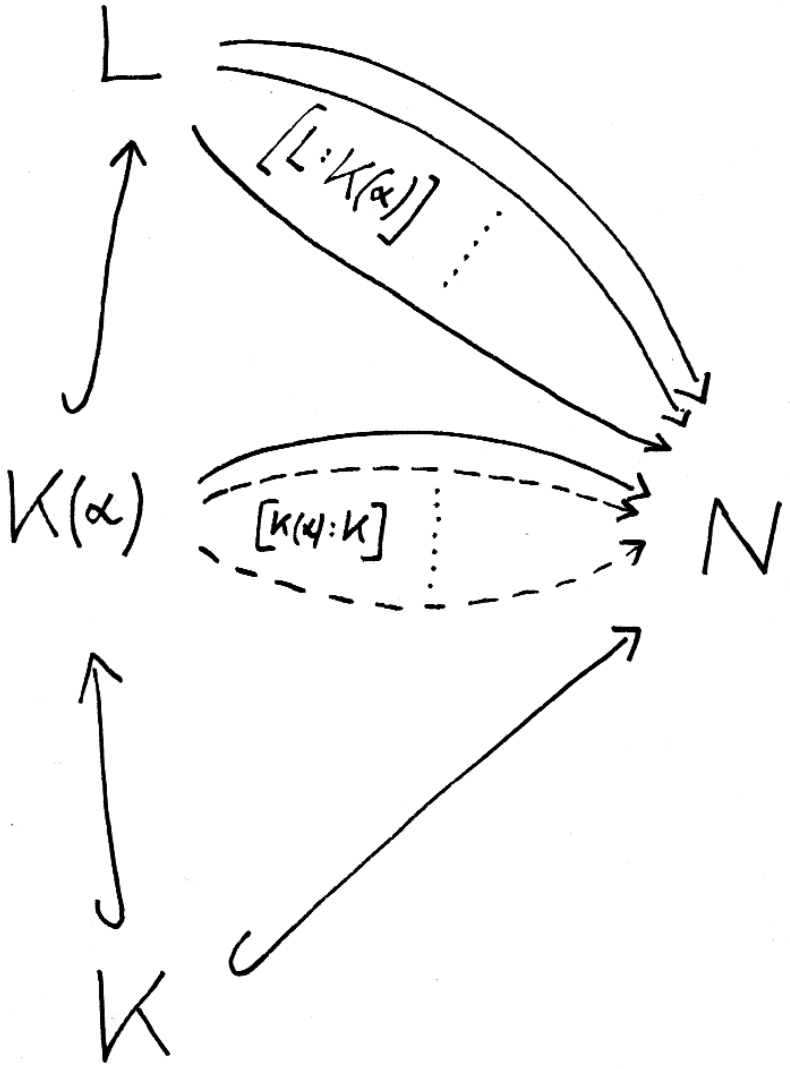


Illustration zum Beweis von 7.9.26, Implikation $2 \Rightarrow 3$. Die durchgezogenen Pfeile ganz oben sollen mögliche Erweiterungen des durchgezogenen Pfeils in der Mitte andeuten. Jeder andere der $[K(\alpha) : K]$ Pfeile in der Mitte besitzt genauso $[L : K(\alpha)]$ Erweiterungen nach ganz oben, nur sind diese nicht eingezeichnet.

Beweis. Zeigen wir $1 \Leftrightarrow 2$ für endliche Erweiterungen, so folgt es mit 7.2.6 im allgemeinen. Wir dürfen uns also für den Rest des Beweises auf den Fall L/K endlich beschränken. $1 \Rightarrow 2$ ist klar. Für $2 \Rightarrow 3$ dürfen wir mit Induktion über den Grad $[L : K]$ annehmen $L = K(\alpha)$. Da α separabel ist, sind die $[L : K]$ Nullstellen seines Minimalpolynoms in N paarweise verschieden und liefern mit 7.8.9 paarweise verschiedene Erweiterungen der Einbettung $K \hookrightarrow N$ zu Körperhomomorphismen $K(\alpha) \hookrightarrow N$. Die Implikation $3 \Rightarrow 4$ ist klar. Für $4 \Rightarrow 1$ argumentieren wir durch Widerspruch: Wäre ein $\alpha \in L$ nicht separabel, so gäbe es nach 7.8.9 für jedes N weniger als $[K(\alpha) : K]$ Ausdehnungen von $K \hookrightarrow N$ zu einer Einbettung $K(\alpha) \hookrightarrow N$ und damit nach Satz 7.8.15 über die maximal mögliche Zahl von Ausdehnungen notwendig auch weniger als $[L : K]$ Ausdehnungen von $K \hookrightarrow N$ zu einer Einbettung $L \hookrightarrow N$. □

Ergänzung 7.9.27 (**Die Diskriminante als Determinante**). Ich erkläre noch eine alternative Beschreibung der Diskriminante, deren Herleitung 7.9.14 verwendet. Ich behaupte genauer für die $a_i \in \mathbb{Z}['\zeta_1, \ldots, \zeta_n]$, die gegeben werden durch die Identität $T^n + a_1 T^{n-1} + \ldots + a_n = (T + \zeta_1) \ldots (T + \zeta_n)$, daß die Determinante der nebenstehenden Matrix M gegeben wird durch die Formel

$$\det M = \prod_{i \neq j} (\zeta_i - \zeta_j)$$

und folglich genau unsere Diskriminante aus 6.9.13 ist. Um das zu zeigen, beachten wir zunächst, daß beide Seiten symmetrische Polynome sind und daß zumindest in $\mathbb{Q}['\zeta_1, \ldots, \zeta_n]$ alle $(\zeta_i - \zeta_j)$ nach 7.9.14 und 2.4.5 und 6.10.10 das Polynom $(\det M)$ teilen. Dann aber wechselt der Ausdruck $(\det M)/(\zeta_i - \zeta_j)$ unter der Vertauschung von ζ_i und ζ_j sein Vorzeichen und muß nach 2.4.5 folglich ein weiteres Mal durch $(\zeta_i - \zeta_j)$ teilbar sein. Mithin ist $\det M$ in $\mathbb{Q}['\zeta_1, \ldots, \zeta_n]$ durch $\prod_{i \neq j}(\zeta_i - \zeta_j)$ teilbar. Sicher ergibt das Wegteilen ein symmetrisches Polynom, das höchstens auf den Hyperebenen $\zeta_i = \zeta_j$ verschwindet. Wäre dies Polynom nicht konstant, so könnten wir mit denselben Argumenten ein weiteres Mal einen Faktor $\prod_{i \neq j}(\zeta_i - \zeta_j)$ herausziehen. Das führt jedoch zu einem Widerspruch, wenn wir etwa erst durch $\zeta_1^{2(n-1)}$ teilen, für $\zeta_2, \ldots, \zeta_n$ paarweise verschiedene rationale Zahlen einsetzen, und $\zeta_1 \in \mathbb{Q}$ gegen ∞ streben lassen: $(\det M)/\zeta_1^{2(n-1)}$ bleibt dann nämlich beschränkt, wie wir sehen, indem wir alle Spalten außer der Ersten mit ζ_1^{-1} multiplizieren, und $(\prod_{i \neq j}(\zeta_i - \zeta_j))/\zeta_1^{2(n-1)}$ strebt gegen eine von Null verschiedene Zahl, aber $(\prod_{i \neq j}(\zeta_i - \zeta_j))^r/\zeta_1^{2(n-1)}$ strebt für $r \geq 2$ stets nach Unendlich. Es gilt also nur noch, die Konstante $c \in \mathbb{Q}$ zu bestimmen mit

$$\det M = c \prod_{i \neq j} (\zeta_i - \zeta_j)$$

Dazu setzen wir $\zeta_i = -\zeta^i$ mit ζ einer primitiven n-ten Einheitswurzel. Dann folgt $(T+\zeta_1)\ldots(T+\zeta_n) = T^n - 1$ und $(\det M) = n^n(-1)^{n-1}$ und andererseits

$$\prod_{i\neq j}(\zeta_i - \zeta_j) = \prod_{i=1}^{n}\left(\zeta^i \prod_{j\neq i}(1-\zeta^{j-i})\right)$$

Das Produkt aller n-ten Einheitswurzeln ist nun sicher $(-1)^{n-1}$ und das zweite Produkt kann berechnet werden als der Wert an der Stelle $t = 1$ des Polynoms $(t^n-1)/(t-1) = t^{n-1} + \ldots + t + 1$. So erhalten wir für die gesuchte Konstante c schließlich $(-1)^{n-1}n^n = (-1)^{n-1}n^n c$ und damit $c = 1$ wie gewünscht.

Übungen

Übung 7.9.28 (**Diskriminante eines Produkts**). Gegeben normierte Polynome f, g zeige man

$$\operatorname{Disk}(fg) = \operatorname{Disk}(f)\operatorname{Res}(f,g)\operatorname{Res}(g,f)\operatorname{Disk}(g)$$

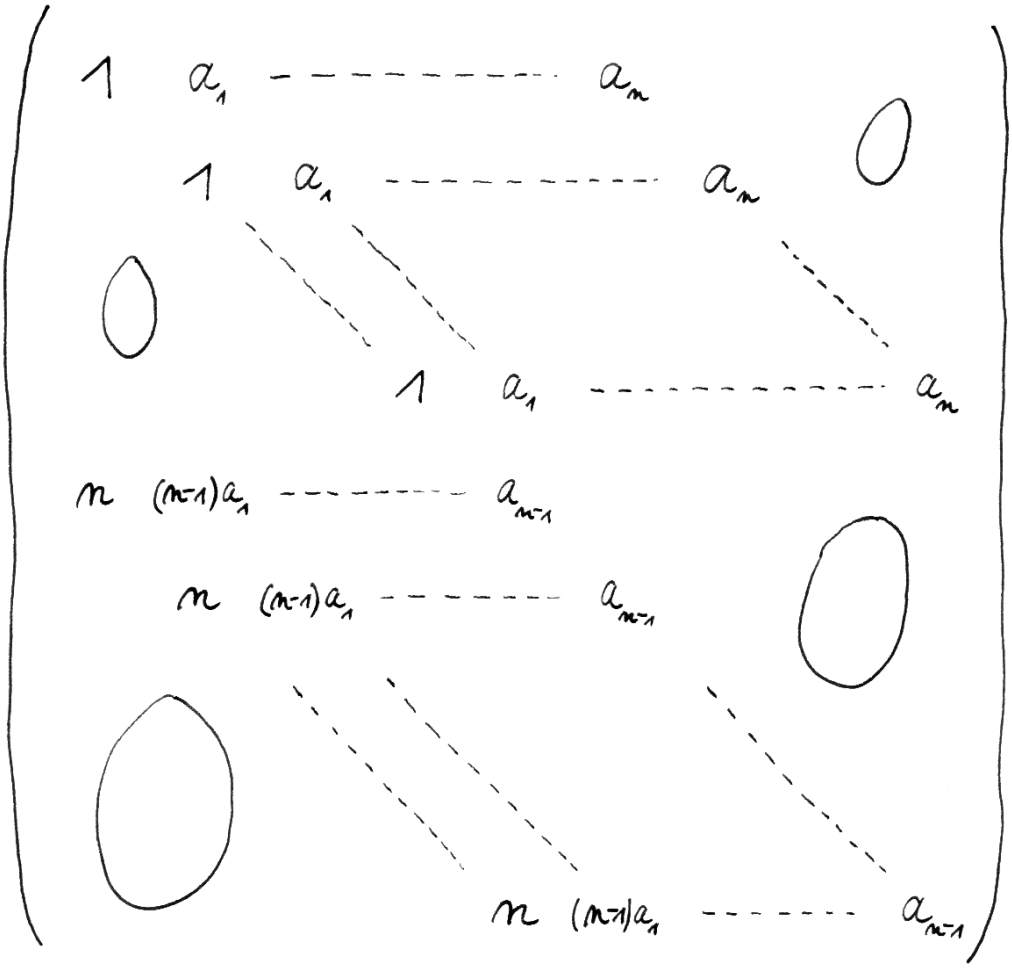
Übung 7.9.29. Man bestimme den normierten größtgradigen gemeinsamen Teiler der beiden Polynome $X^4 + X^3 - 2X^2 + 3X - 15$ und $X^3 - 6X^2 - 12X + 35$ in $\mathbb{Q}[X]$. Haben diese Polynome in einer Körperwerweiterung von $\mathbb{Q}$ eine gemeinsame Nullstelle?

Übung 7.9.30. Finden Sie alle komplexen mehrfachen Nullstellen des Polynoms $X^4 - 4X^3 + 5X^2 - 4X + 4$.

Übung 7.9.31. Man zeige nocheinmal mit Sonderbetrachtungen in kleiner Charakteristik, daß gegeben ein Körper k und $p, q \in k$ das Polynom $X^3 + pX + q$ genau dann nicht separabel ist, wenn gilt $27q^2 + 4p^3 = 0$.

Übung 7.9.32 (**Ableitung und logarithmische Ableitung von Reihen**). Gegeben ein Ring R erklärt man die formale Ableitung einer Laurentreihe $f = \sum a_n t^n \in R(\!(t)\!)$ durch $f' := \sum n a_n t^{n-1}$. Wieder zeige man Summenregel und Produktregel. Für $f \in 1 + tR[\![t]\!]$ und $\mathbb{Q} \subset R$ zeige man zusätzlich $(\log f)' = f'/f$ für $\log f$ wie in **??**.

Ergänzende Übung 7.9.33. Seien P, Q nicht konstante Polynome mit Koeffizienten in einem algebraisch abgeschlossenen Körper k der Charakteristik Null. Man zeige: Haben unsere beiden Polynome dieselben Nullstellen und dieselben „Einsstellen“, gelten also in Formeln für die zugehörigen Abbildungen $P, Q : k \to k$ die Gleichheiten $P^{-1}(0) = Q^{-1}(0)$ und $P^{-1}(1) = Q^{-1}(1)$ von Teilmengen von k, so folgt $P = Q$. Hinweis: Wäre $P \neq Q$, so wäre $P - Q$ ein von Null verschiedenes Polynom mit $|P^{-1}(1) \cup P^{-1}(0)|$ Nullstellen und folglich mindestens diesem Grad. Für d das Maximum der Grade unserer Polynome folgt $d \geq |P^{-1}(1) \cup P^{-1}(0)|$. Für P vom maximalen Grad folgt, daß P' mit Vielfachheiten gerechnet zu viele Nullstellen haben muß und deshalb Null ist.



Die Determinante dieser Matrix stimmt überein mit der Diskriminante des Polynoms $T^n + a_1 T^{n-1} + \ldots + a_n$, wie sie in 6.9.15 für jedes normierte Polynom erklärt wird. In der in 6.10.6 eingeführten Terminologie ist die Diskriminante eines normierten Polynoms f vom Grad n also genau die Resultante $\mathrm{Disk}_n(f) = \mathrm{Res}_{n,n-1}(f, f')$ unseres Polynoms mit seiner Ableitung. Das sei von nun ab auch unsere Definition der Diskriminante $\mathrm{Disk}_n(f)$ eines beliebigen Polynoms f vom Grad $\leq n$. Man kann, wie obige Formel zeigt, von diesem Polynom Disk_n sogar noch einen Faktor a_0 abspalten.

Übung 7.9.34. Ein Polynom mit Koeffizienten in einem Körper der Charakteristik Null ist separabel genau dann, wenn es von keinem Quadrat eines irreduziblen Polynoms geteilt wird.

Übung 7.9.35. Seien $M \supset L \supset K$ Körper. Ist M/L separabel und L/K separabel, so ist M/K separabel. Hinweis: Man ziehe sich zunächst auf den Fall endlicher Erweiterungen zurück und verwende dann 7.9.26, insbesondere $4 \Rightarrow 1$, mit N einer Vergrößerung von M zu einer normalen Erweiterung von K.

Ergänzende Übung 7.9.36. In jeder Körpererweiterung M/K gibt es unter allen Zwischenkörpern $L \subset M$, die separabel sind über K, einen größten. Er heißt der **separable Abschluß von** K **in** M. Hinweis: Man verwende 7.9.35.

Übung 7.9.37. Eine algebraische Körpererweiterung derart, daß nur die Elemente des kleinen Körpers über diesem separabel sind, heißt **rein inseparabel**. Man zeige, daß eine algebraische Erweiterung L/K eines Körpers K der Charakteristik p rein inseparabel ist genau dann, wenn für jedes Element von L die p^r-te Potenz für hinreichend großes r in K liegt. Salopp gesprochen sind also rein inseparable Erweiterungen genau die Erweiterungen, die durch die sukzessive Adjunktion p-ter Wurzeln in Charakteristik p entstehen. Hinweis: 7.9.17.

Ergänzende Übung 7.9.38. Man zeige: Ist M/K eine algebraische Körpererweiterung und $L \subset M$ der separable Abschluß von K in M, so ist die Körpererweiterung M/L rein inseparabel. Hinweis: Man verwende 7.9.35.

Vorschau 7.9.39. Man kann im Fall positiver Charakteristik $p > 0$ auch für jede Körpererweiterung L/K die Menge L_{i} aller Elemente von L betrachten, die unter wiederholtem Anwenden des Frobenius, also unter wiederholtem Bilden der p-ten Potenz irgendwann einmal in K landen. Dann ist L_{i} der größte über K rein inseparable algebraische Unterkörper von L. Auch wenn L/K algebraisch oder sogar endlich ist, muß hier L/L_{i} nicht separabel sein. Das gilt jedoch, wenn zusätzlich L/K eine normale algebraische Körpererweiterung ist, vergleiche 8.1.30.

Übung 7.9.40. Man zeige für jede rein inseparable algebraische Körpererweiterung L/K und jede weitere Körpererweiterung N/K die Abschätzung

$$|\mathrm{Kring}^K(L,N)| \leq 1$$

Ergänzende Übung 7.9.41. Gegeben eine algebraische Körpererweiterung L/K erklärt man ihren **Separabilitätsgrad** als $[L:K]_{\mathrm{s}} := [S:K]$ für $S \subset L$ den separablen Abschluß von K in L.

1. Gegeben eine endliche Körpererweiterung L/K zeige man

$$[L:K]_{\mathrm{s}} := \sup_{N/K} |\mathrm{Kring}^K(L,N)|$$

Das Supremum der Zahl möglicher Homomorphismen ist dabei über alle Körpererweiterungen N/K zu bilden und alle Werte in $\mathbb{N} \sqcup \{\infty\}$ sind erlaubt. Hinweis: 7.9.38 und 7.9.40.

2. Man zeige, daß der Separabilitätsgrad im Fall endlicher Körpererweiterungen multiplikativ ist, daß also für $M/L/K$ endliche Erweiterungen gilt

$$[M : K]_{\mathrm{s}} = [M : L]_{\mathrm{s}}[L : K]_{\mathrm{s}}$$

Die beiden Identitäten aus der vorhergehenden Übung gelten auch für beliebige algebraische Körpererweiterungen. Um das zu zeigen, muß man nur wissen, daß sich jeder Körper in einen algebraisch abgeschlossenen Körper einbetten läßt, und muß sich überlegen, daß für jede algebraische Körpererweiterung L/K und jede algebraisch abgeschlossene Körpererweiterung N/K gilt $[L : K]_{\mathrm{s}} = |\mathrm{Kring}^K(L, N)|$.

Übung 7.9.42 (**Rein inseparable Erweiterungen eines Funktionenkörpers**). Sei k ein vollkommener Körper positiver Charakteristik $p > 0$ und $L/k(T)$ eine endliche rein inseparable Erweiterung seines Funktionenkörpers. So ist unsere Körpererweiterung für genau ein $r \in \mathbb{N}$ zur Körpererweiterung $k(X)/k(T)$ gegeben durch $X \mapsto T^{p^r}$ isomorph. Hinweis: Man mag ohne Beschränkung der Allgemeinheit $[L : k(T)] = p$ annehmen. Dann überlegt man sich, daß in $k(\sqrt[p]{T})$ bereits alle Elemente von $k(T)$ eine p-te Wurzel haben.

Ergänzende Übung 7.9.43. Gegeben ein Körper k induzieren die Einbettungen $k[X] \hookrightarrow k[\![X]\!] \hookrightarrow k(\!(X)\!)$ einen Ringhomomorphismus und nach 2.5.5 eine Einbettung $k(X) \hookrightarrow k(\!(X)\!)$. Man zeige, daß im Fall $\mathrm{char}\, k = 0$ diese Einbettung für rationale Funktionen, die bei $X = 0$ keinen Pol haben, durch ein formales Analogon der Taylorformel beschrieben werden kann. Hierbei gilt es zunächst, die Ableitung eines Quotienten vermittels der Quotientenregel zu erklären.

7.10 Satz vom primitiven Element

Lemma 7.10.1 (Überdeckung durch affine Teilräume). *Ein affiner Raum über einem unendlichen Körper kann nicht durch endlich viele echte affine Teilräume überdeckt werden.*

Beweis. Wir argumentieren durch Widerspruch und gehen von einer Überdeckung durch möglichst wenige Teilräume aus. Wir finden also einen Punkt, der im ersten Teilraum liegt, aber nicht in den anderen, und einen weiteren Punkt, der im zweiten Teilraum liegt, aber nicht in den anderen. Eine Gerade durch diese beiden Punkte trifft jeden unserer Teilräume in höchstens einem Punkt, hat aber selbst unendlich viele Punkte. □

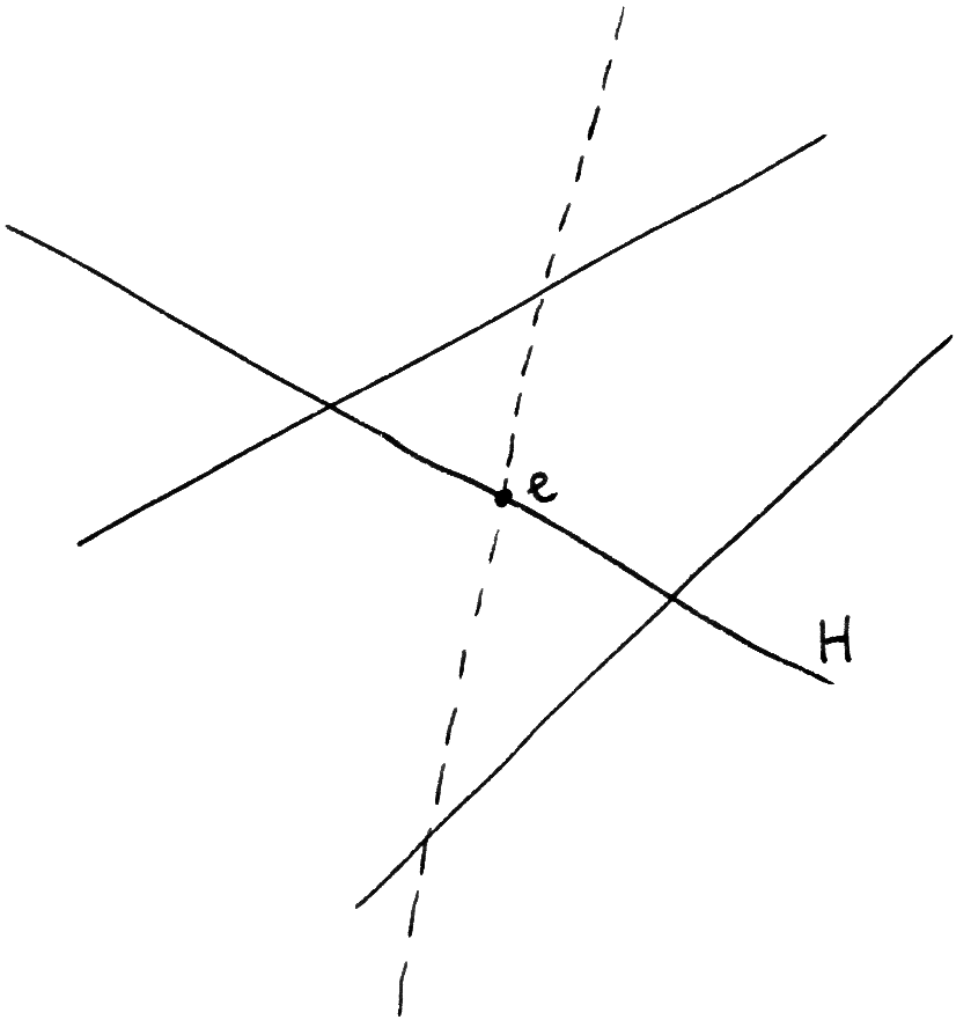


Illustration zum Beweis von 7.10.1

Lemma 7.10.2 (Überdeckung durch Untervektorräume). *Ein Vektorraum kann nicht durch endlich viele Untervektorräume von unendlicher Kodimension überdeckt werden.*

Beweis. Sei sonst $V = U_1 \cup \ldots \cup U_r$ ein Gegenbeispiel mit r kleinstmöglich. Natürlich gilt notwendig $r \geq 2$. Ganz allgemein liefern die offensichtlichen Abbildungen Isomorphismen $U_1/(U_1 \cap U_i) \xrightarrow{\sim} (U_1 + U_i)/U_i$. Wäre das für ein $i > 1$ ein endlichdimensionaler Raum, so hätte mit U_i auch $U_1 + U_i$ unendliche Kodimension in V und wir hätten ein noch kürzeres Gegenbeispiel gefunden. Das kann nicht sein, also haben alle $(U_1 \cap U_i)$ mit $i > 1$ unendliche Kodimension in U_1. Gegeben eine Ursprungsgerade $G \subset V$ haben dann auch alle $(G + U_1) \cap (G + U_i)$ mit $i > 1$ unendliche Kodimension in $G + U_1$ und können wegen der Minimalität unseres Gegenbeispiels $G + U_1$ nicht überdecken, in Formeln

$$G + U_1 \not\subset \bigcup_{i>1} (G + U_i)$$

Dann können sie aber auch für kein $g \in G$ die Nebenklasse $g + U_1$ überdecken und a forteriori liegt keine Nebenklasse $g + U_1$ in der Vereinigung der U_i mit $i > 1$. Wählen wir nun $g \notin U_1$, so kann mithin $g + U_1$ nicht in der Vereinigung der U_i mit $i \geq 1$ enthalten sein. □

7.10.3. Ein Vektorraum V einer Dimension ≥ 2 über einem endlichen Körper $\mathbb{F}$ kann durchaus durch endlich viele echte Untervektorräume überdeckt werden. In der Tat ist $\mathbb{F}^2$ die Vereinigung seiner endlich vielen Ursprungsgeraden L und $V = \mathbb{F}^2 \times W$ damit die Vereinigung seiner echten Teilräume $L \times W$.

Korollar 7.10.4 (Überdeckung durch Teilkörper). *Ein Körper kann nicht durch endlich viele echte Teilkörper überdeckt werden.*

Beweis im Fall von Charakteristik Null. Jeder Unterkörper ist in diesem Fall ein $\mathbb{Q}$-Untervektorraum. Die Behauptung folgt so aus Lemma 7.10.1, nach dem ein $\mathbb{Q}$-Vektorraum nicht durch endlich viele echte Untervektorräume überdeckt werden kann. □

Beweis im Fall eines endlichen Körpers. Ein endlicher Körper kann nicht durch echte Teilkörper überdeckt werden, da seine multiplikative Gruppe nach 3.4.17 zyklisch ist. □

Beweis im Fall eines unendlichen Körpers in positiver Charakteristik. Jeder echte Teilkörper eines unendlichen Körpers ist entweder unendlich oder endlich und hat in beiden Fällen als Untervektorraum in Bezug auf den Primkörper unendliche Kodimension. Die Behauptung folgt so aus Lemma 7.10.2, nach dem ein Vektorraum nicht durch endlich viele Untervektorräume von unendlicher Kodimension überdeckt werden kann. □

Proposition 7.10.5 (Unterscheidung von Körperhomomorphismen). *Gegeben Körpererweiterungen L/K und M/K desselben Grundkörpers K und endlich viele paarweise verschiedene Homomorphismen $\sigma_1, \ldots, \sigma_r \in \mathrm{Kring}^K(L, M)$ von Körpererweiterungen gibt es stets ein Element $\alpha \in L$, dessen Bilder $\sigma_i(\alpha)$ unter unseren Körperhomomorphismen paarweise verschieden sind.*

Beweis. Sicher ist $L_{ij} := \{\beta \in L \mid \sigma_i(\beta) = \sigma_j(\beta)\}$ stets ein Teilkörper von L und für $i \neq j$ ist L_{ij} sogar ein echter Teilkörper von L. Da ein Körper nach 7.10.4 nicht durch endlich viele echte Teilkörper überdeckt werden kann, gibt es stets ein $\alpha \in L \setminus \bigcup_{i \neq j} L_{ij}$. □

Korollar 7.10.6 (Teilkörper und Primitivität). *Eine Körpererweiterung ist genau dann endlich und primitiv, wenn sie nur endlich viele Zwischenkörper zuläßt.*

Beweis. Läßt eine Körpererweiterung L/K nur endlich viele Zwischenkörper zu, so kann sie von ihren echten Zwischenkörpern nach 7.10.4 nicht überdeckt werden. Also gibt es ein $\alpha \in L$, das in keinem echten Zwischenkörper liegt. Dann gilt notwendig $L = K(\alpha)$ und es ist leicht zu sehen, daß α nicht transzendent sein kann. Ist umgekehrt $L = K(\alpha)$ eine primitive endliche Körpererweiterung, so betrachten wir die Abbildung

$$\begin{array}{ccc} \left\{ \begin{array}{c} \text{Zwischenkörper } M, \\ K \subset M \subset K(\alpha) \end{array} \right\} & \to & \left\{ \begin{array}{c} \text{Normierte Teiler in } L[X] \\ \text{des Minimalpolynoms } \mathrm{Irr}(\alpha, K) \end{array} \right\} \\ M & \mapsto & \mathrm{Irr}(\alpha, M) \end{array}$$

Es reicht zu zeigen, daß sie injektiv ist. In der Tat wird aber M über K bereits von den Koeffizienten des Minimalpolynoms $\mathrm{Irr}(\alpha, M)$ erzeugt, denn für den von diesen Koeffizienten über K erzeugten Teilkörper $M' \subset M$ gilt $[L : M'] = \mathrm{grad}(\mathrm{Irr}(\alpha, M)) = [L : M]$. Da jedes Polynom nur endliche viele normierte Teiler besitzt, folgt die Behauptung. □

Satz 7.10.7 (vom primitiven Element). *Ist L/K eine endliche separable Körpererweiterung, so gibt es ein Element $\alpha \in L$ mit $L = K(\alpha)$.*

Beweis. Nach 7.8.25 können wir L vergrößern zu einer normalen Erweiterung N von K. Wegen der Separabilität von L/K gibt es dann nach 7.9.26 genau $[L : K]$ Körperhomomorphismen über K von L nach N, in Formeln

$$|\mathrm{Kring}^K(L, N)| = [L : K]$$

Nach 7.10.5 gibt es Elemente $\alpha \in L$ derart, daß die $\sigma(\alpha)$ für $\sigma \in \mathrm{Kring}^K(L, N)$ paarweise verschieden sind. Gegeben solch ein α liefert die Restriktion eine Injektion $\mathrm{Kring}^K(L, N) \hookrightarrow \mathrm{Kring}^K(K(\alpha), N)$, denn verschiedene $\sigma \neq \tau$ links bilden

auch schon unser α auf verschiedene Elemente von N ab. Die Identität $L = K(\alpha)$ folgt dann unmittelbar aus der Kette von Gleichungen und Ungleichungen

$$[L:K] = |\mathrm{Kring}^K(L,N)| \leq |\mathrm{Kring}^K(K(\alpha),N)| \leq [K(\alpha):K] \leq [L:K] \quad \square$$

Lemma* 7.10.8 (Überdeckung durch Nebenklassen). *Eine abelsche Gruppe kann nicht durch endlich viele Nebenklassen zu Untergruppen von unendlichem Index überdeckt werden.*

Ergänzung 7.10.9. Dies Lemma ist eine gemeinsame Verallgemeinerung unserer beiden Lemmata 7.10.1 und 7.10.2 vom Beginn dieses Abschnitts, aber abgesehen davon für uns nicht von Belang. Noch stärker gilt sogar: Eine Überdeckung einer Gruppe durch endlich viele Linksnebenklassen bleibt eine Überdeckung, wenn wir daraus alle Linksnebenklassen zu Untergruppen von unendlichem Index weglassen. Diese Aussage wird als **Neumann's Lemma** zitiert. Bernhard Neumann studierte in den dreißiger Jahren Mathematik in Freiburg und Berlin. Die Machtübernahme durch die Nationalsozialisten trieb ihn in die Emigration.

