

ALGEBRA UND ZAHLENTHEORIE

Wolfgang Soergel

16. August 2018

Inhaltsverzeichnis

1 Mehr zu Gruppen	5
1.1 Die Frage nach der Klassifikation	5
1.2 Kompositionsreihen	7
1.3 p -Gruppen	11
1.4 Sylowsätze	14
1.5 Symmetrische Gruppen	20
1.6 Alternierende Gruppen*	26
2 Mehr zu Ringen	31
2.1 Restklassenringe	31
2.2 Teilringe	36
2.3 Abstrakter chinesischer Restsatz	37
2.4 Euklidische Ringe und Primfaktorzerlegung	39
2.5 Quotienten von Hauptidealringen	46
2.6 Irreduzible im Ring der Gauß'schen Zahlen	50
2.7 Primfaktorzerlegung in Polynomringen	55
2.8 Kreisteilungspolynome	60
2.9 Symmetrische Polynome	62
2.10 Schranke von Bézout*	68
3 Mehr zu Körpern	76
3.1 Grundlagen und Definitionen	76
3.2 Körpererweiterungen	77
3.3 Elemente von Körpererweiterungen	79
3.4 Endliche Körpererweiterungen	82
3.5 Notationen für Erzeugung**	84
3.6 Konstruktionen mit Zirkel und Lineal	85
3.7 Endliche Körper	91
3.8 Zerfällungskörper	96
3.9 Vielfachheit von Nullstellen	103
3.10 Satz vom primitiven Element	112
3.11 Algebraischer Abschluß*	117
3.12 Schiefkörper über den reellen Zahlen*	123
4 Galoistheorie	126
4.1 Galoiserweiterungen	126
4.2 Anschauung für die Galoisgruppe*	133
4.3 Galoiskorrespondenz	137
4.4 Galoisgruppen von Kreisteilungskörpern	143

4.5	Quadratisches Reziprozitätsgesetz	148
4.6	Radikalerweiterungen	156
4.7	Lösung kubischer Gleichungen	164
4.8	Einheitswurzeln und reelle Radikale*	169
5	Verallgemeinerungen ins Unendliche*	173
5.1	Ordinalzahlen	173
5.2	Wohlordnung und natürliche Zahlen	175
5.3	Dimension als Kardinalität	176
5.4	Anwendungen in der Analysis*	181
6	Ergänzungen zur Körpertheorie*	185
6.1	Tensorprodukte von Körpern	185
6.2	Allgemeiner Translationssatz	186
6.3	Krull-Topologie	189
6.4	Formen von Vektorräumen und Algebren	190
6.5	Kummer-Theorie	194
7	Danksagung	198
8	Vorlesung Algebra und Zahlentheorie WS 16/17	199
	Literaturverzeichnis	203
	Index	204

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 spielt nur eine Nebenrolle. 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 Mehr zu Gruppen

1.1 Die Frage nach der Klassifikation

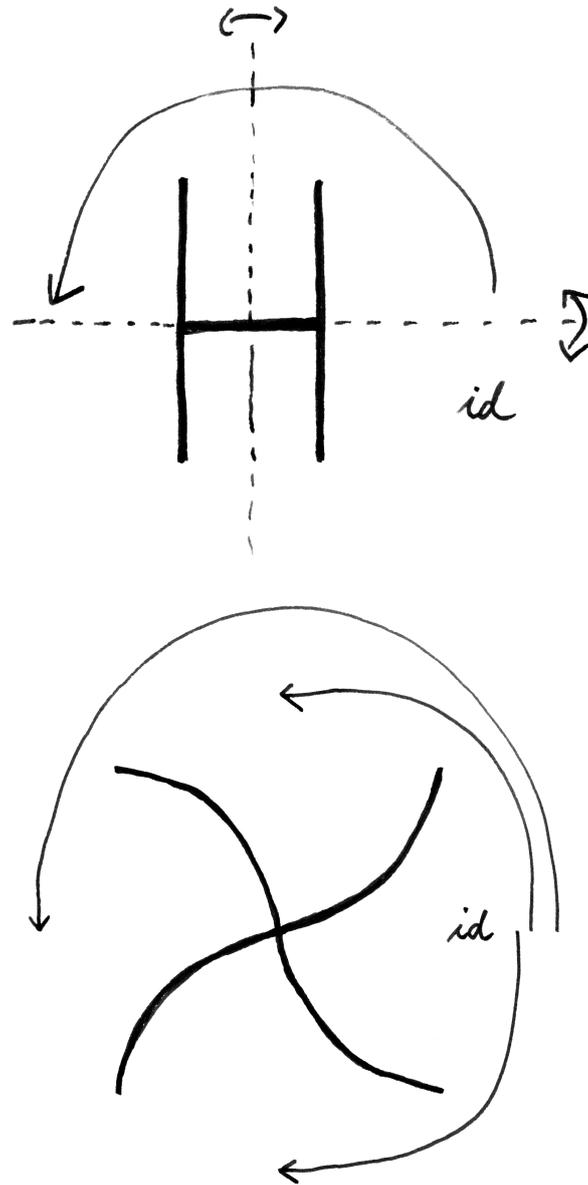
1.1.1. Ich erinnere an die Definition [GR] 3.2.2. Eine **Gruppe** ist eine Menge G mit einer Verknüpfung $G \times G \rightarrow G$, $(a, b) \mapsto ab$ derart, daß für alle $a, b, c \in G$ gilt $(ab)c = a(bc)$, daß es ein Element $1 \in G$ gibt mit $1a = a1 = a \forall a \in G$, und daß es für alle $a, b \in G$ ein Element $c \in G$ gibt mit $ac = b$. Gegeben eine weitere Gruppe H ist ein **Gruppenhomomorphismus** $\varphi : G \rightarrow H$ eine Abbildung von G nach H mit $\varphi(ab) = \varphi(a)\varphi(b)$ für alle $a, b \in G$. Die Menge aller Gruppenhomomorphismen von G nach H notiere ich $\text{Grp}(G, H)$.

1.1.2. 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 1.1.3. 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 $1, \zeta = \exp(2\pi i/3)$ und $\eta = \exp(4\pi i/3)$ 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 [GR] 3.2.16 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.

1.1.4. 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, ebenso viele 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“.

1.2 Kompositionsreihen

1.2.1. Ich erinnere an Restklassen [LA2] 4.1, Normalteiler [LA2] 4.2, Gruppenwirkungen [LA2] 5.1.1, Bahnformel [LA2] 5.2 und Konjugationsklassen [LA2] 5.3.

Definition 1.2.2. 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 1.2.3. Beispiele einfacher Gruppen sind die zyklischen Gruppen von Primzahlordnung und die sogenannten **alternierenden Gruppen**

$$A_r := \ker(\text{sgn} : \mathcal{S}_r \rightarrow \{\pm 1\})$$

aller geraden Permutationen von r Objekten unter der Annahme $r \geq 5$, wie wir als Satz 1.6.2 zeigen werden. Nicht zeigen werden wir, daß die alternierende Gruppe A_5 die kleinste nichtabelsche einfache Gruppe ist. Diese Gruppe ist übrigens genau unsere Ikosaedergruppe aus [LA2] 5.4.3 aller Drehsymmetrien eines Ikosaeders, was wir im anschließenden Satz 1.2.5 zeigen.

Ergänzung 1.2.4. 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 1.2.5. 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

$$60 = 1 + 15 + 20 + 24$$

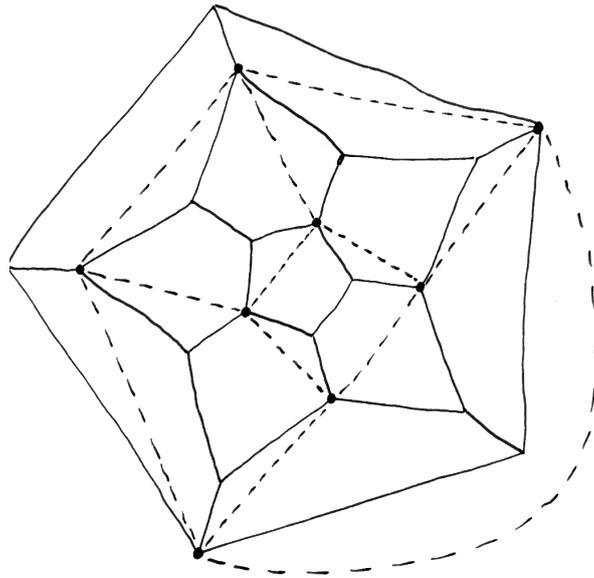
Da je zwei Kanten des Ikosaeders durch eine Drehsymmetrie des Ikosaeders ineinander überführt werden können, bilden die 15 Elemente der Ordnung 2 eine Konjugationsklasse: Sind in der Tat K und L Kanten und d_K, d_L die nichttrivialen Drehsymmetrien, die sie jeweils in sich selbst überführen, und ist g eine Drehsymmetrie mit $g(K) = L$, so gilt $d_K = g^{-1}d_Lg$. 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

$$\varphi : I \rightarrow \mathcal{S}_5$$

Der Kern von $\text{sgn} \circ \varphi : I \rightarrow \{+1, -1\}$ ist ein von 1 verschiedener Normalteiler von I , es folgt $\ker(\text{sgn} \circ \varphi) = I$ und φ induziert einen Gruppenhomomorphismus nach $A_5 = \ker(\text{sgn}) \subset \mathcal{S}_5$. Der Kern von $\varphi : I \rightarrow \mathcal{S}_5$ 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 stehenden 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 [GR] 2.3.45 die zyklische Anordnung „im Uhrzeigersinn“ festlegen, so wird die Gruppe derjenigen Symmetrien unseres Graphen, die diese zyklischen Anordnungen respektieren, genau die Ikosaedergruppe werden.

Definition 1.2.6. Eine **Kompositionsreihe** einer Gruppe G ist eine Folge von Untergruppen

$$G = G_r \supset G_{r-1} \supset \dots \supset G_0 = 1$$

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 $1 \leq i \leq r$. Die Gruppen G_i/G_{i-1} heißen die **Subquotienten** der Kompositionsreihe.

Satz 1.2.7 (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 $G = M_r \supset \dots \supset M_0 = 1$ und $G = N_s \supset \dots \supset N_0 = 1$ 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 1.2.8. Jede abelsche Gruppe mit n Elementen hat als Kompositionsfaktoren die zyklischen Gruppen $\mathbb{Z}/p_i\mathbb{Z}$ für $n = p_1 \dots p_r$ 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 1.6.2 und 1.6.3 diskutiert: 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

$$\begin{array}{ccccccc} G & \supset & M & \supset & \dots & \supset & 1 \\ G & \supset & N & \supset & \dots & \supset & 1 \end{array}$$

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 $(M \cap N) \supset \dots \supset 1$ eine Kompositionsreihe des Schnitts an, so hat die Gruppe G also Kompositionsreihen

$$\begin{array}{ccccccc} G & \supset & M & \supset & & \dots & \supset & 1 \\ G & \supset & M & \supset & (M \cap N) & \supset & \dots & \supset & 1 \\ G & \supset & N & \supset & (M \cap N) & \supset & \dots & \supset & 1 \\ G & \supset & N & \supset & & \dots & \supset & 1 \end{array}$$

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 1.2.9. Man zeige die Aussage des Satzes von Jordan-Hölder 1.2.7, 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 1.2.10. Man zeige: Sind N und B Gruppen und $\tau : B \rightarrow \text{Grp}^\times N$ ein Gruppenhomomorphismus alias eine Operation von B auf N durch Gruppenautomorphismen, notiert $(\tau(a))(n) =: ({}^a n)$, so kann man $N \rtimes B$ mit einer Gruppenstruktur versehen vermittels der Vorschrift

$$(m, a)(n, b) = (m ({}^a n), ab)$$

Diese Gruppe heißt das oder genauer ein **semidirektes Produkt** von N mit B und wird auch notiert als

$$N \rtimes B = N \rtimes_\tau B$$

Man zeige weiter: Ist $\varphi : G \twoheadrightarrow B$ ein surjektiver Gruppenhomomorphismus, N sein Kern und $\psi : B \rightarrow G$ eine Spaltung von φ , so erhalten wir einen Gruppenhomomorphismus $\tau : B \rightarrow \text{Grp}^\times N$ durch $(\tau(b))(n) := \psi(b)n\psi(b)^{-1}$ und die Abbildung $(n, b) \mapsto n\psi(b)$ definiert einen Gruppenisomorphismus

$$N \rtimes B \xrightarrow{\sim} G$$

Ergänzung 1.2.11. Ist speziell eine Gruppe N ein Produkt von n Kopien einer festen Gruppe $N = A^n = A \times \dots \times A$ und operiert eine weitere Gruppe B darauf durch Vertauschung der Faktoren, also in hoffentlich offensichtlicher Weise vermittels eines Gruppenhomomorphismus $B \rightarrow \mathcal{S}_n$, so bezeichnet man das zugehörige semidirekte Produkt als **Kranzprodukt** und notiert es $N \rtimes B =: A \wr B$.

Ergänzende Übung 1.2.12. 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 $\mathcal{S}_3 \xrightarrow{\sim} \text{GL}(2; \mathbb{F}_2)$.

1.3 p -Gruppen

Definition 1.3.1. Das **Zentrum** einer Gruppe G ist die Menge

$$Z(G) := \{x \in G \mid xg = gx \quad \forall g \in G\}$$

derjenigen Gruppenelemente, die mit allen anderen Gruppenelementen kommutieren.

1.3.2. Offensichtlich ist das Zentrum ein Normalteiler, was im Übrigen auch die alternative Beschreibung $Z(G) = \ker(\text{int} : G \rightarrow \text{Grp}^\times(G))$ als Kern eines Gruppenhomomorphismus in den Notationen aus [LA2] 5.3 sofort zeigt.

Definition 1.3.3. Die Standgruppe von $g \in G$ unter der Operation von G auf sich selbst durch Konjugation heißt der **Zentralisator** $Z_G(g)$ von g , in Formeln

$$Z_G(g) = \{x \in G \mid xgx^{-1} = g\}$$

1.3.4. Ist G eine endliche Gruppe, $G = C_1 \sqcup \dots \sqcup C_r$ ihre Zerlegung in Konjugationsklassen und $g_i \in C_i$ jeweils ein Element, so liefert die Bahnformel [LA2] 5.2.2 die sogenannte **Klassengleichung**

$$\begin{aligned} |G| &= |C_1| + \dots + |C_r| \\ &= |G|/|Z_G(g_1)| + \dots + |G|/|Z_G(g_r)| \end{aligned}$$

Die einelementigen Konjugationsklassen sind dabei genau die Konjugationsklassen der Elemente des Zentrums.

Definition 1.3.5. Sei p eine Primzahl. Eine **p -Gruppe** ist eine endliche Gruppe, deren Ordnung eine Potenz von p ist.

1.3.6. Die triviale Gruppe hat p^0 Elemente und ist damit nach unserer Konvention [LA2] 4.4.3 eine p -Gruppe für jede Primzahl p .

Proposition 1.3.7. *Jede nichttriviale p -Gruppe hat nichttriviales Zentrum.*

Beweis. Wir zerlegen unsere Gruppe in Konjugationsklassen $G = C_1 \sqcup \dots \sqcup C_r$. 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

$$|G| \equiv |Z(G)| \pmod{p}$$

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 1.3.8. *Ist die Ordnung einer Gruppe das Quadrat einer Primzahl p , so ist die besagte Gruppe abelsch, in Formeln:*

$$|G| = p^2 \Rightarrow Z(G) = G$$

Beweis. Nach der vorhergehenden Proposition 1.3.7 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 [LA2] 4.1.5 notwendig bereits die ganze Gruppe. \square

Satz 1.3.9 (Struktur von p -Gruppen). *Ist G eine p -Gruppe, so gibt es in G eine Kette $G = G_r \supset G_{r-1} \supset \dots \supset G_0 = 1$ 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 1.3.7 nichttrivales Zentrum $Z(G) \neq 1$. 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 $\bar{G} = \bar{G}_l \supset \dots \supset \bar{G}_1 \supset \bar{G}_0 = 1$ wie gewünscht. Dann nehmen wir $G_i := \text{can}^{-1}(\bar{G}_{i-1})$ für $\text{can} : G \rightarrow \bar{G}$ die Projektion. Wegen [LA2] 4.2.20 erhalten wir so eine Kette von Normalteilern von G . Wegen [LA2] 4.1.6 haben wir $|G_i| = p|\bar{G}_{i-1}| = p^i$. Damit hat G_i/G_{i-1} genau p Elemente. \square

1.3.10. Eine Gruppe G heißt **auflösbar**,) wenn es eine Folge von Untergruppen $G = G_r \supset G_{r-1} \supset G_{r-2} \supset \dots \supset G_0 = 1$ gibt mit G_{i-1} normal in G_i und G_i/G_{i-1} abelsch für $1 \leq i \leq r$. Aus 1.3.17 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 4.6.20 verständlich. Bemerkung 1.6.3 zeigt, daß die symmetrische Gruppe 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 Isomorphismus die einzige nichtauflösbare Gruppe mit 60 Elementen. Beides werden wir aber hier nicht zeigen.

Übungen

Übung 1.3.11. Eine Gruppe G heißt **nilpotent**, wenn es eine Folge $G = G_r \supset G_{r-1} \supset G_{r-2} \supset \dots \supset G_0 = 1$ 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 1.3.9. Natürlich können wir zu jeder Gruppe G die Gruppe $G/Z(G)$

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 1.3.12. 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

$$G^0 := G, G^1 := \langle(G, G)\rangle, \dots, G^{i+1} := \langle(G^i, G)\rangle, \dots$$

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 1.3.13. Eine Gruppe G heißt **überauflösbar**, wenn es eine Folge $G = G_r \supset G_{r-1} \supset G_{r-2} \supset \dots \supset G_0 = 1$ 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 1.3.14. 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 1.3.15. Man bestimme das Zentrum der Gruppe $GL(n; k)$ für $n \in \mathbb{N}$ und k ein Körper. Man bestimme das Zentrum der Symmetriegruppe eines Quadrats.

Übung 1.3.16. 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: [LA2] 4.2.19.

Ergänzende Übung 1.3.17. Gegeben eine Gruppe G erklärt man ihre **derivierete Gruppe** als $\mathcal{D}G := \langle(G, G)\rangle$ und setzt induktiv $\mathcal{D}^{i+1}G := \mathcal{D}(\mathcal{D}^iG)$. Man zeige, daß eine Gruppe genau dann auflösbar ist, wenn ihre höheren derivierten Gruppen irgendwann trivial werden, wenn also in Formeln gilt $\mathcal{D}^iG = 1$ für $i \gg 0$. Man zeige weiter, daß alle höheren derivierten Gruppen Normalteiler von G sind.

1.4 Sylowsätze

Definition 1.4.1. 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 1.4.2. 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.

1.4.3. 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 1.4.4 (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 1.4.5. Ist G eine endliche abelsche Gruppe, so gibt es insbesondere genau eine p -Sylow für alle p . Wir kennen diese Untergruppe schon aus Proposition [LA2] 4.3.17: Es ist genau unsere Untergruppe $G(p)$ aller Elemente von G , deren Ordnung eine p -Potenz ist.

Beispiel 1.4.6. 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. Besitzt G eine echte Untergruppe $H \subsetneq G$ mit $p \nmid |G/H|$, so folgt die Aussage aus der Induktionsannahme. Teilt sonst p den Index $|G/H|$ jeder echten Untergruppe

$H \subsetneq G$, so ist die Kardinalität jeder Konjugationsklasse mit mehr als einem Element teilbar durch p . Aus der Klassengleichung 1.3.4 folgt damit die Kongruenz $|G| \equiv |Z(G)| \pmod{p}$ und p teilt die Ordnung des Zentrums $Z(G)$. Dann gibt es nach [LA2] 4.3.18 in $Z(G)$ 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 .

5. Vor dem weiteren Fortgang des Beweises ergänzen wir nun unseren Satz um einen etwas 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 technischer 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 genau $hQh^{-1} = Q \quad \forall h \in H$. 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 Bahn und damit ist $|QH/H|$ eine p -Potenz. Da aber 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 Sylow $P = x$ gegeben. Für ihre Isotropiegruppe G_x gilt $G_x \supset P$, also ist nach der Bahnformel [LA2] 5.2.2 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 Isotropiegruppe 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 $|G/P|$. \square

Ergänzung 1.4.7. Ein alternativer Beweis des ersten Teils geht so: Man betrach-

tet 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 [GR] 1.1.27.

Korollar 1.4.8 (Satz von Cauchy). *Jeder Primfaktor der Ordnung einer endlichen Gruppe tritt auch als Ordnung eines Elements besagter Gruppe auf.*

1.4.9. Man beachte, daß wir diese Aussage im Fall abelscher Gruppen bereits in [LA2] 4.3.18 bewiesen hatten, und daß wir sie in diesem Fall ihrerseits beim Beweis der Sylowsätze verwendet haben. Einen alternativen Beweis konnten Sie als Übung [LA2] 4.1.13 ausarbeiten. Allgemeinere Teiler der Ordnung einer endlichen Gruppe müssen keineswegs als Ordnung eines Elements besagter Gruppe auftreten. So gibt es etwa in der symmetrischen Gruppe \mathcal{S}_5 gibt es keine Untergruppe mit 15 Elementen, was Sie als Übung gleich zeigen können. 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 1.3.9.