Beweis. Wir argumentieren durch Widerspruch und gehen von einem Gegenbeispiel einer Überdeckung durch möglichst wenige Nebenklassen aus. Bezeichne bei so einem Gegenbeispiel G unsere abelsche Gruppe und $H_0, H_1, \ldots, H_n \subset G$ unsere überdeckenden Nebenklassen. Die zugehörigen Untergruppen notieren wir $\vec{H}_0, \vec{H}_1, \ldots, \vec{H}_n$. Für alle i dürfen wir $|(\vec{H}_0 + \vec{H}_i)/\vec{H}_i| \in \{1, \infty\}$ annehmen, indem wir andernfalls für alle i mit $|(\vec{H}_0 + \vec{H}_i)/\vec{H}_i| < \infty$ die Nebenklasse H_i von $\vec{H}_i$ zur Nebenklasse $\vec{H}_0 + H_i$ von $\vec{H}_0 + \vec{H}_i$ vergrößern und beachten, daß die Untergruppe $\vec{H}_0 + \vec{H}_i$ in diesem Fall immer noch unendlichen Index in G hat. Weiter können unsere Nebenklassen nicht alle Nebenklassen unter derselben Untergruppe sein, wir dürfen also $\vec{H}_0 \not\subset \vec{H}_1$ annehmen. Da wir von einem kleinsten Gegenbeispiel ausgegangen waren, finden wir $g \in H_1 \setminus \bigcup_{i\neq 1} H_i$. Wegen $g \notin H_0$ gilt $g + \vec{H}_0 \subset H_1 \cup H_2 \cup \ldots \cup H_n$ alias

$$\vec{H}_0 \subset \bigcup_{i=1}^{n} \Big((H_i - g) \cap \vec{H}_0 \Big)$$

Hier sind aber die $(H_i - g) \cap \vec{H}_0$ entweder leer oder Nebenklassen unter $\vec{H}_i \cap \vec{H}_0$, das wegen $|(\vec{H}_0 + \vec{H}_i)/\vec{H}_i| = |\vec{H}_0/(\vec{H}_i \cap \vec{H}_0)| \in \{1, \infty\}$ jeweils entweder ganz $\vec{H}_0$ ist oder eine Untergruppe von unendlichem Index. Ersteres kann nicht passieren, da $g + \vec{H}_0$ in keinem der H_i enthalten ist. Wir hätten also ein noch kürzeres Gegenbeispiel konstruiert. Dieser Widerspruch zeigt das Lemma. $\square$

7.11 Algebraischer Abschluß*

7.11.1. In der Literatur ist es üblich, sich bei der Entwicklung der Körpertheorie stark auf den Satz von der Existenz eines algebraischen Abschlusses zu stützen. Das hat meines Erachtens den Nachteil, daß der Beweis dieses Satzes eher mengentheoretischer Natur ist und zu den anderen Themen der Vorlesung nicht recht passen will. Um die Entwicklung der Grundlagen der Algebra von den Schwierigkeiten bei der Formalisierung der Mengenlehre zu entlasten, entwickle ich in diesem Text die Grundzüge der Körpertheorie unabhängig vom Satz über die Existenz eines algebraischen Abschlusses. Ich diskutiere den Satz und seinen Beweis hier nur, damit weiterführende Vorlesungen darauf zurückgreifen können. Der folgende Abschnitt ist also für die weitere Entwicklung dieser Vorlesung unerheblich und kann ohne Schaden übersprungen werden.

7.11.2. Ich erinnere daran, daß eine Körpererweiterung nach 7.8.18 algebraisch heißt, wenn alle Elemente der Erweiterung algebraisch sind über dem Grundkörper. Ich erinnere daran, daß eine Körpererweiterung L/K körperendlich heißt, wenn der Erweiterungskörper über dem Grundkörper als Körper endlich erzeugt ist.

Satz 7.11.3 (über algebraische Körpererweiterungen). *1. Jede körperendliche algebraische Körpererweiterung ist endlich;*

2. *Sei L/K eine Körpererweiterung. Diejenigen Elemente von L, die algebraisch sind über K, bilden einen Unterkörper von L;*

3. *Seien $M \supset L \supset K$ Körper. Ist M algebraisch über L und L algebraisch über K, so ist M algebraisch über K.*

Beweis. 1. Sei $L = K(\alpha_1, \ldots, \alpha_n)$. Sind alle α_i algebraisch über K, so sind sie erst recht algebraisch über $K(\alpha_1, \ldots, \alpha_{i-1})$. Wir betrachten die Körperkette

$$K \subset K(\alpha_1) \subset K(\alpha_1, \alpha_2) \subset \ldots \subset K(\alpha_1, \ldots, \alpha_n) = L$$

Da hier alle Schritte endlich sind nach 7.4.7, ist auch L/K endlich nach 7.4.11.

2. Sind α und $\beta \in L$ algebraisch über K, so haben wir $[K(\alpha, \beta) : K] < \infty$ nach Teil 1. Mithin sind alle Elemente von $K(\alpha, \beta)$ algebraisch über K nach 7.4.7.

3. Für $\alpha \in M$ betrachten wir die Koeffizienten $\beta_0, \ldots, \beta_r \in L$ seines Minimalpolynoms über L. Dann ist α sogar algebraisch über $K(\beta_0, \ldots, \beta_r)$. Der Turm von endlichen Körpererweiterungen

$$K \subset K(\beta_0, \ldots, \beta_r) \subset K(\beta_0, \ldots, \beta_r, \alpha)$$

zeigt damit, daß α algebraisch ist über K. □

Definition 7.11.4. Ein **algebraischer Abschluß** eines Körpers ist eine algebraische Erweiterung durch einen algebraisch abgeschlossenen Körper.

Satz 7.11.5 (über den algebraischen Abschluß). *Jeder Körper besitzt einen algebraischen Abschluß und dieser algebraische Abschluß ist eindeutig bis auf im allgemeinen nicht eindeutigen Isomorphismus von Körpererweiterungen.*

7.11.6. Wegen dieser partiellen Eindeutigkeit erlaubt man sich meist den bestimmten Artikel und eine Notation und spricht von *dem* algebraischen Abschluß eines Körpers K und notiert ihn

$$\bar{K}$$

Ein algebraischer Abschluß von $\mathbb{R}$ wäre etwa der Körper $\mathbb{C}$, wie wir ihn in **??** als Teilring des Rings der reellen (2×2)-Matrizen eingeführt haben, mit der dort konstruierten Einbettung von $\mathbb{R}$. Ein weiterer algebraischer Abschluß wäre der wie in **??** zu $K = \mathbb{R}$ durch das explizite Erklären einer Multiplikation auf $\mathbb{R}^2$ konstruierte Körper, wieder mit der dort konstruierten Einbettung von $\mathbb{R}$. Sicher sind diese beiden Körpererweiterungen von $\mathbb{R}$ isomorph, aber es gibt zwischen ihnen sogar genau zwei Isomorphismen, von denen keiner „besser“ ist als der andere.

7.11.7. Die größte separable Teilerweiterung in einem algebraischen Abschluß eines Körpers nennt man seinen **separablen Abschluß**.

Beweis. Gegeben ein Körper K konstruiert man ohne Schwierigkeiten eine Einbettung $K \hookrightarrow \Omega$ in eine Menge Ω derart, daß es für keine algebraische Erweiterung von K eine surjektive Abbildung nach Ω gibt. Die Menge $\Omega = \mathcal{P}(K[X] \times \mathbb{N})$ wäre etwa eine Möglichkeit: Jedes Element einer algebraischen Erweiterung L von K ist ja eine von endlich vielen Nullstellen eines Polynoms aus $K[X]$, so daß wir unter Zuhilfenahme des Auswahlaxioms eine injektive Abbildung $L \hookrightarrow K[X] \times \mathbb{N}$ finden können. Die Existenz einer Surjektion $L \twoheadrightarrow \Omega$ stünde damit im Widerspruch zu **??**, wonach es keine Surjektion $K[X] \times \mathbb{N} \twoheadrightarrow \mathcal{P}(K[X] \times \mathbb{N})$ geben kann. Jetzt betrachte man die Menge aller Tripel (M, s, φ) bestehend aus einer Teilmenge $M \subset \Omega$, einer Struktur s eines Körpers darauf und einem Köperhomomorphismus $\varphi : K \to M$, bezüglich dessen M algebraisch ist über K. Nach dem Zorn'schen Lemma **??** existiert bezüglich der offensichtlichen Teilordnung ein maximales derartiges Tripel, und bei solch einem maximalen Tripel ist M notwendig algebraisch abgeschlossen: Sonst könnten wir nämlich mit der Kronecker-Konstruktion 7.7.6 eine endliche Erweiterung L/M von M finden und die Einbettung $M \hookrightarrow \Omega$ zu einer Einbettung von Mengen $L \hookrightarrow \Omega$ ausdehnen – hier verwenden wir implizit nocheinmal das Zorn'sche Lemma, nach dem es eine maximale Ausdehnung auf eine Teilmenge von L geben muß, die aber nicht surjektiv sein kann und deshalb bereits auf ganz L definiert sein muß. So erhielten wir ein noch größeres Tripel und dieser Widerspruch zeigt die Existenz. Seien

nun $K \hookrightarrow \bar{K}$ und $K \hookrightarrow E$ zwei algebraische Abschlüsse von K. Nach Proposition 7.11.9 über Ausdehnungen von Körpereinbettungen, die wir im Anschluß beweisen, läßt sich die Identität auf K fortsetzen zu einem Körperhomomorphismus $\varphi : \bar{K} \to E$. Er ist wie jeder Körperhomomorphismus injektiv und liefert für jedes Polynom $P \in K[X]$ eine Bijektion zwischen den Nullstellen von P in $\bar{K}$ und den Nullstellen von P in E. Folglich muß er auch surjektiv sein. □

Alternativer Beweis für die Existenz eines algebraischen Abschlusses. Dieser Beweis basiert auf Grundkenntnissen über maximale Ideale, die in dieser Vorlesung nicht behandelt wurden, genauer auf **??** und **??**. Sei K unser Körper. Wir betrachten die Menge $S = K[X]\backslash K$ aller nicht konstanten Polynome mit Koeffizienten in K und bilden den riesigen Polynomring

$$R = K[X_f]_{f \in S}$$

Hier gibt es also für jedes nichtkonstante Polynom f aus $K[X]$ eine eigene Variable X_f. In diesem riesigen Polynomring betrachten wir das Ideal $\mathfrak{a} \subset R$, das von allen $f(X_f)$ erzeugt wird, und zeigen $\mathfrak{a} \neq R$. Sonst könnten wir nämlich $1 \in R$ schreiben als eine endliche Summe

$$1 = \sum_{f \in E} g_f f(X_f)$$

für $E \subset S$ endlich und geeignete $g_f \in R$. Nun gibt es nach 7.7.4, angewandt auf das Produkt der f aus E, eine Körpererweiterung L von K derart, daß alle f aus E in L eine Nullstelle $\alpha_f \in L$ haben. Für die übrigen $f \in S$ wählen wir Elemente $\alpha_f \in L$ beliebig und betrachten den Einsetzungshomomorphismus

$$\begin{array}{rccc} \varphi : & R & \to & L \\ & X_f & \mapsto & \alpha_f \end{array}$$

Dieser Ringhomomorphismus müßte nun die Eins in R auf die Null in L abbilden und das kann nicht sein. Folglich gilt $\mathfrak{a} \neq R$ und es gibt nach **??**, bei dessen Beweis das Zorn'sche Lemma eingeht, ein maximales Ideal $\mathfrak{m} \supset \mathfrak{a}$. Dann ist $K_1 = R/\mathfrak{m}$ nach **??** ein Körper und jedes nichtkonstante Polynom $f \in K[X]\backslash K$ hat eine Nullstelle in K_1, nämlich die Nebenklasse von X_f. Iterieren wir diese Konstruktion, so erhalten wir ein Kette von Körpern

$$K = K_0 \hookrightarrow K_1 \hookrightarrow K_2 \hookrightarrow \ldots$$

derart, daß jedes nichtkonstante Polynom mit Koeffizienten in K_i eine Nullstelle hat in K_{i+1}. Die aufsteigende Vereinigung $\bigcup_{i=0}^{\infty} K_i$ ist dann ein algebraisch abgeschlossener Körper, der K enthält. □

Ergänzung 7.11.8. Eigentlich hatte ich versprochen, beliebige Vereinigungen nur zu bilden von Systemen von Teilmengen einer bereits anderweitig bekannten Menge, und recht eigentlich müssen unsere Inklusionen auch keine Einbettungen von Teilmengen sein. Wenn Sie es so genau nehmen, muß ich daran erinnern, daß wir disjunkte Vereinigungen von beliebigen Familien von Mengen erlaubt hatten. Dann kann ich mich darauf zurückziehen, daß hier eigentlich der Quotient der disjunkten Vereinigung $\bigsqcup_{i=0}^{\infty} K_i$ nach derjenigen Äquivalenzrelation gemeint sein soll, die erzeugt wird durch die Bedingung, daß für alle i jedes $x \in K_i$ äquivalent sein soll zu seinem Bild in K_{i+1}. Formal ist diese Konstruktion ein Spezialfall der allgemeinen Konstruktion eines „Kolimes in der Kategorie der Mengen“, wie Sie ihn in **??** in voller Allgemeinheit kennenlernen können.

Proposition 7.11.9 (**Ausdehnung von Körpereinbettungen**). *Eine Einbettung eines Körpers in einen algebraisch abgeschlossenen Körper läßt sich auf jede algebraische Erweiterung unseres ursprünglichen Körpers ausdehnen.*

7.11.10. Ist also in Formeln $K \hookrightarrow L$ eine algebraische Körpererweiterung, so läßt sich jede Einbettung $K \hookrightarrow F$ von K in einen algebraisch abgeschlossenen Körper F ausdehnen zu einer Einbettung $L \hookrightarrow F$. Es reicht hier sogar, wenn wir von F nur fordern, daß die Minimalpolynome $\operatorname{Irr}(\alpha, K)$ aller Elemente α irgendeines Erzeugendensystems von L über K vollständig in Linearfaktoren zerfallen, sobald wir sie als Polynome in $F[X]$ betrachten.

Beweis. Ohne Beschränkung der Allgemeinheit dürfen wir $K \subset L$ annehmen. Nach dem Zorn'schen Lemma gibt es unter allen Zwischenkörpern M mit $K \subset M \subset L$, auf die sich unsere Einbettung $K \hookrightarrow F$ fortsetzen läßt, mindestens einen Maximalen. Ich behaupte $M = L$. Sonst gäbe es nämlich $\alpha \in L \backslash M$, und dies α wäre algebraisch über M, mit Minimalpolynom $f \in M[X]$. Die Minimalpolynom hätte eine Nullstelle $\beta \in F$, und nach Proposition 7.8.9 über das Ausdehnen auf primitive Erweiterungen könnten wir dann $M \hookrightarrow F$ fortsetzen zu einer Einbettung $M(\alpha) \to F$ durch $\alpha \mapsto \beta$ im Widerspruch zur Maximalität von M. □

7.11.11. Der algebraische Abschluß des Körpers $\mathbb{Q}$ der rationalen Zahlen ist abzählbar nach 7.8.26.

Beispiel 7.11.12 (**Algebraischer Abschluß endlicher Körper**). Einen algebraischen Abschluß eines endlichen Primkörpers $\mathbb{F}_p$ können wir wie folgt konstruieren: Wir wählen eine Folge $r(0), r(1), \ldots$ von natürlichen Zahlen so, daß jeweils gilt $r(i) | r(i+1)$ und daß jede natürliche Zahl eines unserer Folgenglieder teilt. Dann gibt es nach 7.7.12 Einbettungen $\mathbb{F}_{p^{r(i)}} \hookrightarrow \mathbb{F}_{p^{r(i+1)}}$. Wir wählen nun jeweils eine derartige Einbettung und bilden mit ihrer Hilfe die aufsteigende Vereinigung

$$\bar{\mathbb{F}}_p = \bigcup_{i=0}^{\infty} \mathbb{F}_{p^{r(i)}}$$

Das ist dann offensichtlich ein algebraischer Abschluß von $\mathbb{F}_p$. Wie diese aufsteigende Vereinigung ganz genau zu verstehen ist, hatte ich bereits zu Ende des alternativen Beweises für die Existenz eines algebraischen Abschlusses 7.11.5 erläutert. Der Nachweis, daß wir so in der Tat einen algebraischen Abschluß von $\mathbb{F}_p$ erhalten, ist nicht schwer und bleibe dem Leser überlassen.

7.11.13. Ich erinnere an dem Körper $\mathbb{C}(\!(t)\!)$ der formalen Laurentreihen mit komplexen Koeffizienten aus 2.3.43.

Satz 7.11.14 (Algebraischer Abschluß des Laurentreihenkörpers). *Der in hoffentlich offensichtlicher Weise präzise zu definierende Körper*

$$\bigcup_{\gamma\in\mathbb{N}_{\geq 1}} \mathbb{C}(\!(t^{1/\gamma})\!)$$

der **Puiseux-Reihen mit komplexen Koeffizienten** *ist algebraisch abgeschlossen und damit der algebraische Abschluß des Körpers der formalen Laurentreihen* $\mathbb{C}(\!(t)\!) = \operatorname{Quot}\mathbb{C}[\![t]\!]$.

7.11.15. Analoges gilt, wenn wir $\mathbb{C}$ durch einen beliebigen algebraisch abgeschlossenen Körper der Charakteristik Null ersetzen.

Beweis. Das folgt sofort aus dem im Anschluß bewiesenen Lemma 7.11.17. □

7.11.16. Die obige Konstruktion kann auch für einen beliebigen Koeffizientenring k durchgeführt werden. Wir erhalten so den **Ring der Puiseux-Reihen mit Koeffizienten in** k. Für eine formal befriedigende Definition mag man sich auf das allgemeine Konzept eines „Kolimes“ aus **??** stützen.

Lemma 7.11.17 (Nullstellen von Polynomen in Laurentreihen). *Seien $k = \bar{k}$ ein algebraisch abgeschlossener Körper, $P \in k[\![t]\!][X]$ ein Polynom mit Koeffizienten im Potenzreihenring über k, und $\lambda \in k$ eine n-fache Nullstelle von seinem Bild $\bar{P} \in k[X]$. Wird n nicht von der Charakteristik unseres Körpers geteilt, so besitzt P für geeignetes γ mit $1 \leq \gamma \leq n$ eine Nullstelle in $\lambda + t^{1/\gamma}k[\![t^{1/\gamma}]\!]$.*

7.11.18. Wir erlauben hier nur Nullstellen endlicher Ordnung und machen insbesondere keine Aussage für den Fall, daß $\bar{P} \in k[X]$ das Nullpolynom ist. Mit dem Symbol $k[\![t^{1/\gamma}]\!]$ ist der Ring $k[\![s]\!]$ gemeint mit seiner durch $t \mapsto s^\gamma$ gegebenen Einbettung von $k[\![t]\!]$. Ich bin verblüfft, daß mir der Beweis auch für nicht notwendig normiertes P zu gelingen scheint.

Beweis. Indem wir X durch $X + \lambda$ substituieren, dürfen wir ohne Beschränkung der Allgemeinheit $\lambda = 0$ annehmen. Nach unseren Annahmen hat P dann die Gestalt

$$P(X) = a_0 + a_1X + \ldots + a_nX^n + \ldots + a_NX^N$$

mit $a_0, \ldots, a_{n-1} \in tk[\![t]\!]$ und $a_n \in k^\times + tk[\![t]\!]$. Wir verwenden nun die Bewertung $v : k[\![t]\!] \to \mathbb{N} \sqcup \{\infty\}$, die jeder Potenzreihe a den Grad ihres Terms niedrigster Ordnung $v(a) := \sup\{\nu \mid t^\nu | a\}$ zuordnet. Im Spezialfall $v(a_0) = 1$ alias $a_0 \in k^\times t + t^2 k[\![t]\!]$ führt für unsere Nullstelle der Ansatz

$$\mu_1 t^{1/n} + \mu_2 t^{2/n} + \ldots$$

mit $\mu_i \in k$ zum Ziel. Ist etwa $a_0 \in \tilde{a}_0 t + t^2 k[\![t]\!]$ und $a_n \in \tilde{a}_n + tk[\![t]\!]$, so erhalten wir die Gleichung $\tilde{a}_0 + \tilde{a}_n \mu_1^n = 0$ und können dazu eine Lösung μ_1 finden, die notwendig verschieden ist von Null. Dann erhalten wir leicht induktiv eines unserer μ_i aus den Vorhergehenden: Der wesentliche Punkt ist dabei, daß in einer Entwicklung

$$(\mu_1 t^{1/n} + h)^n = \mu_. t + (n\mu_1^{n-1} t^{(n-1)/n})h + \ldots$$

der Koeffizient des linearen Terms nicht Null ist. Im etwas allgemeineren Fall, daß für das kleinste $k < n$ mit $a_k \neq 0$ auch die Bewertung $b := v(a_k)$ minimal ist unter den Bewertungen der Koeffizienten $v(a_0), \ldots, v(a_{n-1})$, müssen wir „in erster Näherung“ eine Lösung der Gleichung $\tilde{a}_k t^b X^k + \tilde{a}_n X^n = 0$ finden, mit der Notation $\tilde{a} \in k^\times$ für den Koeffizienten der t-Potenz niedrigsten Grades in $a \in k[\![t]\!] \backslash 0$. Solch eine Lösung finden wir in der Form $\mu_1 t^\alpha$ mit $\alpha = b/(n-k)$, und wir finden sogar eine von Null verschiedene Lösung mit $\mu_1 \in k^\times$. Dann führt ähnlich der Ansatz

$$\mu_1 t^\alpha + \mu_2 t^{\alpha + 1/(n-k)} + \mu_3 t^{\alpha + 2/(n-k)} + \ldots$$

für eine Nullstelle mit $\mu_2, \mu_3, \ldots \in k$ zum Erfolg. Um schließlich unser Problem in voller Allgemeinheit zu lösen, dürfen wir ohne Beschränkung der Allgemeinheit $a_0 \neq 0$ annehmen, da ja sonst die Null von $k[\![t]\!]$ bereits eine Lösung ist. Dann suchen wir das Minimum α der $v(a_k)/(n-k)$ mit $0 \leq k < n$, es werde etwa an den Stellen $i, j, \ldots, l$ angenommen, und müssen „in erster Näherung“ eine Lösung der Gleichung

$$\tilde{a}_i t^{v(a_i)} X^i + \tilde{a}_j t^{v(a_j)} X^j + \ldots + \tilde{a}_l t^{v(a_l)} X^l + \tilde{a}_n X^n = 0$$

finden. Wegen $v(a_i) + i\alpha = v(a_j) + j\alpha = \ldots = v(a_l) + l\alpha = n\alpha$ finden wir mit dem Ansatz $X = \mu_1 t^\alpha$ eine Lösung dieser Gleichung, und zwar sogar eine Lösung mit $\mu_1 \in k^\times$. Ist nun γ der Nenner von α in seiner maximal gekürzten Darstellung, so führt wieder der Ansatz

$$\mu_1 t^\alpha + \mu_2 t^{\alpha + 1/\gamma} + \mu_3 t^{\alpha + 2/\gamma} + \ldots$$

und induktiv zu bestimmenden $\mu_2, \mu_3, \ldots \in k$ zum Erfolg. □

Definition 7.11.19. Seien K ein Körper und $\mathcal{P} \subset K[X]\backslash 0$ ein Menge von von Null verschiedenen Polynomen. Unter einem **Zerfällungskörper von** $\mathcal{P}$ verstehen wir eine Körpererweiterung L/K derart, daß (1) jedes Polynom $P \in \mathcal{P}$ in $L[X]$ vollständig in Linearfaktoren zerfällt und daß (2) der Körper L über K erzeugt wird von den Nullstellen der Polynome $P \in \mathcal{P}$.

Übungen

Ergänzende Übung 7.11.20. Man zeige, daß eine Körpererweiterung L/K normal ist genau dann, wenn sie der Zerfällungskörper einer Menge von Polynomen $\mathcal{P} \subset K[X]\backslash 0$ ist. Hinweis: Man kopiere den Beweis von 7.8.23. Bei Punkt 3 dort reicht es, für M einen algebraischen Abschluß von K zu betrachten.

Übung 7.11.21. Gegeben ein endlicher Körper ist die multiplikative Gruppe seines algebraischen Abschlusses in unkanonischer Weise isomorph zur Gruppe aller Elemente von $\mathbb{Q}/\mathbb{Z}$, deren Ordnung teilerfremd ist zur Charakteristik unseres Körpers.

Übung 7.11.22. Ist L/K eine Körpererweiterung durch einen algebraisch abgeschlossenen Körper, so bilden die über K algebraischen Elemente von L einen algebraischen Abschluß von K.

Übung 7.11.23. Sei L/K eine Körpererweiterung durch einen algebraisch abgeschlossenen Körper. Man zeige, daß jede normale Körpererweiterung von K als Körpererweiterung von K isomorph ist zu genau einem Unterkörper $M \subset L$ mit $M \supset K$.

Übung 7.11.24. Unter der **normalen Hülle** einer Körpererweiterung L/K versteht man eine Körpererweiterung N/L derart, daß N/K normal ist und daß es für jede weitere Körpererweiterung N_1/L mit dieser Eigenschaft einen Körperhomomorphismus $N \to N_1$ über K gibt. Man zeige, daß jede algebraische Körpererweiterung eine normale Hülle besitzt, und daß jeder Homomorphismus über K zwischen zwei normalen Hüllen ein Isomorphismus sein muß. Das rechtfertigt dann zu einem gewissen Maße den bestimmten Artikel.

7.12 Schiefkörper über den reellen Zahlen*

7.12.1. Der Inhalt des folgenden Abschnitts ist für die weitere Entwicklung dieser Vorlesung nicht von Belang. Die Thematik schien mir jedoch zu interessant, um sie ganz auszulassen. Anwendungen ergeben sich insbesondere in der Darstellungstheorie endlicher Gruppen und allgemeiner in der abstrakten Theorie nicht notwendig kommutativer Ringe, in der Schiefkörper eine wichtige Rolle spielen. Unter einem Schiefkörper verstehen wir wie in **??** einen Ring R, der nicht der Nullring ist, und in dem alle von Null verschiedenen Elemente Einheiten sind.

Proposition 7.12.2 (Schiefkörper über den reellen Zahlen). *Jede endlichdimensionale $\mathbb{R}$-Ringalgebra, die ein Schiefkörper ist, ist als $\mathbb{R}$-Ringalgebra isomorph zu $\mathbb{R}$, $\mathbb{C}$, oder zum Schiefkörper $\mathbb{H}$ der Quaternionen aus 2.6.4.*

Ergänzung 7.12.3. Statt endlicher Dimension über $\mathbb{R}$ brauchen wir sogar nur anzunehmen, daß unsere Ringalgebra als $\mathbb{R}$-Vektorraum abzählbar erzeugt ist. Derselbe Beweis funktioniert, da wir etwa nach 7.3.12 wissen, daß auch jede Erweiterung abzählbarer Dimension von $\mathbb{R}$ bereits algebraisch ist.

Beweis. Sei K unsere $\mathbb{R}$-Ringalgebra. Die Struktur als $\mathbb{R}$-Ringalgebra liefert uns einen eindeutig bestimmten Homomorphismus von $\mathbb{R}$-Ringalgebren $\mathbb{R} \to K$, der wegen $K \neq 0$ sogar injektiv sein muß. Wir fassen ihn von nun an zur Vereinfachung der Notation als die Inklusion einer Teilmenge $\mathbb{R} \subset K$ auf. Gegeben $\alpha \in K \backslash \mathbb{R}$ können wir unsere Einbettung $\mathbb{R} \hookrightarrow K$ zu einer Einbettung $\mathbb{C} \hookrightarrow K$ fortsetzen, deren Bild α enthält: In der Tat ist die $\mathbb{R}$-Ringalgebra $\mathbb{R}[\alpha]$ ein Integritätsring und nach 7.3.14 notwendig eine echte algebraische Körpererweiterung von $\mathbb{R}$ und muß nach 7.8.30 also isomorph sein zu $\mathbb{C}$. Um die Notation nicht unnötig aufzublähen, denken wir uns von nun an vermittels dieser Einbettung $\mathbb{C}$ als einen Teilkörper $\mathbb{C} \subset K$. Jetzt machen wir K zu einem $\mathbb{C}$-Vektorraum durch Multiplikation von links. Die Multiplikation mit $\mathrm{i} \in \mathbb{C}$ von rechts wird dann ein $\mathbb{C}$-linearer Endomorphismus $J \in \mathrm{End}_{\mathbb{C}} K$ mit $J^2 = -\mathrm{id}_K$. Als Endomorphismus endlicher Ordnung **??** oder einfacher als Endomorphismus der Ordnung Vier ist er diagonalisierbar nach **??** und liefert wegen $J^2 = -\mathrm{id}$ eine Zerlegung $K = K^+ \oplus K^-$ mit $K^\pm = \{a \in K \mid \mathrm{i}\, a = \pm a\, \mathrm{i}\}$. Für alle $\alpha \in K^+$ ist nun $\mathbb{C}[\alpha]$ nach 7.3.14 ein Körper und es folgt $K^+ = \mathbb{C}$. Gilt $K \neq \mathbb{C}$, so gibt es nach dem Beginn des Beweises auch in $K^- \oplus \mathbb{R}$ ein Element j mit $\mathrm{j}^2 = -1$. Setzen wir $\mathrm{j} = \beta + \alpha$ mit $\beta \in K^-$ und $\alpha \in \mathbb{R}$, so folgt $-1 = \mathrm{j}^2 = \beta^2 + 2\alpha\beta + \alpha^2$ mit dem ersten und letzten Term in K^+ und dem mittleren Term in K^-. Damit folgt erst $2\alpha\beta = 0$ und dann $\alpha = 0$ und man erkennt $\mathrm{j} \in K^-$. Für jedes von Null verschiedene $\mathrm{j} \in K^-$ induziert aber die Multiplikation mit j von rechts einen Isomorphismus $K^+ \xrightarrow{\sim} K^-$. Setzen wir $\mathrm{k} := \mathrm{ij}$, so ist also $\{1, \mathrm{i}, \mathrm{j}, \mathrm{ij}\}$ eine $\mathbb{R}$-Basis von K und es gilt $\mathrm{i}^2 = \mathrm{j}^2 = -1$ und $\mathrm{ij} = -\mathrm{ji}$. Daraus aber folgt sofort $\mathrm{k}^2 = -1 = \mathrm{ijk}$. □

Ergänzung 7.12.4. Eine **Kompositionsalgebra** ist ein reeller endlichdimensionaler Skalarproduktraum V mit einer bilinearen Verknüpfung $\mu : V \times V \to V$ derart, daß gilt $\|\mu(v, w)\| = \|v\| \cdot \|w\|$ $\forall v, w \in V$. Topologische Methoden zeigen, daß die Dimension eine Bijektion

$$\left\{ \begin{array}{c} \text{Kompositionsalgebren mit Einselement,} \\ \text{bis auf Isomorphismus} \end{array} \right\} \xrightarrow{\sim} \{0, 1, 2, 4, 8\}$$

liefert. Genauer ist $\mu_v : w \to \mu(v,w)$ für jeden festen Vektor $v \in V$ der Länge Eins orthogonal und induziert folglich eine Permutation der Einheitssphäre von V. Für jedes $w \in V$ gibt es mithin genau ein $\rho(w) = \rho_v(w) \in V$ mit $\mu(v, \rho(w)) = w$. Gilt also $\dim V > 1$ und halten wir einen weiteren Einheitsvektor t mit $t \perp v$ fest, so ist $\mu(t, \rho(w))$ ein Einheitsvektor, der auf w senkrecht steht. Man sieht leicht, daß er stetig von w abhängt und so ein stetiges tangentiales Vektorfeld ohne Nullstelle auf der Einheitsshpäre in V liefert. Mit topologischen Methoden kann man aber zeigen, daß es derartige Vektorfelder nur auf Sphären der Dimensionen $1, 3, 7$ geben kann, daß das also in anderer Terminologie die einzigen **parallelisierbaren Sphären** sind. Die fraglichen Kompositionsalgebren sind 0, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ und die sehr merkwürdige Struktur der sogenannten **Oktaven** $\mathbb{O}$, auch genannt **Oktonionen** oder **Cayley'sche Zahlen**, bei denen die Multiplikation nicht mehr assoziativ ist. Zur Konstruktion dieser Struktur erinnern wir aus 2.6.7 den dort ausgezeichneten Isomorphismus $\mathbb{H} \xrightarrow{\sim} \mathbb{H}^{\mathrm{opp}}$, $q \mapsto \bar{q}$ und setzen $\mathbb{O} := \mathbb{H} \times \mathbb{H}$ mit der nicht assoziativen Multiplikation $\mu((a,b),(x,y)) := (ax - \bar{y}b, b\bar{x} + ya)$. Das Skalarprodukt ist jeweils das „offensichtliche". Mehr dazu findet man etwa bei [E$^+$92].

Übungen

Ergänzende Übung 7.12.5. Explizit gilt für das Skalarprodukt auf den Oktaven $\|(a,b)\|^2 = a\bar{a} + b\bar{b}$. Man zeige, daß die Oktaven in der Tat eine Kompositionsalgebra bilden. Ich empfehle, bei der Rechnung die übrigen gemischten Terme zu zwei Realteilen von Quaternionen zusammenzufassen, die sich dann zu Null addieren. Man zeige weiter: Sind zwei natürliche Zahlen jeweils eine Summe von acht Quadraten, so auch ihr Produkt.

8 Galoistheorie

8.1 Galoiserweiterungen

Definition 8.1.1. Ein Isomorphismus von einem Körper zu sich selbst heißt auch ein **Automorphismus** unseres Körpers. Gegeben eine Körpererweiterung L/K heißt die Gruppe aller Körperautomorphismen von L, die K punktweise festhalten, die **Galoisgruppe** $\mathrm{Gal}(L/K)$ der Körpererweiterung L/K.

Ergänzung 8.1.2. Bezeichnet Ring die Kategorie der Ringe und Ring^K die Kategorie der Ringe unter K, so können wir die Galoisgruppe in kategorientheoretischer Notation schreiben als $\mathrm{Gal}(L/K) = (\mathrm{Kring}^K)^\times(L)$ und im Fall einer endlichen Erweiterung als $\mathrm{Gal}(L/K) = \mathrm{Kring}^K(L,L)$, da dann alle Körperhomomorphismen über K von L in sich selber bereits injektiv und durch Vergleich der K-Dimensionen sogar Isomorphismen sind.

Beispiele 8.1.3. $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ ist eine Gruppe mit zwei Elementen, der Identität und der komplexen Konjugation. Betrachten wir in $\mathbb{R}$ die dritte Wurzel $\sqrt[3]{2}$ von 2, so besteht $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ nur aus der Identität, denn jeder Körperhomomorphismus $\mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(\sqrt[3]{2})$ muß die einzige Lösung der Gleichung $x^3 = 2$ in diesem Körper auf sich selbst abbilden.

Lemma 8.1.4. *Der Grad einer Körpererweiterung ist eine obere Schranke für die Kardinalität ihrer Galoisgruppe. Ist also in Formeln L/K unsere Körpererweiterung, so gilt in $\mathbb{N} \sqcup \{\infty\}$ die Ungleichung*

$$|\mathrm{Gal}(L/K)| \leq [L:K]$$

Beweis. Das folgt sofort aus Satz 7.8.15, nach dem sogar die Zahl der Körperhomomorphismen über K von L in einen beliebigen weiteren Körper M über K beschränkt ist durch der Erweiterunggrad, $|\mathrm{Ring}^K(L,M)| \leq [L:K]$. □

Proposition 8.1.5. *Ist q eine echte Primzahlpotenz und $r \geq 1$, so ist die Galoisgruppe $\mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$ eine zyklische Gruppe der Ordnung r, erzeugt vom* **Frobenius-Homomorphismus** *oder kurz* **Frobenius**

$$F : \mathbb{F}_{q^r} \xrightarrow{\sim} \mathbb{F}_{q^r}, \quad a \mapsto a^q$$

8.1.6. In 2.2.37 hatten wir bereits einen Frobeniushomomorphismus eingeführt. Der Frobeniushomomorphismus hier ist seine l-te Potenz für l gegeben durch $q = p^l$ mit p prim.

Beweis. Sicher erzeugt F in der Galoisgruppe eine zyklische Untergruppe der Ordnung r. Nach dem vorhergehenden Satz 8.1.4 hat die Galoisgruppe jedoch höchstens r Elemente. □

Definition 8.1.7. Eine Körpererweiterung L/K heißt eine **Galoiserweiterung** oder kurz **Galois**, wenn sie normal und separabel ist.

8.1.8. Operiert eine Gruppe G auf einer Menge X, so schreiben wir ganz allgemein X^G für die Menge der Fixpunkte. Ist speziell X ein Körper L und G eine Gruppe von Körperautomorphismen von L, so ist $L^G \subset L$ offensichtlich ein Unterkörper von L. Er heißt der **Fixkörper von** G.

Satz 8.1.9 (Galoiserweiterungen durch Gruppenoperationen). *Seien L ein Körper, G eine endliche Gruppe von Automorphismen von L und L^G der Fixkörper von G. So gilt:*

1. *Jedes Element $\alpha \in L$ ist algebraisch über L^G und sein Minimalpolynom über L^G wird gegeben durch die Formel*

$$\operatorname{Irr}(\alpha, L^G) = \prod_{\beta \in G\alpha} (X - \beta)$$

2. *Die Körpererweiterung L/L^G ist eine endliche Galoiserweiterung vom Grad $[L : L^G] = |G|$ mit Galoisgruppe $\operatorname{Gal}(L/L^G) = G$.*

Beweis. Wir setzen $K := L^G$. Schreiben wir $\prod_{\beta \in G\alpha}(X - \beta) = \sum a_i X^i$, so gilt für jedes Element $\sigma \in G$ die von der Mitte her zu entwickelnde Gleichungskette

$$\sum \sigma(a_i) X^i = \prod_{\beta \in G\alpha} (X - \sigma(\beta)) = \prod_{\beta \in G\alpha} (X - \beta) = \sum a_i X^i$$

Also gehört unser Produkt zu $K[X]$. Es teilt das Minimalpolynom $\operatorname{Irr}(\alpha, K)$, da mit α auch alle $\sigma(\alpha)$ für $\sigma \in G$ Nullstellen des besagten Minimalpolynoms sein müssen. Es wird aber auch vom fraglichen Minimalpolynom geteilt, da es bei α verschwindet. Da unser Produkt ebenso wie das Minimalpolynom normiert ist, müssen diese beiden Polynome übereinstimmen und der erste Punkt ist erledigt. Per definitionem ist dann L/K normal und separabel, also Galois. Als nächstes zeigen wir die Identität

$$[L : K] = |G|$$

Wir bemerken dazu, daß es nach Proposition 7.10.5 über die Unterscheidung von Körperhomomorphismen ein $\alpha \in L$ gibt mit $|G\alpha| = |G|$. Unsere Beschreibung des Minimalpolynoms von α über K zeigt dann $[K(\alpha) : K] = |G|$. Für $\beta \in L$ ist aber auch $K(\alpha, \beta)$ eine endliche separable Erweiterung von K und nach dem Satz vom primitiven Element 7.10.7 gibt es γ mit $K(\alpha, \beta) = K(\gamma)$. Aus $\operatorname{grad}(\operatorname{Irr}(\gamma, K)) \leq |G|$ folgt dann $K(\gamma) = K(\alpha)$ und damit $\beta \in K(\alpha)$. Insgesamt folgt $K(\alpha) = L$ und $[L : K] = [K(\alpha) : K] = |G|$. Mit dieser Erkenntnis

bewaffnet folgern wir schließlich die Gleichheit $G = \mathrm{Gal}(L/K)$ ohne weitere Schwierigkeiten aus der Ungleichungskette

$$|G| \leq |\mathrm{Gal}(L/K)| \leq [L:K] = |G|$$

Hier kommt die mittlere Ungleichung von 8.1.4 her und wir müssen unsere Erkenntnis, daß sie im Fall endlicher Galois-Erweiterungen sogar eine Gleichheit ist, gar nicht bemühen. □

Alternative zum Beweis der Abschätzung $[L:L^G] \leq |G|$. Wir können hier alternativ auch durch Widerspruch mit dem Satz über die lineare Unabhängigkeit von Charakteren argumentieren. Nehmen wir an, die Elemente von G seien $\sigma_1, \ldots, \sigma_r$ und es gebe in L eine um Eins größere über $K := L^G$ linear unabhängige Familie $x_0, \ldots, x_r$. In der Matrix der $\sigma_i(x_j)$ sind dann notwendig die Spalten $\sigma_*(x_j)$ linear abhängig, wir finden also $y_0, \ldots, y_r$ in L nicht alle Null mit $\sum_j y_j \sigma_i(x_j) = 0\ \forall i$. Durch Umnummerieren der x_j dürfen wir hier ohne Beschränkung der Allgemeinheit $y_0 \neq 0$ annehmen, und indem wir von $y_0, \ldots, y_r$ zu $yy_0, \ldots, yy_r$ übergehen, finden wir sogar eine lineare Relation unserer Spaltenvektoren für beliebig vorgegebenes $y_0 = z \in L$. Schreiben wir das um zu $\sum_j \sigma_i^{-1}(y_j)x_j = 0\ \forall i$ und summieren diese Gleichungen, so ergibt sich

$$\sum_j \lambda_j x_j = 0$$

für $\lambda_j = \sum_i \sigma_i^{-1}(y_j)$. Sicher gilt auch $\lambda_j \in K$ für alle j, und aus der linearen Unabhängigkeit der x_j folgt so $\lambda_j = 0$ für alle j und insbesondere $\lambda_0 = 0$. Nach der linearen Unabhängigkeit von Charakteren 7.8.16, angewandt auf die Homomorphismen $\sigma_i : L^\times \to L^\times$, gibt es jedoch ein $z \in L^\times$ mit $\sum_i \sigma_i^{-1}(z) \neq 0$. Das ist der gesuchte Widerspruch. □

8.1.10. Aus 8.1.9 folgt, daß bei einer endlichen Körpererweiterung die Kardinalität der Galoisgruppe sogar den Grad der Körpererweiterung teilen muß, in Formeln

$$|\mathrm{Gal}(L/K)| \mid [L:K]$$

In der Tat folgt für $G := \mathrm{Gal}(L/K)$ sowohl $|G| = [L:L^G]$ als auch $L^G \supset K$, also $|G|[L^G:K] = [L:K]$.

Vorschau 8.1.11. Ist L/K eine endliche Galois-Erweiterung, so ist $\alpha \in L$ nach dem ersten Beweis von 8.1.9 ein primitives Element genau dann, wenn es von keinem Element der Galoisgruppe festgehalten wird. Wir können sogar stets ein $\alpha \in L$ so wählen, daß es mit seinen Galois-Konjugierten eine K-Basis von L bildet: Das sagt uns der „Satz von der Normalbasis“ **??**. Diese schärfere Aussage stimmt keineswegs für jedes primitive Element, wie das Beispiel $L = \mathbb{C}$, $K = \mathbb{R}$, $\alpha = \mathrm{i}$ zeigt.

Satz 8.1.12 (**Charakterisierung endlicher Galoiserweiterungen**). *Seien L/K eine endliche Körpererweiterung und $G = \mathrm{Gal}(L/K)$ ihre Galoisgruppe. So sind gleichbedeutend:*

1. *L/K ist eine Galoiserweiterung;*
2. *Die Ordnung der Galoisgruppe stimmt überein mit dem Grad der Körpererweiterung, in Formeln $|G| = [L : K]$;*
3. *Der Unterkörper K stimmt überein mit dem Fixkörper der Galoisgruppe, in Formeln $K = L^G$.*

Beweis. Wir beginnen mit 1⇒2. Nach (7.9.26, 1⇒3) gibt es für L endlich, separabel und normal über K genau $[L : K]$ Körperhomomorphismen $L \to L$ über K. Als Körperhomomorphismen sind diese natürlich injektiv, und wegen der Gleichheit der K-Dimensionen sind sie dann auch surjektiv. Die Implikation 2⇒3 folgt daraus, daß wir $|G| = [L : L^G]$ ja bereits nach 8.1.9 wissen. Gilt dann außerdem $|G| = [L : K]$ für einen Unterkörper $K \subset L^G$, so erhalten wir aus der Multiplikativität des Grades von Körpererweiterungen unmittelbar erst $[L^G : K] = 1$ und dann $L^G = K$. Die Implikation 3⇒1 folgt direkt aus 8.1.9. □

Ergänzung 8.1.13. Auch für eine beliebige algebraische Körpererweiterung gilt noch, daß sie genau dann Galois ist, wenn der Unterkörper der Fixkörper der Galoisgruppe ist. Hier folgt die eine Implikation aus 8.1.33, und die andere aus 7.11.10.

Beispiel 8.1.14. Unter der Voraussetzung $\mathrm{char}\, K \neq 2$ ist jede quadratische Körpererweiterung L von K Galois mit Galoisgruppe $\mathbb{Z}/2\mathbb{Z}$ und die Elemente $\alpha \in L \backslash K$ mit $\alpha^2 \in K$ sind genau diejenigen von Null verschiedenen Elemente von L, die vom nichttrivialen Element der Galoisgruppe auf ihr Negatives geschickt werden.

Definition 8.1.15. Eine Wirkung einer Gruppe auf einer Menge heißt **treu**, englisch **faithful**, französisch **fidèle**, wenn nur das neutrale Element jedes Element der Menge festhält.

8.1.16. Wir erinnern aus 4.1.7, daß eine Wirkung einer Gruppe auf einer Menge transitiv heißt, wenn unsere Menge nicht leer ist und je zwei ihrer Elemente durch ein geeignetes Gruppenelement ineinander überführt werden können.

Satz 8.1.17 (**Operation der Galoisgruppe auf Nullstellen**). *Gegeben L/K eine endliche normale Körpererweiterung und $P \in K[X]$ ein Polynom betrachte man die Operation der Galoisgruppe $\mathrm{Gal}(L/K)$ auf der Menge $\{\alpha \in L \mid P(\alpha) = 0\}$ der Nullstellen von P in L.*

1. *Ist P ein K-irreduzibles Polynom, das in L zerfällt, so ist die Operation der Galoisgruppe auf seinen L-Nullstellen transitiv;*

2. *Ist $P \in K[X]$ ein beliebiges von Null verschiedenes Polynom und L sein Zerfällungskörper, so ist die Operation der Galoisgruppe auf den L-Nullstellen von P treu.*

Ergänzung 8.1.18. Dasselbe gilt auch ohne daß wir $[L : K] < \infty$ annehmen und folgt in dem Fall unmittelbar aus 7.11.10.

Beweis. Für je zwei Nullstellen α, β von P gibt es nach unserer Proposition 7.8.9 über das Ausdehnen auf primitive Erweiterungen einen Körperhomomorphismus $K(\alpha) \to L$ über K mit $\alpha \mapsto \beta$, der sich dann nach 7.8.13 weiter ausdehnen läßt zu einem Körperhomomorphismus $L \to L$ über K. Treu ist die Operation, da der Zerfällungskörper eines Polynoms bereits von den Nullstellen des besagten Polynoms erzeugt wird. □

8.1.19 (**Grundfrage der Galoistheorie**). Die Grundfrage der Galoistheorie ist, welche Permutationen der Nullstellenmenge eines vorgegebenen irreduziblen Polynoms denn nun von einem Automorphismus seines Zerfällungskörpers oder genauer von einem Element der Galoisgruppe seiner Zerfällungserweiterung herkommen. Man nennt diese Galoisgruppe die **Galoisgruppe unseres irreduziblen Polynoms**. Hierzu gebe ich gleich drei Beispiele.

Beispiel 8.1.20 (**Ein kubisches Polynom mit Galoisgruppe $\mathcal{S}_3$**). Ist L der Zerfällungskörper von $X^3 - 2$ über $\mathbb{Q}$, so kommen alle Permutationen der Nullstellenmenge unseres Polynoms von Elementen der Galoisgruppe her und wir haben folglich $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathcal{S}_3$. In der Tat ist $L/\mathbb{Q}$ normal als Zerfällungskörper und sogar Galois, da in Charakteristik Null jede Körpererweiterung separabel ist. Damit folgt insbesondere $[L : \mathbb{Q}] = |\mathrm{Gal}(L/\mathbb{Q})|$. Jetzt realisieren wir L als einen Teilkörper

$$L = \mathbb{Q}(\sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2}) \subset \mathbb{C}$$

der komplexen Zahlen, mit $\sqrt[3]{2} \in \mathbb{R}$ der reellen dritten Wurzel von 2 und $\zeta = \exp(2\pi\,\mathrm{i}\,/3)$ einer dritten Einheitswurzel. Diese Darstellung zeigt $L \neq \mathbb{Q}(\sqrt[3]{2})$, da ja unser L nicht in $\mathbb{R}$ enthalten ist. In $\mathbb{Q}(\sqrt[3]{2})[X]$ zerfällt unser Polynom $X^3 - 2$ also in einen linearen und einen irreduziblen quadratischen Faktor, folglich ist L eine quadratische Erweiterung von $\mathbb{Q}(\sqrt[3]{2})$. Zusammen ergibt sich $[L : \mathbb{Q}] = 6$ und mithin $|\mathrm{Gal}(L/\mathbb{Q})| = 6$. Die Operation von $\mathrm{Gal}(L/\mathbb{Q})$ auf der Menge $\{\sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2}\}$ definiert nun nach 8.1.17 eine Einbettung $\mathrm{Gal}(L/\mathbb{Q}) \hookrightarrow \mathcal{S}_3$, und da beide Seiten gleichviele Elemente haben, muß diese Einbettung ein Isomorphismus sein.

Beispiel 8.1.21 (**Ein kubisches Polynom mit zyklischer Galoisgruppe**). Ist L der Zerfällungskörper von $X^3 + X^2 - 2X - 1$ über $\mathbb{Q}$, so kommen genau die zyklischen Permutationen der Nullstellenmenge unseres Polynoms von Elementen der Galoisgruppe her und wir haben folglich $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$. In der Tat können wir mit $\zeta = \exp(2\pi\,\mathrm{i}\,/7)$ einer siebten Einheitswurzel die drei komplexen Nullstellen unseres Polynoms schreiben als $\alpha = \zeta + \bar{\zeta}$, $\beta = \zeta^2 + \bar{\zeta}^2$ sowie $\gamma = \zeta^3 + \bar{\zeta}^3$, wie man leicht nachrechnet. Ich bin im übrigen den umgekehrten Weg gegangen und habe mein Polynom aus den Linearfaktoren zu diesen drei Nullstellen zusammenmultipliziert. Wie dem auch sei besitzt unser Polynom keine ganzzahligen Nullstellen, also nach 2.3.41 auch keine Nullstellen in $\mathbb{Q}$, und ist als Polynom vom Grad 3 folglich irreduzibel über $\mathbb{Q}$. Unsere Nullstellen erfüllen nun jedoch die Relationen $\alpha^2 = \beta + 2$, $\beta^2 = \gamma + 2$ und $\gamma^2 = \alpha + 2$, woraus unmittelbar die Behauptung folgt. In 8.7.12 geben wir im übrigen ein Kriterium an, das es erlaubt, die Galoisgruppe einer kubischen Gleichung ganz mechanisch zu bestimmen.

Beispiel 8.1.22 (**Ein kubisches Polynom mit trivialer Galoisgruppe**). Man betrachte den Funktionenkörper $\mathbb{F}_3(T)$ über dem Körper mit drei Elementen und darüber das Polynom $X^3 - T$. Es hat nur eine einzige Nullstelle in seinem Zerfällungskörper, die aber eben eine dreifache Nullstelle ist. Seine Galoisgruppe ist folglich trivial. Im übrigen ist ein Zerfällungskörper hier die Körpererweiterung $\mathbb{F}_3(T) \hookrightarrow \mathbb{F}_3(U)$ mit $T \mapsto U^3$ und darin zerfällt unser Polynom als $X^3 - T = X^3 - U^3 = (X - U)^3$.

Proposition 8.1.23 (**Quotientenkörper eines Invariantenrings**). *Operiert eine endliche Gruppe G auf einem kommutativen Integritätsbereich R, so liefert die offensichtliche Einbettung einen Isomorphismus*

$$\mathrm{Quot}(R^G) \xrightarrow{\sim} (\mathrm{Quot}\, R)^G$$

des Quotientenkörpers seines Invariantenrings mit den Invarianten seines Quotientenkörpers.

Beweis. Jeden Bruch $f/h \in (\mathrm{Quot}\, R)^G$ können wir mit $\prod_{\sigma\in G\setminus 1} \sigma(h)$ erweitern zu einem Bruch, dessen Nenner im Invariantenring R^G liegt, da er ja das Produkt aller $\sigma(h)$ mit $\sigma \in G$ ist und bei diesem Produkt die Gruppenoperation nur die Faktoren permutiert. So ein Bruch kann aber nur dann G-invariant sein, wenn auch sein Zähler in R^G liegt. □

Beispiel 8.1.24. Für jeden Körper k ist nach 8.1.9 und 8.1.23 in den Notationen von 6.9.6 die Erweiterung

$$k('s_1, \ldots, s_n) = k('X_1, \ldots, X_n)^{\mathcal{S}_n} \subset k('X_1, \ldots, X_n)$$

eine Galoiserweiterung mit Galoisgruppe $\mathcal{S}_n$. Unsere Erweiterung ist natürlich auch ein Zerfällungskörper der **allgemeinen Gleichung**

$$T^n + s_1 T^{n-1} + \ldots + s_{n-1} T + s_n$$

Hier fassen wir die s_i schlicht als algebraisch unabhängige Variablen des Funktionenkörpers $k('s_1, \ldots, s_n)$ über k auf. Nach unserer Konvention sollten wir hier vielleicht sogar große Buchstaben vom Ende des Alphabets benutzen, zum Beispiel Y_i statt s_i. Insbesondere ist die allgemeine Gleichung nach 8.1.9 irreduzibel, da ja alle ihre Wurzeln einfach sind und zueinander konjugiert unter der Galoisgruppe. Die Irreduzibilität dieses Polynoms kann aber auch bereits aus 6.7.20 abgeleitet werden.

Übungen

Übung 8.1.25. Gegeben eine endliche separable Körpererweiterung ist ihre normale Hülle Galois. Mutigere zeigen dasselbe, ohne die Endlichkeit vorauszusetzen.

Übung 8.1.26. Gegeben $n \geq 1$ zeige man, daß $\mathbb{C}(X^n) \subset \mathbb{C}(X)$ eine Galoiserweiterung vom Grad n ist mit zyklischer Galoisgruppe.

Ergänzende Übung 8.1.27. Man zeige, daß sich jede endliche Erweiterung eines vollkommenen Körpers zu einer endlichen Galoiserweiterung vergrößern läßt. Man zeige, daß sich wie in **??** behauptet jeder Endomorphismus x eines endlichdimensionalen Vektorraums über einem vollkommenen Körper auf genau eine Weise zerlegen läßt als $x = x_\mathrm{s} + x_\mathrm{n}$ mit x_s halbeinfach, x_n nilpotent und $x_\mathrm{s} x_\mathrm{n} = x_\mathrm{n} x_\mathrm{s}$.

Übung 8.1.28. Man zeige: Gegeben eine Körpererweiterung L/K und zwei verschiedene normierte irreduzible Polynome in $K[X]$ kann kein Element der Galoisgruppe eine Nullstelle des einen Polynoms in eine Nullstelle des anderen Polynoms überführen.

Übung 8.1.29. Sei k ein Körper der Charakteristik p und $\lambda \in k^\times$ und $t = t_\lambda : k(X) \xrightarrow{\sim} k(X)$ der Körperautomorphismus über k mit $X \mapsto X + \lambda$. Man zeige, daß der Körper der Invarianten genau das Bild derjenigen Einbettung $k(Y) \hookrightarrow k(X)$ ist, die durch $Y \mapsto X^p - \lambda^{p-1} X$ gegeben wird. Man zeige, daß auch die induzierte Einbettung $k[Y] \hookrightarrow k[X]$ einen Isomorphismus auf den Ring der t-Invarianten von $k[X]$ induziert.

Ergänzende Übung 8.1.30. Jede normale Körpererweiterung mit trivialer Galoisgruppe ist rein inseparabel im Sinne von 7.9.37. Für jede normale Körpererweiterung K/k mit Galoisgruppe G ist K^G/k rein inseparabel. Hinweis: 7.9.17. Im Fall unendlicher Erweiterungen verwende man 7.11.9.

Ergänzende Übung 8.1.31 (**Satz von Gilmer**). Man zeige, daß eine algebraische Körpererweiterung L/K derart, daß jedes Polynom aus $K[X]$ in L eine Nullstelle hat, ein algebraischer Abschluß von K sein muß. Hinweis: Man beginne mit dem Fall der Charakteristik Null. Jede endliche Körpererweiterung von K besitzt dann nach 7.10.7 ein primitives Element und läßt sich folglich in L einbetten. Gegeben ein Polynom $P \in L[X]$ gilt das insbesondere für seinen Zerfällungskörper über dem von seinen Koeffizienten in L erzeugten Teilkörper über K. Im Fall positiver Charakteristik argumentiere man erst mit dem separablen Abschluß von K in unserem Zerfällungskörper und dann mit 7.9.37.

Übung 8.1.32. Man bestimme die Galoisgruppe des Zerfällungskörpers des Polynoms $X^4 - 5$ über $\mathbb{Q}$ und über $\mathbb{Q}[\mathrm{i}]$.

Ergänzende Übung 8.1.33. Ist L/K eine algebraische, aber nicht notwendig endliche Körpererweiterung und $G \subset \mathrm{Gal}(L/K)$ eine beliebige, nicht notwendig endliche Untergruppe, so ist L/L^G immer noch eine Galoiserweiterung, deren Galoisgruppe jedoch nicht mit G übereinzustimmen braucht. Zum Beispiel erzeugt der Frobenius-Homomorphismus nicht die Galoisgruppe $\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$, aber der Fixkörper seines Erzeugnisses ist dennoch $\mathbb{F}_p$.

Übung 8.1.34. Gegeben eine Körpererweiterung L/K in Charakteristik ungleich zwei und $\alpha, \beta \in L\backslash K$ mit $\alpha^2, \beta^2 \in K$ zeige man $\alpha \in K(\beta) \Leftrightarrow \alpha \in K\beta$. Hinweis: 8.1.14 oder 7.2.10. Gegeben paarweise teilerfremde quadratfreie natürliche Zahlen $a_1, \ldots, a_n$ zeige man, daß a_n kein Quadrat ist in $\mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_{n-1}})$. Hinweis: Andernfalls gäbe es ein kürzestmögliches Gegenbeispiel, und dann wäre $\mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_{n-2}})$ mit $a_{n-1}a_n$ ein noch kürzeres Gegenbeispiel. Schließlich zeige man, daß die Körpererweiterung $\mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_n})$ über $\mathbb{Q}$ Galois ist mit Galoisgruppe $(\mathbb{Z}/2\mathbb{Z})^n$. Diese Aussage kann auch als Spezialfall der sogenannten Kummertheorie **??** verstanden werden.

Übung 8.1.35 (**Artin-Schreier-Erweiterungen**). Gegeben ein Körper F positiver Charakteristik $p > 0$ betrachten wir für $a \in F$ das Polynom $X^p - X - a$. Ist β eine Nullstelle dieses Polynoms in einer Körpererweiterung L/K, so sind die anderen Nullstellen $\beta + \lambda$ für $\lambda \in \mathbb{F}_p$. Insbesondere ist $F(\beta)$ bereits der Zerfällungskörper von $X^p - X - a$ und alle irreduziblen Faktoren von $X^p - X - a$ in $F[X]$ haben denselben Grad, a forteriori den Grad Eins oder den Grad p. Hat unser Polynom keine Nullstelle in F, so ist $F(\beta)/F$ mithin eine Galoiserweiterung vom Grad p zyklischer Galoisgruppe.

Übung 8.1.36. Gegeben eine endliche Galoiserweiterung L/K ist die **Spurabbildung** $\mathrm{S}_L^K : L \to K$ gegeben durch

$$x \mapsto \sum_{\sigma \in \mathrm{Gal}(L/K)} \sigma(x)$$

eine K-lineare von Null verschiedene Abbildung und die **Spurform** $L \times L \to K$ gegeben durch $(x, y) \mapsto \mathrm{S}_L^K(xy)$ ist eine nichtausgeartete Bilinearform aufdem K-Vektorraum L. Hinweis: Lineare Unabhängigkeit von Charakteren 7.8.16. In **??** wird die Spur auf beliebige endliche Körperwerweiterungen verallgemeinert.

8.2 Anschauung für die Galoisgruppe*

8.2.1. Formal ist der nun folgende Abschnitt für die logische Kohärenz dieser Vorlesung nicht von Belang. Es wird darin auch nichts bewiesen. Ich denke jedoch, daß die im folgenden erklärten Ideen bei der historischen Entwicklung der Theorie von zentraler Bedeutung waren und hoffe, daß sie Ihnen beim Verständnis helfen.

8.2.2 (**Reelle Nullstellen einer Familie reeller Polynome**). Zum Aufwärmen betrachten wir zunächst einmal ein normiertes Polynom $P \in \mathbb{R}(t)[X]$ mit Koeffizienten im Funktionenkörper $\mathbb{R}(t) = \operatorname{Quot} \mathbb{R}[t]$ über dem Körper der reellen Zahlen. Sei $E = E_P \subset \mathbb{R}$ die endliche Menge aller Punkte, an denen mindestens ein Koeffizient von P eine Polstelle hat. An jeder anderen Stelle $\lambda \in \mathbb{R}\backslash E$ können wir die Koeffizienten von P bei $t = \lambda$ auswerten und erhalten so ein Polynom $P_\lambda \in \mathbb{R}[X]$. Die Punkte $\lambda \in \mathbb{R}\backslash E$ nennen wir „die Parameter λ, für die P_λ definiert ist“. Die reellen Nullstellen der Polynome P_λ hängen dann vom Parameter λ ab und eine bildliche Darstellung der **simultanen Nullstellenmenge**

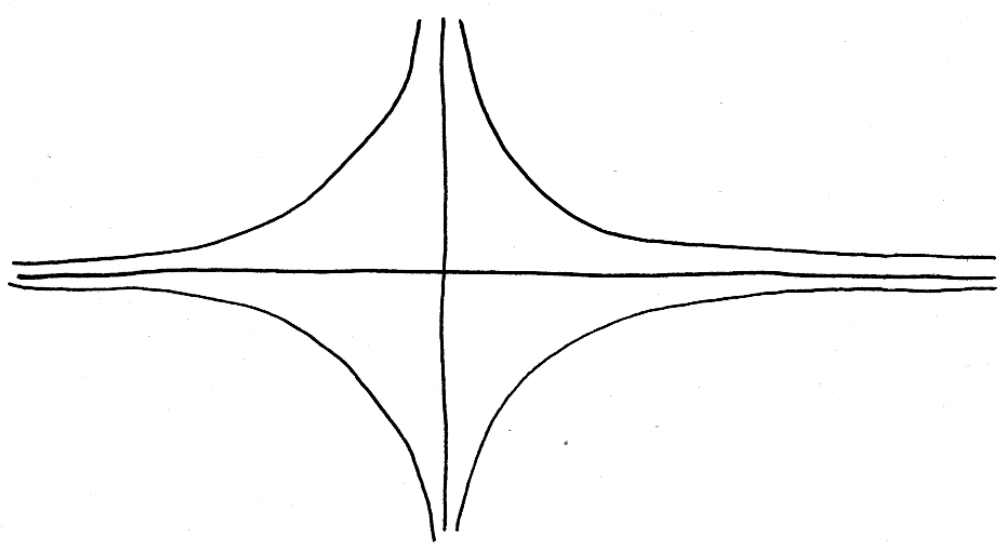
$$\mathcal{Z}(P) := \{(\lambda, \alpha) \in \mathbb{R}^2 \mid \lambda \notin E,\ P_\lambda(\alpha) = 0\}$$

als Teilmenge der Ebene vermittelt eine gewisse Anschauung für diese Abhängigkeit. Ist etwa $P = X^2 - (1/t)$, so ist P_λ definiert für $\lambda \neq 0$ und wir haben $\mathcal{Z}(P) = \{(\lambda, \alpha) \mid \lambda \neq 0,\ \alpha^2 - (1/\lambda) = 0\}$.