Beweis. Sei p unser Primfaktor. Man findet zunächst nach 1.4.4 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 . \square

Proposition 1.4.10. *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 1.4.8 Elemente $a, b \in G$ der Ordnungen 2 und 3. Nach Übung [LA1] 3.3.8 zum Satz von Lagrange gilt $\langle a \rangle \cap \langle b \rangle = 1$, also definiert 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. \square

Korollar 1.4.11. *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. \square

Ergänzung 1.4.12 (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 [LA2] 4.3.5. Gruppen mit 4 oder 9 Elementen sind abelsch nach 1.3.8 und werden damit durch [LA2] 4.4.5 klassifiziert. Gruppen mit 6 Elementen hatten wir in 1.4.10 diskutiert. Für Gruppen mit 10 oder 14 Elementen funktioniert dieselbe Argumentation, wie Sie als Übung 1.4.15 ausarbeiten dürfen. Gruppen mit 8 Elementen klassifizieren wir in 1.4.13, Gruppen mit 12 Elementen klassifizieren Sie in 1.4.19, und jede Gruppe mit 15 Elementen ist zyklisch nach 1.4.11. Bei Gruppen mit 16 Elementen fängt es aber an, unübersichtlich zu werden, es gibt von ihnen bereits 14 Isomorphieklassen.

Ergänzung 1.4.13 (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 $\{\pm 1, \pm i, \pm j, \pm k\}$ nach [LA1] 4.7.4. Um das einzusehen, kann man argumentieren wie folgt: Jede nichtabelsche Gruppe der Ordnung acht besitzt nach [LA1] 1.2.17 Elemente der Ordnung vier, also nach [LA2] 4.2.21 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 ij und auch $k := (-1)ij$ 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 1.4.14. 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 1.4.15. 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 1.4.16. Sind $p > q$ Primzahlen und ist q kein Teiler von $p - 1$, so ist jede Gruppe der Ordnung pq zyklisch. Hinweis: **1.4.11**.

Ergänzende Übung 1.4.17 (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 1.4.18 (Funktorialität semidirekter Produkte). Seien A, M, B, N Gruppen und $\kappa : A \rightarrow \text{Grp}^\times M$ sowie $\tau : B \rightarrow \text{Grp}^\times N$ Gruppenhomomorphismen. Wie bei der Definition semidirekter Produkte in **1.2.10** schreiben wir $(\kappa(a))(m) = : ({}^a m)$ und $(\tau(b))(n) = : ({}^b n)$. Seien weiter $\psi : A \rightarrow B$ und $\varphi : M \rightarrow N$ 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

$$(\varphi \times \psi) : M \rtimes A \rightarrow N \rtimes B$$

Speziell haben wir $N \rtimes_\tau B \cong N \rtimes_\kappa B$ im Fall $\kappa = (\text{int } \varphi) \circ \tau$ für einen Automorphismus $\varphi \in \text{Grp}^\times N$ der Gruppe N .

Ergänzende Übung 1.4.19 (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 $\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$, 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

$$\begin{array}{lll} (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/3\mathbb{Z} & (\mathbb{Z}/2\mathbb{Z})^2 \rtimes \mathbb{Z}/3\mathbb{Z} & (\mathbb{Z}/2\mathbb{Z})^2 \rtimes \mathbb{Z}/3\mathbb{Z} \\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} & \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z} & \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z} \end{array}$$

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 1.4.18 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 1.4.20. Man zeige, daß die 2-Sylow in der symmetrischen Gruppe S_4 der Drehsymmetrien eines Würfels isomorph ist zur Diedergruppe der Ordnung 8.

Ergänzende Übung 1.4.21. 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 1.4.22. 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 1.4.23. Eine Gruppe mit 30 Elementen kann nie einfach sein. Hinweis: Entweder besitzt sie nur eine 3-Sylow oder nur eine 5-Sylow.

1.5 Symmetrische Gruppen

Definition 1.5.1. Eine **Partition** λ einer **natürlichen Zahl** $n \in \mathbb{N}$ ist eine monoton fallende Folge von natürlichen Zahlen $\lambda_1 \geq \lambda_2 \geq \dots$ 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 1.5.2. Die Zahl 5 hat genau sieben Partitionen. Salopp können wir sie beschreiben als die Zerlegungen

$$\begin{aligned} 5 &= 5 \\ 5 &= 4 + 1 \\ 5 &= 3 + 2 \\ 5 &= 3 + 1 + 1 \\ 5 &= 2 + 2 + 1 \\ 5 &= 2 + 1 + 1 + 1 \\ 5 &= 1 + 1 + 1 + 1 + 1 \end{aligned}$$

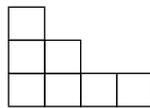
Hier haben wir nur die von Null verschiedenen Folgenglieder aufgeschrieben und sie durch $+$ getrennt. Formal meinen wir zum Beispiel im vierten Fall die Folge $3, 1, 1, 0, 0, \dots$. Zur Abkürzung verwendet man auch oft die sogenannte **exponentielle Schreibweise**, in der unsere Partitionen von 5 der 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 1.5.3. 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

$$((i, j) \in Y \text{ und } i' \leq i \text{ und } j' \leq j) \Rightarrow (i', j') \in Y$$

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

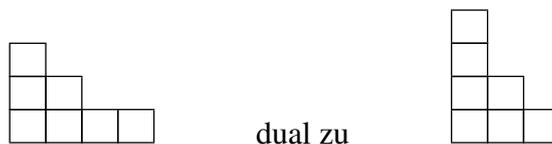


die Menge $\{(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (2, 0), (3, 0)\}$ dar. In der Praxis denke ich bei Youngdiagrammen stets an Bilder dieser Art.

Ergänzung 1.5.4. Jedes Youngdiagramm Y mit n Kästchen im Sinne von 1.5.3 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

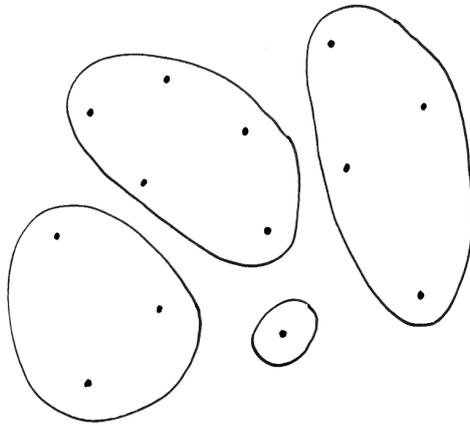
$$\mathcal{P}_n \xleftarrow{z} \mathcal{Y}_n \xrightarrow{s} \mathcal{P}_n$$

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



1.5.5. Unter einer **Partition einer Menge** X verstehen wir wie in [LA2] 5.1.13 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 1.5.5 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 $7 = 3 + 2 + 1 + 1$.

1.5.6. Jede Permutation $\sigma \in \text{Ens}^\times(X)$ 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 $\text{Ens}^\times(X) \rightarrow \mathcal{P}_X$ mit der in 1.5.5 diskutierten Abbildung $\mathcal{P}_X \rightarrow \mathcal{P}_n$ die sogenannte **Zykellängenabbildung** $\text{Ens}^\times(X) \rightarrow \mathcal{P}_n$. Im Fall $X = \{1, \dots, n\}$ ist das eine Abbildung $\mathcal{S}_n \rightarrow \mathcal{P}_n$.

1.5.7. Ich erinnere an die Operation durch Konjugation einer Gruppe auf sich selber aus [LA2] 5.3.1 und an ihre Bahnen, die Konjugationsklassen.

Satz 1.5.8 (Konjugationsklassen in den symmetrischen Gruppen). *Ist X eine endliche Menge mit $|X| = n$ Elementen, so sind die Fasern der Zykellängenabbildung*

$$\text{Ens}^\times(X) \rightarrow \mathcal{P}_n$$

genau die Konjugationsklassen in der Permutationsgruppe $\text{Ens}^\times(X)$.

Ergänzung 1.5.9. Eine analoge Aussage gilt mit demselben Beweis auch für eine beliebige Menge X .

Beweis. Seien Permutationen $\sigma, \tau \in \text{Ens}^\times(X)$ gegeben. Ist $X = X_1 \cup \dots \cup X_r$ die Partition von X in die Bahnen von $\langle \sigma \rangle$, so ist

$$X = \tau(X_1) \cup \dots \cup \tau(X_r)$$

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 $\sigma, \kappa \in \text{Ens}^\times(X)$ unsere beiden Permutationen und

$$\begin{aligned} X &= X_1 \cup \dots \cup X_r \\ X &= Y_1 \cup \dots \cup Y_r \end{aligned}$$

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

$$\begin{aligned} X_i &= \{z, \sigma(z), \sigma^2(z), \dots, \sigma^{r_i}(z) = z\} \\ Y_i &= \{u, \kappa(u), \kappa^2(u), \dots, \kappa^{r_i}(u) = u\} \end{aligned}$$

Definieren wir also $\tau : X_i \xrightarrow{\sim} Y_i$ durch $\tau(\sigma^\nu(z)) = \kappa^\nu(u)$, so kommutiert das Diagramm

$$\begin{array}{ccc} X_i & \xrightarrow{\sigma} & X_i \\ \tau \downarrow & & \downarrow \tau \\ Y_i & \xrightarrow{\kappa} & Y_i \end{array}$$

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 $\kappa = \tau\sigma\tau^{-1}$. \square

Definition 1.5.10. Hat $\langle \sigma \rangle$ außer einer p -elementigen Bahn nur einelementige Bahnen, so nennt man σ einen p -**Zykel**. Die Zweizykel heißen auch **Transpositionen**.

1.5.11 (**Zykelschreibweise für Permutationen**). Eine Möglichkeit, Permutationen zu notieren, besteht darin, unter jedes Element sein Bild zu schreiben, also etwa

$$\tau = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 2 & 3 & 5 & 1 \end{bmatrix}$$

Eine andere Möglichkeit ist die Notation als Produkt paarweise disjunkter Zykeln. Ein p -Zykel σ wird notiert in der Form $\sigma = (z, \sigma(z), \sigma^2(z), \dots, \sigma^{p-1}(z))$ 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 mitnotiert, so daß wir also auch schreiben könnten

$$\tau = (1, 6)(2, 4, 3)$$

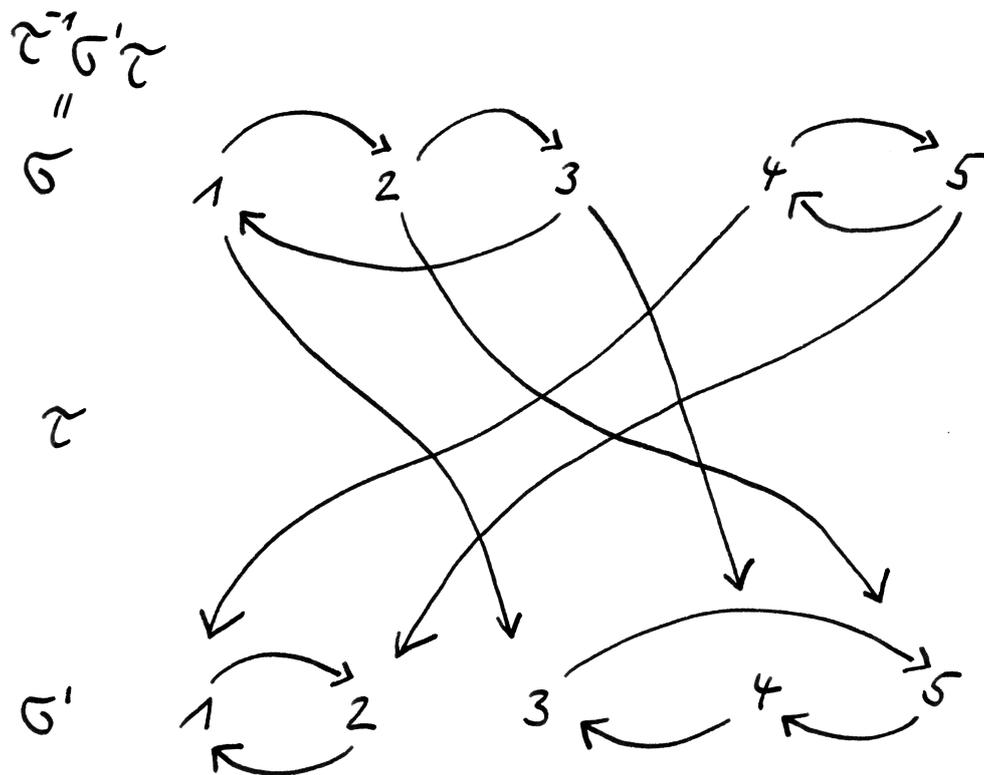
Das ist übrigens auch das Produkt der Transposition $\kappa = (1, 6)$ mit dem Dreizykel $\rho = (2, 4, 3)$ und wir haben $\tau = \kappa\rho = \rho\kappa$, was die Sinnhaftigkeit unserer Notation zeigt. Zwei Zykeln heißen **disjunkt** genau dann, wenn jedes Element von einem der beiden festgehalten wird. Ganz allgemein kommutieren disjunkte Zykeln, so gilt etwa $(1, 6)(2, 3, 4) = (2, 3, 4)(1, 6)$ in \mathcal{S}_6 .

Übungen

Ergänzende Übung 1.5.12 (Partitionen und nilpotente Matrizen). Gegeben ein n -dimensionaler Vektorraum V bildet für jeden nilpotenten Endomorphismus $N \in \text{End } V$ die Folge der Dimensionen $\dim(\text{im } N^r / \text{im } N^{r+1})$ eine Partition von n , und die Fasern der so konstruierten Abbildung

$$\{N \in \text{End } V \mid N \text{ nilpotent}\} \rightarrow \mathcal{P}_n$$

sind genau die Bahnen der Operation von $\text{GL}(V)$ 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 1.5.13. Man zeige, daß die symmetrische Gruppe \mathcal{S}_5 genau sieben Konjugationsklassen besitzt.

Ergänzende Übung 1.5.14. Man zeige, daß das Signum eines p -Zykels stets $(-1)^{p+1}$ ist.

Übung 1.5.15. Man zeige unabhängig von unseren geometrischen Betrachtungen zur Ikosaedergruppe **1.2.5**, 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 1.5.16 (Zentralisatoren in symmetrischen Gruppen). Seien X eine endliche Menge und $\sigma \in \mathcal{S} := \text{Ens}^\times X$ eine Permutation von X . Ihr Zentralisator $Z_{\mathcal{S}}(\sigma)$ nach **1.3.3** 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 $n(i)$ Zyklen der Länge i und keinen Zyklus einer Länge $> r$, so hat das Bild von $Z_{\mathcal{S}}(\sigma) \rightarrow \text{Ens}^\times(X/\langle \sigma \rangle)$ also genau $n(1)!n(2)! \dots n(r)!$ 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 $1^{n(1)} \dots r^{n(r)}$ Stück. Zusammen erhalten wir mit **[LA1] 3.3.11** so

$$|Z_{\mathcal{S}}(\sigma)| = \prod_{i=1}^r n(i)! i^{n(i)}$$

1.6 Alternierende Gruppen*

1.6.1. Die Abbildung sgn , die jeder Permutation $\tau \in \mathcal{S}_r$ ihr Signum zuordnet, ist ein Gruppenhomomorphismus $\text{sgn} : \mathcal{S}_r \rightarrow \{1, -1\}$. Der Kern dieses Gruppenhomomorphismus, d.h. die Gruppe aller geraden Permutationen von r Objekten, heißt die r -te **alternierende Gruppe** und wird notiert als

$$A_r = \ker(\text{sgn} : \mathcal{S}_r \rightarrow \{1, -1\})$$

Satz 1.6.2. Die alternierenden Gruppen A_r sind einfach für $r \geq 5$.

1.6.3. 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 Einfachheit der Ikosaedergruppe unmittelbar einsehen, indem man die Kardinalitäten der Konjugationsklassen berechnet. Dem Beweis des Satzes im allgemeinen schicken wir zwei Lemmata voraus.

1.6.4. 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 1.6.5. *Die symmetrischen Gruppen \mathcal{S}_r werden von den Transpositionen erzeugt, die alternierenden Gruppen A_r von den Dreizykeln.*

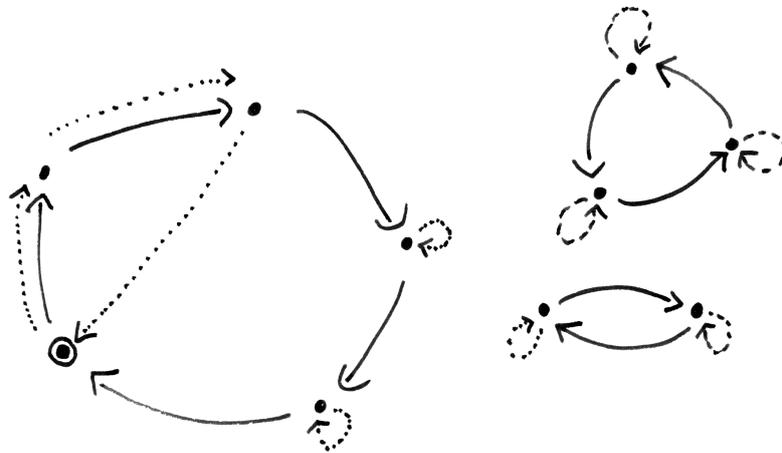
Beweis. Die erste Aussage war Übung [LA1] 5.1.8. Die Zweite folgt daraus, daß man jede Doppeltransposition als Produkt von zwei Dreizykeln schreiben kann, $(ab)(cd) = (abc)(bcd)$, und daß das Produkt von zwei nicht kommutierenden Transpositionen ein Dreizykel ist, $(ab)(ac) = (acb)$. Jedes Produkt einer geraden Zahl von Transpositionen läßt sich demnach auch als ein Produkt von Dreizykeln darstellen. \square

Lemma 1.6.6. *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.*

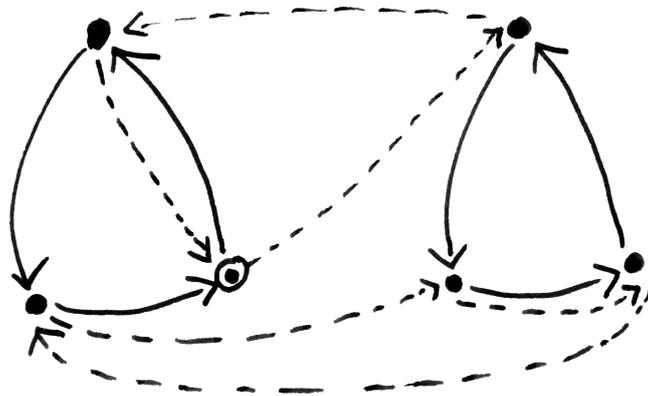
Beweis. Jeder Dreizykel kann als Verknüpfung von zwei Transpositionen seiner drei Elemente dargestellt werden. Haben wir noch zwei weitere Elemente zur Verfügung, so können wir diese beiden Transpositionen durch das Verknüpfen mit der Vertauschung dieser beiden Elemente zu Doppeltranspositionen machen. Das zeigt die erste Aussage. Zwei Doppeltranspositionen $(ab)(cd)$ und $(a'b')(c'd')$ sind konjugiert unter jeder Permutation τ mit $a \mapsto a', \dots, d \mapsto d'$ 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 $a \mapsto a', \dots, c \mapsto c'$ 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. \square

Beweis von 1.6.2. Sei ab jetzt r beliebig und $N \subset A_r$ ein nichttrivialer Normalteiler. Nach dem vorhergehenden Lemma 1.6.6 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 $\text{ord } g \geq 5$, 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 $\text{ord } g = 3$ 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 $\text{ord } g = 2$ 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 . \square

Übungen

Übung 1.6.7. Man zeige, daß die Gruppe aller jeweils nur endlich viele Elemente bewegendenden geraden Permutationen einer unendlichen Menge eine einfache aber nicht endlich erzeugte Gruppe ist.

Ergänzende Übung 1.6.8. 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.