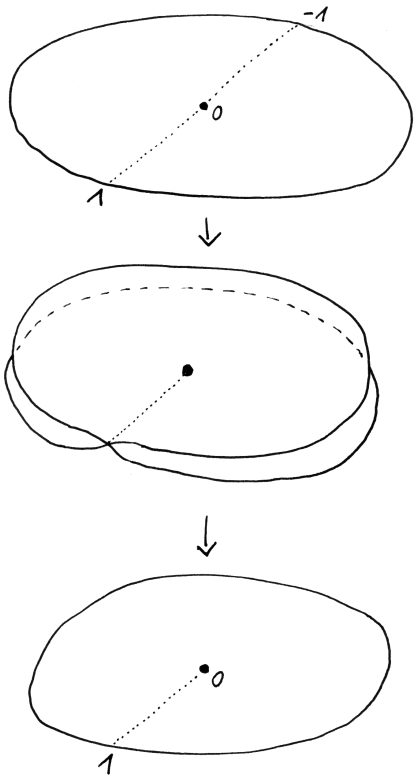
8.2.3 (**Komplexe Nullstellen einer Familie komplexer Polynome**). Nun betrachten wir analog ein normiertes Polynom $P \in \mathbb{C}(z)[X]$ mit Koeffizienten im Funktionenkörper $\mathbb{C}(z) = \operatorname{Quot} \mathbb{C}[z]$ über dem Körper der komplexen Zahlen. Sei wieder $E = E_P \subset \mathbb{C}$ die endliche Menge aller Punkte, an denen mindestens ein Koeffizient von P eine Polstelle hat. An jeder anderen Stelle $\lambda \in \mathbb{C}\backslash E$ können wir die Koeffizienten von P bei $z = \lambda$ auswerten und erhalten so ein Polynom $P_\lambda \in \mathbb{C}[X]$. Die Punkte $\lambda \in \mathbb{C}\backslash E$ nennen wir „die Parameter λ, für die P_λ definiert ist“. Die komplexen Nullstellen der Polynome P_λ hängen dann vom Parameter λ ab und wir betrachten analog die **simultane Nullstellenmenge**

$$\mathcal{Z}(P) := \{(\lambda, \alpha) \in \mathbb{C}^2 \mid \lambda \notin E,\ P_\lambda(\alpha) = 0\}$$

Ist etwa zur Abwechslung diesmal $P = X^2 - z$, so ist P_λ definiert für alle λ und wir haben $\mathcal{Z}(P) = \{(\lambda, \alpha) \mid \alpha^2 - \lambda = 0\}$.



Graphische Darstellung der Menge $\{(\lambda, \alpha) \mid \lambda \neq 0,\ \alpha^2 - 1/\lambda = 0\}$



Dies Bild kam bereits in **??** vor als Illustration für die Abbildung $z \mapsto z^2$ der komplexen Zahlenebene auf sich selbst. Für die durch Adjunktion einer Quadratwurzel aus z entstehende Erweiterung L des Funktionenkörpers $\mathbb{C}(z)$ ist nun $P = X^2 - z$ das Minimalpolynom eines Erzeugers und wir erhalten eine stetige Bijektion $\mathbb{C} \xrightarrow{\sim} Z(P)$ mit stetiger Umkehrung vermittels der Vorschrift $z \mapsto (z^2, z)$. Die Komposition $\mathbb{C} \xrightarrow{\sim} Z(P) \to \mathbb{C}$ mit der Projektion auf die erste Koordinate ist also gerade unsere Abbildung $z \mapsto z^2$. Wir sehen so anschaulich, daß die Galoisgruppe von $L/\mathbb{C}(z)$ gerade $\mathbb{Z}/2\mathbb{Z}$ ist. Ähnlich zeigt diese Anschauung, daß die Galoisgruppe der durch Adjunktion einer n-ten Wurzel von t entstehende und oft $\mathbb{C}(\sqrt[n]{z})/\mathbb{C}(z)$ notierten Körpererweiterung gerade $\mathbb{Z}/n\mathbb{Z}$ sein sollte, was Sie bereits als Übung 8.1.26 formal bewiesen haben.

8.2.4. Gegeben eine stetige Abbildung $p : Z \to C$ von metrischen oder auch von topologischen Räumen verstehen wir unter einer **stetigen Selbstabbildung über** C eine stetige Abbildung $f : Z \to Z$ mit $p \circ f = p$. Das Monoid dieser speziellen Selbstabbildungen notieren wir

$$\mathrm{Top}_p(Z)$$

8.2.5. Ist $p : Z \to C$ eine sogenannte „Überlagerungsabbildung“, so nennen wir die Elemente von $\mathrm{Top}_p(Z)$ auch „Decktransformationen“. Wir diskutieren später, warum wir uns im folgenden bereits diese Terminologie erlauben.

8.2.6 (**Galoisgruppe und Decktransformationen**). Sei $P \in \mathbb{C}(z)[X]$ normiertes irreduzibles Polynom. Wir bilden die Körpererweiterung $L := \mathbb{C}(z)[X]/\langle P(X)\rangle$ und betrachten ihre Galoisgruppe $\Gamma := \mathrm{Gal}(L/\mathbb{C}(z))$. In dieser Situation finden wir stets ein $u \in \mathbb{C}[z]\backslash 0$ derart, daß gilt $P \in \mathbb{C}[z, u^{-1}][X]$ und daß alle Elemente der Galoisgruppe Γ den Teilring

$$L_0 := \mathbb{C}[z, u^{-1}][X]/\langle P(X)\rangle$$

auf sich selber abbilden. In der Tat reicht es dazu, u so zu wählen, daß alle $\gamma(\bar{X})$ für $\gamma \in \Gamma$ zu diesem Teilring gehören, und das ist sicher möglich. Ab nun halten wir solch ein u fest und erhalten offensichtlich eine Bijektion

$$\mathrm{Kring}^{\mathbb{C}}(L_0, \mathbb{C}) \ \tilde{\to}\ \mathcal{Z}(P)_u := \{(\lambda, \alpha) \in \mathcal{Z}(P) \mid u(\lambda) \neq 0\}$$

durch die Vorschrift $\varphi \mapsto (\varphi(z), \varphi(\bar{X}))$. Die Operation von Γ auf L_0 induziert durch Vorschalten eine Rechtsoperation von Γ auf $\mathrm{Kring}^{\mathbb{C}}(L_0, \mathbb{C})$ und vermittels unserer Bijektion eine Rechtsoperation auf $\mathcal{Z}(P)_u$. Die versprochene Anschauung für die Galoisgruppe liefert nun ein Satz, nach dem diese Rechtsoperation einen Isomorphismus

$$\Gamma^{\mathrm{opp}} \ \tilde{\to}\ \mathrm{Top}_{\mathrm{pr}_1}(\mathcal{Z}(P)_u)$$

der Opponierten der Galoisgruppe mit dem Monoid der stetigen Selbstabbildungen über $\mathbb{C}$ des $(u(\lambda) \neq 0)$-Teils der simultanen Nullstellenmenge von P induziert. Wir zeigen im folgenden, daß unsere Rechtsoperation durch stetige Abbildungen über $\mathbb{C}$ geschieht, aber nicht, daß sie einen Isomorphismus liefert. Gegeben $\gamma \in \Gamma$ haben wir sicher $\gamma(\bar{X}) = c_0 + c_1\bar{X} + \ldots + c_{n-1}\bar{X}^{n-1}$ für gewisse $c_\nu \in \mathbb{C}[z, u^{-1}]$. Bezeichnet $(\lambda, \alpha) \mapsto \varphi_{(\lambda,\alpha)}$ die Umkehrabbildung unserer Bijektion $\varphi \mapsto (\varphi(z), \varphi(\bar{X}))$, so finden wir . $(\varphi_{(\lambda,\alpha)} \circ \gamma)(\bar{X}) = c_0(\lambda) + c_1(\lambda)\alpha + \ldots + c_{n-1}(\lambda)\alpha^{n-1}$. Die Rechtsoperation von $\gamma \in \Gamma$ auf $\mathcal{Z}(P)_u$ wird also in Formeln gegeben durch die Vorschrift

$$(\lambda, \alpha) \mapsto (\lambda, c_0(\lambda) + c_1(\lambda)\alpha + \ldots + c_{n-1}(\lambda)\alpha^{n-1})$$

und geschieht insbesondere durch stetige Selbstabbildungen über $\mathbb{C}$. Das löst unser Versprechen ein.

8.2.7 (**Hilfen zur graphischen Darstellung**). Seien $P \in \mathbb{C}(z)[X]$ normiertes irreduzibles Polynom und u wie zuvor. Die Abbildung $\mathrm{pr}_1 : \mathcal{Z}(P)_u \to \mathbb{C}$ hat dann endliche nichtleere Fasern. Weiter ist die Diskriminante von P nicht die Null von $\mathbb{C}(z)$, und ändern wir u dahingehend, daß es auch an allen Null- und Polstellen dieser Diskriminante verschwindet, so hat jede Faser von $\mathrm{pr}_1 : \mathcal{Z}(P)_u \to \mathbb{C}_{u\neq 0}$ genau $\mathrm{grad}\, P$ Elemente und ist nebenbei bemerkt eine „Überlagerung“. Indem wir nun um jede Nullstelle von u einen Kreis zeichnen, der keine andere Nullstelle von u umläuft, und alle diese Kreise durch sich nicht kreuzende Wege mit einem festen Punkt verbinden, und weiter das Urbild eines solchen Gebildes in der simultanen Nullstellenmenge $\mathcal{Z}(P)_u$ zeichnen, erhalten wir eine gewisse Anschauung für die Abbildung $\mathrm{pr}_1 : \mathcal{Z}(P)_u \to \mathbb{C}_{u\neq 0}$ und das Monoid ihrer Decktransformationen. Bezeichnet genauer $S \subset \mathbb{C}^2$ unser in der komplexen Zahlenebene gezeichnetes Gebilde aus verbundenen Kreisen, so liefert die Restriktion auf $\mathrm{pr}_1^{-1}(S)$ eine Bijektion zwischen dem Monoid der Decktransformationen von $\mathrm{pr}_1 : \mathcal{Z}(P)_u \to \mathbb{C}_{u\neq 0}$ und dem Monoid der Decktransformationen von $\mathrm{pr}_1 : \mathrm{pr}_1^{-1}(S) \to S$.

Vorschau 8.2.8. Statt „Funktionen mit Parametern“ betrachtet man auch in der Algebra besser „Funktionen in mehreren Variablen“. Diese Sichtweise können Sie in der Algebraischen Geometrie kennenlernen. Der dort als **??** bewiesene Satz über „Körper und ihre Kurven“ istx eine Variante der obigen Aussagen für einen beliebigen algebraischen Grundkörper statt $\mathbb{C}$. Einen Beweis der oben gegebenen Behauptungen wird man jedoch eher in einer Vorlesung über Riemann'sche Flächen finden, die sich an eine Vorlesung zur Funktionentheorie anschließt.

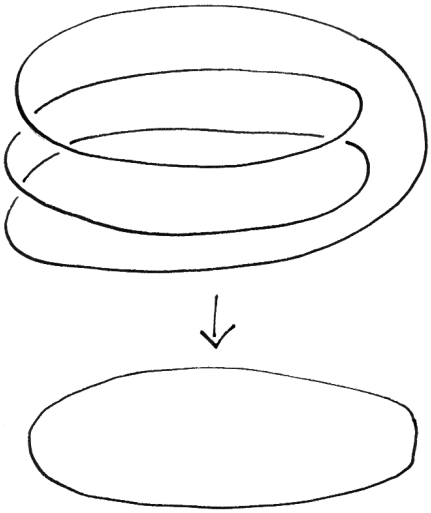
8.3 Zwischenkörper durch Untergruppen

Satz 8.3.1 (Galoiskorrespondenz). *Gegeben eine endliche Galoiserweiterung L/K mit Galoisgruppe $G = \mathrm{Gal}(L/K)$ liefern das Bilden der Galoisgruppe $M \mapsto \mathrm{Gal}(L/M)$ und das Bilden des Fixkörpers $H \mapsto L^H$ zueinander inverse inklusionsumkehrende Bijektionen*

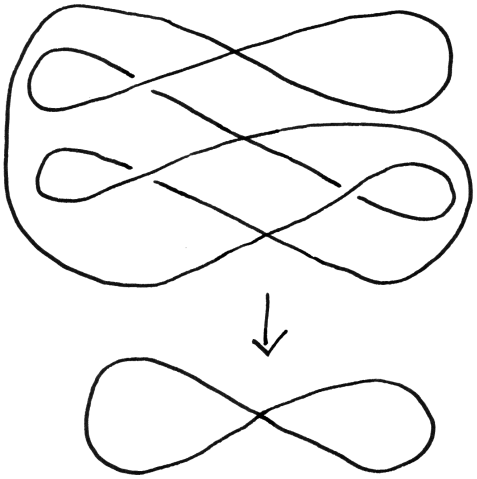
$$\left\{\begin{array}{c}\textit{Zwischenkörper } M\\ \textit{unserer Körpererweiterung}\\ K \subset M \subset L\end{array}\right\} \overset{\sim}{\leftrightarrow} \left\{\begin{array}{c}\textit{Untergruppen } H\\ \textit{ihrer Galoisgruppe}\\ H \subset G\end{array}\right\}$$

$$\begin{array}{ccc} M & \overset{\phi}{\mapsto} & H := \mathrm{Gal}(L/M) \\ M := L^H & \overset{\psi}{\mapsfrom} & H \end{array}$$

Unter dieser Bijektion entsprechen die Normalteiler H von G genau denjenigen Zwischenkörpern M, die normal sind über K, und in diesen Fällen liefert das Ein-



Anschauung für die durch Adjunktion einer dritten Wurzel aus t entstehende Körpererweiterung des Funktionenkörpers $\mathbb{C}(t)$ nach 8.2.7. Ich finde, man sieht in diesem Fall auch recht anschaulich, daß die Galoisgruppe zyklisch von der Ordnung drei sein sollte.



Versuch der bildlichen Darstellung einer Körpererweiterung vom Grad 3 mit trivialer Galoisgruppe, die also insbesondere nicht normal ist.

schränken von Elementen der Galoisgruppe einen Isomomorphismus von Gruppen $G/H \xrightarrow{\sim} \mathrm{Gal}(L^H/K)$ *alias eine kurze exakte Sequenz*

$$\mathrm{Gal}(L/M) \hookrightarrow \mathrm{Gal}(L/K) \twoheadrightarrow \mathrm{Gal}(M/K)$$

Vorschau 8.3.2. In der Sprache der Kategorientheorie ausgedrückt liefert für L/K eine endliche Galoiserweiterung mit Galoisgruppe G der Funktor $\mathrm{Kring}^K(\ , L)$ der K-linearen Körperhomomorphismen nach L eine Äquivalenz von Kategorien

$$\left\{ \begin{array}{c} \text{Körpererweiterungen von } K, \\ \text{die sich in } L \text{ einbetten lassen} \end{array} \right\} \xrightarrow{\approx} \left\{ \begin{array}{c} \text{transitive} \\ G\text{-Mengen} \end{array} \right\}^{\mathrm{opp}}$$

Das folgt aus obigem Satz mit einfachen Zusatzüberlegungen. Umgekehrt kann man auch obigen Satz auch leicht aus dieser Aussage folgern.

Beweis. Nach Eigenschaft 7.8.28 der Normalität und der Definition der Separabilität 7.9.18 ist für jeden Zwischenkörper M auch L/M normal und separabel, also Galois, und damit folgt $\psi \circ \phi = \mathrm{id}$ aus unserer Erkenntnis 8.1.12, daß bei einer endlichen Galoiserweiterung der Grundkörper gerade der Fixkörper der Galoisgruppe ist. Ohne alle Schwierigkeiten folgt $\phi \circ \psi = \mathrm{id}$ aus unserer Erkenntnis 8.1.9, daß das Bilden des Fixkörpers zu einer endlichen Gruppe von Körperautomorphismen stets eine Galoiserweiterung mit besagter Gruppe als Galoisgruppe liefert. Das zeigt die erste Behauptung. Man prüft nun leicht $g(L^H) = L^{gHg^{-1}}$ für alle $g \in G$, das gilt sogar für eine beliebige Operation einer beliebigen Gruppe auf einer beliebigen Menge. In Worten entspricht unter unserer Galoiskorrespondenz also das Verschieben von Zwischenkörpern mit einem Element der Galoisgruppe $g \in G$ der Konjugation von Untergruppen mit besagtem Element $g \in G$. Insbesondere ist L^H invariant unter G genau dann, wenn H in G ein Normalteiler ist. Da aber G nach 8.1.17 transitiv operiert auf den Wurzeln der Minimalpolynome aller Elemente von L, ist L^H invariant unter G genau dann, wenn es normal ist über K. Schließlich faktorisiert dann die durch Einschränken von Körperhomomorphismen gegebene Abbildung $G \to \mathrm{Gal}(L^H/K)$ über G/H und liefert eine Injektion $G/H \hookrightarrow \mathrm{Gal}(L^H/K)$, die mit einem Abzählargument bijektiv sein muß. □

Beispiel 8.3.3. Nach 8.1.5 ist für jede Potenz $q = p^r$ mit $r \geq 1$ einer Primzahl p die Galoisgruppe $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ eine zyklische Gruppe der Ordnung r, erzeugt vom Frobenius-Homomorphismus $a \mapsto a^p$. Die Untergruppen dieser Gruppe $\mathbb{Z}/\mathbb{Z}r$ sind nach 3.3.20 genau die Gruppen $\mathbb{Z}d/\mathbb{Z}r$ für Teiler d von r. Das liefert im Licht der Galoiskorrespondenz 8.3.1 einen neuen Beweis unserer Klassifikation 7.7.12 aller Unterkörper eines endlichen Körpers.

Definition 8.3.4. Eine Körpererweiterung L/K heißt **biquadratisch**, wenn sie den Grad $[L : K] = 4$ hat und erzeugt ist von zwei Elementen $\alpha, \beta \in L$ mit $\alpha^2, \beta^2 \in K$.

Beispiel 8.3.5. $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ ist biquadratisch über $\mathbb{Q}$, denn $(a + b\sqrt{5})^2 = a^2 + 2ab\sqrt{5} + 5b^2$ kann nie 3 sein, weder für $a = 0$ noch für $b = 0$ und erst recht nicht für $a \neq 0$, $b \neq 0$.

Lemma 8.3.6. *Jede biquadratische Erweiterung in einer von zwei verschieneden Charakteristik ist Galois und ihre Galoisgruppe ist die Klein'sche Vierergruppe* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Beweis. Sei $L = K(\alpha, \beta)$ mit $\alpha^2, \beta^2 \in K$ unsere biquadratische Erweiterung. Für die nichttrivialen Elemente $\sigma \in \mathrm{Gal}(L/K(\alpha))$, $\tau \in \mathrm{Gal}(L/K(\beta))$ haben wir

$$\sigma : \begin{cases} \alpha & \mapsto & \alpha \\ \beta & \mapsto & -\beta \end{cases} \qquad \tau : \begin{cases} \alpha & \mapsto & -\alpha \\ \beta & \mapsto & \beta \end{cases}$$

und wir haben $\{\mathrm{id}, \sigma, \tau, \sigma\tau\} \subset \mathrm{Gal}(L/K)$. Das muß dann aber schon die ganze Galois-Gruppe sein. □

8.3.7. Die Klein'sche Vierergruppe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{F}_2^2$ hat fünf Untergruppen: Den Nullpunkt, drei Geraden, und die ganze Gruppe. Sie entsprechen in unserer biquadratischen Erweiterung aus 8.3.6 den Unterkörpern

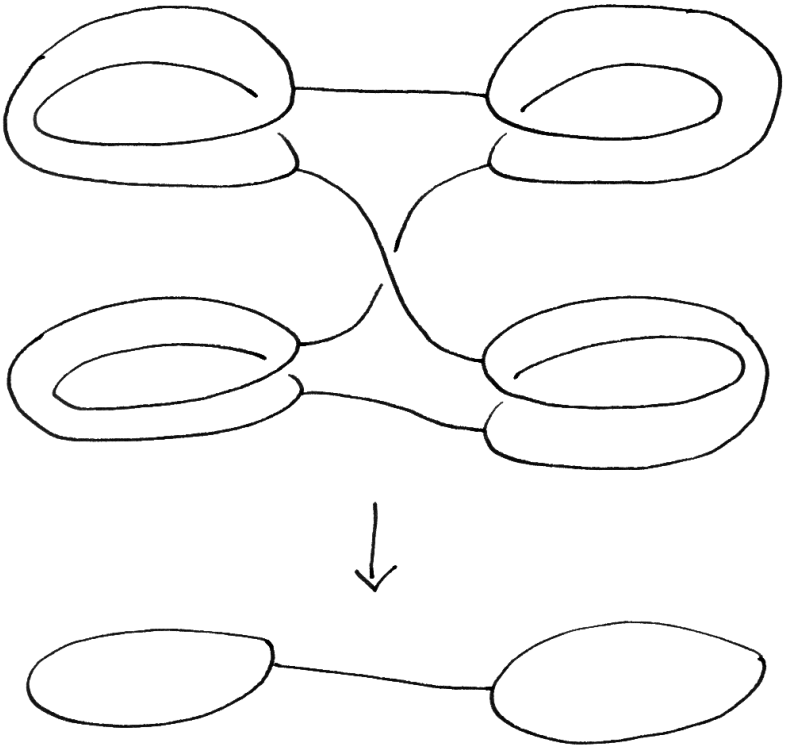
$$L \supset K(\alpha), K(\beta), K(\alpha\beta) \supset K$$

Eine K-Basis von L besteht aus $1, \alpha, \beta, \alpha\beta$, wie die simultane Eigenraumzerlegung von L unter σ und τ zeigt. Ein primitives Element ist zum Beispiel $\alpha + \beta$, da es von keinem nichttrivialen Element der Galoisgruppe festgehalten wird.

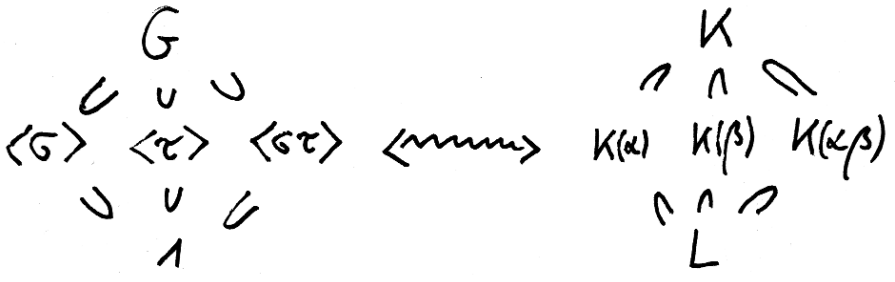
Satz 8.3.8 (Fundamentalsatz der Algebra). *Der Körper der komplexen Zahlen ist algebraisch abgeschlossen.*

8.3.9. Alternative Beweise diskutieren wir in 2.3.25. Als Übung dürfen Sie zeigen, daß aus einem beliebigen angeordneten Körper R, in dem jedes Polynom ungerader Ordnung eine Nullstelle hat und jedes positive Element eine Quadratwurzel, durch Adjunktion einer Quadratwurzel von (-1) bereits ein algebraisch abgeschlossener Körper entsteht.

Beweis. Sei $[L : \mathbb{R}]$ eine endliche normale Erweiterung von $\mathbb{R}$. Sei $G = \mathrm{Gal}(L/\mathbb{R})$ ihre Galoisgruppe und $S \subset G$ eine 2-Sylow von G, die in unseren Konventionen auch die triviale Gruppe sein darf. So haben wir $[L : \mathbb{R}] = |G|$ und $[L : L^S] = |S|$ und folglich ist $L^S/\mathbb{R}$ eine Erweiterung von ungeradem Grad. Da jedes Polynom



Dies Bild ist wie in 8.2.7 zu verstehen und stellt eine biquadratische Erweiterung des Funktionenkörpers $\mathbb{C}(t)$ dar, etwa durch die Adjunktion von Quadratwurzeln aus $(t \pm 1)$, wo die beiden Punkte ± 1 in den beiden Kreisen unten zu denken sind.



Links die fünf Untergruppen der Klein'schen Vierergruppe, rechts die ihnen unter der Galoiskorrespondenz entsprechenden fünf Zwischenkörper einer biquadratischen Erweiterung im Fall einer von Zwei verschiedenen Charakteristik.

aus $\mathbb{R}[X]$ von ungeradem Grad nach dem Zwischenwertsatz **??** eine reelle Nullstelle hat, folgt $L^S = \mathbb{R}$. Mithin haben wir $S = G$ und G ist eine 2-Gruppe. Damit entsteht nach unserem Satz 5.3.8 über die Struktur von p-Gruppen und unter Zuhilfenahme der Galoiskorrespondenz und Übung 8.3.10 die Körpererweiterung L aus $\mathbb{R}$ durch sukzessive Körpererweiterungen vom Grad 2, also nach 7.4.9 durch sukzessive Adjunktion von Quadratwurzeln. Adjungiert man aber eine echte Quadratwurzel zu $\mathbb{R}$, so erhält man $\mathbb{C}$ und in $\mathbb{C}$ hat jedes Element schon eine Quadratwurzel. Daraus folgt $L = \mathbb{R}$ oder $L = \mathbb{C}$. □

Übungen

Übung 8.3.10. Gegeben eine endliche Galoiserweiterung L/K und zwei Untergruppen $I \subset H$ ihrer Galoisgruppe zeige man für den Grad der Erweiterung der zugehörigen Fixkörper die Formel

$$[L^I : L^H] = |H/I|$$

Hinweise: 8.1.12, 7.4.11, 3.1.5, 8.3.1.

Übung 8.3.11. Man drücke $\sqrt{3}$ aus als Polynom in $\sqrt{3} + \sqrt{5}$ mit rationalen Koeffizienten: Das muß möglich sein, da dies Element nach 8.3.7 primitiv ist in $\mathbb{Q}(\sqrt{3}, \sqrt{5})$.

Übung 8.3.12. Seien L/K eine endliche Körpererweiterung und $K_1, K_2 \subset L$ zwei Zwischenkörper mit K_i/K Galois und $K_1 \cap K_2 = K$. So ist auch der von K_1 und K_2 erzeugte Unterkörper $K_1K_2 \subset L$ Galois über K und es gilt $\mathrm{Gal}(K_1K_2/K) \tilde{\to} \mathrm{Gal}(K_1/K) \times \mathrm{Gal}(K_2/K)$ vermittels der Restriktionen.

Ergänzende Übung 8.3.13. Sei L/K eine endliche Galoiserweiterung mit Galoisgruppe G und sei $H \subset G$ eine Untergruppe. Man konstruiere einen Isomorphismus zwischen $\mathrm{Gal}(L^H/K)$ und dem Quotienten N/H nach H des **Normalisators** $N = \mathrm{N}_G(H) := \{g \in G \mid gHg^{-1} = H\}$ von H in G.

Übung 8.3.14. Für jeden Körper k, dessen Charakteristik kein Teiler von n ist, hat der Zerfällungskörper des Polynoms

$$T^n + a_2T^{n-2} + \ldots + a_{n-1}T + a_n$$

mit Koeffizienten im Funktionenkörper $k('a_2, \ldots, a_n)$ in $n-1$ algebraisch unabhängigen Veränderlichen als Galoisgruppe die volle symmetrische Gruppe $\mathcal{S}_n$. Hinweis: Man gehe aus von 8.1.24; Die Galoisgruppe eines Polynoms über einem Körper K ändert sich nicht unter Substitutionen des Typs $T = Y + \lambda$ für $\lambda \in K$; die Galoisgruppe ändert sich nicht beim Übergang zu Funktionenkörpern $\mathrm{Gal}(L/K) = \mathrm{Gal}(L(X)/K(X))$. Die Irreduzibilität folgt bereits aus 6.7.20.

Ergänzung 8.3.15. Bei der Behandlung kubischer Gleichungen in 8.7.6 werden wir sehen, daß auch im Fall eines Körpers k der Charakteristik drei das Polynom $T^3 + pT + q$ über $k('p, q)$ die volle symmetrische Gruppe als Galoisgruppe hat. Andererseits ist im Fall eines Körpers k der Charakteristik zwei das Polynom $T^2 + p$ über $k('p)$ inseparabel und seine Galoisgruppe ist trivial und ist nicht die volle symmetrische Gruppe.