1.6.9. 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 1.6.10. In dieser Übung sollen Sie zeigen, daß die Gruppe $\text{SL}(2; \mathbb{F}_5)$ genau fünf 2-Sylows besitzt und daß die Operation dieser Gruppe auf der Menge ihrer 2-Sylows einen Isomorphismus

$$\text{SL}(2; \mathbb{F}_5) / \{\pm \text{id}\} \xrightarrow{\sim} A_5$$

mit der sogenannten „alternierenden Gruppe“ aller geraden Permutationen einer fünfelementigen Menge induziert. Den Quotienten auf der linken Seite notiert man auch $\text{PSL}(2; \mathbb{F}_5)$, er liegt als Untergruppe vom Index 2 in der Gruppe

$\text{PGL}(2; \mathbb{F}_5)$ aller von invertierbaren Matrizen induzierten Automorphismen der projektiven Gerade alias dem Quotienten von $\text{GL}(2; \mathbb{F}_5)$ nach der Gruppe der vier darin enthaltenen Diagonalmatrizen. Ich rate, der Reihe nach folgendes zu zeigen:

1. Jedes Element der Ordnung 4 in $\text{SL}(2; \mathbb{F}_5)$ ist diagonalisierbar und der Normalisator seines Erzeugnisses ist eine 2-Sylow. Jede 2-Sylow enthält 6 Elemente der Ordnung 4.
2. Es gibt in $\text{SL}(2; \mathbb{F}_5)$ genau dreißig Elemente der Ordnung 4 und fünf 2-Sylows, und der Schnitt von je zwei verschiedenen 2-Sylows besteht nur aus $\pm \text{id}$.
3. Jede 2-Sylow von $\text{PSL}(2; \mathbb{F}_5)$ ist eine Klein'sche Vierergruppe und operiert nach 1.4.21 frei auf der Menge der vier anderen 2-Sylows. Vom Bild unseres Homomorphismus $\text{PSL}(2; \mathbb{F}_5) \rightarrow \mathcal{S}_5$ wissen wir damit, daß es alle Doppeltranspositionen enthält und aus höchstens 60 Elementen besteht. Nach 1.6.6 muß dieses Bild folglich die A_5 sein.

Ergänzung 1.6.11. 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.

2 Mehr zu Ringen

2.1 Restklassenringe

2.1.1. Wir erinnern die grundlegenden Definitionen zu Ringen aus [LA1] 4.1: 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 $a(b + c) = ab + ac$ und $(a + b)c = ac + bc$ gelten.

2.1.2. 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 $\text{Mat}(n; R)$ der $(n \times n)$ -Matrizen mit Einträgen aus einem beliebigen Ring R mit der Addition und Multiplikation von Matrizen als Verknüpfung.

2.1.3. Eine Abbildung $\varphi : R \rightarrow S$ 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.

2.1.4. 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 $\text{Ring}(R, S)$.

2.1.5. Die Stärke der Ringtheorie liegt unter anderem darin, daß es sehr viele Verfahren 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 [LA1] 4.3.40 und Matrizenringen. Wir besprechen im folgenden zusätzlich das Bilden von Restklassenringen.

Satz 2.1.6 (Universelle Eigenschaft surjektiver Ringhomomorphismen). *Seien $s : R \twoheadrightarrow Q$ ein surjektiver Ringhomomorphismus und $\varphi : R \rightarrow S$ ein beliebiger Ringhomomorphismus. Genau dann existiert ein Ringhomomorphismus $\bar{\varphi} : Q \rightarrow S$ mit $\varphi = \bar{\varphi} \circ s$, wenn gilt $\ker(\varphi) \supset \ker(s)$.*

2.1.7. 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

$$(\circ s) : \text{Ring}(Q, S) \xrightarrow{\sim} \{\varphi \in \text{Ring}(R, S) \mid \ker(\varphi) \supset \ker(s)\}$$

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

$$\begin{array}{ccc} R & \xrightarrow{s} & Q \\ & \searrow t & \downarrow \bar{\varphi} \\ & & S \end{array}$$

Man formuliert diesen Satz auch mit den Worten, φ **faktoriere 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 [LA2] 4.2.1 zitieren, finden wir schon mal eine Abbildung $\bar{\varphi}$ wie behauptet. Man prüft leicht, daß sie ein Ringhomomorphismus ist. \square

2.1.8 (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 $\bar{t} : Q \rightarrow P$ mit $\bar{t} \circ s = t$ und $\bar{s} : P \rightarrow Q$ mit $\bar{s} \circ t = s$ nach 2.1.6 offensichtlich zueinander inverse Isomorphismen $Q \xrightarrow{\bar{t}} P \xrightarrow{\bar{s}} Q$. Salopp gesprochen wird also bei einem surjektiven Ringhomomorphismus „das Ziel bereits durch den Ausgangsraum und den Kern festgelegt bis auf eindeutigen Isomorphismus“.

Definition 2.1.9. 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 $IR \subset I$.

2.1.10. 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 2.1.11. Ein Ideal von \mathbb{Z} ist dasselbe wie eine Untergruppe von \mathbb{Z} , die Ideale von \mathbb{Z} sind also nach [LA1] 3.3.4 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.

2.1.12. Ist $\varphi : R \rightarrow S$ 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 2.1.13 (Restklassenringe). *Seien R ein Ring und $I \subset R$ ein Ideal. So gibt es einen von R ausgehenden surjektiven Ringhomomorphismus mit I als Kern.*

2.1.14. Nach 2.1.8 ist ein surjektiver Ringhomomorphismus mit Kern I eindeutig bis auf das Nachschalten eines eindeutigen Isomorphismus. Wir notieren ihn

$$\text{can} = \text{can}_q : R \twoheadrightarrow R/I$$

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 $\text{can}(a) = \bar{a}$.

Beispiel 2.1.15. Den Spezialfall der Restklassenringe $\mathbb{Z}/m\mathbb{Z}$ kennen wir bereits aus [LA1] 4.2.4.

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 $\bar{m} : R/I \times R/I \rightarrow R/I$ derart, daß mit der Multiplikation m in der oberen Horizontale das Diagramm

$$\begin{array}{ccc} R \times R & \xrightarrow{m} & R \\ q \times q \downarrow & & \downarrow q \\ R/I \times R/I & \xrightarrow{\bar{m}} & R/I \end{array}$$

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 [LA2] 4.2.27 geprüft. Es ist dann leicht zu sehen, daß \bar{m} als Multiplikation die Nebenklassengruppe R/I zu einem Ring macht. \square

2.1.16. Ganz allgemein ist ein Schnitt von Idealen eines Rings R stets wieder ein Ideal. Gegeben eine Teilmenge $T \subset R$ bezeichnen 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

$$\langle T \rangle = \{a_1 t_1 b_1 + \dots + a_n t_n b_n \mid n \geq 0, a_i, b_i \in R, t_i \in T\}$$

Hierbei ist der leere Ausdruck mit $n = 0$ wie üblich als die Null von R zu verstehen. Ist $T = \{t_1, \dots, t_r\}$ eine endliche Menge, so schreiben wir auch $\langle T \rangle = \langle t_1, \dots, t_r \rangle$. 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 $\langle T \rangle = \langle \! \! \langle T \rangle \! \! \rangle$. Ideale, die von einem einzigen Element erzeugt werden können, heißen **Hauptideale**. Insbesondere ist nach [LA1] 3.3.4 jedes Ideal in \mathbb{Z} ein Hauptideal.

Ergänzung 2.1.17. 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 im Fall eines kommutativen Rings $\langle T \rangle_R$. Im Fall eines nichtkommutativen Rings dahingegen meint $\langle T \rangle_R$ das von T erzeugte Rechtsideal, wie es in [KAG] 1.5.4 eingeführt wird.

Ergänzung 2.1.18 (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 Nicht-Existenz eindeutiger Primfaktorzerlegungen in sogenannten „Ganzheitsringen von Zahlkörpern“ zu umgehen. Das einfachste Beispiel $\mathfrak{o} = \mathbb{Z}[\sqrt{-5}]$ für dieses Phänomen besprechen wir in 2.4.8. 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 verstehen, so gilt in dieser Menge aller Ideale nämlich das Analogon der eindeutigen Primfaktorzerlegung, vergleiche etwa [KAG] 5.9.8. 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 gilt. Kummer konnte das in einigen Fällen bereits selbst zeigen und bezeichnete deshalb die Elemente dieses größeren Monoids, das er selbst auf noch verschlungeneren Wegen konstruierte, als „ideale Zahlen“.

2.1.19. Gegeben ein Krings R und Elemente $a, b \in R$ ist a ein Teiler von b genau dann, wenn gilt $\langle a \rangle \ni b$ oder gleichbedeutend $\langle a \rangle \supset \langle b \rangle$. Gegeben ein Krings 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 gibt mit $au = b$.

Beispiel 2.1.20 (Quotienten von Polynomringen). Gegeben ein Körper k und ein Polynom $P \in k[X]$ vom Grad $\text{grad } P = d \geq 1$ bilden die Nebenklassen der Monome $1, X, X^2, \dots, X^{d-1}$ eine k -Basis des Restklassenrings $k[X]/\langle P \rangle$. Genauer liefert Polynomdivision mit Rest [LA1] 4.3.15 für jeden Krings k und jedes normierte Polynom $P \in k[X]$, daß die Polynome von einem Grad $\leq (\text{grad } P) - 1$ 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

$$k[X]^{\leq (\text{grad } P)-1} \xrightarrow{\sim} k[X]/\langle P \rangle$$

Beispiel 2.1.21. Wir erinnern die komplexen Zahlen \mathbb{C} mit ihrem ausgezeichneten Element $i \in \mathbb{C}$. Das Einsetzen von i für X im Sinne von [LA1] 4.3.5 liefert mithilfe der universellen Eigenschaft des Quotienten 2.1.13 Isomorphismen von Ringen $\mathbb{R}[X]/\langle X^2 + 1 \rangle \xrightarrow{\sim} \mathbb{C}$ und $\mathbb{Z}[X]/\langle X^2 + 1 \rangle \xrightarrow{\sim} \mathbb{Z}[i]$. Hier ist $\mathbb{Z}[i]$ im Sinne von 2.2.1 zu verstehen als der Ring aller komplexen Zahlen mit ganzzahligem Real- und Imaginärteil.

2.1.22. Gegeben ein Krings k und ein Element $\lambda \in k$ kommutiert das Diagramm

$$\begin{array}{ccc} & k[X] & \\ \delta_\lambda \swarrow & & \searrow q \\ k & \xrightarrow{\sim} & k[X]/\langle X - \lambda \rangle \end{array}$$

mit der Auswertungsabbildung δ_λ und der von der Einbettung $k \hookrightarrow k[X]$ induzierten unteren Horizontalen.

Vorschau 2.1.23. Ich führe an dieser Stelle den Begriff des maximalen Ideals noch nicht ein, da er mir für die Ziele dieser Vorlesung ein Umweg scheint. Ich zeige in 2.5.5 nur, daß der Restklassenring eines Hauptidealrings nach dem von einem irreduziblen Element erzeugten Hauptideal ein Körper ist. Die Erkenntnis, daß das allgemeiner für beliebige Restklassenringe von kommutativen Ringen zu maximalen Idealen gilt, erkläre und verwende ich erst in [KAG] 1.10.6 folgende.

2.1.24 (**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 $R[X] \rightarrow (R/I)[X]$ aus [LA1] 4.3.11 offensichtlich einen Isomorphismus

$$R[X]/I[X] \xrightarrow{\sim} (R/I)[X]$$

Übungen

Ergänzende Übung 2.1.25. 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.

2.2 Teilringe

Definition 2.2.1. 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 2.2.2. Die in [LA1] 4.1.5 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 2.2.1. 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 eines 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 $\mathbb{Z} \times \mathbb{Z}$.

2.2.3. 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 $a_1, \dots, a_n \in S$ bezeichnet man mit

$$R[a_1, \dots, a_n] \subset S$$

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.

2.2.4. Die Notation aus 2.2.1 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 $R[a_1, \dots, a_n]$ auch beschreiben als das Bild des Einsetzungshomomorphismus $R[X_1, \dots, X_n] \rightarrow S$ 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 $R'[X_1, \dots, X_n]$. Diese Notation gibt es jedoch vorerst nur in diesem Skriptum.

2.2.5. Gegeben ein Ringhomomorphismus $\varphi : R \rightarrow S$ ist nach 2.1.12 der Kern $\ker \varphi$ ein Ideal von R und das Bild $\text{im } \varphi$ offensichtlich ein Teilring von S . Nach 2.1.13 und dem Isomorphiesatz [LA2] 4.2.12 faktorisiert φ dann über einen Ringisomorphismus

$$R \twoheadrightarrow R/(\ker \varphi) \xrightarrow{\sim} \text{im } \varphi \hookrightarrow S$$

Übungen

Ergänzende Übung 2.2.6. Seien $K \subset L$ Körper, $I \subset K[X_1, \dots, X_n]$ ein Ideal. Bezeichne $\langle IL[X_1, \dots, X_n] \rangle$ das von I im Polynomring über L erzeugte Ideal. So gilt

$$I = K[X_1, \dots, X_n] \cap \langle IL[X_1, \dots, X_n] \rangle$$

Hinweis: Jedes Element von $\langle IL[X_1, \dots, X_n] \rangle$ hat die Gestalt $c_1 f_1 + \dots + c_r f_r$ mit $f_\nu \in I$ und $c_\nu \in L$ linear unabhängig über K .

Übung 2.2.7. Man zeige, daß der Teilring $\mathbb{Q}[\sqrt{2}] \subset \mathbb{R}$ ein Körper ist.

Übung 2.2.8. Man zeige, daß \mathbb{Z} der einzige Teilring von \mathbb{Q} ist, der endlich erzeugt ist als abelsche Gruppe.

2.3 Abstrakter chinesischer Restsatz

2.3.1. Gegeben Ringe R_1, \dots, R_s bilden wir den **Produkt**ring $R_1 \times \dots \times R_s$ mit komponentenweiser Addition und Multiplikation. Gegeben ein weiterer Ring R und Ringhomomorphismen $f_i : R \rightarrow R_i$ erhalten wir natürlich einen Ringhomomorphismus

$$\begin{aligned} (f_1, \dots, f_s) : R &\rightarrow R_1 \times \dots \times R_s \\ r &\mapsto (f_1(r), \dots, f_s(r)) \end{aligned}$$

Genauer sind die Projektionen Ringhomomorphismen $\text{pr}_i : R_1 \times \dots \times R_s \rightarrow R_i$ und das Nachschalten der Projektionen liefert für jeden weiteren Ring R eine Bijektion

$$\text{Ring}(R, R_1 \times \dots \times R_s) \xrightarrow{\sim} \text{Ring}(R, R_1) \times \dots \times \text{Ring}(R, R_s)$$

In der Terminologie [LA2] 8.6.8 liefert unsere Konstruktion also ein Produkt in der Kategorie der Ringe.

Definition 2.3.2. 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 bzw. 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.

2.3.3. Für das Produkt zweier Ideale ist die Notation \mathfrak{ab} 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 2.3.4 (Abstrakter chinesischer Restsatz). *Seien $\mathfrak{a}_1, \dots, \mathfrak{a}_s$ Ideale eines Rings R . Gilt $\mathfrak{a}_i + \mathfrak{a}_j = R$ für $i \neq j$, so ist die offensichtliche Abbildung eine Surjektion*

$$\kappa : R \twoheadrightarrow R/\mathfrak{a}_1 \times \dots \times R/\mathfrak{a}_s$$

mit dem Schnitt der \mathfrak{a}_i als Kern. Für einen Kring R fällt dieser Schnitt auch zusammen mit dem Produktideal $\langle \mathfrak{a}_1 \dots \mathfrak{a}_s \rangle$ und wir erhalten einen Ringisomorphismus

$$R/\langle \mathfrak{a}_1 \dots \mathfrak{a}_s \rangle \xrightarrow{\sim} R/\mathfrak{a}_1 \times \dots \times R/\mathfrak{a}_s$$

Beispiel 2.3.5. Der Name dieses Satzes rührt von seiner Bedeutung im Ring der ganzen Zahlen her, die wir bereits in [LA2] 4.3.11 folgende besprochen hatten.

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 $(\bar{r}, 0, \dots, 0)$ im Bild liegt. Es reicht sogar, wenn wir das für $r = 1$ zeigen, denn aus $\kappa(x) = (\bar{1}, 0, \dots, 0)$ folgt $\kappa(rx) = \kappa(r)\kappa(x) = (\bar{r}, 0, \dots, 0)$. 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

$$\kappa(a_i) = (1, *, \dots, *, 0, *, \dots, *)$$

mit einer Null an der i -ten Stelle. Für das Bild des Produkts der a_i folgt dann $\kappa(a_2 a_3 \dots a_s) = (1, 0, \dots, 0)$ 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 $\mathfrak{a} \cap \mathfrak{b} = \langle \mathfrak{ab} \rangle$, 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 $\mathfrak{a}_1 + \langle \mathfrak{a}_2 \dots \mathfrak{a}_s \rangle = R$. Mit vollständiger Induktion erhalten wir dann $\mathfrak{a}_1 \cap (\mathfrak{a}_2 \cap \dots \cap \mathfrak{a}_s) = \mathfrak{a}_1 \cap \langle \mathfrak{a}_2 \dots \mathfrak{a}_s \rangle = \langle \mathfrak{a}_1 \langle \mathfrak{a}_2 \dots \mathfrak{a}_s \rangle \rangle = \langle \mathfrak{a}_1 \mathfrak{a}_2 \dots \mathfrak{a}_s \rangle$. \square

2.3.6. 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 2.3.7 (Polynominterpolation). Seien k ein Körper und $n \in \mathbb{N}$. Wir finden stets ein Polynom $P \in k[X_1, \dots, X_n]$, 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 $P \in k[X_1, \dots, X_n]$ bis zum Grad $m - 1$ vorzugeben“ meinen wir, seine Nebenklasse in $k[X_1, \dots, X_n]/\langle I(p)^m \rangle$ 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. \square

2.4 Euklidische Ringe und Primfaktorzerlegung

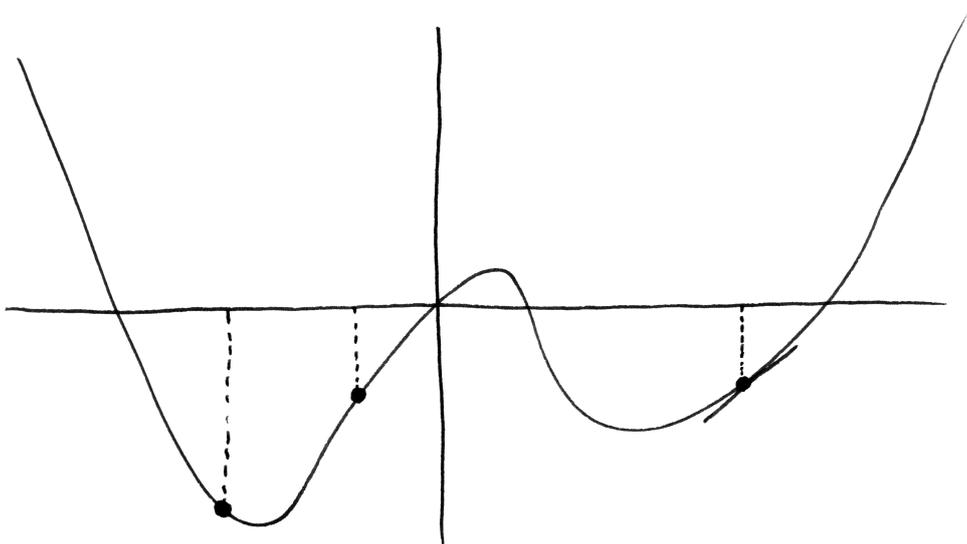
2.4.1. Die folgende schematische Übersicht soll die Struktur dieses Abschnitts und die Beziehungen der darin neu eingeführten Begriffe untereinander verdeutlichen:

Interessante Ringe, etwa \mathbb{Z} , $\mathbb{Z}[i]$, 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, d.h. Ringe mit „eindeutiger Primfaktorzerlegung“.

Wir arbeiten nun unser Schema von unten nach oben ab und beginnen mit faktoriellen Ringen.

Definition 2.4.2. Ein Element a eines Krings R heißt **irreduzibel** oder genauer **irreduzibel in R** , wenn beide folgenden Aussagen gelten:

1. a ist keine Einheit, in Formeln $a \notin R^\times$;
2. In jeder Darstellung von a als Produkt von zwei Kringlelementen ist einer der beiden Faktoren eine Einheit, in Formeln $a = bc \Rightarrow b \in R^\times$ oder $c \in R^\times$.



Eine Interpolation in einer Variablen mit vorgegebenen Werten an zwei Punkten und vorgegebenem Wert und Wert der Ableitung an einem weiteren Punkt.

Beispiele 2.4.3. Die Null ist nie irreduzibel: Im Nullring ist sie eine Einheit, in anderen Ringen 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} .

2.4.4. Ich erinnere daran, daß man unter einem **Integritätsbereich** einen von Null verschiedenen Ring versteht, bei dem das Produkt je zweier von Null verschiedener Elemente stets auch wieder von Null verschieden ist.

Definition 2.4.5. Ein Ring R heißt **faktoriell**, wenn R ein kommutativer Integritätsbereich ist und wenn zusätzlich gilt:

1. Jedes $a \in R \setminus 0$ läßt sich darstellen als ein Produkt von irreduziblen Elementen und einer Einheit, in Formeln $a = up_1 \dots p_n$ mit $u \in R^\times$, p_i irreduzibel und $n \geq 0$.
2. Diese Darstellung ist eindeutig bis auf Einheiten und die Reihenfolge der Faktoren. Ist genauer $a = u'p'_1 \dots p'_n$ eine zweite Darstellung wie eben, so gilt $n = n'$ und es gibt eine Permutation $\tau \in \mathcal{S}_n$ von n sowie Einheiten $u_i \in R^\times$ mit $p'_i = u_i p_{\tau(i)}$ für $1 \leq i \leq n$.