8.4 Galoisgruppen von Kreisteilungskörpern

8.4.1. Gegeben $n \geq 1$ interessieren wir uns nun für den Zerfällungskörper über $\mathbb{Q}$ des Polynoms $X^n - 1$. Dieser Zerfällungsköper heißt der n-te **Kreisteilungskörper** und wird unter Mißbrauch der Notation bezeichnet mit $\mathbb{Q}(\sqrt[n]{1})$. Er ist normal als Zerfällungskörper und separabel über $\mathbb{Q}$ wegen Charakteristik Null und mithin eine Galois-Erweiterung von $\mathbb{Q}$. Ich stelle mir als n-ten Kreisteilungskörper meist konkret den Unterkörper $\mathbb{Q}(\zeta) \subset \mathbb{C}$ vor mit $\zeta = \mathrm{e}^{2\pi\mathrm{i}/n}$. Auch ohne Rückgriff auf den Körper der komplexen Zahlen wissen wir nach 3.4.17, daß die n-ten Einheitswurzeln in $\mathbb{Q}(\sqrt[n]{1})$ eine zyklische Gruppe der Ordnung n bilden. Die Erzeuger dieser Gruppe heißen die **primitiven n-ten Einheitswurzeln**. Nach unserer Definition der Kreisteilungspolynome in 6.8.1 sind sie gerade die Nullstellen des n-ten Kreisteilungspolynoms

$$\Phi_n = \prod_{\operatorname{ord}\zeta = n} (X - \zeta)$$

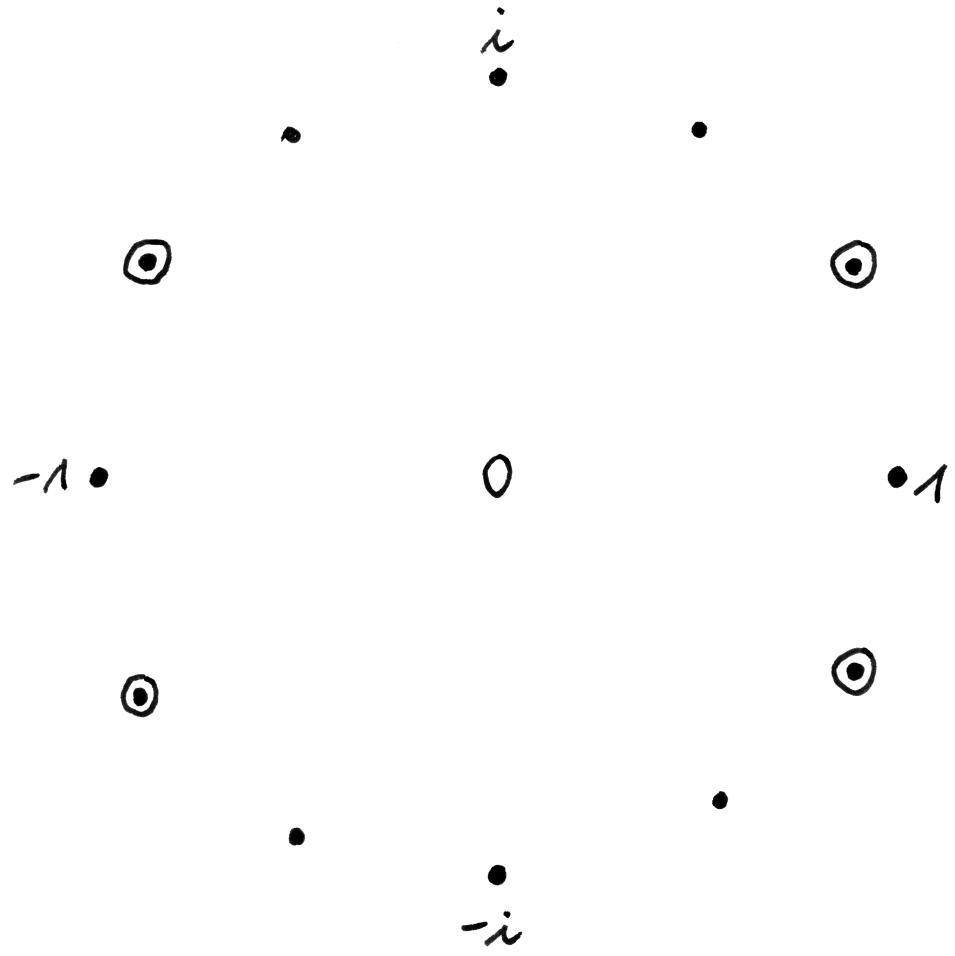
Wir hatten schon in 6.8.1 mit Induktion über n gezeigt, daß dieses Polynom Koeffizienten in $\mathbb{Q}$ und sogar in $\mathbb{Z}$ hat, und 6.8.4 besagte, daß für $n = p$ prim das p-te Kreisteilungspolynom Φ_p irreduzibel ist in $\mathbb{Q}[X]$. Nun zeigen wir ganz allgemein, daß für alle $n \geq 1$ das n-te Kreisteilungspolynom Φ_n irreduzibel ist in $\mathbb{Q}[X]$. Nach 6.7.11 ist das ganz allgemein für normierte Polynome in $\mathbb{Z}[X]$ gleichbedeutend dazu, irreduzibel zu sein in $\mathbb{Z}[X]$.

Satz 8.4.2 (Galoisgruppen der Kreisteilungskörper). *1. Die Kreisteilungspolynome $\Phi_n(X)$ sind irreduzibel in $\mathbb{Q}[X]$;*

2. Bezeichnet μ_n die Gruppe der n-ten Einheitswurzeln im n-ten Kreisteilungskörper $\mathbb{Q}(\sqrt[n]{1})$ und $\mathrm{Aut}(\mu_n)$ ihre Automorphismengruppe, so liefern die offensichtichen Abbildungen Isomorphismen

$$\mathrm{Gal}(\mathbb{Q}(\sqrt[n]{1})/\mathbb{Q}) \xrightarrow{\sim} \mathrm{Aut}(\mu_n) \xleftarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^\times$$

Auf diese Weise erhalten wir einen ausgezeichneten Isomorphismus zwischen der Galoisgruppe des n-ten Kreisteilungskörpers und der Einheitengruppe des Restklassenrings $\mathbb{Z}/n\mathbb{Z}$;



Die zwölften Einheitswurzeln in $\mathbb{C}$, eingekringelt die vier primitiven zwölften Einheitswurzeln

3. *Gegeben zwei primitive n-te Einheitswurzeln $\zeta, \xi \in \mathbb{Q}(\sqrt[n]{1})$ existiert genau ein Körperhomomorphismus $\sigma : \mathbb{Q}(\sqrt[n]{1}) \to \mathbb{Q}(\sqrt[n]{1})$ mit $\sigma(\zeta) = \xi$.*

8.4.3. Die Irreduzibilität der Kreisteilungspolynome für prime Einheitswurzeln haben wir bereits in 6.8.4 gezeigt. In diesem Fall vereinfacht sich der Beweis entsprechend.

8.4.4. Wählt man eine Einbettung des n-ten Kreisteilungskörpers $\mathbb{Q}(\sqrt[n]{1})$ nach $\mathbb{C}$, so ist das Bild stets der von $\mathbb{Q}$ und $\mathrm{e}^{2\pi\mathrm{i}/n}$ in $\mathbb{C}$ erzeugte Teilkörper. Von den Automorphismen unseres Kreisteilungskörpers läßt sich jedoch außer der Identität nur ein einziger stetig auf $\mathbb{C}$ fortsetzen, und dieser Automorphismus ist für jede Wahl der Einbettung derselbe und kann beschrieben werden als der Automorphismus, der jede Einheitswurzel auf ihr multiplikatives Inverses wirft.

8.4.5. Ich schicke dem Beweis einige allgemeine Betrachtungen zu zyklischen Gruppen voraus. Für $n \geq 1$ liefert ja sicher die Multiplikation einen Isomorphismus $(\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ zwischen der Einheitengruppe unseres Restklassenrings und der Automorphismengruppe seiner zyklischen Gruppe. Die Umkehrabbildung kann angegeben werden durch die Abbildungsvorschrift $\psi \mapsto \psi(1)$ für jeden Automorphismus ψ. Ist allgemeiner C irgendeine additiv notierte zyklische Gruppe der Ordnung n, so erhalten wir folglich einen Isomorphismus $(\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Aut}(C)$ durch die Abbildungsvorschrift $a \mapsto (c \mapsto ac)$, und ist μ irgendeine multiplikativ notierte zyklische Gruppe der Ordnung n, so erhalten wir ebenso einen Isomorphismus $(\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Aut}(\mu)$ durch die Abbildungsvorschrift $a \mapsto (\zeta \mapsto \zeta^a)$. Des weiteren gibt es für je zwei Erzeuger einer zyklischen Gruppe genau einen Automorphismus, der den einen in den anderen überführt.

Beweis. 1. Ist ζ eine primitive n-te Einheitswurzel, so sind alle anderen primitiven n-ten Einheitswurzeln von der Form ζ^a für $a \in \mathbb{Z}$ mit a teilerfremd zu n alias mit $\langle a, n\rangle = \langle 1\rangle$. Sei nun $\Phi_n = fg$ eine Zerlegung in $\mathbb{Z}[X]$ mit f dem Minimalpolynom von ζ. Sicher ist dann auch g normiert. Es reicht zu zeigen, daß für jede Nullstelle $\zeta \in \mathbb{C}$ von f und $p \in \mathbb{N}$ prim mit $p \nmid n$ auch ζ^p eine Nullstelle von f ist, denn dann sind alle Wurzeln von Φ_n schon Wurzeln von f und es folgt $\Phi_n = f$. Aber sei sonst p prim mit $p \nmid n$ und $g(\zeta^p) = 0$. Nach Annahme teilt dann f das Polynom $g(X^p)$ in $\mathbb{Q}[X]$ und nach Gauß sogar in $\mathbb{Z}[X]$ und nach Übergang zu $\mathbb{F}_p[X]$ ist $\bar{f}$ Teiler von $\bar{g}(X^p) = \bar{g}^p$. Dann haben aber $\bar{f}$ und $\bar{g}$ eine gemeinsame Nullstelle im Zerfällungskörper von $X^n - 1$ über $\mathbb{F}_p$, und das steht im Widerspruch dazu, daß nach 7.9.14 das Polynom $X^n - 1$ über $\mathbb{F}_p$ für $p \nmid n$ keine mehrfachen Nullstellen in seinem Zerfällungskörper hat.

2. Sicher wird $\mathbb{Q}(\sqrt[n]{1})$ erzeugt von jeder primitiven n-ten Einheitswurzel ζ, und da Φ_n nach Teil 1 ihr Minimalpolynom ist, folgt mit 7.3.3

$$[\mathbb{Q}(\sqrt[n]{1}) : \mathbb{Q}] = \deg \Phi_n = |(\mathbb{Z}/n\mathbb{Z})^\times|$$

Sicher liefert die Operation der Galoisgruppe auf den n-ten Einheitswurzeln weiter eine Einbettung $\mathrm{Gal}(\mathbb{Q}(\sqrt[n]{1})/\mathbb{Q}) \hookrightarrow \mathrm{Aut}(\mu_n)$ und nach 4.3.3 haben wir einen kanonischen Isomorphismus $(\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Aut}(\mu_n)$. Da diese drei Gruppen alle gleichviele Elemente haben, folgt der Satz. □

8.4.6. Man erklärt die **Euler'sche φ-Funktion** $\varphi : \mathbb{Z}_{\geq 1} \to \mathbb{Z}_{\geq 1}$ durch die Vorschrift

$$\begin{array}{rcl} \varphi(n) & = & \text{Zahl der zu } n \text{ teilerfremden } d \in \mathbb{N} \text{ mit } 1 \leq d \leq n \\ & = & \text{Zahl der Erzeuger der Gruppe } \mathbb{Z}/n\mathbb{Z} \\ & = & |\{x \in \mathbb{Z}/n\mathbb{Z} \mid \mathrm{ord}(x) = n\}| \\ & = & |(\mathbb{Z}/n\mathbb{Z})^\times| \end{array}$$

Wir haben etwa $\varphi(1) = \varphi(2) = 1$, $\varphi(3) = \varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$ und so weiter. Nach 8.4.2 haben wir auch $\varphi(n) = \deg \Phi_n = [\mathbb{Q}(\sqrt[n]{1}) : \mathbb{Q}]$.

Satz 8.4.7 (Konstruierbarkeit regelmäßiger n-Ecke). *Genau dann ist das regelmäßige n-Eck konstruierbar mit Zirkel und Lineal, wenn der Wert $\varphi(n)$ der Euler'schen φ-Funktion an der Stelle n eine Zweierpotenz ist.*

Beweis. Sei ζ eine primitive n-te Einheitswurzel. Ist $\varphi(n) = [\mathbb{Q}(\zeta) : \mathbb{Q}]$ keine Zweierpotenz, so kann ζ nicht konstruierbar sein nach 7.6.4. Ist $\varphi(n)$ eine Zweierpotenz, so ist $G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ eine 2-Gruppe. Nach 5.3.8 oder einfacher induktiv nach 3.3.18 gibt es dann in G eine Kette von Normalteilern von G der Gestalt

$$G = G_r \supset G_{r-1} \supset \ldots \supset G_0 = 1$$

mit $G_i/G_{i-1} \cong \mathbb{Z}/2\mathbb{Z}$ für $1 \leq i \leq r$. Deren Fixkörper bilden eine Kette

$$\mathbb{Q} = K_r \subset K_{r-1} \subset \ldots \subset K_0 = \mathbb{Q}(\zeta)$$

von Teilkörpern mit $[K_{i-1} : K_i] = 2$ für $1 \leq i \leq r$. Diese Kette hinwiederum zeigt mit 7.6.2, daß ζ konstruierbar ist. □

Lemma 8.4.8 (Rechenregeln für die Euler'sche φ-Funktion). *1. Sind positive natürliche Zahlen n und m teilerfremd, so gilt $\varphi(nm) = \varphi(n)\varphi(m)$;*

2. Für p eine Primzahl und $r \geq 1$ beliebig gilt $\varphi(p^r) = p^{r-1}(p-1)$.

Beweis. 1. Der Isomorphismus $\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ von Ringen induziert einen Isomorphismus $(\mathbb{Z}/nm\mathbb{Z})^\times \cong (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times$ der zugehörigen Einheitengruppen.

2. Es gibt p^{r-1} Vielfache n von p mit $1 \leq n \leq p^r$, also gilt

$$\varphi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1)$$ □

8.4.9 (**Diskussion der Zahlen n mit $\varphi(n)$ eine Zweierpotenz**). Damit $\varphi(n)$ eine Zweierpotenz ist, darf nach den eben erklärten Rechenregeln 8.4.8 nur der Primfaktor 2 in n mehrfach vorkommen, und alle anderen Primfaktoren müssen die Gestalt $2^r + 1$ haben. Nur dann kann aber $2^r + 1$ eine Primzahl sein, wenn r selbst eine Zweierpotenz ist, denn sonst wäre $r = st$ mit $t > 1$ ungerade, und wir könnten die Gleichung

$$(1 - X^t) = (1 - X)(1 + X + \ldots + X^{t-1})$$

spezialisieren zu $X = -2^s$ und so $1 + 2^r$ nichttrivial faktorisieren. Genau dann ist also $\varphi(n)$ eine Zweierpotenz, wenn alle Primfaktoren von n Fermat'sche Primzahlen im Sinne der folgenden Bemerkung sind und keine Primfaktoren außer der Zwei mehrfach vorkommen.

Ergänzung 8.4.10. Die Zahlen $F_k := 1+2^{2^k}$ heißen **Fermat'sche Zahlen**. F_0, F_1, F_2, F_3, F_4 sind prim, aber $F_5 = 1+2^{32} = 641 \cdot 6700417$ ist nach Euler nicht prim. Es ist nicht bekannt, ob es außer den 5 Ersten noch weitere Fermat'sche Zahlen gibt, die prim sind. Bekannt ist, daß die Fermat'schen Zahlen F_k für $5 \leq k \leq 32$ nicht prim sind, jedenfalls habe ich das 2020 mit Zitat in Wikipedia gelesen.

Ergänzung 8.4.11. Wie gesagt kann $\varphi(m)$ auch interpretiert werden als die Ordnung der Einheitengruppe des Restklassenrings $\mathbb{Z}/m\mathbb{Z}$, in Formeln

$$\varphi(m) = |(\mathbb{Z}/m\mathbb{Z})^\times|$$

Wenden wir auf diese Gruppe unsere Erkenntnis 3.3.8 an, daß die Ordnung jedes Elements einer endlichen Gruppe die Gruppenordnung teilt, so erhalten wir für b teilerfremd zu m insbesondere die sogenannte **Euler'sche Kongruenz**

$$b^{\varphi(m)} \equiv 1 \pmod{m}$$

Ergänzung 8.4.12. Wenn man die Eulersche φ-Funktion einführt, so darf die witzige Identität

$$n = \sum_{d|n} \varphi(d)$$

nicht fehlen. Um sie zu zeigen bemerke man, daß auch für jedes Vielfache $n = cd$ einer Zahl d schon gilt $\varphi(d) = |\{x \in \mathbb{Z}/n\mathbb{Z} \mid \operatorname{ord}(x) = d\}|$. In der Tat liefert nämlich die Multiplikation mit c eine Einbettung $\mathbb{Z}/d\mathbb{Z} \hookrightarrow \mathbb{Z}/n\mathbb{Z}$, deren Bild genau aus allen $x \in \mathbb{Z}/n\mathbb{Z}$ besteht, deren Ordnung d teilt.

Übungen

Übung 8.4.13. Man zeige, daß man aus einem regelmäßigen 7-Eck mit Zirkel und Lineal ein regelmäßiges 35-Eck konstruieren kann. Hinweis: Man verwende 7.6.10.

Übung 8.4.14. Wieviele zu 140000 teilerfremde Zahlen a mit $1 \leq a \leq 140000$ gibt es?

Übung 8.4.15 (**Konstruierbarkeitskriterium**). Man zeige: Eine algebraische komplexe Zahl ist konstruierbar genau dann, wenn der Grad des Zerfällungskörpers ihres Minimalpolynoms über $\mathbb{Q}$ eine Zweierpotenz ist.

Übung 8.4.16. Man zeige, daß die Einheitswurzeln des n-ten Kreisteilungskörpers für gerades n genau die n-ten Einheitswurzeln sind und für ungerades n genau die $2n$-ten Einheitswurzeln.

Übung 8.4.17. Man zeige für die Euler'sche φ-Funktion und alle $n \geq 1$ die Identität $\varphi(n^2) = n\varphi(n)$.

Übung 8.4.18. Seien $m, n \geq 1$ natürliche Zahlen und k ihr kleinstes gemeinsames Vielfaches. Man zeige $\mathbb{Q}(\sqrt[n]{1},\ \sqrt[m]{1}) = \mathbb{Q}(\sqrt[k]{1})$ für beliebige entsprechende primitive Einheitswurzeln Hinweis: Ist $k = an = bm$ mit $(a, b) = 1$, so gibt es x, y mit $ax + by = 1$ alias $\zeta_k = (\zeta_k^a)^x(\zeta_k^b)^y$.

Übung 8.4.19. Gegeben $n > 2$ zeige man, daß im Kreisteilungskörper $\mathbb{Q}(\sqrt[n]{1}) = \mathbb{Q}(\zeta)$ für ζ eine primitive n-te Einheitswurzel gilt $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})] = 2$ und $[\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}(\zeta)] = \varphi(n)/2$. Man folgere $\Phi_n(X) = X^{\varphi(n)}\Phi_n(X^{-1})$.

8.5 Quadratisches Reziprozitätsgesetz

8.5.1. Gegeben ganze Zahlen $a, b \in \mathbb{Z}$ stellen wir uns nun die Frage, ob es ganze Zahlen $x, y \in \mathbb{Z}$ gibt mit

$$a = x^2 + by$$

Ist das der Fall, so nennt man a einen **quadratischen Rest modulo** b. Gleichbedeutend können wir auch fragen, ob eine Restklasse $\bar{x} \in \mathbb{Z}/b\mathbb{Z}$ existiert mit $\bar{a} = \bar{x}^2$, ob also $\bar{a}$ ein Quadrat ist in $\mathbb{Z}/b\mathbb{Z}$. Es mag a priori nicht klar sein, ob diese Frage derart wichtig ist, daß ihre Behandlung einen eigenen Abschnitt verdient. A posteriori hat sich die Untersuchung dieser Frage und ihrer Verallgemeinerungen jedoch als derart fruchtbar erwiesen, daß es mir angemessen scheint, sie hier zu diskutieren. Zunächst reduzieren wir unsere Frage dazu auf den Fall b prim und erklären dann, wie sie in diesem Fall durch das sogenannte „quadratische Reziprozitätsgesetz" gelöst wird. Es gibt verschiedene Beweise des quadratischen Reziprozitätsgesetzes, dessen verblüffende Aussage viele Mathematiker fasziniert hat. Wir geben hier einen Beweis mit den Methoden der Galoistheorie. Er ist vielleicht nicht der elementarste Beweis, aber in meinen Augen doch der Beweis, bei dem am wenigsten „gezaubert" wird. Darüber hinaus weist er die Richtung, in der die meines Erachtens interessantesten Verallgemeinerungen zu finden sind.

8.5.2 (**Reduktion auf $b = p^n$ eine Primzahlpotenz**). Gegeben $b_1, b_2 \in \mathbb{Z}$ teilerfremd ist a ein Quadrat modulo $b_1 b_2$ genau dann, wenn es ein Quadrat ist modulo b_1 und ein Quadrat modulo b_2. Das folgt unmittelbar aus unserem Ringisomorphismus

$$\mathbb{Z}/b_1 b_2 \mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/b_1\mathbb{Z} \times \mathbb{Z}/b_2\mathbb{Z}$$

alias dem chinesischen Restsatz 3.3.11. Nach dieser Bemerkung werden wir uns bei der Untersuchung unserer ursprünglichen Frage auf den Fall beschränken, daß b eine echte Primzahlpotenz ist. Für Zahlen b, deren Primfaktorzerlegung wir nicht kennen, ist uns damit zwar wenig geholfen, aber für diese b ist nun einmal schlicht kein schnelles Verfahren bekannt, mit dem die Frage entschieden werden könnte, ob ein gegebenes a quadratischer Rest modulo b ist oder nicht.

8.5.3 (**Reduktion auf a teilerfremd zu $b = p^n$**). Sei nun also b eine echte Primzahlpotenz, sagen wir $b = p^n$. Ist dann $a = p^r\alpha$ die Darstellung von a als Produkt mit α teilerfremd zu p, so ist die Gleichung

$$a = p^r\alpha = x^2 + yp^n$$

für $r \geq n$ bereits mit $x = 0$ lösbar. Haben wir dahingegen $r + t = n$ mit $t > 0$, so folgt aus der Identität $p^r\alpha = x^2 + yp^r p^t$, daß die maximale p-Potenz, die die rechte Seite teilt, entweder gerade ist oder mindestens p^{r+1}. Diese Gleichung ist also für $t > 0$ nur unter der Annahme r gerade lösbar, und unter dieser Annahme genau dann, wenn die Gleichung

$$\alpha = \tilde{x}^2 + yp^t$$

lösbar ist alias wenn α ein Quadrat ist modulo p^t. Auf diese Weise können wir uns bei der Untersuchung unserer ursprünglichen Frage weiter auf den Fall zurückziehen, daß b eine echte Primzahlpotenz ist und zusätzlich a teilerfremd zu b.

8.5.4 (**Reduktion von $b = p^n$ auf $b = p$ für $p \neq 2$**). Ist p eine ungerade Primzahl und a teilerfremd zu p, so ist a ein Quadrat modulo p^n für $n \geq 2$ genau dann, wenn a ein Quadrat ist modulo p. Das folgt leicht aus 3.4.32 oder besser seinem Beweis, wo Sie gezeigt haben, daß die Projektion $(\mathbb{Z}/p^n\mathbb{Z})^\times \twoheadrightarrow (\mathbb{Z}/p\mathbb{Z})^\times$ faktorisiert über einen Isomorphismus mit der Projektion als zweitem Pfeil in der Form

$$(\mathbb{Z}/p^n\mathbb{Z})^\times \xrightarrow{\sim} \mathbb{Z}/p^{n-1}\mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^\times \twoheadrightarrow (\mathbb{Z}/p\mathbb{Z})^\times$$

Da die Zwei teilerfremd ist zu p, ist nun jedes Element von $\mathbb{Z}/p^{n-1}\mathbb{Z}$ das Doppelte von einem anderen, und das beendet auch bereits unsere Reduktion. Durch Induktion über n kann man sogar explizit eine Lösung finden: Gegeben $\tilde{x}, \tilde{y} \in \mathbb{Z}$

mit $a = \tilde{x}^2 + \tilde{y}p^n$ machen wir zur Lösung der Gleichung $a = x^2 + yp^{n+1}$ den Ansatz $x = \tilde{x} + \lambda p^n$ und finden für λ die Gleichung

$$a = \tilde{x}^2 + 2\lambda p^n \tilde{x} + \lambda^2 p^{2n} + yp^{n+1}$$

Wegen $a - \tilde{x}^2 = \tilde{y}p^n$ kann sie umgeschrieben werden zu

$$2\lambda\tilde{x} = \tilde{y} - \lambda^2 p^n - yp$$

Da nun nach Annahme 2 und a und damit auch $\tilde{x}$ invertierbar sind in $\mathbb{Z}/p\mathbb{Z}$, hat diese Gleichung stets eine Lösung λ.

8.5.5 (**Reduktion von $b = 2^n$ auf $b = 8$**). Eine ungerade Zahl ist ein quadratischer Rest modulo 2^n für $n \geq 3$ genau dann, wenn sie ein quadratischer Rest ist modulo 8 alias kongruent zu 1 modulo 8. Daß diese Bedingung notwendig ist, scheint mir offensichtlich. Um zu zeigen, daß sie auch hinreichend ist, erinnern wir wieder aus 3.4.32 oder besser seinem Beweis, daß sich die offensichtliche Surjektion $(\mathbb{Z}/2^n\mathbb{Z})^\times \twoheadrightarrow (\mathbb{Z}/8\mathbb{Z})^\times$ als rechte Vertikale in ein kommutatives Diagramm

$$\begin{array}{ccccc} (\mathbb{Z}/2^n\mathbb{Z})^\times & \tilde{\to} & \mathbb{Z}/2^{n-2}\mathbb{Z} \times (\mathbb{Z}/4\mathbb{Z})^\times & \tilde{\to} & \mathbb{Z}/2^{n-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \\ \downarrow & & \downarrow & & \downarrow \\ (\mathbb{Z}/8\mathbb{Z})^\times & \tilde{\to} & \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/4\mathbb{Z})^\times & \tilde{\to} & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \end{array}$$

mit den offensichtlichen Surjektionen in den Vertikalen einbetten läßt. Aus diesem Diagramm ist die Behauptung dann unmittelbar ersichtlich. Um eine explizite Lösung zu finden, machen wir wieder Induktion über s und gehen also aus von einer Lösung der Gleichung $a = x^2 + y2^s$ mit $s \geq 3$. Ist y gerade, also $y = 2\tilde{y}$, so steht unsere Lösung für $s + 1$ schon da. Sonst ersetzen wir x durch $x + 2^{s-1}$ und finden so auch eine Lösung mit y gerade.

8.5.6. Mit diesen Überlegungen haben wir also unsere ursprüngliche Frage zurückgeführt auf die Frage, welche Zahlen quadratische Reste sind modulo ungerader Primzahlen und modulo 8. Ganz allgemein wissen wir seit 2.3.37, wiewiele Elemente eines endlichen Körpers $\mathbb{F}$ Quadrate sind, nämlich im Fall der Charakteristik Zwei alle und im Fall einer von 2 verschiedenen Charakteristik knapp über die Hälfte, genauer $(|\mathbb{F}| + 1)/2$ Elemente. Aber welche? In 8.5.18 erklären wir, wie diese Frage für endliche Primkörper durch das Zusammenwirken von quadratischem Reziprozitätsgesetz 8.5.7 und Ergänzungssatz 8.5.14 effizient gelöst werden kann.

Satz 8.5.7 (Quadratisches Reziprozitätsgesetz). *Seien p und q zwei verschiedene ungerade Primzahlen.*

1. *Ist p oder q kongruent zu 1 modulo 4, so ist p ein Quadrat modulo q genau dann, wenn q ein Quadrat ist modulo p;*

2. *Sind p und q kongruent zu 3 modulo 4, so ist p ein Quadrat modulo q genau dann, wenn q kein Quadrat ist modulo p.*

Beispiel 8.5.8. Wir betrachten $p = 7$ und $q = 103$. Wir finden $103 \equiv 5 \pmod 7$ und durch Ausprobieren sehen wir, daß $0, 1, 2, 4$ die einzigen Quadrate im Körper mit 7 Elementen sind. Insbesondere ist 103 kein Quadrat modulo 7. Unsere Primzahlen sind nun beide kongruent zu 3 modulo 4, und Teil zwei des quadratischen Reziprozitätsgesetzes sagt uns dann, daß 7 notwendig ein Quadrat modulo 103 sein muß. Ausprobieren liefert in der Tat $25^2 = 625 = 6 \times 103 + 7$.

8.5.9 (**Allgemeines zu zyklischen Gruppen**). Wir schicken dem Beweis einige allgemeine Überlegungen voraus. Ich erinnere zunächst daran, daß nach 3.4.26 jede nichttriviale zyklische Gruppe G gerader Ordnung $2n$ genau eine Untergruppe mit zwei Elementen und genau eine Untergruppe vom Index 2 hat. Für den in additiver Notation geschriebenen Gruppenhomomorphismus

$$(n\cdot) : G \to G$$

ist das Bild die einzige Untergruppe mit zwei Elementen und der Kern die einzige Untergruppe vom Index 2. Für den in additiver Notation geschriebenen Gruppenhomomorphismus

$$(2\cdot) : G \to G$$

ist dahingegen das Bild die einzige Untergruppe vom Index 2 und der Kern die einzige Untergruppe mit zwei Elementen.

Beispiel 8.5.10. Im Fall der additiven Gruppe $\mathbb{Z}/2n\mathbb{Z}$ ist $\{\bar 0, \bar n\} = n\mathbb{Z}/2n\mathbb{Z}$ die einzige zweielementige Untergruppe und $2\mathbb{Z}/2n\mathbb{Z}$ die einzige Untergruppe vom Index 2.

8.5.11. Im Fall der multiplikativen Gruppe $\mathbb{F}_p^\times$ für p eine ungerade Primzahl ist entsprechend $\{1, -1\}$ die einzige zweielementige Untergruppe und $(\mathbb{F}_p^\times)^2$ einzige Untergruppe vom Index 2 und das Potenzieren mit $(p-1)/2$ ist ein surjektiver Gruppenhomomorphismus $\mathbb{F}_p^\times \twoheadrightarrow \{1, -1\}$ mit Kern $(\mathbb{F}_p^\times)^2$. Wir führen nun für p prim und $a \in \mathbb{Z}$ das sogenannte **Legendre-Symbol** ein durch die Vorschrift

$$\left(\frac{a}{p}\right) := \begin{cases} 0 & a \text{ ist ein Vielfaches von } p; \\ 1 & a \text{ ist ein Quadrat modulo } p\text{, aber kein Vielfaches von } p; \\ -1 & \text{sonst.} \end{cases}$$

Für p eine ungerade Primzahl erhalten wir damit die Kongruenz

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$$

In der Tat folgt das für a teilerfremd zu p aus den vorhergehenden Überlegungen und in den anderen Fällen ist es eh klar. Des weiteren hängt auch für beliebige Primzahlen p das Legendresymbol nur von der Restklasse modulo p ab und es gilt die Multiplikativität

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

In der Tat folgt das für a und b teilerfremd zu p aus den vorhergehenden Überlegungen und in den anderen Fällen ist es eh klar.

8.5.12 (**Quadratische Teilerweiterungen in Galoiserweiterungen**). Seien L/K eine endliche Galoiserweiterung und $G := \mathrm{Gal}(L/K)$ ihre Galoisgruppe. Gegeben eine Untergruppe $H \subset G$ der Galoisgruppe vom Index 2 ist nach der Galoiskorrespondenz oder auch bereits nach 8.1.9 ihr Fixkörper L^H eine quadratische Erweiterung von K. Ist die Charakteristik kein Teiler von $|H|$, so kann dieser Fixkörper offensichtlich beschrieben werden durch die Formel

$$L^H = \left\{ \sum_{\sigma\in H} \sigma(\gamma) \,\middle|\, \gamma \in L \right\}$$

Die Bedingung an die Charakteristik wird dabei für die Inklusion $\subset$ benötigt, weil man damit $\alpha \in L^H$ schreiben kann als $\alpha = |H|^{-1}\sum_{\sigma\in H}\sigma(\alpha)$. Gilt zusätzlich $\mathrm{char}\, K \neq 2$, so sind die Elemente $\alpha \in L^H\backslash K$ mit $\alpha^2 \in K$ genau die Eigenvektoren zum Eigenwert (-1) des nichttrivialen Elements τ der zweielementigen Gruppe $\mathrm{Gal}(L^H/K) \cong G/H$ und man überlegt sich leicht, daß dieser Eigenraum beschrieben werden kann als

$$\mathrm{Eig}(\tau|L^H;-1) = \left\{ \sum_{\sigma\in H}\sigma(\gamma) - \sum_{\sigma\ \in G\backslash H}\sigma(\gamma) \,\middle|\, \gamma \in L \right\}$$

Gegeben $\gamma \in L$ gilt für $\alpha := \sum_{\sigma\in H}\sigma(\gamma) - \sum_{\sigma\ \in G\backslash H}\sigma(\gamma)$ auch ohne Vorausetzungen an die Charakteristik stets $\alpha \in L^H$ und $\alpha^2 \in K$ sowie unter den zusätzlichen Annahmen $\alpha \neq 0$ und $\mathrm{char}(K) \neq 2$ zusätzlich $L^H = K(\alpha) = K + K\alpha$.

8.5.13 (**Quadratwurzeln in Kreisteilungskörpern**). Gegeben p eine ungerade Primzahl betrachten wir den p-ten Kreisteilungskörper $\mathbb{Q}(\sqrt[p]{1})$ und erinnern unseren Isomorphismus $\mathbb{F}_p^\times \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\sqrt[p]{1}),\mathbb{Q})$ aus 8.4.2 und die Erkenntnis aus 3.4.17, daß $\mathbb{F}_p^\times$ eine zyklische Gruppe ist. Nach 8.5.9 hat die Galoisgruppe genau eine Untergruppe vom Index Zwei. Nach der Galoiskorrespondenz liegt damit in $\mathbb{Q}(\sqrt[p]{1})$ genau eine quadratische Erweiterung von $\mathbb{Q}$ und nach 8.5.12 und 8.5.11 hat für $\zeta \in \mathbb{Q}(\sqrt[p]{1})$ eine primitive p-te Einheitswurzel das Element

$$\alpha := \sum_{a\in\mathbb{F}_p^\times} \left(\frac{a}{p}\right)\zeta^a$$

die Eigenschaft $\alpha^2 \in \mathbb{Q}$. Dies Element α erzeugt folglich, wenn es nicht Null ist, die fragliche quadratische Erweiterung. Wir zeigen nun genauer durch explizite Rechnung die Formel

$$\alpha^2 = (-1)^{\frac{p-1}{2}} p$$

In der Tat, beachten wir $(\frac{ab^2}{p}) = (\frac{a}{p})$, so ergibt sich durch Substitution von ab für a die zweite Gleichung der Kette

$$\alpha^2 = \sum_{a,b \in \mathbb{F}_p^\times} \left(\frac{ab}{p}\right) \zeta^{a+b} = \sum_{a \in \mathbb{F}_p^\times} \left(\frac{a}{p}\right) \sum_{b \in \mathbb{F}_p^\times} (\zeta^{a+1})^b$$

Bei $a = -1$ ergibt sich ganz rechts der Beitrag $(\frac{-1}{p})(p-1)$. Bei $a \neq -1$ beachten wir, daß für $\eta = \zeta^{a+1}$ wie für jede primitive p-te Einheitswurzel die Relation

$$1 + \eta + \eta^2 + \ldots + \eta^{p-1} = 0$$

erfüllt ist, so daß die Summanden mit $a \neq -1$ jeweils den Beitrag $-(\frac{a}{p})$ liefern. Da nun die Summe der $(\frac{a}{p})$ über alle $a \in \mathbb{F}_p^\times$ verschwindet, und erst dafür brauchen wir $p \neq 2$, liefern alle Summanden mit $a \neq -1$ zusammen den Beitrag $(\frac{-1}{p})$ und mit 8.5.11 folgern wir

$$\alpha^2 = \left(\frac{-1}{p}\right) p = (-1)^{\frac{p-1}{2}} p$$

Im übrigen folgt $\alpha^2 \in \mathbb{Z}$ auch ohne alle Rechnung aus der Identität $\mathbb{Q} \cap \mathbb{Z}[\zeta] = \mathbb{Z}$. Um sie einzusehen, bemerkt man, daß $\mathbb{Z}[\zeta]$ eine endlich erzeugte abelsche Gruppe ist, der Schnitt ist mithin nach 3.4.1 auch eine endlich erzeugte abelsche Gruppe. Andererseits aber ist er auch ein Teilring von $\mathbb{Q}$, und diese beiden Eigenschaften zusammen zeigen nach Übung 6.2.8 bereits, daß unser Schnitt $\mathbb{Z}$ sein muß. Explizit prüft man für eine von Null verschiedene dritte Einheitswurzel ζ leicht $(\zeta - \zeta^2)^2 = -3$ und damit $\pm\sqrt{-3} \in \mathbb{Q}(\sqrt[3]{1})$. Die Beziehung zwischen regelmäßigem Fünfeck und dem goldenen Schnitt **??** zeigt weiter $\sqrt{5} \in \mathbb{Q}(\sqrt[5]{1})$.

Beweis des quadratischen Reziprozitätsgesetzes. Sei weiter p eine ungerade Primzahl. Wir betrachten die eindeutige quadratische Teilerweiterung unseres p-ten Kreisteilungskörpers, die wir in 8.5.13 bestimmt hatten zu $\mathbb{Q}(\zeta) \supset \mathbb{Q}(\alpha) \supset \mathbb{Q}$ mit $\alpha^2 = (-1)^{\frac{p-1}{2}} p$. Die Teilringe

$$\mathbb{Z}[\zeta] \supset \mathbb{Z}[\alpha] \supset \mathbb{Z}$$

sind offensichtlich stabil unter der Galoisgruppe $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. Jede Primzahl $q \neq p$ liefert unter $\mathbb{Z}\backslash p\mathbb{Z} \twoheadrightarrow \mathbb{F}_p^\times \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ ein Element σ_q der Galoisgruppe

mit $\sigma_q(\zeta) = \zeta^q$ und der von diesem Element auf $R := \mathbb{Z}[\zeta]/q\mathbb{Z}[\zeta]$ induzierte Ringautomorphismus ist folglich der Frobenius $r \mapsto r^q$. Das Bild von α in R notieren wir

$$\bar{\alpha} \in R$$

Das Bild der offensichtlichen Einbettung $\mathbb{F}_q \hookrightarrow R$ notieren wir von nun an kurzerhand auch $\mathbb{F}_q \subset R$. Wir nehmen nun zusätzlich $q \neq 2$ an und sind dann in genau einem der beiden folgenden Fälle:

1. $\bar{\alpha} \in \mathbb{F}_q$ und $\bar{\alpha}^2 \in (\mathbb{F}_q^\times)^2$ und $\sigma_q(\bar{\alpha}) = \bar{\alpha}$;
2. $\bar{\alpha} \notin \mathbb{F}_q$ und $X^2 - \bar{\alpha}^2$ irreduzibel in $\mathbb{F}_q[X]$ und $\mathbb{F}_q[\bar{\alpha}] \cong \mathbb{F}_{q^2}$ und $\sigma_q(\bar{\alpha}) = -\bar{\alpha}$.

Nun haben wir $\bar{\alpha}^2 = (-1)^{\frac{p-1}{2}}\bar{p}$ und zusammen mit unserer vergleichsweise banalen Erkenntnis $\sigma_q(\alpha) = (\frac{q}{p})\alpha$ folgt

$$\left(\frac{-1}{q}\right)^{\frac{p-1}{2}}\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$$

Zusammen mit unserer Erkenntnis $(\frac{-1}{q}) = (-1)^{\frac{q-1}{2}}$ aus 8.5.11 folgt dann das quadratische Reziprozitätsgesetz. □

Proposition 8.5.14 (Ergänzungssatz). *Für jede ungerade Primzahl p gilt*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{für } p \equiv \pm 1 \pmod 8; \\ -1 & \text{für } p \equiv \pm 3 \pmod 8. \end{cases}$$

Beweis. Wir beginnen wie beim Beweis des Reziprozitätsgesetzes und betrachten feiner

$$\beta := (\alpha + 1)/2 = \sum_{a \in (\mathbb{F}_p^\times)^2} \zeta^a$$

Dann haben wir wieder $\mathbb{Z}[\zeta] \supset \mathbb{Z}[\beta] \supset \mathbb{Z}$ und diese Teilringe sind stabil unter der Galoisgruppe $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ und für alle zu p teilerfremden ganzen Zahlen q finden wir

$$\sigma_q(\beta) = \begin{cases} \beta & \text{falls } (\frac{q}{p}) = 1; \\ \beta - \alpha & \text{falls } (\frac{q}{p}) = -1. \end{cases}$$

Unsere Einbettungen induzieren weiter für alle $q \in \mathbb{Z}$ Einbettungen

$$\mathbb{Z}[\zeta]/q\mathbb{Z}[\zeta] \supset \mathbb{Z}[\beta]/q\mathbb{Z}[\beta] \supset \mathbb{Z}/q\mathbb{Z}$$

Man kann das etwa daraus folgern, daß $\mathbb{Z}[\zeta]$ eine freie abelsche Gruppe vom Rang $p-1$ mit Erzeugern $1, \zeta, \ldots, \zeta^{p-2}$ oder besser Erzeugern $\zeta, \ldots, \zeta^{p-1}$ ist. Für jede Primzahl q ist damit der von σ_q auf $\mathbb{Z}[\beta]/q\mathbb{Z}[\beta]$ induzierte Ringautomorphismus

der Frobeniushomomorphismus. Weiter finden wir $\beta^2 = (\alpha^2 + 2\alpha + 1)/4$. Da wir stets $\alpha^2 = (-1)^{\frac{p-1}{2}} p = 4u+1$ schreiben können mit $u \in \mathbb{Z}$, ergibt sich $\beta^2 = u+\beta$ und das Einsetzen von $\bar{\beta}$ für X induziert einen Ringisomorphismus

$$\mathbb{F}_q[X]/\langle X^2 - X - u\rangle \xrightarrow{\sim} \mathbb{Z}[\beta]/q\mathbb{Z}[\beta]$$

Wir sind also in genau einem der folgenden zwei Fälle:

1. Das Polynom $X^2 - X - u$ ist irreduzibel in $\mathbb{F}_q[X]$ und es gilt $\sigma_q(\bar{\beta}) \neq \bar{\beta}$;
2. Das Polynom $X^2 - X - u$ ist reduzibel in $\mathbb{F}_q[X]$ und es gilt $\sigma_q(\bar{\beta}) = \bar{\beta}$.

Für $q \neq 2$ fallen wir von hier aus auf die bereits beim Beweis des Reziprozitätsgesetzes angestellten Überlegungen zurück. Für $q = 2$ jedoch zeigt das

$$(-1)^u = \left(\frac{2}{p}\right)$$

Die Parität von u hängt nun offensichtlich nur von der Restklasse von p modulo 8 ab und kurzes Durchprobieren zeigt, daß wir so genau den Ergänzungssatz erhalten. □

Vorschau 8.5.15. In der „algebraischen Zahlentheorie“ werden gewisse Tricks der vorhergehenden Argumentation zu einer Theorie ausgebaut. Gegeben ein **Zahlkörper** alias eine endliche Körpererweiterung $K/\mathbb{Q}$ kann man ganz allgemein in K stets einen ausgezeichneten Teilring konstruieren, der als abelsche Gruppe endlich erzeugt ist und der stabil ist unter der Galoisgruppe $G := \mathrm{Gal}(K/\mathbb{Q})$, nämlich den sogenannten **Ganzheitsring** oder **Ganzzahlenring**

$$R = \mathfrak{o}_K := \{r \in K \mid r \text{ ist Nullstelle eines normierten Polynoms aus } \mathbb{Z}[X]\}$$

Daß diese Teilmenge $R \subset K$ in der Tat ein Teilring ist, zeigen wir in **??**. In unserem Beispiel $\mathbb{Q}(\zeta) \supset \mathbb{Q}(\alpha) \supset \mathbb{Q}$ sind die Ganzheitsringe gerade die Teilringe $\mathbb{Z}[\zeta] \supset \mathbb{Z}[\beta] \supset \mathbb{Z}$, die wir beim Beweis des Ergänzungssatzes haben vom Himmel fallen lassen. Gegeben eine Erweiterung L/K von Zahlkörpern mit Ganzheitsringen $\mathfrak{o}_L \supset \mathfrak{o}_L$ ist nach **??** dann für jedes Ideal $\mathfrak{a} \subset \mathfrak{o}_K$ die offensichtliche Abbildung eine Injektion $\mathfrak{o}_K/\mathfrak{a} \hookrightarrow \mathfrak{o}_L/\mathfrak{a}\mathfrak{o}_L$.

8.5.16. Die Abbildung $n \mapsto (-1)^{\frac{n-1}{2}}$ von der Menge der ungeraden ganzen Zahlen in das Monoid der Vorzeichen ist die Verknüpfung der Restklassenabbildung mit dem einzigen Gruppenisomorphismus

$$2\mathbb{Z} + 1 \to (\mathbb{Z}/4\mathbb{Z})^\times \xrightarrow{\sim} \mathbb{Z}^\times$$

Insbesondere ist sie multiplikativ alias ein Monoidhomomorphismus.

8.5.17. Die Abbildung $n \mapsto (-1)^{\frac{n^2-1}{8}}$ von der Menge der ungeraden ganzen Zahlen in das Monoid der Vorzeichen ist die Verknüpfung der Restklassenabbildung mit einem surjektiven Gruppenhomomorphismus

$$2\mathbb{Z}+1 \to (\mathbb{Z}/8\mathbb{Z})^\times \twoheadrightarrow \mathbb{Z}^\times$$

Insbesondere ist sie multiplikativ alias ein Monoidhomomorphismus. In diesem Fall beachte man, daß es sogar vier Gruppenhomomorphismen $(\mathbb{Z}/8\mathbb{Z})^\times \to \mathbb{Z}^\times$ alias $\mathbb{F}_2^2 \to \mathbb{F}_2$ gibt, von denen drei surjektiv sind.

Ergänzung 8.5.18. Will man Legendre-Symbole tatsächlich ausrechnen, so erweist sich deren Erweiterung zu den sogenannten **Jacobi-Symbolen** als praktisch. Man definiert genauer für $a \in \mathbb{Z}$ beliebig und $n \in \mathbb{N}_{\geq 1}$ mit Primfaktorzerlegung $n = p_1 p_2 \ldots p_r$ das Jacobi-Symbol als Produkt von Legendre-Symbolen

$$\left(\frac{a}{n}\right) := \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_r}\right)$$

Aus den entsprechenden Eigenschaften des Legendre-Symbols folgt, daß auch das Jacobi-Symbol nur von der Restklasse von a modulo n abhängt und daß gilt

$$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right) \quad \text{und für } n \text{ ungerade} \quad \left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}.$$

Schließlich folgt aus dem quadratischen Reziprozitätsgesetz 8.5.7, daß allgemeiner für je zwei ungerade Zahlen $m, n \geq 1$ das **Reziprozitätsgesetz für Jacobi-Symbole**

$$\left(\frac{m}{n}\right) = (-1)^{\frac{n-1}{2}\frac{m-1}{2}}\left(\frac{n}{m}\right)$$

gilt, denn auch die Vorzeichen sind multiplikativ in ungeraden m und n, wie man durch Fallunterscheidung prüft. Für jede ungerade Zahl $n \geq 1$ folgt schließlich aus dem Ergänzungssatz 8.5.14 mühelos der **Ergänzungssatz für Jacobi-Symbole**

$$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}} = \begin{cases} 1 & \text{für } n \equiv \pm 1 \pmod 8; \\ -1 & \text{für } n \equiv \pm 3 \pmod 8. \end{cases}$$

Für die Primzahlen 1231 und 1549 finden wir so etwa

$$\begin{aligned}
&\left(\tfrac{1231}{1549}\right) = \left(\tfrac{1549}{1231}\right) = \left(\tfrac{318}{1231}\right) = \left(\tfrac{2}{1231}\right)\left(\tfrac{159}{1231}\right) = \left(\tfrac{159}{1231}\right) = -\left(\tfrac{1231}{159}\right) = -\left(\tfrac{118}{159}\right) = \\
&= -\left(\tfrac{2}{159}\right)\left(\tfrac{59}{159}\right) = -\left(\tfrac{59}{159}\right) = -\left(\tfrac{159}{59}\right) = -\left(\tfrac{41}{59}\right) = -\left(\tfrac{59}{41}\right) = -\left(\tfrac{18}{41}\right) = \\
&= -\left(\tfrac{2}{41}\right)\left(\tfrac{9}{41}\right) = -\left(\tfrac{9}{41}\right) = -\left(\tfrac{41}{9}\right) = -\left(\tfrac{5}{9}\right) = -\left(\tfrac{9}{5}\right) = -\left(\tfrac{4}{5}\right) = -\left(\tfrac{2}{5}\right)^2 = -1
\end{aligned}$$

mit unserem Reziprozitätsgesetz und Ergänzungssatz für Jacobi-Symbole. Die Zahl 1231 ist demnach kein quadratischer Rest modulo 1549. Alternativ hätten wir

auch den Rest von $1231^{1548/2} = 1231^{774}$ modulo 1548 ausrechnen können. Das dauert so lange auch wieder nicht, da wir zur Beschleunigung der Rechnung 774 in eine Summe von Zweierpotenzen entwickeln können als $774 = 512+256+4+2$, und dann müssen wir nur noch neun Quadrate in $\mathbb{Z}/1549\mathbb{Z}$ berechnen und vier dieser Quadrate in $\mathbb{Z}/1549\mathbb{Z}$ multiplizieren. Ganz so schnell wie obige Rechnung geht das dann aber doch nicht.

Übungen

Übung 8.5.19. Sei $a \in \mathbb{Z}$ fest vorgegeben. Man zeige: Ob a ein Quadrat ist modulo einer Primzahl q hängt nur von der Restklasse von q modulo $4a$ ab.

Ergänzung 8.5.20. Im Fall $a = -1$ kennen wir das das Resultat der vorhergehenden Übung 8.5.19 im Übrigen bereits aus 6.6.5. In der Sprache der algebraischen Zahlentheorie ist das eine starke Aussage über die Beziehungen zwischen dem „Verzweigungsverhalten der Erweiterung $\mathbb{Q}(\sqrt{a})/\mathbb{Q}$ an verschiedenen Primstellen“. Unser Beweis des Reziprozitätsgesetzes, das erst mal den Fall a prim liefert, geht aus vom explizit bekannten Verzweigungsverhalten bei Kreisteilungserweiterungen und folgert das Resultat daraus durch eine Art Galois-Abstieg.

Ergänzende Übung 8.5.21. Ein berühmter **Satz von Kronecker-Weber** besagt, daß jede endliche Galoiserweiterung des Körpers $\mathbb{Q}$ der rationalen Zahlen mit abelscher Galoisgruppe als Unterkörper eines Kreisteilungskörpers realisiert werden kann. Man zeige das für alle quadratischen Erweiterungen von $\mathbb{Q}$.

Ergänzung 8.5.22. Man mag den Satz von Kronecker-Weber interpretieren als eine explizite Beschreibung der „maximalen abelschen Erweiterung“ von $\mathbb{Q}$: Sie entsteht durch die Adjunktion aller Einheitswurzeln. **Hilbert's zwölftes Problem** fragt nach einer ähnlich expliziten Beschreibung der „maximalen abelschen Erweiterung“ eines beliebigen Zahlkörpers, als da heißt, eines beliebigen Körpers der Charakteristik Null von endlichem Grad über $\mathbb{Q}$.

Übung 8.5.23. Ist 283 ein quadratischer Rest modulo 397? Hinweis: 397 ist eine Primzahl.

Übung 8.5.24. Gibt es eine Quadratzahl, deren Darstellung im Dezimalsystem mit der Ziffernfolge 39 endet? Für welche Ziffern $a, b \in \{0, 1, \ldots, 9\}$ gibt es eine Quadratzahl, die mit der Ziffernfolge ab endet?

8.6 Radikalerweiterungen

Definition 8.6.1. Eine Galoiserweiterung mit zyklischer Galoisgruppe heißt eine **zyklische Erweiterung**. Eine Galoiserweiterung mit abelscher Galoisgruppe heißt eine **abelsche Erweiterung**.

8.6.2. Zerfällt das Polynom $X^n - 1$ in einem Körper vollständig in Linearfaktoren, so sagen wir, der besagte Körper **enthalte alle n-ten Einheitswurzeln**. Wir sagen, eine Körpererweiterung L/K **entstehe durch Adjunktion einer n-ten Wurzel**, wenn gilt $L = K(\alpha)$ für ein $\alpha \in L$ mit $\alpha^n \in K$.

Satz 8.6.3 (Zyklische Erweiterungen). *Seien K ein Körper und $n \geq 2$ eine natürliche Zahl derart, daß unser Körper alle n-ten Einheitswurzeln enthält und daß seine Charakteristik n nicht teilt. So gilt:*

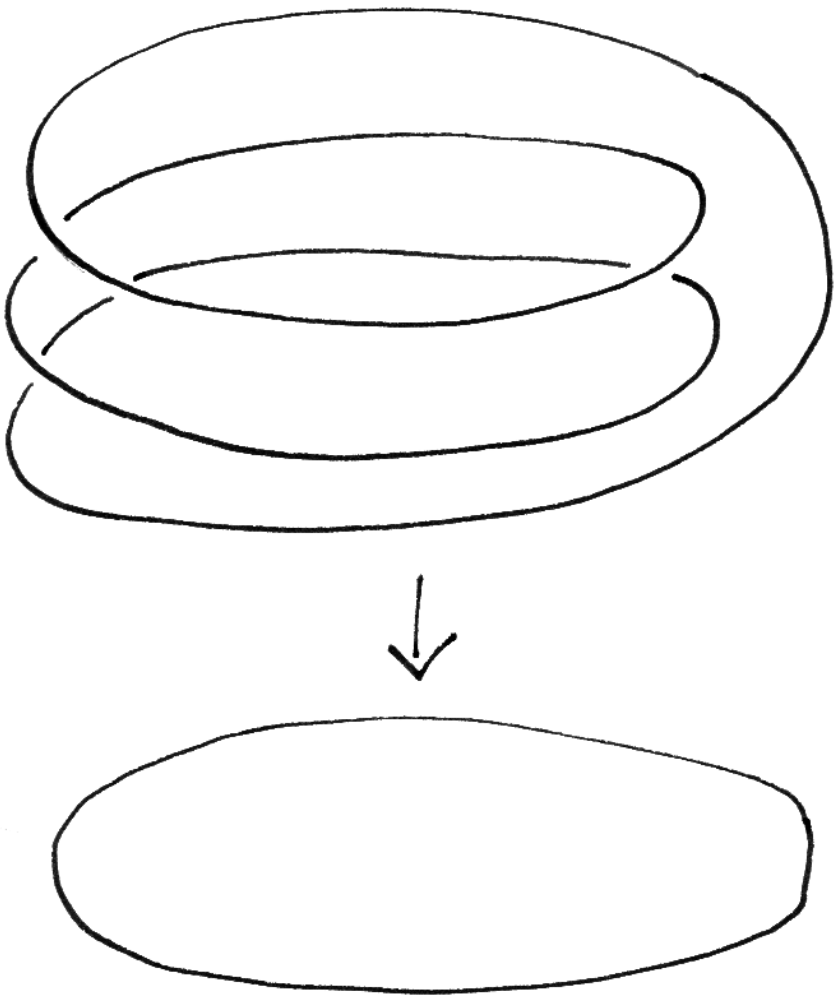
1. *Alle zyklischen Erweiterungen von K vom Grad n entstehen durch die Adjunktion einer n-ten Wurzel;*
2. *Adjungieren wir zu K eine n-te Wurzel, so erhalten wir eine zyklische Erweiterung, deren Grad n teilt.*

8.6.4. Der Beweis des ersten Teils beschreibt die Elemente sogar genauer, deren n-te Potenz im Grundkörper liegt und die unsere Erweiterung erzeugen: Es handelt sich genau um die Eigenvektoren eines beliebigen Erzeugers der Galoisgruppe mit einer primitiven n-ten Einheitswurzel als Eigenwert. Im Fall einer quadratischen Erweiterung wissen wir das schon länger.

8.6.5 (**Adjunktion von Einheitswurzeln und anderen Wurzeln im Vergleich**). Man beachte den fundamentalen Unterschied zwischen der Erweiterung eines Körpers durch n-te Einheitswurzeln und der Erweiterung eines Körpers mit n-ten Einheitswurzeln durch n-te Wurzeln aus von Eins verschiedenen Elementen: Setzen wir der Einfachkeit halber Charakteristik Null voraus, so ist im ersten Fall nach 8.4.2 und 8.6.10 die Ordnung der Galois-Gruppe ein Teiler von $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$ und im zweiten Fall ein Teiler von n.

Beweis. 2. Bezeichne $\mu_n \subset K^\times$ die Gruppe der n-ten Einheitswurzeln. Entsteht $L = K(\alpha)$ durch Adjunktion einer n-ten Wurzel aus $a = \alpha^n \in K$, so sind die Wurzeln des Polynoms $X^n - a$ genau alle $\zeta\alpha$ mit ζ den n-ten Einheitswurzeln und unsere Erweiterung ist folglich Galois. Weiter erhalten wir eine Injektion der Galois-Gruppe in die Gruppe μ_n der n-ten Einheitswurzeln, indem wir jedem $\sigma \in \mathrm{Gal}(L/K)$ diejenige Einheitswurzel ζ zuordnen mit $\sigma(\alpha) = \zeta\alpha$, also die Einheitswurzel $\sigma(\alpha)/\alpha$. An dieser Stelle verwenden wir, daß unser Grundkörper K alle n-ten Einheitswurzeln enthält, um nämlich zu zeigen, daß $\sigma \mapsto \sigma(\alpha)/\alpha$ ein Gruppenhomomorphismus $\mathrm{Gal}(L/K) \to \mu_n$ ist. Da nach 3.4.17 jede endliche Gruppe von Einheitswurzeln zyklisch ist, liefert die Adjunktion n-ter Wurzeln in der Tat zyklische Erweiterungen, deren Ordnung n teilt.

1. Sei umgekehrt L/K eine zyklische Erweiterung vom Grad n. Sei $\sigma \neq \mathrm{id}$ ein Erzeuger der Galoisgruppe. Wir fassen σ auf als eine K-lineare Abbildung



Anschauung für die durch Adjunktion einer dritten Wurzel aus T entstehenden Körpererweiterung des Funktionenkörpers $\mathbb{C}(T)$. In 8.2.7 wird erklärt, wie auch dies Bild zu interpretieren ist. Ich finde, man sieht in diesem Fall auch recht anschaulich, daß die Galoisgruppe zyklisch von der Ordnung drei ist.

$\sigma : L \to L$. Da gilt $\sigma^n = \mathrm{id}$ nach Voraussetzung und da $X^n - 1$ in $K[X]$ vollständig in Linearfaktoren zerfällt und paarweise verschiedene Nullstellen hat, ist σ nach der im Anschluß bewiesenen Proposition 8.6.6 diagonalisierbar und seine Eigenwerte sind n-te Einheitswurzeln. Da aus $\sigma(\alpha) = \zeta\alpha$ und $\sigma(\beta) = \eta\beta$ für n-te Einheitswurzeln ζ und η folgt $\sigma(\alpha\beta) = \zeta\eta\alpha\beta$, bilden die Eigenwerte von σ sogar eine Untergruppe $U \subset \mu_n$. Enthielte diese Untergruppe nicht alle n-ten Einheitswurzeln, so gäbe es einen Teiler d von n mit $d \neq n$ derart, daß σ^d als einzigen Eigenwert die 1 hätte. Dann müßte aber σ^d aufgrund seiner Diagonalisierbarkeit bereits selbst die Identität sein im Widerspruch zu unseren Annahmen. Also besteht U aus allen n-ten Einheitswurzeln und es gibt ein von Null verschiedenes $\alpha \in L$ mit $\sigma(\alpha) = \zeta\alpha$ für ζ eine primitive n-ten Einheitswurzel. Wir haben dann notwendig $\sigma(\alpha^n) = \alpha^n$, also $\alpha^n \in K$, aber die Potenzen $\alpha, \alpha^2, \ldots, \alpha^n$ sind linear unabhängig über K als Eigenvektoren zu paarweise verschiedenen Eigenwerten von σ. Es folgt $[K(\alpha) : K] = n$ und damit $L = K(\alpha)$. □

Proposition 8.6.6. *Seien f ein Endomorphismus eines Vektorraums V über einem Körper K und $P \in K[X]$ ein normiertes Polynom ohne mehrfache Nullstellen, das in K vollständig in Linearfaktoren zerfällt und f annulliert, in Formeln $P(f) = 0$. So ist f diagonalisierbar und seine Eigenwerte sind Nullstellen von P.*

Beweis. Man wähle einen festen Vektor $v \in V$ und suche dazu einen normierten Teiler $Q = (X - \lambda_1) \ldots (X - \lambda_r)$ von P kleinstmöglichen Grades r mit $Q(f) : v \mapsto 0$. Dann ist $E := \langle v, f(v), f^2(v), \ldots f^{r-1}(v)\rangle$ ein unter f stabiler Untervektorraum von V. Andererseits ist $(f - \lambda_2) \ldots (f - \lambda_r)v$ nach Annahme nicht Null und folglich ein Eigenvektor von f zum Eigenwert λ_1 in E. In derselben Weise finden wir auch Eigenvektoren zu den Eigenwerten $\lambda_2, \ldots, \lambda_r$. Da Eigenvektoren zu paarweise verschiedenen Eigenwerten linear unabhängig sind nach **??**, ist damit $f|_E$ diagonalisierbar und v eine Summe von Eigenvektoren von f. Die Proposition folgt. □

Zweiter Beweis. Wenn man bereits weiß, daß ein Endomorphismus eines endlichdimensionalen Vektorraums genau dann diagonalisierbar ist, wenn sein Minimalpolynom vollständig in Linearfaktoren zerfällt und keine mehrfachen Nullstellen hat, so bleibt im Fall eines endlichdimensionalen Raums nichts zu zeigen. Der Fall eines unendlichdimensionalen Raums ist für uns aber eh nicht relevant, und man kann sich von dort auch unschwer auf den Fall eines endlichdimensionalen Raums zurückziehen. □

Dritter Beweis. Der chinesische Restsatz liefert einen Ringisomorphismus

$$K[X]/\langle P\rangle \xrightarrow{\sim} K[X]/\langle X - \lambda_1\rangle \times \ldots \times K[X]/\langle X - \lambda_n\rangle$$

für λ_i die Nullstellen von P. Ist $1 = e_1 + \ldots + e_n$ die zugehörige Zerlegung der Eins in die Einselemente der Faktoren und vereinbaren wir für jeden Vektor $v \in V$

und $Q \in K[X]/\langle P\rangle$ die Notation $Qv = (Q(f))(v)$, so wird $v = e_1v + \ldots + e_nv$ eine Zerlegung mit $e_iv \in \mathrm{Eig}(f;\lambda_i)$. □

Korollar 8.6.7 (**Adjunktion primer Wurzeln**). *Seien p eine Primzahl und K ein Körper einer Charakteristik $\mathrm{char}\, K \neq p$, der alle p-ten Einheitswurzeln enthält. Genau dann ist eine echte Erweiterung unseres Körpers Galois vom Grad p, wenn sie durch Adjunktion einer p-ten Wurzel entsteht.*

Beweis. Eine Galoiserweiterung von Primzahlordnung ist notwendig zyklisch, denn jede Gruppe von Primzahlordnung ist zyklisch. Das Korollar folgt damit aus 8.6.3. □

Definition 8.6.8. Sind in einem Körper Ω zwei Teilkörper $K, L \subset \Omega$ gegeben, so bezeichnet $(KL) \subset \Omega$ den von K und L in Ω erzeugten Teilkörper. Man nennt diesen Körper das **Kompositum von K und L**.

8.6.9 (**Diskussion der Notation**). Für das Kompositum ist die abkürzende Notation $(KL) = KL$ üblich. Ich verwende hier etwas pedantisch die Notation (KL), da ja KL in unseren Konventionen **??** a priori nur die Menge aller Produkte bedeutet und man oft runde Klammern als Symbol für die „Erzeugung als Körper“ verwendet.

Satz 8.6.10 (**Translationssatz der Galoistheorie**). *Seien in einem Körper Ω zwei Teilkörper $K, L \subset \Omega$ gegeben. Ist $L \supset (K \cap L)$ eine endliche Galoiserweiterung, so ist auch $(KL) \supset K$ eine endliche Galoiserweiterung und die Restriktion liefert einen Isomorphismus von Galoisgruppen*

$$\mathrm{Gal}((KL)/K) \xrightarrow{\sim} \mathrm{Gal}(L/K \cap L)$$

8.6.11. Insbesondere gilt dieser Situation $[L : K \cap L] = [(KL) : K]$. Ohne die Galois-Bedingung gilt das im Allgemeinen nicht. Als Gegenbeispiel betrachte man in $\Omega := \mathbb{C}$ die von zwei verschiedenen dritten Wurzeln aus 2 über $\mathbb{Q}$ erzeugten Teilkörper K und L. Da jeder von ihnen nur zwei Teilkörper hat, muß hier gelten $K \cap L = \mathbb{Q}$. Ihr Kompositum (KL) hat Grad 6 über $\mathbb{Q}$ und damit Grad 2 über K und über L.