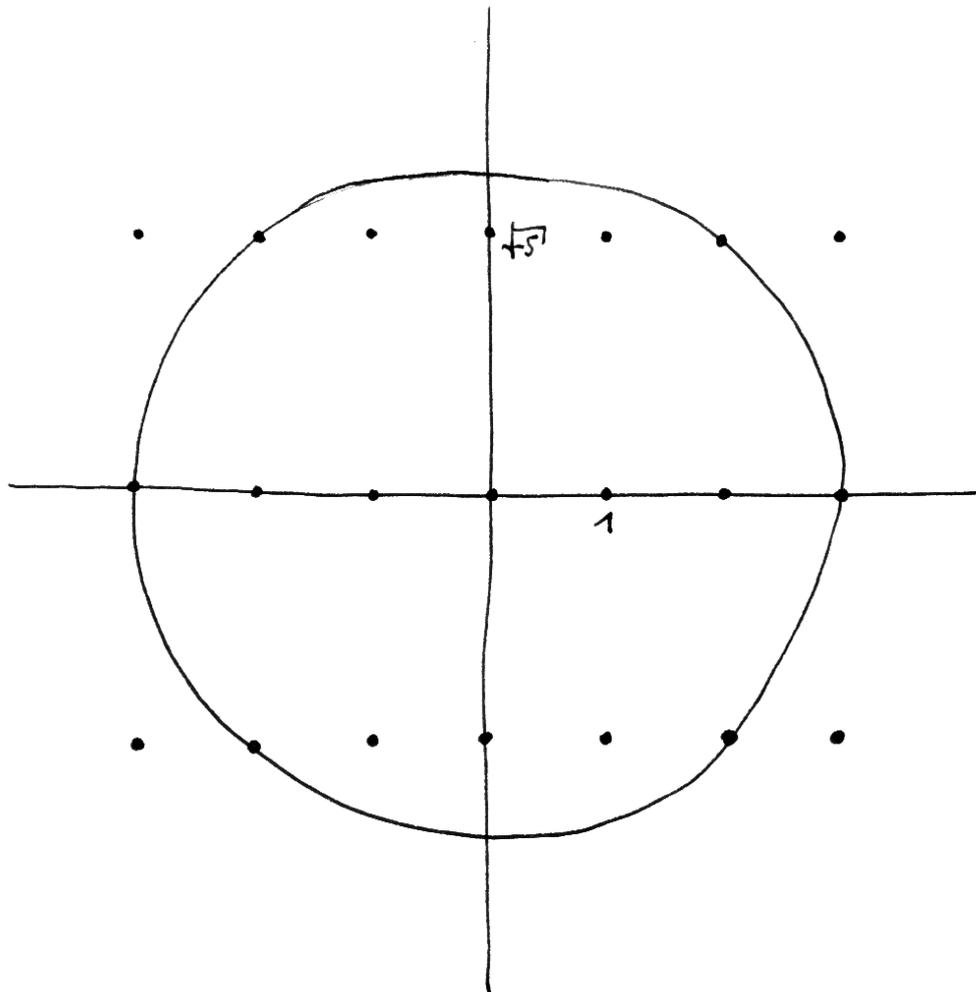
2.4.6. Unsere einzigen Beispiele für faktorielle Ringe sind bisher \mathbb{Z} und alle Körper. Im folgenden werden wir viele weitere Beispiele für faktorielle Ringe kennenlernen. Insbesondere zeigen wir, daß Polynomringe über Körpern stets faktoriell sind.

Ergänzung 2.4.7. Gegeben ein Integritätsbereich bilden die von Null verschiedenen Elemente ein Monoid, und die Definition eines faktoriellen Rings 2.4.5 ist äquivalent zu einer Forderung an die Struktur dieses Monoids: Ein Ring ist faktoriell genau dann, wenn er ein Integritätsbereich ist und das multiplikative Monoid seiner von Null verschiedenen Elemente isomorph ist zum Produkt einer kommutativen Gruppe mit dem Monoid aller fast überall verschwindenden Abbildungen von einer Menge in das additive Monoid \mathbb{N} .

Beispiele 2.4.8 (Ein Integritätsbereich, der nicht faktoriell ist). Als Beispiel für einen nicht faktoriellen Integritätsbereich betrachten wir den Teilring $\mathbb{Z}[\sqrt{-5}]$ der komplexen Zahlen, der gegeben wird durch

$$\mathbb{Z}[\sqrt{-5}] := \{a + bi\sqrt{5} \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$$

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 $|zw| = |z||w|$



Einige Elemente des Rings $\mathbb{Z}[\sqrt{-5}]$ als Punkte in der Gauß'schen Zahlenebene

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.

$ z ^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	$\pm 3, (\pm 2) + (\pm \sqrt{-5})$

Definition 2.4.9. Ein Ring R heißt ein **Hauptidealring**, wenn R ein kommutativer Integritätsbereich ist und jedes Ideal von R ein Hauptideal ist, also von einem einzigen Element erzeugt wird.

Beispiel 2.4.10. Nach [LA1] 3.3.4 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.

2.4.11. Ein Element a eines Hauptidealrings ist irreduzibel genau dann, wenn das von ihm erzeugte Hauptideal nicht Null und nicht der ganze Krings ist, jedes echt größere Hauptideal aber der ganze Krings ist, in Formeln ausgedrückt: Wenn gilt $0 \neq \langle a \rangle \neq R$ und $(\langle a \rangle \subseteq \langle b \rangle \Rightarrow \langle b \rangle = R)$.

Satz 2.4.12. *Jeder Hauptidealring ist faktoriell.*

Ergänzung 2.4.13. 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 die wir in 2.4.22 einen Beweis ohne Auswahlaxiom geben.

Beweis. Wir zeigen als erstes, daß sich in einem Hauptidealring jedes Element $a \in R \setminus 0$ zerlegen läßt als Produkt einer Einheit mit endlich vielen irreduziblen Elementen. Wir bemerken dazu, daß in einem Integritätsbereich R die Gleichheit $\langle a \rangle = \langle b \rangle$ von Hauptidealen äquivalent ist zu $a = ub$ mit einer Einheit $u \in R^\times$. Jetzt argumentieren wir durch Widerspruch. Gäbe es $a \in R \setminus 0$, das sich nicht in ein Produkt einer Einheit mit höchstens endlich vielen Irreduziblen zerlegen läßt,

so wäre insbesondere a selbst weder eine Einheit noch 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 eine Zerlegung in ein Produkt von Irreduziblen besitzen. Wir dürfen ohne Beschränkung der Allgemeinheit annehmen, a_1 habe keine Zerlegung in Irreduzible, und können schreiben $a_1 = a_2 b_2$ mit $a_2, b_2 \notin R^\times$ und a_2 ohne Zerlegung in Irreduzible. Indem wir so weitermachen, finden wir 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 $\langle h \rangle$. Andererseits ist diese Vereinigung aber auch das Erzeugnis $\langle h \rangle = \langle a, a_1, a_2, \dots \rangle$ der a_i . Es folgt eine Relation der Gestalt $h = r a + r_1 a_1 + \dots + r_n a_n$ 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 die Existenz der Zerlegung. Jetzt zeigen wir die Eindeutigkeit. Dazu vereinbaren wir folgende Definition.

Definition 2.4.14. Sei R ein kommutativer Ring. Ein Element $p \in R$ heißt ein **Primelement** oder kurz **prim**, falls es (1) weder Null noch eine Einheit ist und falls (2) aus $p|ab$ folgt $p|a$ oder $p|b$.

2.4.15 (**Diskussion der Terminologie**). Mir scheint diese Terminologie 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: Von ihrer ursprünglichen Definition her versteht man unter Primzahlen ja viel eher die positiven irreduziblen Elemente dieses Rings. Andererseits wäre es auch natürlich, in einem beliebigen kommutativen Ring diejenigen Elemente als Primelemente zu bezeichnen, die im Sinne von [KAG] 2.7.4 „ein Primideal erzeugen“, aber dann müßten wir in der obigen Definition auch die Null als Primelement zulassen. So gesehen sitzt man mit der obigen allgemein gebräuchlichen Definition eines Primelements leider zwischen allen Stühlen.

2.4.16. Primelemente in Integritätsbereichen sind offensichtlich stets irreduzibel, aber irreduzible Elemente müssen auch in Integritätsbereichen im allgemeinen nicht prim sein. In einem faktoriellen Ring sind die Primelemente genau die irreduziblen Elemente. Um allerdings zu beweisen, daß ein Hauptidealring faktoriell ist, brauchen wir ein weiteres Lemma.

Lemma 2.4.17. *In einem Hauptidealring sind die Primelemente genau die irreduziblen Elemente.*

Beweis. Wir müssen nur zeigen, daß jedes irreduzible Element ein Primelement ist. Sei also R unser Hauptidealring und sei $p \in R$ irreduzibel. Seien $a, b \in R$

gegeben mit $p|ab$. Wir nehmen an $p \nmid a$ und folgern $p|b$. Denn sei $\langle a, p \rangle$ das von a und p erzeugte Ideal. Es ist nach Annahme ein Hauptideal, sagen wir $\langle a, p \rangle = \langle d \rangle$. Da p irreduzibel ist, liegt nach 2.4.11 über dem von p erzeugten Hauptideal als einziges weiteres Hauptideal der ganze Ring, in Formeln gilt also $\langle d \rangle = \langle p \rangle$ oder $\langle d \rangle = \langle 1 \rangle$. Da p nicht a teilt, folgt $\langle d \rangle \neq \langle p \rangle$, also $\langle d \rangle = \langle 1 \rangle$. Mithin können wir schreiben $1 = ax + py$ für geeignete $x, y \in R$. Es folgt $b = abx + pby$ und aus $p|ab$ erhalten wir wie gewünscht $p|b$. \square

Damit sind also alle irreduziblen Elemente in unserem Hauptidealring R Primelemente. Ist nun p'_1 ein Faktor unserer alternativen Zerlegung von a , so gibt es ein i mit $p'_1|p_i$ und damit $p'_1 = u_1 p_i$ für eine Einheit u_1 . Wir setzen $i = \tau(1)$, kürzen in beiden Produkten, und beenden den Beweis mit Induktion. \square

Definition 2.4.18. Ein **euklidischer Ring** ist ein kommutativer Integritätsbereich mit einer Abbildung $\sigma : R \setminus 0 \rightarrow \mathbb{N}$ 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 $\sigma(r) < \sigma(a)$.

2.4.19. Grob gesagt 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 2.4.20. 1. $R = \mathbb{Z}$ mit $\sigma(n) = |n|$;

2. $R = k[X]$ für einen Körper k und $\sigma(P) = \text{grad } P$, siehe [LA1] 4.3.15;

3. $R = \mathbb{Z}[i] = \{x + yi \mid x, y \in \mathbb{Z}\}$, $\sigma(x + yi) = x^2 + y^2$. Dieser Ring der sogenannten **Gauß'schen Zahlen** ist als Teilring von \mathbb{C} zu verstehen. Wir werden dies Beispiel in 2.6 noch ausführlich besprechen.

Satz 2.4.21. *Jeder euklidische Ring ist ein Hauptidealring und damit insbesondere faktoriell.*

Beweis. Sei $I \subset R$ ein Ideal. Ist $I = 0$, so ist $I = \langle 0 \rangle$ ein Hauptideal. Sonst finden wir $a \in I \setminus 0$ mit $\sigma(a)$ kleinstmöglich. Wir behaupten $I = \langle a \rangle$. Gäbe es nämlich $b \in I \setminus \langle a \rangle$, 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 2.4.22 (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 diesen beiden Hauptidealen müßte also echt kleiner sein als das Minimum von σ auf $\langle a \rangle$. Es gäbe mithin Einheiten $u, v \in R^\times$ mit $\sigma(ub) < \sigma(a)$ und $\sigma(vc) < \sigma(a)$. Dann aber müßten ub und vc und damit auch b und c Faktorisierungen in Irreduzible besitzen und damit auch a selbst. Dieser Widerspruch zeigt die Behauptung.

2.4.23. Der vorhergehende Satz 2.4.21 und sein Beweis verallgemeinern Satz [LA1] 3.3.4 über die Untergruppen von \mathbb{Z} und den dort gegebenen Beweis.

Korollar 2.4.24. *Der Polynomring in einer Veränderlichen mit Koeffizienten einem Körper ist stets ein Hauptidealring und ist insbesondere stets faktoriell.*

Beweis. Wie in 2.4.20 ausgeführt wird, ist unser Polynomring ein euklidischer Ring. Das Korollar folgt damit aus 2.4.21. \square

2.4.25. 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 manchmal präziser 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 2.4.26. Die irreduziblen Polynome in $\mathbb{C}[X]$ sind nach [LA1] 4.3.26 genau die Polynome vom Grad Eins. Die irreduziblen Polynome in $\mathbb{R}[X]$ sind nach [LA1] 4.3.28 genau die Polynome vom Grad Eins sowie die Polynome vom Grad Zwei ohne reelle Nullstelle. Die irreduziblen Polynome in $\mathbb{Q}[X]$ zu bestimmen, ist dagegen schwieriger.

2.5 Quotienten von Hauptidealringen

Definition 2.5.1. 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 partiell geordneten 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 2.5.2. Die maximalen Ideale in \mathbb{Z} sind genau die Ideale $p\mathbb{Z} \subset \mathbb{Z}$ für p eine Primzahl. Ist k ein Körper, so ist $\langle X - a \rangle \subset k[X]$ ein maximales Ideal, für alle $a \in k$, und es ist leicht zu sehen, daß wir so im Fall eines algebraisch abgeschlossenen Körpers bereits alle maximalen Ideale von $k[X]$ erhalten.

Vorschau 2.5.3. Der Nullring besitzt überhaupt kein maximales Ideal. In [KAG] 1.10.3 zeigen wir, daß er der einzige Ring ohne maximales Ideal ist.

Proposition 2.5.4 (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. \square

Satz 2.5.5 (Quotienten von Hauptidealringen). *Für ein von Null verschiedenes Element $a \neq 0$ eines Hauptidealrings sind gleichbedeutend:*

1. *Der Quotient nach dem Hauptideal $\langle a \rangle$ ist ein Körper;*
2. *Unser Element a ist irreduzibel;*
3. *Das Hauptideal $\langle a \rangle$ ist maximal.*

Beweis. $1 \Leftrightarrow 3$ haben wir schon in 2.5.4 in größerer Allgemeinheit gezeigt. Wir zeigen nun noch (Nicht 2) \Leftrightarrow (Nicht 3). Sei R unser Hauptidealring. Ist a nicht irreduzibel, so ist entweder $a \in R^\times$ oder es gibt eine Zerlegung $a = bc$ mit $b, c \notin R^\times$. Im ersten Fall ist $\langle a \rangle = R$ nicht maximal. Im zweiten Fall gilt $\langle a \rangle \subsetneq \langle b \rangle \subsetneq R$ und $\langle a \rangle = R$ ist wieder nicht maximal. Damit haben wir \Rightarrow gezeigt. Ist umgekehrt das Hauptideal $\langle a \rangle$ nicht maximal, so gibt es ein Ideal I mit $\langle a \rangle \subsetneq I \subsetneq R$ und nach Annahme ein Element $b \in R$ mit $\langle b \rangle = I$, also mit

$$\langle a \rangle \subsetneq \langle b \rangle \subsetneq R$$

Wegen $\langle b \rangle \neq R$ ist b keine Einheit und wegen $a \in \langle b \rangle$ gibt es c mit $a = bc$ und wegen $\langle a \rangle \neq \langle b \rangle$ ist c auch keine Einheit. Also ist a nicht irreduzibel. \square

Beispiel 2.5.6. Gegeben $p \in \mathbb{Z}$ ist $\mathbb{Z}/p\mathbb{Z}$ ist genau dann ein Körper, wenn p oder $-p$ eine Primzahl ist.

Beispiel 2.5.7. $\mathbb{R}[X]/\langle X^2 + 1 \rangle$ ist ein Körper, genauer induziert das Einsetzen von i für X einen Isomorphismus dieses Körpers mit \mathbb{C} .

Beispiel 2.5.8. $\mathbb{R}[X]/\langle X^2 + 2 \rangle$ ist ein Körper, genauer induziert das Einsetzen von $i\sqrt{2}$ für X einen Isomorphismus dieses Körpers mit \mathbb{C} .

Beispiel 2.5.9. $\mathbb{R}[X]/\langle X + 1 \rangle$ ist ein Körper, genauer induziert das Einsetzen von -1 für X einen Isomorphismus dieses Körpers mit \mathbb{R} .

Beispiel 2.5.10. $\mathbb{R}[X]/\langle X^2 - 1 \rangle$ 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 $\mathbb{R} \times \mathbb{R}$ besitzt Nullteiler: Es gilt darin ja etwa $(1, 0) \cdot (0, 1) = (0, 0)$.

Übungen

Übung 2.5.11. 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 2.5.12. Man zeige, daß $\mathbb{Z}[X]$ kein Hauptidealring ist.

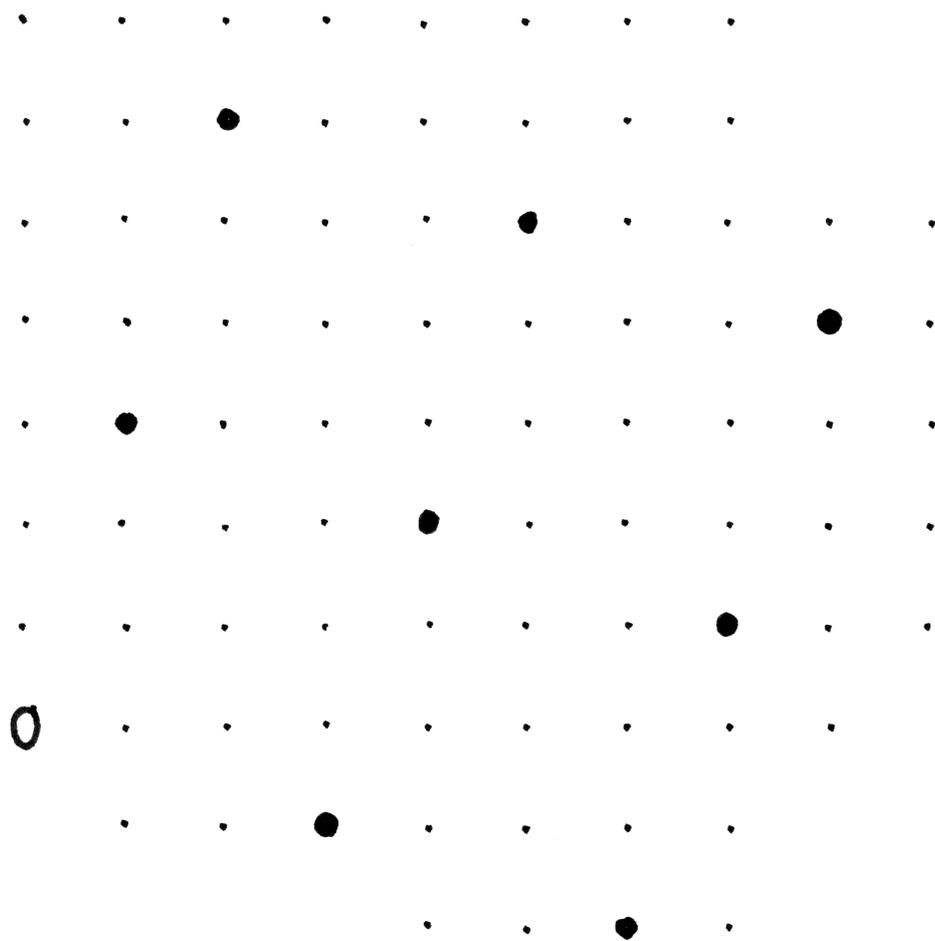
Übung 2.5.13. Sei k ein Körper. Man zeige: (1) Alle Polynome vom Grad 1 sind irreduzibel in $k[X]$. (2) Ist $P \in k[X]$ irreduzibel und $\text{grad } P > 1$, so hat P keine Nullstelle in k . (3) Ist $P \in k[X] \setminus k$ vom Grad $\text{grad } P \leq 3$ und hat P keine Nullstelle in k , so ist P 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 2.5.14. 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 2.5.15. Man zeige: Gegeben ein Körper k ist der Ring $k[[X]]$ der formalen Potenzreihen mit Koeffizienten aus k aus [LA1] 4.3.40 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 2.5.16. Sei k ein Körper und seien $f, g \in k[T] \setminus 0$ teilerfremde Polynome. Man zeige, daß es dann für jedes Polynom h Polynome a, b gibt mit $h = af + bg$. Man zeige, daß man hier (a, b) sogar so wählen kann, daß gilt $\text{grad } a < \text{grad } g$, und daß im Fall $\text{grad}(h) \leq \text{grad}(f) + \text{grad}(g) - 1$ 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 2.5.17. Sei R ein faktorieller Ring und $q \in \text{Quot}(R)$ ein Element seines Quotientenkörpers und $n \geq 1$ mit $q^n \in R$. Man zeige $q \in R$.