Vorschau 8.6.12. Der obige Translationssatz gilt auch ohne die Annahme, unsere Erweiterung sei endlich. Sogar wenn wir nur $L \supset (K \cap L)$ normal annehmen, folgt bereits $(KL) \supset K$ normal und die Restriktion liefert einen Isomorphismus von Galoisgruppen. Wir zeigen das in **??**.

Beweis. Mit $L/(K \cap L)$ ist auch $(KL)/K$ erzeugt von endlich vielen separablen Elementen beziehungsweise ein Zerfällungskörper. Also ist $(KL)/K$ Galois und K ist nach 8.1.12 der Fixkörper der Galoisgruppe $K = (KL)^G$ für

$G = \mathrm{Gal}((KL)/K)$. Da L normal ist über $(K \cap L)$, stabilisieren alle Körperautomorphismen von (KL) über K den Unterkörper L, und die durch Restriktion gegebene Abbildung $\rho : \mathrm{Gal}((KL)/K) \to \mathrm{Gal}(L/(K \cap L))$ zwischen den Galoisgruppen ist offensichtlich injektiv. Der Fixkörper des Bildes von ρ ist aber genau $L^{\rho(G)} = K \cap L$, und das zeigt mit unserem Satz 8.1.9 über Galoiserweiterungen durch Gruppenoperationen $\rho(G) = \mathrm{Gal}(L/(K \cap L))$ alias die Surjektivität der Restriktionsabbildung. □

Korollar 8.6.13. *Sind in einem Körper Ω Teilkörper M sowie $T \supset S$ gegeben und ist $T \supset S$ endlich und Galois, so ist auch $(TM) \supset (SM)$ endlich und Galois und die Restriktion liefert eine Inklusion von Galoisgruppen*

$$\mathrm{Gal}((TM)/(SM)) \hookrightarrow \mathrm{Gal}(T/S)$$

Beweis. Wir wenden den Translationssatz an auf $K := T$ und $L := (SM)$. Mit $T \supset S$ ist ja erst recht $T \supset (T \cap (SM))$ Galois, etwa nach der Galoiskorrespondenz. Also ist nach dem Translationssatz 8.6.10 auch die Körpererweiterung $(TM) = (T(SM)) \supset (SM)$ Galois und letztere beiden Erweiterungen haben nach dem Translationssatz dieselbe Galoisgruppe. □

Definition 8.6.14. Sei L/K eine Körpererweiterung. Wir nennen L eine **Radikalerweiterung von** K, wenn es eine Körperkette

$$K = K_0 \subset K_1 \subset K_2 \subset \ldots \subset K_r = L$$

gibt derart, daß der nächstgrößere Körper jeweils entsteht durch Adjunktion einer Wurzel, daß es also in Formeln jeweils $\alpha_i \in K_i$ und $n_i \geq 2$ gibt derart, daß gilt $\alpha_i^{n_i} \in K_{i-1}$ und $K_i = K_{i-1}(\alpha_i)$.

8.6.15. Das Wort „Radikal“ ist der lateinische Ausdruck für „Wurzel“. Unsere Radikalerweiterungen würde man also auf Deutsch bezeichnen als „Erweiterungen, die durch sukzessives Wurzelziehen entstehen“.

Definition 8.6.16. Sei M/K eine Körpererweiterung. Wir sagen, ein Element $\alpha \in M$ läßt sich **darstellen durch Radikale über** K, wenn sich $K(\alpha)$ in eine Radikalerweiterung von K einbetten läßt.

Beispiel 8.6.17. Die folgende reelle Zahl läßt sich darstellen durch Radikale über dem Körper $\mathbb{Q}$ der rationalen Zahlen:

$$\frac{\sqrt[7]{\sqrt[5]{6}+3}+13}{\sqrt[2]{3}+8} - \sqrt[17]{19876} + \sin(\pi/7)$$

Definition 8.6.18. Seien K ein Körper und $P \in K[X]\backslash 0$ ein von Null verschiedenes Polynom. Wir sagen, die Gleichung $P(X) = 0$ läßt sich **auflösen durch Radikale**, wenn sich alle Nullstellen des Polynoms P in seinem Zerfällungskörper durch Radikale über K darstellen lassen.

8.6.19. Ist unser Polynom irreduzibel, so läßt es sich offensichtlich genau dann auflösen durch Radikale, wenn sich eine Nullstelle durch Radikale über K darstellen läßt.

8.6.20. Ich erinnere, daß eine Gruppe G nach 5.3.9 **auflösbar** heißt, wenn es eine Folge von Untergruppen $G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_r = 1$ gibt mit G_i normal in G_{i-1} und G_{i-1}/G_i abelsch für $1 \leq i \leq r$.

Proposition 8.6.21 (**Radikalerweiterungen und Galoiserweiterungen**). *Sei K ein Körper der Charakteristik $\operatorname{char} K = 0$ und sei L/K eine Körpererweiterung von K. So sind gleichbedeutend:*

1. *Die Erweiterung L läßt sich einbetten in eine Radikalerweiterung des Körpers K;*
2. *Die Erweiterung L läßt sich einbetten in eine endliche Galoiserweiterung des Körpers K mit auflösbarer Galoisgruppe.*

Beweis. $2 \Rightarrow 1$. Sei L/K eine endliche Galoiserweiterung mit auflösbarer Galoisgruppe $G = \operatorname{Gal}(L/K)$. So gibt es eine Folge von Untergruppen

$$G = G_0 \supset G_1 \supset \ldots \supset G_r = 1$$

mit G_i normal in G_{i-1} und G_{i-1}/G_i zyklisch von Primzahlordnung für $1 \leq i \leq r$. Die zugehörige Kette von Fixkörpern ist eine Kette von zyklischen Erweiterungen von Primzahlordnung

$$K = K_0 \subset K_1 \subset \ldots \subset K_r = L$$

Adjungieren wir eine primitive $|G|$-te Einheitswurzel ζ, so erhalten wir nach dem Translationssatz 8.6.10 oder besser seinem Korollar 8.6.13 und zusätzlich unserer Diskussion von Kreisteilungserweiterungen für den ersten Schritt wieder eine Kette

$$K = K_0 \subset K_0(\zeta) \subset K_1(\zeta) \subset \ldots \subset K_r(\zeta) = L(\zeta)$$

von Galoiserweiterungen. Nach unserem Satz über Adjunktion primer Wurzeln 8.6.7 ensteht hier auch jede höhere Stufe durch Adjunktion einer geeigneten Wurzel aus der vorherigen Stufe. Mithin läßt sich L in eine Radikalerweiterung von K einbetten, nämlich in die Radikalerweiterung $L(\zeta)$.

$1 \Rightarrow 2$. Sei L/K eine Radikalerweiterung. Offensichtlich können wir L auch erhalten, indem wir sukzessive Wurzeln von Primzahlordnung $\sqrt[p_i]{a_i}$ adjungieren, für geeignete Primzahlen p_i. Es gibt also eine Körperkette

$$K = K_0 \subset K_1 \subset K_2 \subset \ldots \subset K_r = L$$

sowie geeignete $\alpha_i \in K_i$ und Primzahlen p_i derart, daß für alle $i \geq 1$ gilt $K_i = K_{i-1}(\alpha_i)$ und $\alpha_i^{p_i} \in K_{i-1}$. Ist n das Produkt dieser p_i und adjungieren wir zu L eine primitive n-te Einheitswurzel ζ, so ist im Körperturm

$$K = K_0 \subset K_0(\zeta) \subset K_1(\zeta) \subset \ldots \subset K_r(\zeta) = L(\zeta)$$

jeder Schritt eine abelsche Erweiterung: Das folgt, indem wir den Translationssatz der Galoistheorie oder besser sein Korollar 8.6.13 im ersten Schritt auf die nach 8.4.2 abelsche Kreisteilungserweiterung $\mathbb{Q} \subset \mathbb{Q}(\zeta)$ anwenden und danach auf die $K_i \subset K_{i+1}$. Vergrößern wir nun $L(\zeta)$ zu einer normalen Erweiterung N/K und darin das Kompositum $M \subset N$ aller $\varphi(L(\zeta))$ mit $\varphi \in \mathrm{Ring}^K(L(\zeta), N)$, also in anderer Terminologie die normale Hülle M von $L(\zeta)$, so ist M eine Galoiserweiterung von K und es gibt einen Körperturm

$$K = M_0 \subset M_1 \subset M_2 \subset \ldots \subset M_t = M$$

derart, daß jede Stufe eine abelsche Erweiterung ist: Um solch einen Körperturm anzugeben, zählen wir unsere φ auf als $\varphi_1, \ldots, \varphi_m$, beginnen mit $M_1 = M_0(\zeta)$ und adjungieren der Reihe nach $\varphi_1(\alpha_1)$, $\varphi_1(\alpha_2), \ldots$, $\varphi_1(\alpha_r)$, $\varphi_2(\alpha_1)$, $\varphi_2(\alpha_2)$, $\ldots, \varphi_2(\alpha_r), \ldots,$ $\varphi_m(\alpha_1)$, $\varphi_m(\alpha_2), \ldots$, $\varphi_m(\alpha_r)$. Die Galoiskorrespondenz zeigt dann, daß die Galoisgruppe $\mathrm{Gal}(M/K)$ auflösbar ist. □

Satz 8.6.22 (Auflösbarkeit von Gleichungen durch Radikale). *Seien K ein Körper der Charakteristik $\mathrm{char}\, K = 0$ und $P \in K[X]\backslash 0$ ein von Null verschiedenes Polynom. So sind gleichbedeutend:*

1. *Die Gleichung $P(X) = 0$ läßt sich auflösen durch Radikale;*
2. *Die Galoisgruppe des Zerfällungskörpers von P über K ist auflösbar.*

Beweis. Die Gleichung $P(X) = 0$ läßt sich auflösen durch Radikale genau dann, wenn sich der Zerfällungskörper L unseres Polynoms in eine Radikalerweiterung von K einbetten läßt. Nach Proposition 8.6.21 ist das gleichbedeutend dazu, daß sich L in eine endliche Galoiserweiterung M des Körpers K mit auflösbarer Galoisgruppe einbetten läßt. Und da L schon selbst Galois ist und da seine Galoisgruppe $\mathrm{Gal}(L/K)$ ein Quotient der Galoisgruppe $\mathrm{Gal}(M/K)$ ist, und da nach 5.3.15 Quotienten auflösbarer Gruppen auflösbar sind, ist das auch gleichbedeutend dazu, daß L selbst eine auflösbare Galoisgruppe hat. □

Proposition 8.6.23. *Hat ein irreduzibles Polynom fünften Grades aus $\mathbb{Q}[X]$ genau drei reelle und zwei komplexe Nullstellen, so ist seine Galoisgruppe die volle symmetrische Gruppe $\mathcal{S}_5$ und ist damit nicht auflösbar.*

Beweis. Die komplexe Konjugation τ vertauscht zwei Nullstellen und läßt die übrigen fest. Da die Galoisgruppe G transitiv auf der 5-elementigen Menge der Nullstellen operiert, teilt nach der Bahnformel 5 die Gruppenordnung und es gibt nach 5.4.8 ein $g \in G$ von der Ordnung $\operatorname{ord} g = 5$. Man sieht etwa mit **??**, daß g und τ schon ganz $\mathcal{S}_5$ erzeugen. □

Beispiel 8.6.24. Das Polynom $X(X^2+4)(X^2-4) = X^5 - 16X$ hat genau drei reelle Nullstellen und Extrema bei $X = \pm 2/\sqrt[4]{5}$ mit Werten $\pm 32(\frac{1}{5} - 1)1/\sqrt[4]{5}$, die im Absolutbetrag größer sind als zwei. Das Polynom $X^5 - 16X + 2$ hat also ebenfalls genau drei reelle und zwei komplexe Nullstellen, und es ist darüber hinaus irreduzibel in $\mathbb{Q}[X]$ nach dem Eisensteinkriterium 6.8.2. Seine Galoisgruppe ist nach 8.6.23 folglich nicht auflösbar, und damit kann nach 8.6.22 die Gleichung $X^5 - 16X + 2 = 0$ nicht durch Radikale gelöst werden.

Beispiel 8.6.25. Das Polynom $X^5 - 2$ in $\mathbb{Q}[X]$ ist irreduzibel nach dem Eisensteinkriterium 6.8.2. Es ist jedoch durchaus auflösbar durch Radikale.

8.6.26 (**Adjunktion höherer Wurzeln**). Seien K ein Körper und $a \in K$ ein Element und $n \geq 1$. Ich will diskutieren, wie eine Körpererweiterung $K(\alpha)$ mit $\alpha^n = a$ und der Zerfällungskörper von $X^n - a$ aussehen können. Zunächst einmal muß ein Polynom der Gestalt $X^n - a$ nicht irreduzibel sein, wie bereits $X^2 - 1 = (X+1)(X-1)$ zeigt. Im Zerfällungskörper von $X^n - a$ müssen auch keineswegs alle n-ten Wurzeln von a isomorphe Teilkörper erzeugen, etwa haben wir $X^4 - 9 = (X^2+3)(X^2-3)$ und $\mathbb{Q}(\mathrm{i}\sqrt{3})$ ist nicht isomoph zu $\mathbb{Q}(\sqrt{3})$.

Übungen

Übung 8.6.27. Gegeben Primzahlen p, q ist die Galoisgruppe des Zerfällungskörpers L von $X^p - q \in \mathbb{Q}[X]$ isomorph zum semidirekten Produkt $\mathbb{F}_p \rtimes \mathbb{F}_p^\times$ in Bezug auf die offensichtliche Wirkung von $\mathbb{F}_p^\times$ auf $\mathbb{F}_p$. Hinweis: Mit 8.7.8 kann man das sogar allgemeiner zeigen für $q \in \mathbb{Q}^\times \setminus (\mathbb{Q}^\times)^p$. Wählt man zu einem Erzeuger von $\mathrm{Gal}(\mathbb{Q}(\sqrt[p]{1})/\mathbb{Q})$ ein Urbild $\rho \in \mathrm{Gal}(L/\mathbb{Q})$, so ist $\sigma := \rho^p$ von der Ordnung $p-1$ und restringiert zu einem Erzeuger von $\mathrm{Gal}(\mathbb{Q}(\sqrt[p]{1})/\mathbb{Q})$.

Übung 8.6.28. Seien in einem Körper Ω zwei Teilkörper $K, L \subset \Omega$ gegeben. Sind $K \supset (K \cap L)$ und $L \supset (K \cap L)$ endliche Galoiserweiterungen, so ist auch $(KL) \supset (K \cap L)$ eine endliche Galoiserweiterung und die Restriktionen liefern einen Gruppenisomorphismus

$$\mathrm{Gal}((KL)/K \cap L) \xrightarrow{\sim} \mathrm{Gal}(K/K \cap L) \times \mathrm{Gal}(L/K \cap L)$$

8.7 Lösung kubischer Gleichungen

8.7.1. Jetzt interessieren wir uns für **kubische Gleichungen**, also Gleichungen der Gestalt

$$x^3 + ax^2 + bx + c = 0$$

Ihre Galoisgruppen sind auflösbar als Untergruppen von $\mathcal{S}_3$, also müssen sich kubische Gleichungen zumindest in Charakteristik Null durch Radikale lösen lassen. Um explizite Lösungsformeln anzugeben, bringen wir zunächst durch die Substitution $x = y - a/3$ den quadratischen Term zum Verschwinden und gehen über zu einer Gleichung der Gestalt $y^3 + py + q = 0$. Für die Lösungen derartiger Gleichungen gibt der folgende Satz eine explizite Formel.

Satz 8.7.2. *Gegeben komplexe Zahlen p, q erhält man genau die Lösungen der Gleichung $y^3 + py + q = 0$, wenn man in der* **Cardano'schen Formel**

$$y_{1/2/3} = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$

bei beiden Summanden dieselbe Quadratwurzel fest wählt und dann die beiden Kubikwurzeln so zieht, daß ihr Produkt gerade $-p/3$ ist.

8.7.3. Dasselbe gilt sogar für jeden beliebigen algebraisch abgeschlossenen Körper einer von zwei und drei verschiedenen Charakteristik. Dieser Trick war bei den Italienern schon im 16. Jahrhundert bekannt und wurde von den Experten sorgsam geheimgehalten. Diese schlagende Anwendung der komplexen Zahlen war der Ausgangspunkt ihres Siegeszugs in der höheren Mathematik. Selbst wenn alle drei Nullstellen unserer kubischen Gleichung reell sind, ist es nicht möglich, unser Lösungsverfahren ohne die Verwendung der komplexen Zahlen anzuwenden. Die Bemerkung 8.7.10 zeigt, daß der Übergang zu komplexen Zahlen hier wirklich notwendig und nicht etwa nur unserer Ungeschicklichkeit geschuldet ist.

Beweis. Daß wir auf diese Weise wirklich nur Lösungen unserer Gleichung erhalten, kann man unschwer nachrechnen. Daß wir alle Lösungen erhalten, folgt auch recht schnell: Stimmen zwei derartige Lösungen überein, sagen wir $u + v = \zeta u + \zeta^{-1} v$ für verträgliche Wahlen u und v der beiden Kubikwurzeln und eine primitive dritte Einheitswurzel ζ, so folgern wir $(1 - \zeta)u = (\zeta^{-1} - 1)v$, also $\zeta u = v$, also $u^3 = v^3$, damit das Verschwinden der Diskriminante $27q^2 + 4p^3$, und damit gibt es auch nur höchstens zwei Lösungen nach 6.9.17. Stimmen alle drei so konstruierten Lösungen überein, so folgt zusätzlich $\zeta^{-1} u = v$, also $u = v = 0$ und $q = p = 0$ und unsere Gleichung hat in der Tat als einzige Lösung $y = 0$. □

8.7.4. Wie wir sehen, ist es nicht schwer, die Cardano'sche Formel nachzuprüfen. Ich will nun erklären, wie man durch Galois-Theorie auf diese Formel geführt wird, und beginne mit einer Vorbemerkung zur linearen Algebra.

8.7.5 (**Zerlegung unter Endomorphismus endlicher Ordnung**). Seien K ein Körper und V ein K-Vektorraum und $f : V \to V$ eine K-lineare Abbildung und $n \in \mathbb{N}$ mit $f^n = \mathrm{id}$. Die Charakteristik $\mathrm{char}\, K$ sei kein Teiler von n und das Polynom $X^n - 1$ zerfalle vollständig in K. Wir wissen etwa aus 8.6.6, daß sich jeder Vektor $v \in V$ eindeutig als eine Summe von Elementen der Eigenräume von f zu den verschiedenen Eigenwerten darstellen lassen muß. Hier geben wir nun diese Darstellung ganz explizit an. Gegeben eine n-te Einheitswurzeln $\zeta \in K$ setzen wir dazu

$$v_\zeta := \frac{1}{n} \sum_{i=0}^{n-1} \zeta^i f^i(v)$$

So gilt $f(v_\zeta) = \zeta^{-1} v_\zeta$ alias $v_\zeta \in \mathrm{Eig}(f; \zeta^{-1})$ aus $\sum_{\zeta^n=1} \zeta^i = 0$ für $0 < i < n$ folgt

$$v = \sum_{\zeta^n=1} v_\zeta$$

Das ist also die Darstellung von v als Summe von Elementen der jeweiligen Eigenräume von f.

8.7.6 (**Herleitung der Cardano'schen Formeln**). Sei nun L/K eine endliche Galoiserweiterung mit der symmetrischen Gruppe $\mathcal{S}_3$ als Galoisgruppe. Die geraden Permutationen bilden einen Normalteiler A_3 und dessen Fixkörper ist ein Zwischenkörper $Q \subset L$ mit L/Q Galois vom Grad 3 und Q/K Galois vom Grad 2. Gilt $\mathrm{char}\, K \neq 3$ und enthält K eine nichttriviale dritte Einheitswurzel ζ und ist σ ein Erzeuger der Galoisgruppe $\mathrm{Gal}(L/Q)$, so können wir nach 8.7.5 und in der Notation von dort jedes $\alpha \in L$ schreiben als

$$\alpha = \alpha_1 + \alpha_\zeta + \alpha_{\zeta^2}$$

mit $\alpha_1 \in Q$ und $\alpha_\zeta^3, \alpha_{\zeta^2}^3 \in Q$ und bei uns auch $\alpha_\zeta \alpha_{\zeta^2} \in Q = L^\sigma$. Jetzt nehmen wir speziell an, L sei der Zerfällungskörper eines Polynoms $Y^3 + pY + q \in K[Y]$ und es habe die Zerlegung

$$Y^3 + pY + q = (Y - \alpha)(Y - \beta)(Y - \gamma)$$

mit $\alpha, \beta, \gamma \in L$. Dann war unser Polynom notwendig irreduzibel und separabel und die Operation der Galoisgruppe auf den Nullstellen induziert einen Isomorphismus

$$\mathrm{Gal}(L/K) \xrightarrow{\sim} \mathrm{Ens}^\times\{\alpha, \beta, \gamma\}$$

zwischen der Galoisgruppe und der Gruppe aller Permutationen der drei Nullstellen, deren Bezeichnung wir so wählen können, daß gilt $\sigma(\alpha) = \beta$ und $\sigma(\beta) = \gamma$.

Da nun der quadratische Term unseres kubischen Polynoms nach Annahme verschwindet, gilt

$$\begin{aligned} \alpha+\beta+\gamma &= 0 \\ \alpha\beta+\beta\gamma+\gamma\alpha &= p \\ -\alpha\beta\gamma &= q \quad = \quad \alpha^2\beta+\beta^2\alpha \end{aligned}$$

So erhalten wir $\alpha_1 = 0$ und obige Gleichung spezialisiert zu

$$\alpha = u + v$$

mit $u^3, v^3 \in Q$ und

$$\begin{aligned} 3u &= \alpha+\zeta\beta+\zeta^2\gamma \quad = \quad (1-\zeta^2)\alpha+(\zeta-\zeta^2)\beta \\ 3v &= \alpha+\zeta^2\beta+\zeta\gamma \quad = \quad (1-\zeta)\alpha+(\zeta^2-\zeta)\beta \end{aligned}$$

Diese Gleichungen liefern

$$\begin{aligned} 9uv &= \alpha^2+\beta^2+\gamma^2+(\zeta+\zeta^2)(\alpha\beta+\alpha\gamma+\beta\gamma) \\ &= (\alpha+\beta+\gamma)^2+(\zeta+\zeta^2-2)(\alpha\beta+\alpha\gamma+\beta\gamma) \\ &= -3p \end{aligned}$$

alias $uv = -p/3$. Weiter kann man das nichttriviale Element τ der Galoisgruppe $\mathrm{Gal}(Q/K)$ erhalten als die Einschränkung von $\tau \in \mathrm{Gal}(L/K)$ mit $\tau(\alpha) = \beta$ und $\tau(\beta) = \alpha$ und unter der zusätzlichen Annahme $\mathrm{char}\, K \neq 2$ erhalten wir

$$\begin{aligned} u^3 &= a+b \\ v^3 &= c+d \end{aligned}$$

mit $a, c, b^2, d^2 \in K$ und

$$\begin{aligned} 2a &= (u^3+\tau(u^3)) \qquad 2b \;=\; (u^3-\tau(u^3)) \\ 2c &= (v^3+\tau(v^3)) \qquad 2d \;=\; (v^3-\tau(v^3)) \end{aligned}$$

Von b wissen wir a priori, daß es ein Vielfaches von $E := (\alpha-\beta)(\beta-\gamma)(\gamma-\alpha) = 2\alpha^3+3\alpha^2\beta-3\alpha\beta^2-2\beta^3$ sein muß, da dies Element auch invariant ist unter σ und antiinvariant unter τ. Bereits im Zusammenhang mit symmetrischen Polynomen in 6.9.17 hatten wir $E^2 = -4p^3-27q^2$ gefunden. Wir rechnen fleißig weiter und erhalten $3u/(1-\zeta^2) = \alpha-\zeta^2\beta$ und dann

$$\begin{aligned} 9u^3/(\zeta-\zeta^2) &= \alpha^3-3\zeta^2\alpha^2\beta+3\zeta\alpha\beta^2-\beta^3 \\ 9\tau(u^3)/(\zeta-\zeta^2) &= -\alpha^3+3\zeta\alpha^2\beta-3\zeta^2\alpha\beta^2+\beta^3 \\ 18a/(\zeta-\zeta^2) &= 3(\zeta-\zeta^2)(\alpha^2\beta+\alpha\beta^2) \\ a &= -q/2 \\ 18b/(\zeta-\zeta^2) &= 2\alpha^3+3(\alpha^2\beta-\alpha\beta^2)-2\beta^3 \\ b &= (\zeta-\zeta^2)E/18 \end{aligned}$$

unter Beachtung von $q = -\alpha\beta\gamma = \alpha^2\beta + \beta^2\alpha$ und $(\zeta - \zeta^2)^2 = -3$ im vorvorletzten Schritt. Die Formeln für v unterscheiden sich von denen für u nur dadurch, daß darin ζ und ζ^2 vertauscht sind. Dieselbe Rechnung liefert damit

$$\begin{aligned} c &= -q/2 \\ d &= (\zeta^2 - \zeta)E/18 \end{aligned}$$

So erhalten wir wegen $a = c$ und $d = -b$ schließlich

$$\begin{aligned} \alpha &= u + v \\ &= \sqrt[3]{-(q/2) + b} + \sqrt[3]{-(q/2) - b} \end{aligned}$$

mit der Maßgabe, daß die beiden dritten Wurzeln mit $uv = -p/3$ zu wählen sind und daß gilt $b^2 = -3E^2/3^4 2^2 = (p/3)^3 + (q/2)^2$. Das sind genau die Cardano'schen Formeln.

Ergänzung 8.7.7 (**Die Cardano'schen Formeln für Kringe**). Ist unser Polynom nicht irreduzibel oder besteht seine Galoisgruppe nur aus den drei geraden Permutationen der drei Nullstellen, so funktioniert das obige Argument nur noch in mehr oder weniger stark modifizierter Form. Wir können aber ganz allgemein den Kring $k := \mathbb{Z}[2^{-1}, 3^{-1}, \zeta]$ betrachten für eine von Eins verschiedene dritte Einheitswurzel ζ und auf dem Polynomring

$$L := k[{}'\alpha, \beta, \gamma]$$

die Gruppe $\mathcal{S}_3$ der Permutationen der drei Variablen operieren lassen. Dann ist der Invariantenring der Polynomring $K := k[{}'p, q, r]$ mit

$$(Y - \alpha)(Y - \beta)(Y - \gamma) = Y^3 + rY^2 + pY + q$$

Die Injektion $K \hookrightarrow L$ induziert auf den Quotienten beider Ringe nach dem von $-r = \alpha + \beta + \gamma$ erzeugt Ideal wieder eine Injektion $\bar{K} \hookrightarrow \bar{L}$ und $\mathcal{S}_3$ operiert auch auf dem Quotienten und $\bar{K}$ ist der Invariantenring und wir haben $\bar{L} = k[{}'\alpha, \beta]$ sowie $\bar{K} = k'[p, q]$ mit der Bezeichnung $\alpha, \beta, \gamma, p, q$ für die Bilder dieser Elemente in den jeweiligen Quotientenringen. In diesem Kontext bleiben alle unsere Rechnungen sinnvoll und wir erhalten $\alpha = u + v$ mit $uv = -p/3$ und $u^3 = -(q/2) + b$ sowie $v^3 = -(q/2) - b$ mit $b^2 = (p/3)^3 + (q/2)^2$. Hierdurch sind zwar u und v nicht eindeutig bestimmt, aber wenn wir eine Wahl fest treffen und dann $\alpha := u + v$ sowie $\beta := \zeta u + \zeta^{-1} v$ sowie $\gamma := \zeta^{-1} u + \zeta v$ setzen, so prüft man in $\bar{L}$ der Tat

$$(Y - \alpha)(Y - \beta)(Y - \gamma) = Y^3 + pY + q$$

Alle diese Formeln bleiben nun natürlich richtig unter jedem Homomorphismus von $\bar{L}$ in einen beliebigen Körper oder sogar beliebigen Ring und bedeuten die

Cardano'schen Formeln in großer Allgemeinheit. Wir haben bei der Herleitung sogar den Vorteil, daß wir zusätzlich den Ringautomorphismus $\kappa : k \xrightarrow{\sim} k$ mit $\kappa(\zeta) = \zeta^2$ und $\kappa^2 = \mathrm{id}$ zur Verfügung haben. Offensichtlich gilt dann $\kappa(u) = v$ und das formalisiert die Beobachtung in obiger Rechnung, daß „für v alles genauso geht wie für u, nur mit ζ und ζ^2 vertauscht".

Ergänzung 8.7.8 (**Ziehen primer Wurzeln**). Gegeben ein Körper K und eine Primzahl p ist für $a \in K$ das Polynom $X^p - a$ entweder irreduzibel oder es besitzt eine Nullstelle. In der Tat zerfällt unser Polynom in seinem Zerfällungskörper für eine p-te Einheitswurzel ζ als $X^p - a = \prod_{\nu=1}^{p}(X - \zeta^\nu b)$. Zerfällt es nun in K als $X^p - a = fg$ mit f, g normiert und $0 < d := \operatorname{grad} f < p$, so kann man aus dem konstanten Term von f und a eine p-te Wurzel von a zusammenmultiplizieren. In der Tat hat der konstante Term c von f die Gestalt $c = (-1)^d \xi b^d$ für eine p-te Einheitswurzel ξ. Es folgt $c^p = b^{dp} = a^d$. Damit führt der Ansatz $(c^n a^m)^p = a$ zur Gleichung $a^{nd+mp} = a$ alias $nd + mp = 1$ und jede Lösung $(m, n) \in \mathbb{Z}^2$ liefert für $a \neq 0$ eine p-ten Wurzel $c^n a^m$ von a in K. Der Fall $a = 0$ ist eh unproblematisch.

Ergänzung 8.7.9 (**Ziehen beliebiger Wurzeln**). In [Rom06, 14.1.4] findet man ein hinreichendes und notwendiges Kriterium für die Irreduzibilität des Polynoms $T^n - a \in K[T]$ gegeben $n \in \mathbb{N}_{>0}$ beliebig und K ein beliebiger Körper und $a \in K$. Daß das nicht ganz trivial sein kann, zeigt die Zerlegung

$$X^4 + 4a^4 = \big((X^2 + 2a^2) + 2aX\big)\big((X^2 + 2a^2) - 2aX\big)$$

Dort können wir natürlich noch $X = T^r$ substitutieren. Weiter ist $X^m - a^m$ offensichtlich durch $X - a$ teilbar, und auch diese Teilbarkeit bleibt bei der Substitution $X = T^r$ erhalten. Gilt also $4|n$ und $a \in -4K^4$, so ist $T^n - a$ nicht irreduzibel, und gibt es $m > 1$ mit $m|n$ und $a \in K^m$, so ist $T^n - a$ auch nicht irreduzibel. Das Kriterium sagt nun, daß wenn keine dieser beiden Bedingungen zutrifft, daß dann unser Polynom $T^n - a$ auch in der Tat irreduzibel ist.