Die Elemente des von $1 + 3i$ 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.

2.6 Irreduzible im Ring der Gauß'schen Zahlen

Lemma 2.6.1. *Der Ring $\mathbb{Z}[i]$ der Gauß'schen Zahlen ist euklidisch und mithin faktoriell.*

Beweis. Die Elemente des von einem festen von Null verschiedenen Element $0 \neq a = x + iy \in \mathbb{Z}[i]$ im Ring $\mathbb{Z}[i]$ 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 $b \in \mathbb{Z}[i]$ 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 $\sigma(a) = |a|^2$. \square

2.6.2. 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 $0, 1, 4, 9, 16, 25, \dots$

2.6.3. Gegeben ein faktorieller Ring R bezeichne $\text{irk}(R)$ die Menge **Irreduziblenklassen**, als da heißt der Bahnen irreduzibler Elemente von R unter der Einheiten-
gruppe R^\times . Gegeben ein irreduzibles $r \in R$ bezeichne $[r] \in \text{irk}(R)$ seine Klasse.

Proposition 2.6.4 (Irreduziblenklassen in Invariantenringen). *Seien R ein faktorieller Ring und Γ eine endliche Gruppe von Automorphismen von R derart, daß auch der Ring R^Γ der Γ -Invarianten faktoriell ist. So erhalten wir eine Bijektion*

$$\text{irk}(R^\Gamma) \xrightarrow{\sim} \text{irk}(R)/\Gamma$$

durch die Abbildung, die jedem R^Γ -irreduziblen Element p die Menge seiner R -irreduziblen Faktoren π zuordnet, und die Vielfachheit von π in p teilt $|\Gamma_{[\pi]}|$.

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. 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 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 Isotropiegruppe der Irreduziblenklasse $[\pi]$, so haben wir genauer

$$p = \eta \prod_{\bar{\gamma} \in \Gamma/\Gamma_{[\pi]}} \gamma(\pi)^r$$

mit einer Einheit $\eta \in R^\times$, die von der Wahl der Repräsentanten γ unserer Nebenklassen $\bar{\gamma}$ abhängt, und für $d = |\Gamma_{[\pi]}|$ folglich $p^d \in b(\pi)^r R^\times$ alias $d = rn$. \square

Beispiel 2.6.5 (Irreduzible im Ring der Gauß'schen Zahlen). Betrachten wir nun $R := \mathbb{Z}[i]$ und Γ die zweielementige Gruppe bestehend aus der Identität und der komplexen Konjugation, so erhalten wir als Invariantenring $R^\Gamma = \mathbb{Z}$ und finden eine Bijektion

$$\text{irk}(\mathbb{Z}) \xrightarrow{\sim} \text{irk}(\mathbb{Z}[i])/\Gamma$$

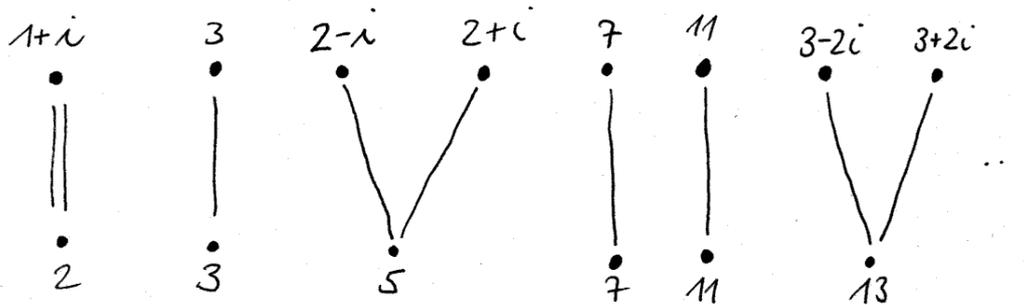
Sie ordnet jeder Primzahl $p \in \mathbb{Z}$ die Menge aller Irreduziblenklassen $[\pi]$ zu mit $\pi|p$. Der Ring der Gauß'schen Zahlen besitzt genau vier Einheiten, als da sind $1, -1, i,$ und $-i$. Damit sind wir für jede Primzahl p in genau einem der folgenden Fälle:

1. $p \mapsto \{[\pi], [\bar{\pi}]\}$ mit $[\pi] \neq [\bar{\pi}]$. Dann gilt nach der letzten Aussage der Proposition notwendig $p = \varepsilon\pi\bar{\pi}$ für eine Einheit ε , die dann offensichtlich sogar Eins sein muß, also $p = \pi\bar{\pi}$;
2. $p \mapsto \{[\pi], [\bar{\pi}]\}$ mit $[\pi] = [\bar{\pi}]$. Dann sind wir nach der letzten Aussage der Proposition in genau einem der folgenden Unterfälle:
 - (a) Die Vielfachheit von π in p ist Eins, also $p = \varepsilon\pi$ für eine Einheit $\varepsilon \in \{\pm 1, \pm i\}$;
 - (b) Die Vielfachheit von π in p ist Zwei, also $p = \varepsilon\pi^2$ für eine Einheit $\varepsilon \in \{\pm 1, \pm i\}$, und dann folgt auch wieder $p = \pi\bar{\pi}$;

Für den Fall 2 bemerken wir, daß diejenigen Gauß'schen Zahlen, die sich von ihrem komplex Konjugierten höchstens um das Produkt mit einer Einheit unterscheiden, reell, rein imaginär, oder von der Gestalt $a \pm ai$ mit $a \in \mathbb{Z}$ sein müssen. An Irreduziblen letzterer Art gibt es offensichtlich nur die vier Elemente $\pm 1 \pm i$, und diese gehören alle zu derselben Irreduziblenklasse $[1 + i]$, die wegen $2 = (1 + i)(1 - i) = -i(1 + i)^2$ die Primzahl 2 teilt. Es ist damit klar, daß nur die Primzahl $p = 2$ zum Fall 2(b) gehört. Zum Fall 2(a) gehören alle Primzahlen $p \in \mathbb{N}$, die im Ring der Gauß'schen Zahlen irreduzibel bleiben. Wir zeigen im Anschluß als Proposition 2.6.6, daß genau die Primzahlen $p \in \mathbb{N}$ mit $p \equiv 3 \pmod{4}$ im Ring der Gauß'schen Zahlen irreduzibel bleiben, wohingegen alle Primzahlen $p \in \mathbb{N}$ mit $p \equiv 1 \pmod{4}$ zum Fall 1 gehören und zerfallen als $p = \pi\bar{\pi}$ mit $[\pi] \neq [\bar{\pi}]$.

Proposition 2.6.6. *Für eine Primzahl $p \in \mathbb{N}$ sind gleichbedeutend:*

1. p bleibt nicht prim im Ring $\mathbb{Z}[i]$ der Gauß'schen Zahlen;
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 $p = 2$;



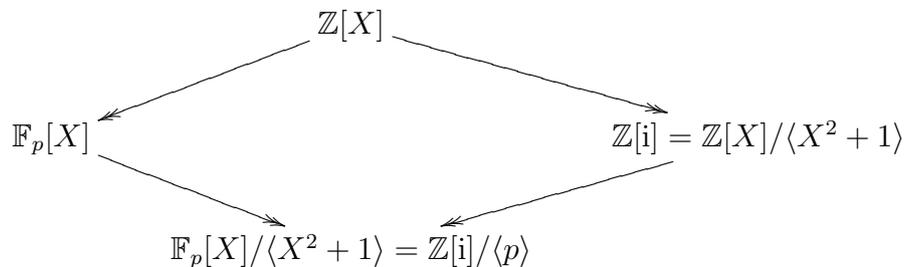
Versuch einer graphischen Darstellung des Zerfallens der gewöhnlichen Primzahlen im Ring der Gauß'schen Zahlen. Die Zwei ist ein Sonderfall, weil bei ihr ein irreduzibles Element des Rings der Gauß'schen Zahlen als zweifacher Faktor auftritt.

4. Das Polynom $(X^2 + 1)$ ist nicht irreduzibel in $\mathbb{F}_p[X]$;

5. (-1) ist ein Quadrat in \mathbb{F}_p .

Beispiele 2.6.7. $2 = 1^2 + 1^2, 5 = 1^2 + 2^2, 13 = 2^2 + 3^2, 17 = 1^2 + 4^2, \dots$

Beweis. Ist $\pi = x + iy$ 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 $1 \Rightarrow 2$. Aus $p = x^2 + y^2$ folgt umgekehrt $p = (x + iy)(x - iy)$, also haben wir auch $2 \Rightarrow 1$. Die Implikation $2 \Rightarrow 3$ 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. $1 \Leftrightarrow 4$ folgert man durch die Betrachtung des Diagramms von Ringen



Alle vier Morphismen sind hierbei Surjektionen mit einem Hauptideal als Kern. Nach 2.5.5 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. $4 \Leftrightarrow 5$ ist evident. Schließlich zeigen wir noch $3 \Rightarrow 5$. Sicher ist nämlich -1 ein Quadrat in \mathbb{F}_2 . Unter der Voraussetzung $p \equiv 1 \pmod{4}$ gilt dasselbe in \mathbb{F}_p . Wir wissen nämlich aus [LA2] 4.4.17, 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 . \square

2.6.8. Man beachte, daß jede Gauß'sche Zahl ungleich Null durch Multiplikation mit einer Einheit auf genau eine Gauß'sche Zahl $x + iy$ 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 $p \in \mathbb{N}$ in ein Produkt irreduzibler Elemente von $\mathbb{Z}[i]$ hat nach unserem Satz folgende Gestalt:

$$\begin{array}{ll}
 p \equiv 3 \pmod{4} & p = p; \\
 p \not\equiv 3 \pmod{4} & p = (x + iy)(x - iy) \text{ für } x^2 + y^2 = p.
 \end{array}$$

Beschränken wir uns auf die irreduziblen Elemente $x + iy$ 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 $2 = -i(1 + i)^2$ hat.

Ergänzung 2.6.9. 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 eben die Zauberformel auswendig hersagen können!

Korollar 2.6.10 (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 $a \in \mathbb{Z}[i]$ gibt mit $n = a\bar{a}$. Ist $n \neq 0$ und $a = \varepsilon\pi_1\pi_2 \dots \pi_r$ eine Darstellung als Produkt einer Einheit ε mit Primelementen, von denen wir π_1, \dots, π_s weder reell noch rein imaginär annehmen und π_{s+1}, \dots, π_r aus \mathbb{N} , so muß

$$n = (\varepsilon\bar{\varepsilon})(\pi_1\bar{\pi}_1) \dots (\pi_s\bar{\pi}_s)\pi_{s+1}\pi_{s+1} \dots \pi_r\pi_r$$

die Primfaktorzerlegung in \mathbb{N} sein. Damit folgt das Korollar aus unserer Beschreibung ?? der Primelemente im Ring der Gauß'schen Zahlen. \square

2.6.11. 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 $n = (x + iy)(x - iy)$ finden, also alle Zerlegungen $n = a\bar{a}$, wobei der Übergang von a zu εa mit einer Einheit $\varepsilon \in \mathbb{Z}[i]^\times$ und der Übergang von a zu \bar{a} bis auf Reihenfolge dieselbe Zerlegung liefert. Dafür ist es besonders übersichtlich, mit dem in 2.6.8 beschriebenen Repräsentantensystem modulo Einheiten aller irreduziblen Elemente zu arbeiten, das stabil wird unter der komplexen Konjugation, sobald wir die Ausnahmestelle $1 + i$ entfernen.

Übungen

Übung 2.6.12. Man bestimme sämtliche Zerlegungen von 1000000 in eine Summe von zwei Quadratzahlen.

2.7 Primfaktorzerlegung in Polynomringen

2.7.1. Gegeben ein faktorieller Ring R und ein irreduzibles Element $p \in R$ erklären wir die zugehörige p -**Bewertung** oder englisch **valuation**

$$v_p : \text{Quot } R \rightarrow \mathbb{Z} \sqcup \{\infty\}$$

als die eindeutig bestimmte Abbildung mit $v_p(p^n a/b) = n$ für $a, b \in R \setminus 0$ teilerfremd zu p und mit $v_p(0) = \infty$. Offensichtlich gilt $v_p(fg) = v_p(f) + v_p(g)$ für alle $f, g \in R$.

Beispiele 2.7.2. $v_2(16/6) = 3$, $v_3(16/6) = -1$, $v_5(16/6) = 0$. Ist k ein Körper und $R = k[t]$, so ist per definitionem $\text{Quot } R = k(t)$ der Funktionenkörper und für $\lambda \in k$ ist $v_{(t-\lambda)}(f)$ die Nullstellenordnung beziehungsweise das Negative der Polstellenordnung der gebrochen rationalen Funktion f an der Stelle λ .

2.7.3 (**Bewertung von Polynomen**). Gegeben ein faktorieller Ring R mit einem irreduziblen Element p und ein Polynom $A = a_n X^n + \dots + a_1 X + a_0 \in (\text{Quot } R)[X]$ erklären wir seine p -**Bewertung** durch

$$v_p(A) := \min(v_p(a_i))$$

Speziell ist das Nullpolynom das einzige Polynom A mit $v_p(A) = \infty$.

Beispiele 2.7.4. Als Beispiel für die Bewertung eines Polynoms mit rationalen Koeffizienten haben wir etwa $v_2(10X^2 + 6X + 8) = 1$.

Proposition 2.7.5 (Lemma von Gauß). Gegeben ein faktorieller Ring R und ein irreduzibles Element $p \in R$ und Polynome $A, B \in (\text{Quot } R)[X]$ 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 $R/\langle p \rangle$ und dann auch $(R/\langle p \rangle)[X]$ Integritätsbereiche sind. \square

Definition 2.7.6. 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 $P \in (\text{Quot } R)[X]$ nennen wir **primitiv** oder genauer **R -primitiv**, wenn es bereits in $R[X]$ liegt und dort primitiv ist.

2.7.7 (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.

2.7.8. Offensichtlich ist ein Polynom $A \in (\text{Quot } R)[X]$ 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 $A \in (\text{Quot } R)[X] \setminus 0$ ein Element $c \in \text{Quot } R$ mit cA primitiv.

2.7.9 (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 [2.7.5](#) und ist auch im wesentlichen die Aussage, auf die wir uns dort beim Beweis zurückgezogen haben.

Beispiele 2.7.10. 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 2.7.11 (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 $(\text{Quot } R)[X]$.*

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 $\text{Quot } R = K$. Gegeben $P \in R[X]$ zerlegen wir $P = Q_1 \dots Q_n$ als Produkt von irreduziblen Polynomen in $K[X]$ und schreiben $Q_i = c_i \tilde{Q}_i$ mit $c_i \in K^\times$ und \tilde{Q}_i primitiv. So erhalten wir eine Zerlegung $P = c \tilde{Q}_1 \dots \tilde{Q}_n$ mit \tilde{Q}_i primitiv und irreduzibel in $K[X]$ sowie $c \in K^\times$. Nach dem Lemma von Gauß [2.7.5](#) folgt $v_p(c) = v_p(P) \geq 0$ für alle Irreduziblen p von R und damit $c \in R$. Wir können also c faktorisieren in $c = up_1 \dots p_r$ mit $u \in R^\times$, $p_i \in R$ irreduzibel, und folgern so die Existenz einer Zerlegung von P

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. Ist $P = u'p'_1 \dots p'_{r'}S_1 \dots S_{n'}$ eine weitere Zerlegung von P in ein Produkt einer Einheit mit irreduziblen Elementen, sagen wir $u' \in R^\times$, $p'_i \in R$ irreduzibel und $S_j \in R[X]$ primitiv und irreduzibel in $K[X]$, so liefert die Eindeutigkeit der Primfaktorzerlegung in $K[X]$ zunächst $n = n'$ und $S_i = q_i \tilde{Q}_{\sigma(i)}$ für geeignetes $\sigma \in \mathcal{S}_n$ und $q_i \in K^\times$. Dann folgt $q_i \in R^\times$, und schließlich aus der Faktorialität von R die Gleichheit $r = r'$ sowie die Existenz einer Permutation $\tau \in \mathcal{S}_r$ und von Einheiten $u_i \in R^\times$ mit $p'_i = u_i p_{\tau(i)}$. \square

Ergänzung 2.7.12. Die Zerlegung eines Polynoms aus $\mathbb{Z}[X]$ in irreduzible Faktoren kann im Prinzip durch Ausprobieren in endlicher Zeit bestimmt werden. Ein Polynom 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 2.7.13. *Sei R ein faktorieller Ring. Ist ein von Null verschiedenes Polynom $P \in R[X] \setminus 0$ nicht irreduzibel als Element des Polynomrings $P \in (\text{Quot } R)[X]$, 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. \square

Beispiel 2.7.14. 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 2.7.15. *Für jeden Körper k ist der Polynomring $k[X_1, \dots, X_n]$ faktoriell. Sogar $\mathbb{Z}[X_1, \dots, X_n]$ ist ein faktorieller Ring.*

Korollar 2.7.16. 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 2.7.17. In 2.10.2 werden wir genauer die „Schranke von Bézout“ für die maximal mögliche Zahl gemeinsamer Nullstellen herleiten.

Beweis. Unsere Polynome haben nach der Beschreibung 2.7.11 der irreduziblen Elemente in Polynomringen über faktoriellen Ringen außer Einheiten erst recht keine gemeinsamen Teiler im Ring $k(X)[Y]$. Da dieser Ring nach 2.4.24 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 dem 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. \square

Übungen

Übung 2.7.18. 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 $P, Q \in R[X]$.

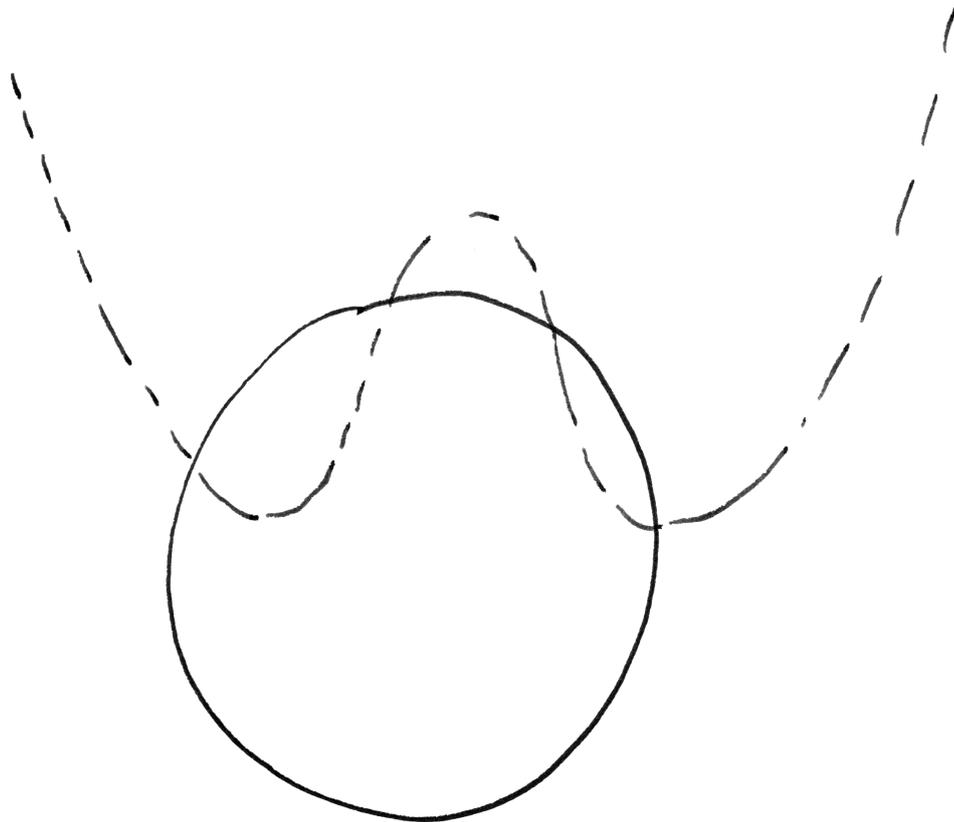
Übung 2.7.19. Sei k ein Körper. Gibt es für ein Polynom P aus dem Polynomring $P \in k[X_1, \dots, X_n]$ ein Element $Q \in k(X_1, \dots, X_n)$ aus dem Quotientenkörper mit $Q^2 = P$, so ist Q bereits selbst ein Polynom, in Formeln $Q \in k[X_1, \dots, X_n]$. Hinweis: 2.5.17.

Übung 2.7.20. Seien k ein Körper und $0 < n(1) < n(2) < \dots < n(r) < n$ natürliche Zahlen, $r \geq 0$. Man zeige, daß das Polynom

$$T^n + a_r T^{n(r)} + \dots + a_1 T^{n(1)} + a_0$$

irreduzibel ist in $K[T]$, für $K = \text{Quot } k[a_0, \dots, a_r]$ der Funktionenkörper. Hinweis: Jede Zerlegung käme nach 2.7.18 und 2.7.11 notwendig von einer Zerlegung im Polynomring $k[a_0, \dots, a_r, T]$ her und müßte unter dem Einsetzen $a_1 = \dots = a_r = 0$ zu einer Zerlegung von $T^n + a_0$ in $k[a_0, T]$ führen.

Übung 2.7.21. 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: 2.7.18.



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 durchgezogenen 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 2.7.22 (**Satz über rationale Nullstellen**). Man zeige: Gegeben ein Polynom

$$a_n T^n + \dots + a_1 T + a_0$$

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 .

2.8 Kreisteilungspolynome

2.8.1. 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

$$\Phi_d(X) = \prod_{\text{ord } \zeta=d} (X - \zeta)$$

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 [LA1] 4.3.15 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 $\text{grad}(\Phi_n) = \varphi(n)$, 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 4.4.2 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 $\exp(2\pi i/n)$ als Nullstelle hat. Natürlich haben wir für $p > 1$ stets die Zerlegung $X^p - 1 = (X - 1)(X^{p-1} + X^{p-2} + \dots + X + 1)$, 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 2.8.2 (Eisensteinkriterium). Sei $P = a_n X^n + \dots + a_1 X + a_0 \in \mathbb{Z}[X]$ ein Polynom mit ganzzahligen Koeffizienten und p eine Primzahl. Gilt $p \nmid a_n$, $p \mid a_{n-1}, \dots, p \mid a_0$ und $p^2 \nmid a_0$, so ist P irreduzibel in $\mathbb{Q}[X]$.

2.8.3. 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 2.7.13 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 $\bar{P} = \bar{a}_n X^n$ 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 $\bar{a}_n X^n$ 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. \square

Korollar 2.8.4. Gegeben eine Primzahl p ist das p -te Kreisteilungspolynom $\Phi_p(X) = X^{p-1} + X^{p-2} + \dots + X + 1$ 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 2.8.2. \square

Ergänzung 2.8.5. 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, daß jede ganze Zahl als Koeffizient mindestens eines Kreisteilungspolynoms vorkommt [Suz87, SDAT00].

Übungen

Übung 2.8.6 (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 Φ_1, \dots, Φ_8 .

Übung 2.8.7. 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 2.8.8. 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 2.8.9. Man zerlege $(X^n - Y^n)$ in $\mathbb{C}[X, Y]$ in ein Produkt irreduzibler Faktoren.

Ergänzende Übung 2.8.10 (Quantisierte Binomialkoeffizienten). Ist \mathbb{F} ein endlicher Körper mit q Elementen, so ist die Zahl der k -dimensionalen Teilräume von \mathbb{F}^n genau

$$\frac{(q^n - 1)(q^n - q) \dots (q^n - q^{k-1})}{(q^k - 1)(q^k - q) \dots (q^k - q^{k-1})}$$

Setzen wir $[n]_q := q^{n-1} + q^{n-2} + \dots + 1 = (q^n - 1)/(q - 1)$, so können wir unser Ergebnis auch darstellen als

$$\frac{[n]_q [n-1]_q \dots [n-k+1]_q}{[k]_q [k-1]_q \dots [1]_q}$$

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.

2.9 Symmetrische Polynome

Definition 2.9.1. Sei k ein Ring. Für jede Permutation $\sigma \in \mathcal{S}_n$ setzen wir die Identität auf k fort zu einem Ringhomomorphismus

$$\begin{array}{ccc} \sigma : k[X_1, \dots, X_n] & \rightarrow & k[X_1, \dots, X_n] \\ & & X_i \mapsto X_{\sigma(i)} \end{array}$$

Ein Polynom $f \in k[X_1, \dots, X_n]$ heißt **symmetrisch**, wenn gilt $f = \sigma f \quad \forall \sigma \in \mathcal{S}_n$. Die Menge aller symmetrischen Polynome ist ein Teilring des Polynomrings $k[X_1, \dots, X_n]$. Wir notieren ihn $k[X_1, \dots, X_n]^{\mathcal{S}_n}$.

2.9.2. 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**.

2.9.3. 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 2.9.4. Das Produkt $X_1 \dots X_n$ und die Summe $X_1 + \dots + X_n$ sind symmetrische Polynome. Allgemeiner definieren wir die **elementarsymmetrischen Polynome** in n Veränderlichen $s_i(X_1, \dots, X_n) \in \mathbb{Z}[X_1, \dots, X_n]^{\mathcal{S}_n}$ durch die Identität

$$(T + X_1)(T + X_2) \dots (T + X_n) = T^n + s_1 T^{n-1} + s_2 T^{n-2} + \dots + s_n$$

im Ring $\mathbb{Z}[X_1, \dots, X_n][T]^{\mathcal{S}_n} = \mathbb{Z}[X_1, \dots, X_n]^{\mathcal{S}_n}[T]$, 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 $I \subset \{1, \dots, n\}$. Speziell ergibt sich $s_1 = X_1 + \dots + X_n$ und $s_2 = X_1 X_2 + X_1 X_3 + \dots + X_1 X_n + X_2 X_3 + \dots + X_2 X_n + \dots + X_{n-1} X_n$ und $s_n = X_1 \dots X_n$.

2.9.5. Gegeben ein kommutativer Ring k sind für beliebige $\zeta_1, \dots, \zeta_n \in k$ 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 2.9.6 (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*

$$k[X_1, \dots, X_n]^{\mathcal{S}_n} = k[s_1, \dots, s_n]$$

mit einem „Freiheitsstrichlein“ an der eröffnenden Klammer im Sinne unserer Notation 2.2.4.

Beispiel 2.9.7. Wir haben $X_1^3 + X_2^3 + X_3^3 = s_1^3 - 3s_1 s_2 + 3s_3$.

Beispiel 2.9.8. Die Darstellung von $(X_1 - X_2)^2$ durch elementarsymmetrische Polynome ist

$$\begin{aligned} (X_1 - X_2)^2 &= (X_1 + X_2)^2 - 4X_1 X_2 \\ &= s_1^2 - 4s_2 \end{aligned}$$

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 $s_1, \dots, s_n \in k[X_1, \dots, X_n]^{S_n}$ sofort $k[X_1, \dots, X_n]^{S_n} \supset k[s_1, \dots, s_n]$. Für das weitere verwenden wir die Multiindexnotation wie in [AN2] 2.2.3 und vereinbaren für einen Multiindex $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$ die Abkürzung

$$X^\alpha := X_1^{\alpha_1} \dots X_n^{\alpha_n}$$

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

$$\begin{aligned} (\alpha_1, \dots, \alpha_n) \geq (\beta_1, \dots, \beta_n) &\Leftrightarrow \alpha_1 > \beta_1 \\ &\text{oder} \\ &\alpha_1 = \beta_1 \text{ und } (\alpha_2, \dots, \alpha_n) \geq (\beta_2, \dots, \beta_n). \end{aligned}$$

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 $(1, \dots, 1, 0, \dots, 0)$ mit i Einsen vorneweg und dann nur noch Nullen. Gälte unsere Inklusion \subset nicht, so könnten wir unter allen symmetrischen Funktionen außerhalb von $k[s_1, \dots, s_n]$ 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

$$\alpha = (\alpha_1, \dots, \alpha_n) \text{ mit } \alpha_1 \geq \dots \geq \alpha_n$$

Dann hat das Produkt

$$g := s_1^{\alpha_1 - \alpha_2} s_2^{\alpha_2 - \alpha_3} \dots s_{n-1}^{\alpha_{n-1} - \alpha_n} s_n^{\alpha_n}$$

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 $k[s_1, \dots, s_n]$. Dann gehört aber auch f

selbst zu $k[s_1, \dots, s_n]$ im Widerspruch zu unseren Annahmen. Um schließlich die lineare Unabhängigkeit der Monome $s_1^{\gamma_1} \dots s_n^{\gamma_n}$ 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. \square

Definition 2.9.9. Gegeben ein Multiindex $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$ verwenden wir wie in [AN2] 2.2.3 die Notation

$$|\alpha| := \alpha_1 + \dots + \alpha_n$$

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 genau einem Grad. Das Produkt zweier homogener Polynome ist wieder homogen, und ist unser Produkt nicht Null, so ist sein Grad die 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.

Beispiel 2.9.10. Das Polynom $X^3Y^3Z + X^2Z^5 - 98X^4YZ^2$ ist homogen vom Grad 7. Ein elementarsymmetrisches Polynom s_d ist stets homogen vom Grad d .

Beispiel 2.9.11 (Diskriminante eines kubischen Polynoms). Wir versuchen, $\Delta = (X - Y)^2(Y - Z)^2(Z - X)^2$ durch elementarsymmetrische Funktionen auszudrücken, wo ich statt X_1, X_2, X_3 übersichtlicher X, Y, Z geschrieben 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

$$0 = a^2b^2 - 4a^3c + 18abc - 4b^3 - 27c^2$$

Man nennt das Negative $\Delta_3 := -\Delta$ dieses Ausdrucks in den Koeffizienten die **Diskriminante**. Das Vorzeichen führen wir hier nur ein, um keine Unstimmigkeiten mit unserer allgemeinen Definition 2.9.14 aufkommen zu lassen. Es sind jedoch auch andere Konventionen in Gebrauch.

2.9.12 (**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.

2.9.13. Ist speziell $T^3 + pT + q = (T - \alpha)(T - \beta)(T - \gamma)$ ein Polynom mit Nullstellen α, β, γ ohne quadratischen Term, so ergibt sich für die Diskriminante die Formel

$$-(\alpha - \beta)^2(\beta - \gamma)^2(\gamma - \alpha)^2 = 4p^3 + 27q^2$$

Satz 2.9.14. *Es gibt genau ein Polynom, genannt die n -te Diskriminante $\Delta_n \in \mathbb{Z}[a_1, \dots, a_n]$, mit der Eigenschaft, daß beim Einsetzen derjenigen Polynome $a_i \in \mathbb{Z}[\zeta_1, \dots, \zeta_n]$, die durch die Identität $T^n + a_1T^{n-1} + \dots + a_n = (T + \zeta_1) \dots (T + \zeta_n)$ gegeben werden, im Polynomring $\mathbb{Z}[\zeta_1, \dots, \zeta_n]$ gilt*

$$\Delta_n(a_1, \dots, a_n) = \prod_{i \neq j} (\zeta_i - \zeta_j)$$

Beweis. Unser Produkt ist offensichtlich symmetrisch und läßt sich nach 2.9.6 folglich eindeutig schreiben als Polynom in den elementarsymmetrischen Polynomen. \square

2.9.15. Für jeden kommutativen Integritätsbereich k und jedes normierte Polynom $T^n + a_1T^{n-1} + \dots + a_n$ im Polynomring $k[T]$, das in $k[T]$ vollständig in Linearfaktoren zerfällt, sind für die eben definierte Diskriminante Δ_n offensichtlich gleichbedeutend:

1. $\Delta_n(a_1, \dots, a_n) = 0$;
2. Das Polynom $T^n + a_1T^{n-1} + \dots + a_n$ hat mehrfache Nullstellen.

Man nennt das Element $\Delta_n(a_1, \dots, a_n) \in k$ auch die **Diskriminante des normierten Polynoms** $T^n + a_1T^{n-1} + \dots + a_n$. Eine explizite Formel für die Diskriminante geben wir in 3.9.23.

Übungen

Übung 2.9.16. Was ist die Summe der $\lambda_1^3 + \lambda_2^3 + \lambda_3^3 + \lambda_4^3$ dritten Potenzen der vier komplexen Nullstellen $\lambda_1, \dots, \lambda_4$ des Polynoms $X^4 + 3X^3 - 5X^2 + X + 1$?

Ergänzende Übung 2.9.17. Man zeige für symmetrische Polynome im Fall $n \geq k$ die Identität

$$s_{2k}(X_1, \dots, X_n, -X_1, \dots, -X_n) = (-1)^k s_k(X_1^2, \dots, X_n^2)$$

Ergänzende Übung 2.9.18. 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 2.9.19. Sei k ein Körper einer von Zwei verschiedenen Charakteristik. Ein Polynom $f \in k[X_1, \dots, X_n]$ heißt **antisymmetrisch** genau dann, wenn gilt $\sigma f = \text{sgn}(\sigma) f \quad \forall \sigma \in \mathcal{S}_n$. Man zeige, daß die antisymmetrischen Polynome genau die Produkte von $\prod_{i < j} (X_i - X_j)$ mit symmetrischen Polynomen sind. Hinweis: [LA1] 4.4.5. Man zeige dasselbe auch allgemeiner im Fall eines faktoriellen Rings k einer von Zwei verschiedenen Charakteristik.

Ergänzende Übung 2.9.20. Ist der Koeffizientenring k ein unendlicher Integritätsbereich, so ist ein Polynom $f \in k[X_1, \dots, X_n]$ homogen vom Grad d genau dann, wenn gilt

$$f(\lambda X_1, \dots, \lambda X_n) = \lambda^d f(X_1, \dots, X_n) \quad \forall \lambda \in k$$

Übung 2.9.21. Man stelle $X^4 + Y^4 + Z^4 + W^4$ als Polynom in den elementarsymmetrischen Polynomen dar.

Ergänzende Übung 2.9.22. Ist R ein Kring mit einer Primzahl p als Charakteristik, so bilden die Elemente $a \in R$ mit $a^p = a$ einen Teilring.

Ergänzende Übung 2.9.23. Der Ring der symmetrischen Funktionen in n Veränderlichen mit Koeffizienten aus \mathbb{Q} wird auch als Ring erzeugt von \mathbb{Q} und den Potenzsummen $X_1^k + \dots + X_n^k$ für $1 \leq k \leq n$. Eine $(n \times n)$ -Matrix A über einem Körper der Charakteristik Null ist nilpotent genau dann, wenn für die Spuren ihrer Potenzen gilt

$$0 = \operatorname{tr}(A) = \operatorname{tr}(A^2) = \dots = \operatorname{tr}(A^n)$$

Übung 2.9.24. 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 $X_1^3 + X_2^3 + \dots + X_{14}^3 = s_1^3 - 3s_1s_2 + 3s_3$.

Übung 2.9.25. Sei k ein Körper und seien $f, g \in k[X, Y] \setminus 0$ teilerfremde homogene Polynome der Grade 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: [2.5.16](#).

2.10 Schranke von Bézout*

Definition 2.10.1. 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

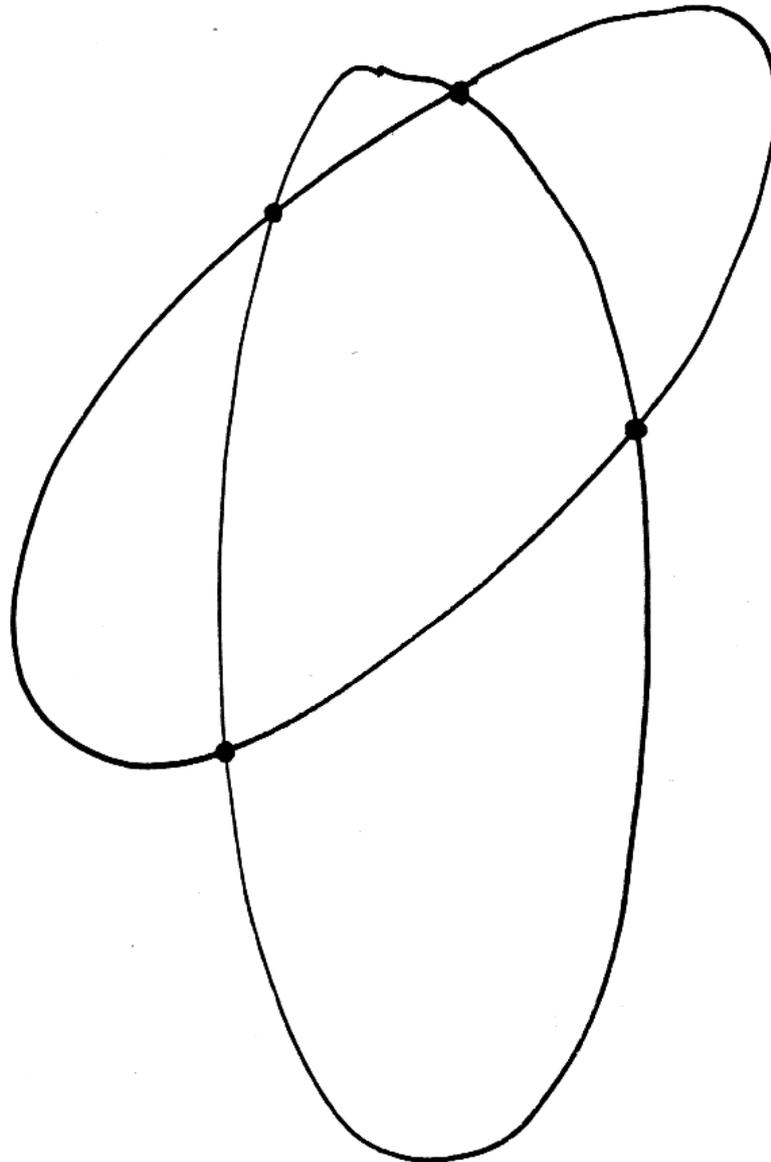
$$\operatorname{grad} f = \sup\{p + q \mid c_{pq} \neq 0\}$$

Speziell geben wir im Lichte von [\[AN1\] 2.1.2](#) dem Nullpolynom den Grad $-\infty$. Analog definieren wir auch den Grad eines Polynoms in beliebig vielen Veränderlichen.

Satz 2.10.2 (Schranke von Bézout). *Sei k ein Körper und seien im Polynomring $k[X, Y]$ 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 2.10.3. 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 [\[KAG\] 6.5.6](#) lernen.

Beispiel 2.10.4. Ist eines unserer beiden Polynome von der Gestalt $a_n X^n + \dots + a_1 X + a_0 - Y$ und seine Nullstellenmenge mithin der Graph des Polynoms $a_n X^n + \dots + a_1 X + a_0$ in einer Veränderlichen, so kann man diese Schranke schnell



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.

einschauen: Man setzt einfach in das andere Polynom $Y = a_n X^n + \dots + a_1 X + a_0$ ein und erhält ein Polynom in X , das eben nur höchstens so viele Nullstellen haben kann, wie sein Grad ist.