8.7.10 (**Notwendigkeit des Ausgreifens in die komplexen Zahlen**). Sei eine kubische Gleichung $X^3 + pX + q = 0$ mit $p, q \in \mathbb{R}$ gegeben, die drei reelle Lösungen besitzt, von denen jedoch keine zum Koeffizientenkörper $K := \mathbb{Q}(p, q) \subset \mathbb{R}$ gehört, etwa $X^3 - \frac{3}{4}X + \frac{3}{16}$. Wir zeigen, daß es dann nicht möglich ist, eine Kette

$$K = K_0 \subset K_1 \subset \ldots \subset K_r \subset \mathbb{R}$$

von Teilkörpern von $\mathbb{R}$ so zu finden, daß unser Polynom in K_r vollständig zerfällt und K_{i+1} jeweils durch Adjunktion der positiven l_i-ten Wurzel aus einem positiven Element $a_i \in K_i$ entsteht, in Formeln

$$K_{i+1} = K_i(\sqrt[l_i]{a_i})$$

Ohne Beschränkung der Allgemeinheit dürfen wir hier die l_i als prim annehmen. Weiter ist das Quadrat $\Delta = -4p^3 - 27q^2$ des Produkts der Differenzen der Nullstellen aus 6.9.17 in unserem Fall notwendig positiv und wir dürfen $K_1 = K(\sqrt{\Delta})$ annehmen. Unser irreduzibles kubisches Polynom ist dann auch irreduzibel über K_1, denn es kann erst in einer Körpererweiterung vom Grad Drei eine Nullstelle haben. Seinen Zerfällungskörper Z über K können wir in eine Körperkette $K \subset K_1 \subset Z \subset \mathbb{R}$ einfügen und Z/K_1 ist dann Galois vom Grad $[Z : K_1] = 3$. Gegeben eine Wurzel $\alpha \in \mathbb{R}$ unseres kubischen Polynoms mit $\alpha \notin K_s$ ist für $s \geq 1$ nach dem Translationssatz also $K_s(\alpha)/K_s$ Galois vom Grad Drei. Für r kleinstmöglich mit $\alpha \in K_r$ muß damit $[K_r : K_{r-1}]$ ein Vielfaches von Drei sein. Wegen $K_r = K_{r-1}(\sqrt[l]{a})$ mit $a = a_r$ und $l = l_r$ prim muß aber nach 8.7.8 unser Polynom $X^l - a$ irreduzibel gewesen sein in $K_{r-1}[X]$ und wir folgern $[K_r : K_{r-1}] = l$. Zusammen zeigt das $l = 3$ und $K_r = K_{r-1}(\alpha)$ und damit K_r/K_{r-1} Galois vom Grad drei. Dann hinwiederum muß $X^3 - a$ in K_r vollständig in Linearfaktoren zerfallen und K_r muß drei dritte Einheitswurzeln enthalten und das steht im Widerspruch zu unserer Annahme $K_r \subset \mathbb{R}$. Der Übergang ins Komplexe oder alternativ die Verwendung trigonometrischer Funktionen zu ihrer Lösung „durch Radikale“ ist in anderen Worten unumgänglich. Lateinisch spricht man bei reellen Gleichungen dritten Grades dieser Art vom **casus irreducibilis**.

Übungen

Ergänzende Übung 8.7.11. Sei $n \geq 1$ und K ein Körper, der alle n-ten Einheitswurzeln enthält und dessen Charakteristik n nicht teilt. Man zeige: Gegeben $a \in K$ ist das Polynom $X^n - a$ irreduzibel in $K[X]$ genau dann, wenn a für keinen Teiler $d > 1$ von n eine d-te Wurzel in K besitzt.

Übung 8.7.12. Ein irreduzibles Polynom dritten Grades der Gestalt $Y^3 + pY + q$ mit Koeffizienten in einem Körper k der Charakteristik $\operatorname{char} k \neq 2$ hat genau dann die Galoisgruppe $\mathcal{S}_3$ über k, wenn $-4p^3 - 27q^2$ kein Quadrat in k ist. In unserer Terminologie ist $-4p^3 - 27q^2$ das Negative der Diskriminante unseres Polynoms, aber hier sind auch andere Konventionen verbreitet.

Beispiel 8.7.13. Das Polynom $X^3 - 2$ hat nach 8.1.20 oder 8.7.12 die Galoisgruppe $\mathcal{S}_3$ über $\mathbb{Q}$, denn $-108 = (-27)4$ ist kein Quadrat in $\mathbb{Q}$. Dasselbe Polynom hat jedoch Galoisgruppe A_3 über $\mathbb{Q}(\sqrt[3]{1})$ nach unserem Satz über Radikalerweiterungen 8.6.3. Damit alles zusammenpaßt, muß -108 ein Quadrat im dritten Kreisteilungskörper $\mathbb{Q}(\sqrt[3]{1})$ sein. Zum Glück stimmt das auch, für ζ eine primitive dritte Einheitswurzel gilt nämlich $(\zeta - \zeta^{-1})^2 = -3$.

8.8 Einheitswurzeln und reelle Radikale*

8.8.1. Die Tabelle

	sin	cos
π	0	-1
$\pi/2$	1	0
$\pi/3$	$\sqrt{3}/2$	$1/2$
$\pi/4$	$1/\sqrt{2}$	$1/\sqrt{2}$
$\pi/5$	$\sqrt{5-\sqrt{5}}/2\sqrt{2}$	$(\sqrt{5}+1)/4$
$\pi/6$	$1/2$	$\sqrt{3}/2$
$\pi/7$	?	?
$\pi/8$	$\sqrt{\frac{1}{2}-\sqrt{2}}$	$\sqrt{\frac{1}{2}+\sqrt{2}}$
$\pi/9$	?	?
$\pi/10$	$(\sqrt{5}-1)/4$	$\sqrt{5+\sqrt{5}}/2\sqrt{2}$
$\pi/11$	?	?

aus **??** zeigt einige $n \geq 1$, für die $\sin(\pi/n)$ und $\cos(\pi/n)$ in geschlossener Form als „reelle algebraische Ausdrücke“ dargestellt werden können, ohne daß wir bei der Berechnung der besagten Ausdrücke den Körper der reellen Zahlen verlassen müßten. Sie zeigt auch einige Fragezeichen für Fälle, in denen keine derartige Darstellung zur Verfügung steht. Wir zeigen im Folgenden, daß das nicht etwa an unserer Ungeschicklichkeit liegt, sondern daß es derartige reelle Darstellungen für die meisten n schlicht nicht gibt. Diese Aussage gilt es zunächst einmal zu präzisieren.

Definition 8.8.2. Gegeben eine Körpererweiterung $F \subset E$ definieren wir den **Radikalabschluß von** F **in** E als den kleinsten Zwischenkörper $R \subset E$ derart, daß für alle $p \geq 1$ gilt $(x^p \in R) \Rightarrow (x \in R)$. Wir notieren ihn

$$R = \mathrm{rad}(F \subset E)$$

Beispiel 8.8.3. Die folgende reelle Zahl gehört zum Radikalabschluß des Körpers $\mathbb{Q}$ der rationalen Zahlen im Körper $\mathbb{R}$ der reellen Zahlen:

$$\frac{\sqrt[7]{\sqrt[5]{6}+3}+13}{\sqrt[2]{3}+8} - \sqrt[17]{19876}$$

Definition 8.8.4. Gegeben eine Körpererweiterung $F \subset E$ definieren wir den **Quadratwurzelabschluß von** F **in** E als den kleinsten Zwischenkörper $Q \subset E$ derart, daß gilt $(x^2 \in Q) \Rightarrow (x \in Q)$. Wir notieren ihn

$$Q = \mathrm{quad}(F \subset E)$$

8.8.5. Den Quadratwurzelabschluß $\mathrm{quad}(\mathbb{Q} \subset \mathbb{C})$ der rationalen Zahlen in den komplexen Zahlen hatten wir bereits in 7.6.2 betrachtet und gezeigt, daß er genau aus allen konstruierbaren Zahlen besteht.

Satz 8.8.6 (Markus Rost). *Der Radikalabschluß der rationalen Zahlen in den reellen Zahlen trifft jeden Kreisteilungskörper nur innerhalb des Quadratwurzelabschlusses der rationalen Zahlen in den reellen Zahlen. Für jedes* $n \in \mathbb{N}$ *gilt also in Formeln*

$$\mathrm{rad}(\mathbb{Q} \subset \mathbb{R}) \cap \mathbb{Q}(\sqrt[n]{1}) \quad \subset \quad \mathrm{quad}(\mathbb{Q} \subset \mathbb{R})$$

Ergänzung 8.8.7. Für jeden Teilkörper $K \subset \mathbb{R}$ und jedes $n \geq 1$ gilt allgemeiner $\mathrm{rad}(K \subset \mathbb{R}) \cap K(\sqrt[n]{1}) \subset \mathrm{quad}(K \subset \mathbb{R})$. Der Beweis ist im wesentlichen derselbe.

8.8.8. Der Satz von Rost zeigt, daß $\cos(2\pi/7)$ nicht zum Radikalabschluß von $\mathbb{Q}$ in $\mathbb{R}$ gehören kann. In der Tat gehört diese reelle Zahl zu einem Kreisteilungskörper und müßte nach dem Satz von Rost anderfalls sogar zum Quadratwurzelabschluß von $\mathbb{Q}$ in $\mathbb{R}$ gehören. Das steht jedoch im Widerspruch zu unserer Erkenntnis, daß das regelmäßige Siebeneck nicht mit Zirkel und Lineal konstruiert werden kann. Weiter ist $\cos(2\pi/7)$ nach 8.1.21 auch eine von drei reellen Nullstellen des Polynoms $X^3 + X^2 - 2X - 1$. Wir sehen so ein weiteres Mal, daß kubische Gleichungen mit rationalen Koeffizienten, selbst wenn sie drei reelle Nullstellen haben, im allgemeinen nicht durch „algebraische Rechenoperationen im Rahmen der reellen Zahlen“ gelöst werden können. Im übrigen ist $\cos(2\pi/7)$ ein Erzeuger des Schnitts des siebten Kreisteilungskörpers mit der reellen Achse, dieser Schnitt muß Grad $6/2 = 3$ über $\mathbb{Q}$ haben, und besagtes Polynom ist gerade das Minimalpolynom von $\cos(2\pi/7)$ über $\mathbb{Q}$.

8.8.9. Genau dann gehört $\sin(\pi/n)$ zum Radikalabschluß der rationalen Zahlen in den reellen Zahlen, wenn das regelmäßige n-Eck konstruierbar alias $\varphi(n)$ eine Zweierpotenz ist. In der Tat liegt $\sin(\pi/n)$ sicher in einem Kreisteilungskörper. Liegt $\sin(\pi/n)$ auch im Radikalabschluß $\mathrm{rad}(\mathbb{Q} \subset \mathbb{R})$ der rationalen in den reellen Zahlen, so folgt $\sin(\pi/n) \in \mathrm{quad}(\mathbb{Q} \subset \mathbb{R})$ aus dem Satz 8.8.6 von Rost. Damit ist $\sin(\pi/n)$ aber nach 7.6.2 konstruierbar und damit dann unschwer auch das regelmäßige n-Eck. Der Beweis der Gegenrichtung bleibe dem Leser überlassen.

Beweis des Satzes von Rost 8.8.6. Wir halten eine natürliche Zahl $n \geq 1$ für den folgenden Beweis fest und vereinbaren die Abkürzung $Q := \mathrm{quad}(\mathbb{Q} \subset \mathbb{R})$ für den Quadratwurzelabschluß der rationalen Zahlen in den reellen Zahlen und $E := \mathbb{Q}(\sqrt[n]{1})$ für den n-ten Kreisteilungskörper, mit einem E wie Einheitswurzel. Um den Satz zu zeigen, reicht es sicher nachzuweisen, daß für jeden Teilkörper $R \subset \mathbb{R}$ mit der Eigenschaft $R \cap E \subset Q$ auch der durch Adjunktion einer primen reellen Wurzel, also durch Adjunktion eines Elements $x \in \mathbb{R}$ mit $x^p \in R$ für eine Primzahl p entstehende Teilkörper $R(x) \subset \mathbb{R}$ diese Eigenschaft hat. Im Fall $[R(x) : R] < p$ folgt aus unseren Annahmen bereits $R(x) = R$. In der Tat haben wir für $q = [R(x) : R]$ und $a = x^p$ ja

$$\det_R(x|R(x))^p = \det_R(x^p|R(x)) = a^q$$

Es gibt also $c \in R$ mit $c^p = a^q$. Im Fall $q < p$ können wir $1 = \alpha p + \beta q$ schreiben, es folgt $a = a^{\alpha p+\beta q} = (a^\alpha c^\beta)^p$ und a hat bereits eine p-te Wurzel $y = a^\alpha c^\beta$ in R, woraus wegen $R \subset \mathbb{R}$ und $x \in \mathbb{R}$ folgt $y = \pm x$ und $R(x) = R$. Es bleibt also nur noch, den Fall $[R(x) : R] = p$ zu diskutieren und in diesem Fall die Implikation

$$R \cap E \subset Q \quad \Rightarrow \quad R(x) \cap E \subset Q$$

zu zeigen. Im Fall $R(x) \cap E = R \cap E$ ist das klar. Sonst ist $(R(x) \cap E)/(R \cap E)$ eine nichttriviale Galoiserweiterung, denn das sind beides Zwischenkörper einer endlichen abelschen Erweiterung. Nach dem Translationssatz 8.6.10 ist dann auch $((R(x) \cap E)R)/R$ eine nichttriviale Galoiserweiterung. Da $R(x)/R$ Primzahlgrad hat, folgt $((R(x) \cap E)R) = R(x)$, und $R(x)/R$ ist mithin selbst eine Galoiserweiterung vom Grad p. Das Polynom $X^p - a$ ist dann notwendig das Minimalpolynom von x über R, und da jede Galoiserweiterung normal ist, müssen alle seine Nullstellen auch zu $R(x)$ gehören, also alle ζx für ζ eine beliebige p-te Einheitswurzel. Damit müssen aber alle p-ten Einheitswurzeln zu $R(x)$ gehören, also zu $\mathbb{R}$, und das gilt nur im Fall $p = 2$. Mithin sind wir in diesem Fall, und durch das Rückverfolgen unserer Argumente erhalten wir

$$[(R(x) \cap E) : (R \cap E)] = 2$$

Der Körper $R(x) \cap E$ entsteht also aus dem Teilkörper $R \cap E \subset Q$ durch Adjunktion einer Quadratwurzel. Folglich liegt $R(x) \cap E$ in der Tat bereits selbst im Quadratwurzelabschluß Q von $\mathbb{Q}$ in $\mathbb{R}$. □

9 Danksagung

Als Quellen habe ich besonders [Lor96] und [Lan74] genutzt. Auch [E+92] war hilfreich. Für Korrekturen und Verbesserungen danke ich Anna Breucker, Katharina Wendler, René Recktenwald, Meinolf Geck, Theo Grundhöfer, Christina Pflanz, . . .

10 Vorlesung Algebra und Zahlentheorie WS 19/20

Es handelte sich um eine vierstündige Vorlesung, also 4×45 Minuten Vorlesung, mit 2 Stunden Übungen.

22.10 Gruppen **??** und Gruppenhomomorphismen **??**. Monoide, Magmas **??**. Klassifikation der Gruppen mit höchstens vier Elementen 5.1 zu Fuß. Klassifikation der Gruppen F mit fünf Elementen durch Theorie: Untergruppen „richtige“ Definition. Untergruppen von $\mathbb{Z}$ nach 1.3.4, Nebenklassen 3.1 und Lagrange: F hat nur die beiden Untergruppen 1 und F.

24.10 Bijektion $\mathrm{Grp}(\mathbb{Z}, G) \xrightarrow{\sim} G$, $\varphi \mapsto \varphi(1)$ nach **??** für jede Gruppe G. Also für $|G| = 5$ Surjektion $\mathbb{Z} \twoheadrightarrow G$ durch $1 \mapsto g$ mit $g \neq e$. Universelle Eigenschaft surjektiver Gruppenhomomorphismen 3.2.1. Normalteiler 3.2 und Quotient danach. Isomorphiesätze. Ordnung von Gruppenelementen, Struktur zyklischer Gruppen. Gruppen von Primzahlordnung sind zyklisch. Kleiner Fermat für Kongruenzen von Potenzen modulo Primzahl.

29.10 Existenz und Eindeutigkeit der Primfaktorzerlegung 1.4.8. Satz über den größten gemeinsamen Teiler. Euklidischer Algorithmus. Chinesischer Restsatz mit zwei Resten. Beide Klassifikationen endlich erzeugter abelscher Gruppen angegeben. Elementarteilersatz bewiesen.

31.10 Beide Klassifikationen endlich erzeugter abelscher Gruppen bewiesen. Endliche Untergruppen der multiplikativen Gruppe eines Körpers sind zyklisch. Operationen von Gruppen und Monoiden auf Mengen. Bahnen als homogene Räume. Bahnformel.

5.11 Operation durch Konjugation. Endliche Untergruppen der Drehgruppe bis auf Konjugation. Einfache Gruppen. Klassengleichung. Konjugationsklassen in der Ikosaedergruppe. Die Ikosaedergruppe ist einfach 5.2.5. Kompositionsreihen und Satz von Jordan-Hölder, noch ohne Beweis.

7.11 Beweis Jordan-Hölder. Struktur von p-Gruppen. Sylowsätze. Gruppen mit 6 und 15 Elementen. Gruppen mit 8 Elementen ohne Beweis.

12.11 Die natürlichen Zahlen axiomatisch, 1.1.2 bis 1.1.17, nicht Kürzungsregel **??**, nicht Anordnung 1.1.19, aber noch 1.1.21 und **??** und Definition der Multiplikation.

14.11 Leonardo vertritt mich. Ringe und Restklassenringe $\mathbb{Z}/m\mathbb{Z}$ ohne Diffie-Hellmann. Quotient eines Rings nach einem Ideal 6.1.13.

19.11 Teilringe und Notationen für ihre Erzeugung. Notationen für Erzeugung von Idealen. Beispiele für Restklassenringe, insbesondere $\mathbb{R}[X]/\langle P\rangle$ für Polynome vom Grad zwei und allgemeinere Polynome. Abstrakter chinesischer Restsatz und Bezug zur Interpolation. Quotientenkörper eines kommutativen Integritätsbereichs und seine universelle Eigenschaft. Damit $\mathbb{Q}$ aus $\mathbb{Z}$ konstruiert.

21.11 Euklidische Ringe, Faktorielle Ringe, Hauptidealringe, Beispiele, deren Beziehung untereinander. Quotienten von Hauptidealringen. Der Ring der Gauß'schen Zahlen ist euklidisch.

26.11 Gauß'sche Zahlen und Summen von zwei Quadraten. Polynomringe über faktoriellen Ringen noch ohne Beweis.

28.11 Polynomringe über faktoriellen Ringen. Gemeinsame Nullstellen von zwei teilerfremden Polynomen in zwei Variablen. Kreisteilungspolynome, Eisensteinkriterium, Irreduzibilität des p-ten Kreisteilungspolynoms für p prim.

3.12 Symmetrische Polynome, Hauptsatz. Diskriminante eines Polynoms vom Grad Drei. Nicht allgemeine Diskriminante. Schranke von Bézout mit Beweisskizze.

5.12 Körpererweiterungen. Algebraische und transzendente Elemente. Minimalpolynom. Endliche Körpererweiterungen, Grad einer Körpererweiterung. Elemente von endlicher Körpererweiterung sind algebraisch.

10.12 Quadratische Körpererweiterungen. Multiplikativität des Grades. Konstruktionen mit Zirkel und Lineal.

12.12 Endliche Körper und deren Unterkörper. Zerfällungskörper definiert, Satz über Eindeutigkeit formuliert, aber noch nicht bewiesen. Satz über Ausdehnung von Körperhomomorphismen auf primitive algebraische Erweiterungen bewiesen, aber kurz. Beweis nochmal!

17.12 Eindeutigkeit des Zerfällungskörpers. Normale Erweiterungen. Angekündigt: Algebraischer Abschluß.

19.12 Algebraischer Abschluß.

7.1 Separable Polynome. Definition separabler Körpererweiterungen. Noch nicht, daß von separablen Elementen erzeugte Körpererweiterungen separabel sind.

9.1 Charakterisierung separabler Körpererweiterungen. Unmöglichkeit einer Überdeckung eines Körpers durch endlich viele echte Teilkörper. Satz vom primitiven Element, Körpererweiterungen mit nur endlich vielen Zwischenkörpern, Unterscheidung von Körperhomomorphismen an einem einzigen Element.

14.1 Galoiserweiterungen und ihre Beschreibung als Erweiterungen über dem Fixkörper. Beispiele für Galoisgruppen.

16.1 Galoisgruppe der allgemeinen Gleichung. Anschauung. Galois-Korrespondenz.

21.1 Biquadratische Erweiterungen. Beweis mit Galoistheorie, daß $\mathbb{C}$ algebraisch abgeschlossen ist. Irreduzibilität von Kreisteilungspolynomen. Galoisgruppen von Kreisteilungskörpern.

23.1 Hinreichendes Kriterium für die Konstruierbarkeit regelmäßiger n-Ecke mit Zirkel und Lineal. Euler'sche φ-Funktion. Reziprozitätsgesetz. Beweis bis zu $\alpha^2 = (-1)^{\frac{p-1}{2}} p$ für ein gewisses explizites α im p-ten Kreisteilungskörper. Legendre-Symbole bereits eingeführt.

28.1 Beweis von Reziprozitätsgesetz und Ergänzungssatz. Jacobi-Symbole, ihre Eigenschaften und ihr Nutzen. Zyklische Erweiterungen, der Beweis eines Lemmas aus der linearen Algebra steht aber noch aus, ebenso das Korollar über Erweiterungen von Primzahlordnung.

30.1 Lemma aus der linearen Algebra. Erweiterungen von Primzahlordnung. Translationssatz. Radikalerweiterungen. Hauptsatz noch nicht bewiesen über auflösbare Galoisgruppen und auflösbare Gleichungen.

4.2 Hauptsatz über auflösbare Galoisgruppen und auflösbare Gleichungen. Beispiel einer Gleichung fünften Grades, die sich nicht durch Radikale lösen läßt. Cardano'sche Formeln. Begonnen mit deren Herleitung aus der Galoistheorie.

6.2 Herleitung der Cardano'schen Formeln aus der Galoistheorie. Notwendigkeit des Ausgreifens in die komplexen Zahlen.

11.2 Ansage: Tutoren werden gesucht. Mehr zu Zahlbereichen: Konstruktion $\mathbb{Z}$ aus $\mathbb{N}$ und $\mathbb{R}$ aus $\mathbb{Q}$.

13.2 Quaternionen?

11 Vorlesung Algebra und Zahlentheorie WS 16/17

Es handelte sich um eine vierstündige Vorlesung, also 4×45 Minuten Vorlesung, mit 2 Stunden Übungen.

19.10 Gruppen und Gruppenhomomorphismen. Klassifikation der Gruppen mit höchstens vier Elementen 5.1 zu Fuß. Klassifikation der Gruppen F mit fünf Elementen durch Theorie: Untergruppen, Untergruppen von $\mathbb{Z}$ nach 1.3.4, Nebenklassen 3.1 und Lagrange: F hat nur die beiden Untergruppen 1 und F. Bijektion $\mathrm{Grp}(\mathbb{Z}, G) \xrightarrow{\sim} G, \varphi \mapsto \varphi(1)$ für jede Gruppe G. Also für $|G| = 5$ Surjektion $\mathbb{Z} \twoheadrightarrow G$ durch $1 \mapsto g$ mit $g \neq e$. Universelle Eigenschaft surjektiver Gruppenhomomorphismen.

21.10 Normalteiler 3.2 und Quotient danach. Isomorphiesätze. Ordnung von Gruppenelementen, Struktur zyklischer Gruppen. Gruppen von Primzahlordnung sind zyklisch. Kleiner Fermat für Kongruenzen von Potenzen modulo Primzahl. Existenz und Eindeutigkeit der Primfaktorzerlegung. Satz über den größten gemeinsamen Teiler.

26.10 Chinesischer Restsatz mit zwei Resten. RSA-Verschlüsselung. Einfache Gruppen, Satz von Jordan-Hölder. Operationen von Gruppen und Monoiden auf Mengen. Operation durch Konjugation ganz kurz. Noch nicht Bahnformel.

28.10 Bahnen als homogene Räume. Bahnformel. Operation durch Konjugation. Konjugationsklassen in der Würfelgruppe und der Ikosaedergruppe. Die Ikosaedergruppe ist einfach 5.2.5.

2.11 Struktur von p-Gruppen. Gruppen mit p^2 Elementen sind abelsch. Sylow-Sätze bewiesen. Noch nachholen: Jeder Primteiler der Ordnung einer abelschen Gruppe ist die Ordnung eines Elements 3.3.15, 3.3.17.

4.11 Jeder Primteiler der Ordnung einer abelschen Gruppe ist die Ordnung eines Elements 3.3.15, 3.3.17. Klassifikation endlich erzeugter abelscher Gruppen durch Multimengen von Primpotenzen, ohne Beweis. Gruppen mit 6 Elementen mit Beweis. Gruppen mit 8 Elementen ohne Beweis. Dann Konstruktion der natürlichen Zahlen im Rahmen der Mengenlehre. Konstruktion der Addition, noch ohne Beweis der Eigenschaften.

9.11 Konstruktion und Eigenschaften der Addition. Ringe, Ringhomomorphismen. Universelle Eigenschaft surjektiver Ringhomomorphismen. Ideale. Konstruktion von Restklassenringen, noch nicht ganz fertig.

11.11 Konstruktion von Restklassenringen. Von Teilmengen erzeugte Ideale. Quotientenringe von Polynomringen nach von normierten Polynomen erzeugten

Hauptidealen. Konstruktion von $\mathbb{C}$ als Quotient $\mathbb{R}[X]/\langle X^2+1\rangle$. Teilringe. Von Teilmengen erzeugte Teilringe. Algebraische Unabhängigkeit. Produkte von Ringen. Abstrakter chinesischer Restsatz. Interpolation als Beispiel.

16.11 Euklidische Ringe, Faktorielle Ringe, Hauptidealringe, Beispiele, deren Beziehung untereinander. Quotienten von Hauptidealringen. Noch nicht der Ring der Gauß'schen Zahlen.

18.11 Gauß'sche Zahlen und Summen von zwei Quadraten. Endliche Untergruppen der multiplikativen Gruppe eines Körpers sind zyklisch. Konstruktion des Quotientenkörpers. Bewertung auf dem Quotientenkörper eines faktoriellen Rings an einem irreduziblen Element.

23.11 Polynomringe über faktoriellen Ringen, Bewertung von Polynomen, Lemma von Gauß. Zwei teilerfremde Polynome in zwei Variablen haben höchstens endlich viele gemeinsame Nullstellen. Kreisteilungspolynome haben ganze Zahlen als Koeffizienten. Noch nicht Irreduzibilität von Kreisteilungspolynomen.

25.11 Irreduzibilität von Kreisteilungspolynomen. Eisensteinkriterium. Symmetrische Polynome, Hauptsatz.

30.11 Diskriminante eines Polynoms vom Grad Drei. Allgemeine Diskriminante. Schranke von Bézout mit Beweis.

2.12 Konstruktion der ganzen Zahlen aus den natürlichen Zahlen. Konstruktion der reellen Zahlen.

7.12 Körpererweiterungen. Algebraische und transzendente Elemente. Minimalpolynom.

9.12 Endliche und algebraische Körpererweiterungen. Quadratische Körpererweiterungen.

14.12 Konstruktionen mit Zirkel und Lineal. Angefangen mit endlichen Körpern. Gezeigt, daß deren Kardinalität stets Charakteristik hoch Grad über dem Primkörper ist.

16.12 Endliche Körper und deren Unterkörper. Zerfällungskörper definiert, Satz über Eindeutigkeit formuliert, aber noch nicht bewiesen. Satz über Ausdehnung von Körperhomomorphismen auf primitive algebraische Erweiterungen bewiesen, aber kurz. Beweis nochmal!

21.12 Ausdehnungen von Körperhomomorphismen. Maximalzahl, Existenz. Eindeutigkeit des Zerfällungskörpers. Normale Erweiterungen, Definition und Anschauung. Formuliert, aber nicht bewiesen, daß Zerfällungskörper normal sind.

23.12 Ich will nur die Ableitung einführen mit Summen- und Produktregel und zeigen, daß mehrfache Nullstellen Nullstellen der Ableitung sind. Dann habe über den Koordinatisierungssatz geredet und gezeigt, wie man in jeder Desargues-Ebene Richtungsvektoren einführt. Nicht gezeigt, daß diese eine kommutative Gruppe bilden.

11.1 Ableitung von Polynomen und Separabilität von Polynomen und Körpererweiterungen. Noch nicht den Satz über die Zahl von Ausdehnungen von Körperhomomorphismen auf separable Erweiterungen fertig bewiesen.

13.1 Satz über separable Körpererweiterungen fertig bewiesen. Satz vom primitiven Element, Charakterisierung endlicher primitiver Körpererweiterungen. Konstruktion und Eindeutigkeit des algebraischen Abschlusses.

18.1 Galoisgruppe, Galois-Erweiterungen. Galois-Erweiterungen über Fixkörper. Transitive treue Operation der Galoisgruppe eines Zerfällungskörpers eines irreduziblen Polynoms auf den Nullstellen. Noch nicht: Invarianten eines Quotientenkörpers.

20.1 Galoisgruppe der allgemeinen Gleichung. Anschauung für die Galoisgruppe. Galois-Korrespondenz, aber noch keine Anwendungen dazu.

25.1 Biquadratische Erweiterungen. Beweis mit Galoistheorie, daß $\mathbb{C}$ algebraisch abgeschlossen ist. Irreduzibilität von Kreisteilungspolynomen.

27.1 Galoisgruppen von Kreisteilungskörpern und hinreichendes Kriterium für die Konstruierbarkeit regelmäßiger n-Ecke mit Zirkel und Lineal. Euler'sche φ-Funktion.

1.2 Erweiterungen durch Radikale: Zyklische Erweiterungen, Translationssatz, Zusammenhang zwischen Radikalerweiterungen und endlichen Galoiserweiterungen mit auflösbarer Galoisgruppe. Noch nicht Auflösbarkeit von Gleichungen gleichbedeutend zur Auflösbarkeit ihrer Galoisgruppe.

3.2 Auflösbarkeit von Gleichungen gleichbedeutend zur Auflösbarkeit ihrer Galoisgruppe. Unmöglichkeit der Auflösung kubischer Gleichungen nur durch reelle Wurzeln aus positiven reellen Zahlen selbst im Fall von drei reellen Lösungen.

8.2 Herleitung der Cardano'schen Formeln aus der Galoistheorie. Quadratisches Reziprozitätsgesetz, Legendre-Symbol, Beispiele. Quadratische Erweiterungen in Kreisteilungskörpern zu Einheitswurzeln von ungerader Primzahlordnung. Beides noch ohne Beweis.

10.2 Beweis quadratisches Reziprozitätsgesetz. Beweis quadratische Erweiterungen in Kreisteilungskörpern zu Einheitswurzeln von ungerader Primzahlordnung.

Literatur

[Art] Emil Artin. *Galois Theory*.

[Bes40] A. S. Besicovitch. On the linear independence of fractional powers of integers. *J. London Math. Soc.*, 15:3–6, 1940.

[E+92] Ebbinghaus et al. *Zahlen*. Springer, 1992.

[Lan74] Serge Lang. *Algebra*. Addison-Wesley, 1974.

[Lor96] Falko Lorenz. *Einführung in die Algebra I*. Spektrum, 1996.

[Rom06] Steven Roman. *Field theory*, volume 158 of *Graduate Texts in Mathematics*. Springer, New York, second edition, 2006.

[Rus05] Lucio Russo. *Die vergessene Revolution oder die Wiedergeburt des antiken Wissens*. Springer, 2005. Übersetzung aus dem Italienischen.

[SDAT00] S. A. Katre S. D. Adhikari and Dinesh Thakur. *Cyclotomic fields and related topics*. Bhaskaracharya Pratishthana, Pune, 2000.

[Suz87] Jiro Suzuki. On coefficients of cyclotomic polynomials. *Proc. Japan Acad. Ser. A Math. Sci. 63*, 63(7):279–280, 1987.

[Wei74] André Weil. *Basic Number Theory*. Springer, 1974.

Indexvorwort

Hier werden die Konventionen zum Index erläutert. Kursive Einträge bedeuten, daß ich die fragliche Terminologie oder Notation in der Literatur gefunden habe, sie aber selbst nicht verwende. Bei den Symbolen habe ich versucht, sie am Anfang des Index mehr oder weniger sinnvoll gruppiert aufzulisten. Wenn sie von ihrer Gestalt her einem Buchstaben ähneln, wie etwa das $\cup$ dem Buchstaben u oder das $\subset$ dem c, so liste ich sie zusätzlich auch noch unter diesem Buchstaben auf. Griechische Buchstaben führe ich unter den ihnen am ehesten entsprechenden deutschen Buchstaben auf, etwa ζ unter z und ω unter o.

Index