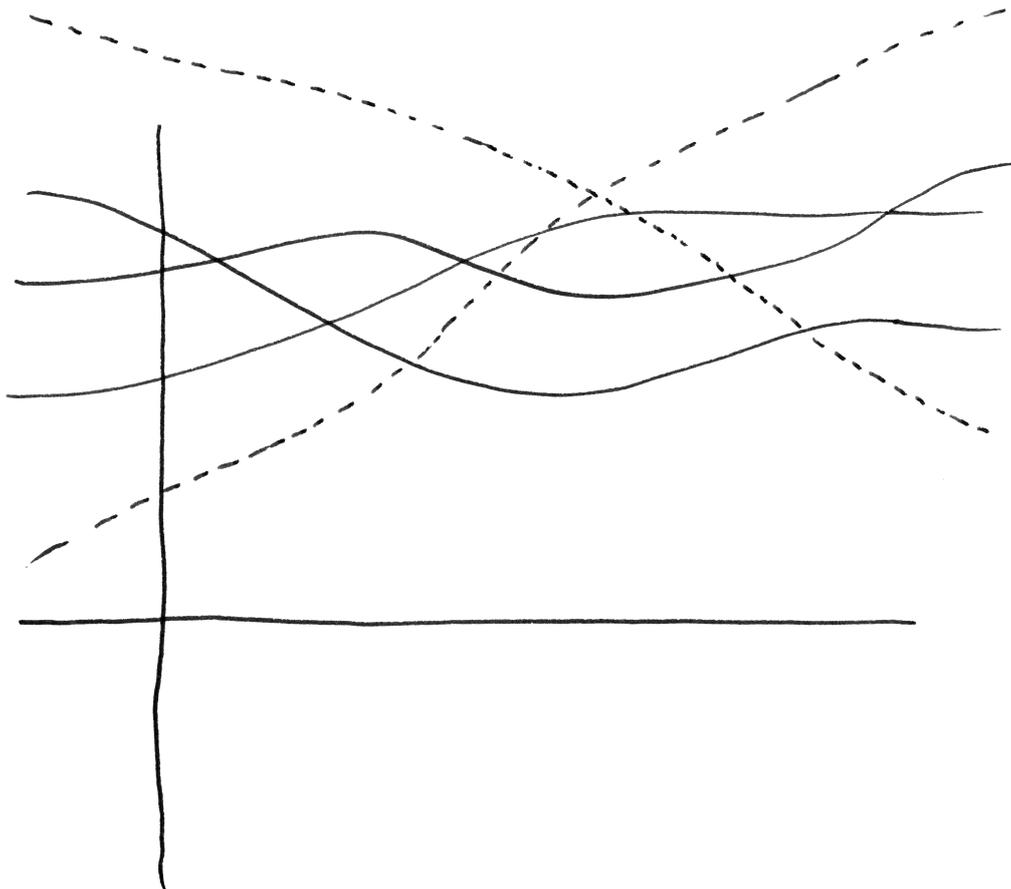
Beweis. Sicher reicht es, wenn wir unsere Schranke zeigen für geeignet transformierte Polynome $f \circ \varphi, g \circ \varphi$ mit $\varphi \in \text{GL}(2; k)$ als da heißt $\varphi : k^2 \xrightarrow{\sim} k^2$ linear. Wir interessieren uns hier insbesondere für die Scherungen $\varphi_\lambda : k^2 \rightarrow k^2, (x, y) \mapsto (x + \lambda y, y)$ mit $\lambda \in k$. Gegeben $f \in k[X, Y]$ ein Polynom vom Totalgrad $\text{grad } f = n$ 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 2.7.16 schon, daß 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 $f \circ \varphi_\lambda$ bzw. $g \circ \varphi_\lambda$ beide Monome der Gestalt cY^n bzw. dY^m mit $c \neq 0 \neq d$ enthalten, für $n = \text{grad } f, m = \text{grad } g$, 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

$$\begin{aligned} f &= Y^n + a_1(X)Y^{n-1} + \dots + a_n(X) \\ g &= Y^m + b_1(X)Y^{m-1} + \dots + b_m(X) \end{aligned}$$

haben mit $a_i, b_j \in k[X], \text{grad } a_i \leq i, \text{grad } b_j \leq j$, 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“ $R(f, g) \in k[X]$, und in 2.10.9 zeigen wir, daß diese Resultante als Polynom in X höchstens den Grad nm hat. Das beendet dann den Beweis. \square

Satz 2.10.5 (über die Resultante). Gegeben $m, n \geq 0$ gibt es genau ein Polynom mit ganzzahligen Koeffizienten in $n + m$ Veränderlichen, sagen wir $R \in \mathbb{Z}[a_1, \dots, a_n, b_1, \dots, b_m]$ derart, daß unter der Substitution der a_i und b_j durch diejenigen Elemente von $\mathbb{Z}[\zeta_1, \dots, \zeta_n, \xi_1, \dots, \xi_m]$, die erklärt sind durch die Gleichungen

$$\begin{aligned} T^n + a_1 T^{n-1} + \dots + a_n &= (T + \zeta_1) \dots (T + \zeta_n), \\ T^m + b_1 T^{m-1} + \dots + b_m &= (T + \xi_1) \dots (T + \xi_m), \end{aligned}$$



Das Nullstellengebilde von $f = Y^3 + a_2(X)Y^2 + \dots + a_0(X)$ als durchgezogene und von $g = Y^2 + b_1(X)Y + \dots + b_0(X)$ als gestrichelte Linien. Über jedem Punkt der x -Achse liegen genau drei bzw. zwei Lösungen von f bzw. g .

im Polynomring in den ζ_i und ξ_j gilt

$$R(a_1, \dots, a_n, b_1, \dots, b_m) = \prod_{i=1, j=1}^{n, m} (\zeta_i - \xi_j)$$

Definition 2.10.6. Gegeben normierte Polynome $f(T) = T^n + a_1 T^{n-1} + \dots + a_n$ und $g(T) = T^m + b_1 T^{m-1} + \dots + b_m$ mit Koeffizienten in einem Kring k benutzen wir die Abkürzung

$$R(a_1, \dots, a_n, b_1, \dots, b_m) = R(f, g)$$

und nennen dies Element von k die **Resultante von f und g** .

2.10.7 (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 2.10.8. Im Fall $m = n = 2$ folgt aus $T^2 + a_1 T + a_2 = (T - \zeta_1)(T - \zeta_2)$ und $T^2 + b_1 T + b_2 = (T - \xi_1)(T - \xi_2)$ unmittelbar

$$\begin{aligned} a_2 &= \zeta_1 \zeta_2, & a_1 &= \zeta_1 + \zeta_2, \\ b_2 &= \xi_1 \xi_2, & b_1 &= \xi_1 + \xi_2, \end{aligned}$$

Eine kurze Rechnung liefert dann

$$(\zeta_1 - \xi_1)(\zeta_2 - \xi_2)(\zeta_1 - \xi_2)(\zeta_2 - \xi_1) = (a_2 - b_2)^2 - (a_2 + b_2)a_1 b_1 + a_2 b_1^2 + b_2 a_1^2$$

Der Ausdruck rechts in den Koeffizienten ist also die Resultante der Polynome $f(T) = T^2 + a_1 T + a_2$ und $g(T) = T^2 + b_1 T + b_2$. 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 $\prod_{i=1, j=1}^{n, m} (\zeta_i - \xi_j) \in \mathbb{Z}[\zeta_1, \dots, \zeta_n][\xi_1, \dots, \xi_m]$ ist symmetrisch in den ξ_j und liegt nach **2.9.6** folglich in

$$\mathbb{Z}[\zeta_1, \dots, \zeta_n][b_1, \dots, b_m] = \mathbb{Z}[b_1, \dots, b_m][\zeta_1, \dots, \zeta_n]$$

Unser Polynom ist aber auch symmetrisch in den ζ_i , folglich liegt es wieder nach **2.9.6** sogar in $\mathbb{Z}[b_1, \dots, b_m][a_1, \dots, a_n]$. \square

2.10.9 (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 $\mathbb{Z}[\zeta_1, \dots, \zeta_n, \xi_1, \dots, \xi_m]$ ist die Resultante ja offensichtlich homogen vom Grad mn . Dahingegen sind die $a_i \in \mathbb{Z}[\zeta_1, \dots, \zeta_n]$ homogen vom Grad i und die $b_j \in \mathbb{Z}[\xi_1, \dots, \xi_m]$ homogen vom Grad j . Aus der algebraischen Unabhängigkeit der elementarsymmetrischen Polynome folgt, daß ein Monom $a_1^{\lambda_1} \dots a_n^{\lambda_n} b_1^{\mu_1} \dots b_m^{\mu_m}$ nur dann mit von Null verschiedenem Koeffizienten in der Resultante auftauchen kann, wenn gilt

$$\lambda_1 + 2\lambda_2 + \dots + n\lambda_n + \mu_1 + 2\mu_2 + \dots + m\mu_m = nm$$

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 2.10.10 (Die Resultante als Determinante). Sei M die Matrix aus nebenstehendem Bild. Eine explizite Formel für die Resultante ist

$$R(a_1, \dots, a_n, b_1, \dots, b_m) = \det M$$

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 2.3.4, wenn wir etwa das Urbild kleinsten Grades von $(0, 1) \in R/\langle f \rangle \times R/\langle g \rangle$ in R 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 [LA1] 4.4.5, 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 2.10.5 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.

Übungen

Ergänzende Übung 2.10.11. Zwei beliebige homogene Polynome $f(X, Y) = a_0X^n + a_1X^{n-1}Y + \dots + a_nY^n$ und $g(X, Y) = b_0X^m + b_1X^{m-1}Y + \dots + b_mY^m$ 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**.

3 Mehr zu Körpern

3.1 Grundlagen und Definitionen

Beispiele 3.1.1. Ein Körper ist nach [LA1] 4.2.24 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 [LA1] 4.6 zu jedem kommutativen Integritätsbereich R seinen Quotientenkörper $\text{Quot } R$ konstruiert, zum Beispiel ist $\text{Quot } \mathbb{Z} = \mathbb{Q}$ unser Körper der rationalen Zahlen und $\text{Quot } K[X] = K(X)$ der Funktionenkörper über einem gegebenen Körper K . Weiter ist nach 2.5.5 der Restklassenring R/pR von einem Hauptidealring nach dem von einem irreduziblen Element $p \in R$ erzeugten Ideal ein Körper, speziell die Restklassenringe $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ für p eine Primzahl in \mathbb{Z} und $K[X]/\langle P \rangle$ für $P \in K[X]$ ein irreduzibles Polynom im Polynomring $K[X]$ über einem Körper K .

Definition 3.1.2. 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.

3.1.3. 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** .

3.1.4. Für jeden Körper K erinnern wir uns aus [LA1] 4.2.29 an die Definition seiner **Charakteristik**, eines Elements $(\text{char } K) \in \mathbb{N}$, durch die Identität

$$\ker(\mathbb{Z} \rightarrow K) = \mathbb{Z} \cdot (\text{char } K)$$

Hier meint $\mathbb{Z} \rightarrow K$ den nach [LA1] 4.1.10 eindeutig bestimmten Ringhomomorphismus von \mathbb{Z} nach K .

3.1.5 (**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 $1 + 1 + \dots + 1 = 0$ (d Summanden), so ist das kleinstmögliche derartige $d > 0$ die Charakteristik $d = \text{char } K$ von K , und gibt es kein derartiges d , so hat K die Charakteristik Null.

Lemma 3.1.6 (Kleinster Unterkörper eines Körpers). *Die Charakteristik eines Körpers ist entweder Null oder eine Primzahl und es gilt:*

$$\begin{aligned} \text{char } K = 0 &\quad \Leftrightarrow \quad \text{Der kleinste Unterkörper von } K \text{ ist isomorph zu } \mathbb{Q}; \\ \text{char } K = p > 0 &\quad \Leftrightarrow \quad \text{Der kleinste Unterkörper von } K \text{ ist isomorph zu } \mathbb{F}_p. \end{aligned}$$

Beweis. Sei $d = \text{char } K$. Da wir eine Inklusion $\mathbb{Z}/d\mathbb{Z} \hookrightarrow K$ haben, muß $\mathbb{Z}/d\mathbb{Z}$ nullteilerfrei sein, also ist die Charakteristik eines Körpers nach [LA1] 4.2.25 entweder null oder eine Primzahl. Im Fall $\text{char } K = p > 0$ prim induziert $\mathbb{Z} \rightarrow K$ unter Verwendung der universellen Eigenschaft des Resklassenrings 2.1.13 oder spezieller 2.2.5 einen Isomorphismus von $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ auf einen Unterkörper von K . Im Fall $d = 0$ induziert $\mathbb{Z} \rightarrow K$ unter Verwendung der universellen Eigenschaft des Quotientenkörpers [LA1] 4.6.5 einen Isomorphismus von $\mathbb{Q} = \text{Quot } \mathbb{Z}$ auf einen Unterkörper von K . Man prüft leicht, daß die Bilder jeweils die kleinsten Unterkörper von K sind. \square

3.2 Körpererweiterungen

Definition 3.2.1. 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 3.2.2. 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 3.2.3. In 3.8.7 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 Erweiterungs-Begriffs.

Definition 3.2.4 (Erzeugung von Körpererweiterungen). Gegeben eine Körpererweiterung L/K und Elemente des Erweiterungskörpers $\alpha_1, \dots, \alpha_n \in L$ bezeichnet man mit $K(\alpha_1, \dots, \alpha_n) \subset L$ 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 $K[\alpha_1, \dots, \alpha_n] \subset L$. Eine Körpererweiterung L/K heie **körperendlich**,

wenn der Erweiterungskörper über dem Grundkörper als Körper endlich erzeugt ist, wenn es also in Formeln endlich viele Elemente $\alpha_1, \dots, \alpha_n \in L$ gibt mit

$$L = K(\alpha_1, \dots, \alpha_n)$$

3.2.5 (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 2.2.4 ein „Freiheitsstrichlein“ oben an die eröffnende Klammer und schreiben $K('X)$ für den Funktionenkörper in einer Variablen X .

Ergänzung 3.2.6. 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 $K({}_l T)$. Gegeben Körper $K \subset L$ und eine Teilmenge $T \subset L$ kann der von K und T erzeugte Teilkörper $K({}_l T) \subset L$ von L beschrieben werden als die Vereinigung aller von endlichen Teilmengen von T über K erzeugten Teilkörper, in Formeln

$$K({}_l T) = \bigcup_{\substack{n \geq 0 \\ \alpha_1, \dots, \alpha_n \in T}} K(\alpha_1, \dots, \alpha_n)$$

Beispiele 3.2.7. Wir haben $\mathbb{R}(i) = \mathbb{R}[i] = \mathbb{C}$ 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 3.2.8. 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 [GR] 3.4.15. Man schreibe das Inverse von $7 + \sqrt{2}$ in dieser Form.

Übung 3.2.9. Man zeige $\sqrt{5} \notin \mathbb{Q}(\sqrt{2})$.

Übung 3.2.10. Gegeben $a, b \in \mathbb{Q}^\times$ zeige man, daß gilt $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{b})$ genau dann, wenn a/b in \mathbb{Q} ein Quadrat ist.

Übung 3.2.11. 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 3.9.10 zusammen.

Ergänzung 3.2.12. Sehr viel allgemeiner kann man für paarweise verschiedene Primzahlen p, q, \dots, w und beliebige $n, m, \dots, r \geq 2$ zeigen, daß gilt

$$\sqrt[n]{p} \notin \mathbb{Q}(\sqrt[m]{q}, \dots, \sqrt[r]{w})$$

Das und vieles weitere in dieser Richtung lernt man in der algebraischen Zahlentheorie, die auf dieser Vorlesung aufbaut.

Übung 3.2.13. Seien K ein Körper und $P \in K[X] \setminus K$ ein nichtkonstantes Polynom. So ist der Ringhomomorphismus $K[Y] \rightarrow K[X]$ mit $Y \mapsto P$ injektiv und die davon induzierte Körpererweiterung $K(Y) \hookrightarrow K(X)$ hat als Grad den Grad von P .

3.3 Elemente von Körpererweiterungen

Definition 3.3.1. 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 [AN1] 2.4.2.

3.3.2. Gegeben eine Körpererweiterung L/K und ein Element $\alpha \in L$ betrachten wir die Auswertungsabbildung

$$\begin{array}{ccc} K[X] & \rightarrow & L \\ Q & \mapsto & Q(\alpha) \end{array}$$

Ist α transzendent, so ist diese Abbildung injektiv und induziert nach der universellen Eigenschaft des Quotientenkörpers [LA1] 4.6.5 einen Isomorphismus $K(X) = \text{Quot } K[X] \xrightarrow{\sim} K(\alpha) \subset L$. Den anderen Fall klärt der folgende Satz.

Satz 3.3.3 (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** $P = \text{Irr}(\alpha, K)$ 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

$$K[X]/\langle \text{Irr}(\alpha, K) \rangle \xrightarrow{\sim} K(\alpha)$$

5. Ist $d = \text{grad}(\text{Irr}(\alpha, K))$ der Grad des Minimalpolynoms von α über K , so bilden die Potenzen $1, \alpha, \alpha^2, \dots, \alpha^{d-1}$ eine Basis des K -Vektorraums $K(\alpha)$.

Beispiel 3.3.4. Wir betrachten die Körpererweiterung \mathbb{C}/\mathbb{R} . Das Element $i \in \mathbb{C}$ ist algebraisch über \mathbb{R} mit Minimalpolynom $\text{Irr}(i, \mathbb{R}) = X^2 + 1$. Wir haben $\mathbb{R}(i) = \mathbb{C}$ und die Abbildung $\mathbb{R}[X] \rightarrow \mathbb{C}$ mit $X \mapsto i$ definiert einen Ringisomorphismus $\mathbb{R}[X]/\langle X^2 + 1 \rangle \xrightarrow{\sim} \mathbb{C}$. Die beiden Elemente $1 = i^0$ und $i = i^1$ bilden eine Basis von \mathbb{C} über \mathbb{R} .

Beweis. Da $K[X]$ nach 2.4.24 ein Hauptidealring ist und da das Auswerten $\varphi_\alpha : K[X] \rightarrow L$ 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 2.2.5 weiter eine Einbettung $K[X]/\langle P \rangle \hookrightarrow L$, folglich ist $K[X]/\langle P \rangle$ ein Integritätsbereich. Nach 2.5.5 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 2.1.20 bilden für $d = \text{grad } P$ die Bilder der Potenzen $1, X, X^2, \dots, X^{d-1}$ eine Basis von $K[X]/\langle P \rangle$ über K , und damit bilden dann auch $1, \alpha, \alpha^2, \dots, \alpha^{d-1}$ eine Basis von $K(\alpha)$ über K . \square

3.3.5. 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 wegen der Nullteilerfreiheit unseres Erweiterungskörpers sofort zum Widerspruch $P(\alpha) \neq 0$ führen.

3.3.6. 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

$$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \mid a, b, c \in \mathbb{Q}\}$$

3.3.7. 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 3.3.8. 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 3.3.9. Gegeben eine Körpererweiterung L/K und ein Element $a \in L$, das algebraisch ist über K , zeige man, daß das Minimalpolynom $\text{Irr}(a; K)$ bis auf ein Vorzeichen mit dem charakteristischen Polynom nach [LA1] 5.6.9 des durch Multiplikation mit a gegebenen Endomorphismus des K -Vektorraums $K(a)$ zusammenfällt. Hinweis: Cayley-Hamilton.

Übung 3.3.10. Man bestimme das Minimalpolynom der komplexen Zahl $1 + i$ über \mathbb{R} .

Ergänzende Übung 3.3.11. 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 3.3.12. 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 [AN2] ?? und abzählbar viele gebrochen rationale Funktionen aus $\mathbb{C}(X)$ können nur abzählbar viele Polstellen haben.

Übung 3.3.13. 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 3.3.14. 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 .

3.4 Endliche Körpererweiterungen

Definition 3.4.1. 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**.

3.4.2 (**Diskussion der Terminologie**). Jede endliche Körpererweiterung ist körperendlich im Sinne unserer Definition 3.2.4, 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.

3.4.3 (**Grad einer primitiven Körpererweiterung**). Ist L/K eine Körpererweiterung und $\alpha \in L$ algebraisch über K , so stimmt nach dem letzten Teil des Satzes 3.3.3 über das Minimalpolynom der Grad $[K(\alpha) : K]$ der von α erzeugten Körpererweiterung überein mit dem Grad $\text{grad}(\text{Irr}(\alpha, K))$ des Minimalpolynoms von α über K . Daher rührt wohl auch die Begriffsbildung des „Grades einer Körpererweiterung“. Wir vereinbaren für diese Zahl die abkürzende Bezeichnung

$$\text{grad}_K(\alpha) := \text{grad}(\text{Irr}(\alpha, K)) = [K(\alpha) : K]$$

und nennen sie den **Grad von α über K** .

Ergänzung 3.4.4 (Diskussion der Notation). Man kann sich fragen, warum man für den Grad einer Körpererweiterung 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 3.4.5. Es gilt $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, $[\mathbb{C} : \mathbb{R}] = 2$, $[\mathbb{R} : \mathbb{Q}] = \infty$.

Beispiel 3.4.6. 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 [LA1] 5.6.26.

Proposition 3.4.7. 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 3.3.3. Die Implikation $2 \Rightarrow 3$ ist offensichtlich. Aber falls gilt $\dim_K L' < \infty$, können die Potenzen α^ν von α für $\nu = 0, 1, 2, \dots$ nicht K -linear unabhängig sein, also $3 \Rightarrow 1$. \square

Definition 3.4.8. Eine Körpererweiterung vom Grad 2 heißt eine **quadratische Körpererweiterung**.

Proposition 3.4.9 (Quadratische Körpererweiterungen). Für eine Körpererweiterung L/K mit $\text{char } K \neq 2$ 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 $\alpha \in L \setminus K$ mit $\alpha^2 \in K$.

Beweis. $2 \Rightarrow 1$ ist klar. Für die andere Richtung $1 \Rightarrow 2$ beachte man, daß jedes $\beta \in L \setminus K$ 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 $\alpha = \beta + \frac{a}{2}$. \square

Ergänzung 3.4.10. Wir werden in 3.7.1 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 3.4.11 (Multiplikatивität 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, \dots, m_r eine Basis von M über L und l_1, \dots, 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 . \square

Korollar 3.4.12 (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 $[L : K] = [L : K(\alpha)][K(\alpha) : K]$. \square

Beispiel 3.4.13. Es gilt $\sqrt{2} \notin \mathbb{Q}(\sqrt[3]{2})$. In der Tat sind nach 2.5.13 die Polynome $X^2 - 2$ und $X^3 - 2$ irreduzibel in $\mathbb{Q}[X]$, nach 3.3.6 sind sie also bereits die Minimalpolynome von $\sqrt{2}$ bzw. $\sqrt[3]{2}$, und folglich hat $\sqrt{2}$ den Grad 2 über \mathbb{Q} und $\sqrt[3]{2}$ den Grad 3.

Korollar 3.4.14. Seien L/K ein Körpererweiterung und $\alpha_1, \dots, \alpha_n \in L$ algebraisch über K . So ist $K(\alpha_1, \dots, \alpha_n)$ endlich über K und insbesondere sind alle Elemente dieser Körpererweiterung auch algebraisch über K .

Beweis. Im Körperturm $K \subset K(\alpha_1) \subset K(\alpha_1, \alpha_2) \subset \dots \subset K(\alpha_1, \dots, \alpha_n)$ sind alle Schritte endliche Körpererweiterungen. Nach 3.4.11 ist also auch die ganze Erweiterung endlich. \square

Übungen

Ergänzende Übung 3.4.15. 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 3.4.16. Sei K ein Körper und seien $P, Q \in K[X]$ irreduzibel mit $\text{grad } P$ und $\text{grad } Q$ 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 3.4.17. Die durch den Funktionenkörper $K(X)$ über einem vorgegebenen Körper K gegebene Körpererweiterung $K(X)/K$ ist stets körperendlich, aber nie endlich.

Übung 3.4.18. 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 2.7.21 und 3.3.14.

3.5 Notationen für Erzeugung**

3.5.1. 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;
- [] 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;
- $\langle \rangle, \langle \rangle, [\rangle, [\rangle, (\rangle$ 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**;
- $\langle \rangle, \langle \rangle, [\rangle, [\rangle$ 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 3.5.2. Wir schreiben also etwa $k[x_1, \dots, x_n] = k[x_1, \dots, x_n]$ für Polynomring über k in den Variablen x_1, \dots, x_n . Der freie k -Vektorraum über einer Menge X aus [LA1] 2.3.4 kann nun bezeichnet werden kann 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 $\langle X \rangle_k = \langle X \rangle_k \subset M$ für den von X erzeugten Untervektorraum, kürzen $\langle \{x_1, \dots, x_n\} \rangle_k = \langle x_1, \dots, x_n \rangle_k = k\langle x_1, \dots, x_n \rangle$ ab und lassen k ganz weg, wenn wir hoffen, daß es aus dem Kontext hervorgeht oder wenn 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 Teilkring und sind x_1, \dots, x_n Elemente von R , so notieren wir $k[x_1, \dots, x_n] \subset R$ 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.

3.6 Konstruktionen mit Zirkel und Lineal

Definition 3.6.1. 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 3.6.2 (Konstruierbarkeit und quadratische Erweiterungen). *Die folgenden beiden Teilmengen K und Q von \mathbb{C} stimmen überein:*

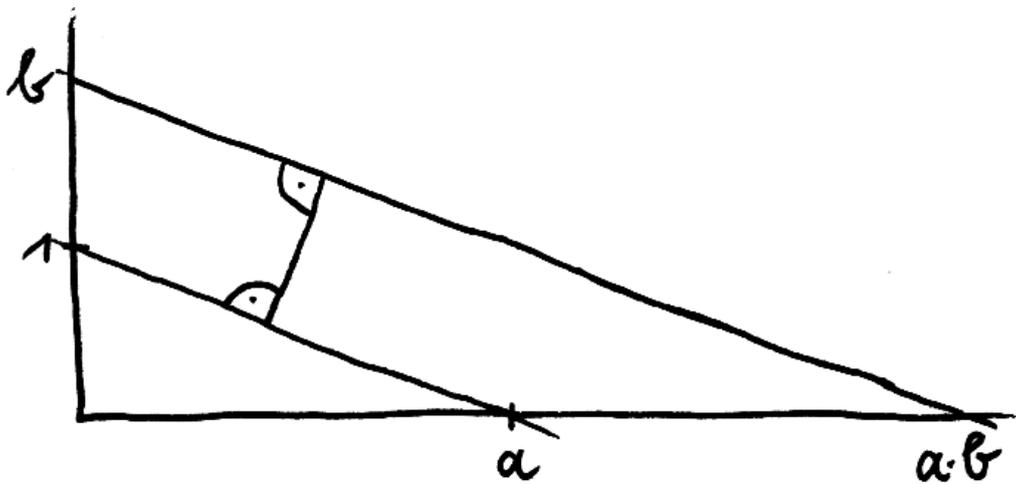
1. *Die kleinste Teilmenge $K \subset \mathbb{C}$, die 0 und 1 enthält und stabil ist unter elementaren Konstruktionen, also die Eigenschaft hat, daß jede aus K elementar konstruierbare komplexe Zahl wieder in K liegt. Wir nennen die Elemente von K die **konstruierbaren Zahlen**;*
2. *Die kleinste Teilmenge $Q \subset \mathbb{C}$, die sowohl ein Teilkörper ist als auch stabil unter dem Bilden von Quadratwurzeln.*

3.6.3. 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.

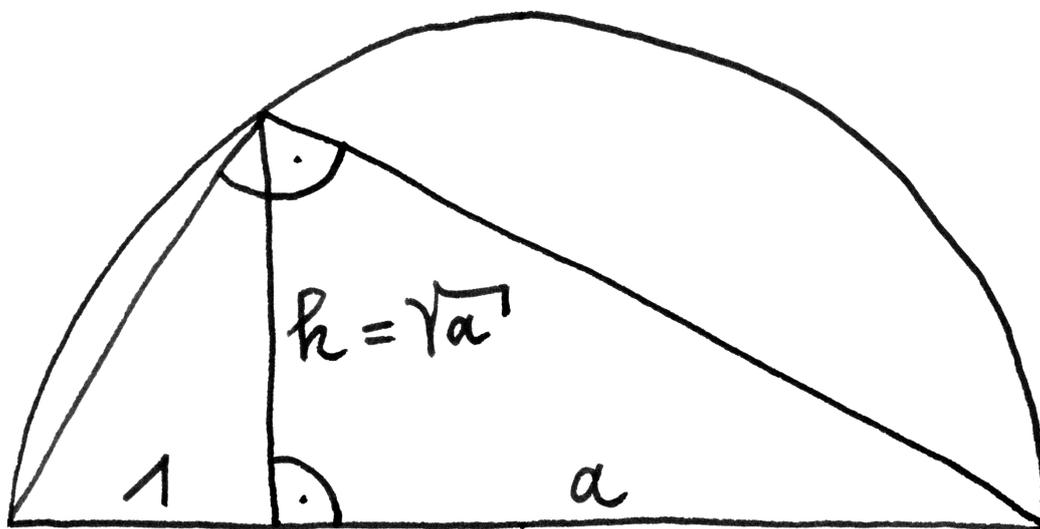
Beweis. Wir beginnen mit der Inklusion $Q \subset K$. Dazu reicht es zu zeigen, daß $K \subset \mathbb{C}$ ein Teilkörper und stabil unter dem Bilden von Quadratwurzeln ist. Offensichtlich ist K stabil unter Addition. Um die Stabilität unter Multiplikation und Inversenbildung zu zeigen beachten wir, 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. $\operatorname{Re}(a)$ und $\operatorname{Im}(a)$ 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} . Er ist stabil unter dem Bild 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 erhalten $Q \subset K$. Wir



Die Konstruktion von Produkten und Inversen



Die Konstruktion der Wurzel

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 $z = x + iy$ 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 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 $K \subset Q$. \square

Korollar 3.6.4 (Eine notwendige Bedingung für Konstruierbarkeit). *Jede konstruierbare Zahl ist algebraisch und ihr Grad über \mathbb{Q} ist eine Zweierpotenz.*

Vorschau 3.6.5. Das Umgekehrte gilt nicht. Es gibt durchaus algebraische komplexe Zahlen, deren Grad über \mathbb{Q} eine Zweierpotenz ist, die aber keineswegs konstruierbar sind. Ein hinreichendes und notwendiges Kriterium können Sie in [4.4.15](#) 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 $\mathbb{Q}(\alpha_1, \alpha_2, \dots, \alpha_r)$ für Folgen $\alpha_1, \alpha_2, \dots, \alpha_r$ komplexer Zahlen mit der Eigenschaft $\alpha_i^2 \in \mathbb{Q}(\alpha_1, \alpha_2, \dots, \alpha_{i-1})$ 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

$$\mathbb{Q} = K_0 \subset K_1 \subset \dots \subset K_r$$

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 [3.4.12](#) ein Teiler von $[K_r : \mathbb{Q}]$. \square

Korollar 3.6.6 (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 3.6.7. Wir werden in 4.4.7 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 3.6.8. 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 3.6.9. Die Frage der **Würfelerdopplung**, 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 2.8.4 und der Gleichheit 3.3.6 vom Grad einer primitiven Körpererweiterung und dem Grad des Minimalpolynoms eines jeden Erzeugers hat $\exp(2\pi i/7)$ den Grad 6 über \mathbb{Q} und ist nach 3.6.4 also nicht konstruierbar.

2. Nach 3.3.6 hat die gesuchte Länge $\sqrt[3]{2}$ als algebraische Zahl den Grad 3 über \mathbb{Q} und ist nach 3.6.4 also nicht konstruierbar.

3. Sicher gilt $\exp(2\pi i/3) \in K$. Es reicht, $\exp(2\pi i/9) \notin K$ zu zeigen. Sicher ist $\exp(2\pi i/9) = \zeta$ 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 2.8.6. 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 3.6.4 nicht konstruierbar sein. In 4.4.2 werden wir zeigen, daß alle Kreisteilungspolynome irreduzibel sind. Hier basteln wir nur ein schnelles Argument für unseren speziellen Fall zusammen, vergleiche auch 2.8.7. 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 2.8.2 folgern, daß unser Polynom irreduzibel ist. \square

Satz 3.6.10 (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.*

3.6.11. Gegeben eine Teilmenge $A \subset \mathbb{C}$ nennen wir die Elemente der Menge K_A aus 3.6.10 die **aus A konstruierbaren Zahlen**. Der Beweis unserer Variante ist vollständig analog zum Beweis von 3.6.2 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° mit Zirkel und Lineal dritteln, denn für die primitive achte Einheitswurzel $a = (i - 1)/\sqrt{2}$ ist a^3 eine Nullstelle von $X^3 - a$. Andererseits läßt sich ein durch einen transzendenten 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.

3.7 Endliche Körper

Satz 3.7.1 (Klassifikation endlicher Körper). *Die Kardinalität eines endlichen Körpers ist stets eine Primzahlpotenz, und zu jeder Primzahlpotenz gibt es umgekehrt bis auf Isomorphismus genau einen endlichen Körper mit dieser Kardinalität.*

3.7.2. Gegeben eine 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. Ich erinnere daran, daß bei mir die 1 nach [LA2] 4.4.3 keine Primzahlpotenz ist.

Vorschau 3.7.3. Man kann zeigen, daß jeder endliche Schiefkörper schon ein Körper ist, siehe zum Beispiel [Wei74], I, §1.

Beweis. Ein endlicher Körper \mathbb{F} hat sicher positive Charakteristik $p = \text{char } \mathbb{F} > 0$. Nach 3.1.6 ist 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

$$\{\text{endliche Körper, bis auf Isomorphismus}\} \xrightarrow{\sim} \{\text{Primzahlpotenzen}\}$$

liefert. Wir unterbrechen nun den Beweis durch einen Satz und zwei Lemmata, um die nötigen Hilfsmittel bereitzustellen. \square

Satz 3.7.4 (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 $L[X]$ vollständig in Linearfaktoren zerfällt.*

Beweis. Das folgt mit Induktion aus dem anschließenden Lemma 3.7.7, wenn wir beachten, daß nach [LA1] 4.2.42 jeder Körperhomomorphismus injektiv ist. \square

3.7.5. 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** . In 3.7.9 werden wir zeigen, daß die Körpererweiterung $K(\alpha)$ von K im Fall eines K -irreduziblen Polynoms P von der Wahl von L und α im wesentlichen gar nicht abhängt.

Vorschau 3.7.6. Natürlich folgt obiger Satz auch unmittelbar aus der Existenz eines algebraischen Abschlusses 3.11.5. 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 3.7.7 (Adjunktion von Nullstellen). *Seien K ein Körper und $P \in K[X] \setminus K$ ein nichtkonstantes Polynom. So gibt es einen Körperhomomorphismus $i : K \rightarrow L$ derart, daß das Bild $i(P)$ von P unter der von i auf den Polynomringen induzierten Abbildung $i = i_{[X]} : K[X] \rightarrow L[X]$ eine Nullstelle in L hat.*

3.7.8. Die Adjunktion von Quadratwurzeln haben Sie möglicherweise bereits sozusagen zu Fuß als Übung [GR] 3.4.14 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 [GR] 3.4.14 beschriebenen Körpererweiterung anzugeben.

Beweis. Sei ohne Beschränkung der Allgemeinheit P irreduzibel in $K[X]$. Dann ist $L := K[X]/\langle P \rangle$ nach 2.5.5 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

$$i : K \rightarrow L = K[X]/\langle P \rangle$$

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 $P = a_n X^n + \dots + a_1 X + a_0$ mit Koeffizienten $a_\nu \in K$ sofort $i(P) = \bar{a}_n X^n + \dots + \bar{a}_1 X + \bar{a}_0$ und dann

$$(i(P))(\bar{X}) = \bar{a}_n \bar{X}^n + \dots + \bar{a}_1 \bar{X} + \bar{a}_0 = \overline{a_n X^n + \dots + a_1 X + a_0} = \bar{P} = 0 \square$$

3.7.9. Gegeben ein Körper K und ein irreduzibles Polynom $P \in K[X]$ und eine Körpererweiterung $K \subset L$ und eine Nullstelle $\alpha \in L$ 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 3.7.10. 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 3.7.11. *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 [LA1] 4.2.36 ist die Abbildung $F : L \rightarrow L, a \mapsto a^q$ 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. \square

Beweis von 3.7.1, 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 3.7.4 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 3.7.11 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 [LA2] 4.3.8, 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 [LA2] 4.4.17 gibt es solche Erzeuger und damit auch solche Faktoren und mit 3.3.3 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. \square

3.7.12. 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 3.8.2 über die Eindeutigkeit von Zerfällungskörpern. Die Existenz folgt wie oben daraus, daß $X^q - X$ keine mehrfachen Nullstellen hat, aber das kann man nach 3.9.12 auch daraus folgern, daß die Ableitung dieses Polynoms keine Nullstellen hat.

Satz 3.7.13 (Endliche Erweiterungen endlicher Körper). *Gegeben ein endlicher Körper F liefert die Kardinalität eine Bijektion*

$$\begin{array}{ccc} \{\text{Unterkörper } K \subset F\} & \xrightarrow{\sim} & \{q \in \mathbb{N} \mid \exists d \in \mathbb{N} \text{ mit } q^d = |F|\} \\ K & \mapsto & |K| \end{array}$$

3.7.14. 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 4.3.3 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 betrachten wir schließlich die Identität

$$(Y - 1)(Y^{c-1} + Y^{c-2} + \dots + 1) = Y^c - 1$$

Aus dieser Identität folgt

$q - 1$	teilt	$q^r - 1$	für beliebige natürliche Zahlen q und r ,
$X^a - 1$	teilt	$X^{ca} - 1$	für beliebiges a ,
$X^{q-1} - 1$	teilt	$X^{q^r-1} - 1$	nach den beiden vorhergehenden Punkten,
$X^q - X$	teilt	$X^{q^r} - X$	nach Multiplikation mit X .

Ist nun q eine Primzahlpotenz und $r \geq 1$ eine natürliche Zahl, so zerfällt also das Polynom $X^q - X$ über \mathbb{F}_{q^r} in Linearfaktoren und nach 3.7.11 bilden dann seine Nullstellen einen Unterkörper von \mathbb{F}_{q^r} mit q Elementen. □

Übungen

Übung 3.7.15. Ein endlicher Körper kann nie algebraisch abgeschlossen sein.

Übung 3.7.16. 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 3.7.17 (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

$$(X^d P^{-n})_{n \geq 1, \text{grad } P > d \geq 0}$$

für $P \in k[X]$ normiert und irreduzibel zuzüglich drittens der 1 aus $k(X)$. Für den Fall k algebraisch abgeschlossen vergleiche man [LA1] 4.6.11. Sonst ziehe man sich für den Beweis der linearen Unabhängigkeit mit 3.7.4 auf den Fall von in Linearfaktoren zerfallenden Nennern zurück.

Ergänzende Übung 3.7.18. Man bestimme die Partialbruchzerlegung, also die Darstellung in der Basis aus 3.7.17, von $(1 + x^4)^{-1}$ in $\mathbb{R}(X)$.

Übung 3.7.19. Man zeige, daß es im Polynomring über einem endlichen Körper irreduzible Polynome von jedem positiven Grad gibt.

Ergänzende Übung 3.7.20. Geben Sie Verknüpfungstabellen für die Addition und die Multiplikation eines Körpers mit vier Elementen an.

3.8 Zerfällungskörper

Definition 3.8.1. Sei K ein Körper und $P \in K[X] \setminus 0$ 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 3.8.2 (Existenz und Eindeutigkeit von Zerfällungskörpern). *Seien K ein Körper und $P \in K[X] \setminus 0$ 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.*

3.8.3. Die Existenz eines Zerfällungskörpers folgt leicht aus Satz 3.7.4, 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 Existenz zeigen wir erst nach dem Beweis von 3.8.12.

3.8.4 (**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 3.8.5. Sei K ein Kring. Unter einem K -**Kring** verstehen wir ein Paar (L, i) bestehend aus einem Kring L und einem Ringhomomorphismus $i : K \rightarrow L$. Ist (M, j) ein weiterer K -Kring, so verstehen wir unter einem **Homomorphismus von K -Kringen** $L \rightarrow M$ einen Ringhomomorphismus $\varphi : L \rightarrow M$ mit $\varphi \circ i = j$. Alternativ sprechen wir auch von einem **Homomorphismus über K** . Die Menge aller solchen Homomorphismen notieren wir

$$\text{Kring}^K(L, M)$$

Einen bijektiven Ringhomomorphismus über K nennen wir auch einen **Isomorphismus von K -Kringen** oder einen **Isomorphismus über K** .

Beispiel 3.8.6. Unser Satz [LA1] 4.3.5 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

$$\text{Kring}^K(K[X], R) \xrightarrow{\sim} R$$

liefert. Die Umkehrabbildung ordnet jedem b den durch das Einsetzen von b erklärten Ringhomomorphismus $K[X] \rightarrow R$ zu.

Definition 3.8.7. 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 3.2.3 angedeutet. Wenn wir pedantisch sein wollen, sprechen wir auch 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 $j : K \rightarrow M$ ein weiterer Körperhomomorphismus, so nennen wir einen Körperhomomorphismus $L \rightarrow M$ über K auch eine **Ausdehnung** von j auf L und benutzen Notationen wie zum Beispiel $\tilde{j} : L \rightarrow M$.

Ergänzung 3.8.8. Ist K ein Körper, so ist jeder K -Kring im Sinne der vorhergehenden Definition 3.8.5 eine K -Kringalgebra im Sinne unserer Definition [LA2]

8.8.1, und jede K -Kringalgebra A wird umgekehrt durch den einzigen Homomorphismus $K \rightarrow A$ von K -Kringalgebren zu einem K -Kring. Diese beiden Konzepte sind also äquivalent.

Proposition 3.8.9 (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*

$$\begin{array}{ccc} \text{Kring}^K(K(\alpha), M) & \xrightarrow{\sim} & \{\beta \in M \mid \text{Irr}(\alpha, K)(\beta) = 0\} \\ \varphi & \mapsto & \varphi(\alpha) \end{array}$$

3.8.10. In der Formulierung dieser Proposition haben wir beim Auswerten des Polynoms $\text{Irr}(\alpha, K) \in K[X]$ auf $\beta \in M$ stillschweigend die Elemente von K mit ihren Bildern in M unter j identifiziert. Dieselbe abkürzende Notation ist gemeint, wenn wir im gleich folgenden Beweis den Teilkörper $K(\beta) \subset M$ bilden.

Beispiel 3.8.11. Wir haben im Fall $K = \mathbb{Q}$, $M = \mathbb{C}$, $\alpha = i$ etwa

$$\begin{array}{ccc} \text{Kring}^{\mathbb{Q}}(\mathbb{Q}(i), \mathbb{C}) & \xrightarrow{\sim} & \{\beta \in \mathbb{C} \mid \beta^2 + 1 = 0\} \\ \varphi & \mapsto & \varphi(i) \end{array}$$

Beweis. Sicher induziert das Auswerten eine injektive Abbildung zwischen den angegebenen Mengen und wir müssen nur noch die Surjektivität zeigen. Nach 3.3.3 haben wir jedoch für jede Nullstelle β von $\text{Irr}(\alpha, K)$ in M Isomorphismen

$$K(\alpha) \xleftarrow{\sim} K[X]/\langle \text{Irr}(\alpha, K) \rangle \xrightarrow{\sim} K(\beta)$$

mit $\bar{X} \mapsto \alpha$ bzw. $\bar{X} \mapsto \beta$, und diese liefern unmittelbar die gesuchte Einbettung $K(\alpha) \xrightarrow{\sim} K(\beta) \subset M$ mit $\alpha \mapsto \beta$. \square

Proposition 3.8.12 (Ausdehnbarkeitskriterium). *Seien $K(\alpha_1, \dots, \alpha_n)$ eine endliche Erweiterung eines Körpers K und $j : K \hookrightarrow M$ eine Einbettung von K in einen Körper M derart, daß die Minimalpolynome $\text{Irr}(\alpha_\nu, K)$ aller unserer Erzeuger α_ν in $M[X]$ vollständig in Linearfaktoren zerfallen. So läßt sich die Einbettung j ausdehnen zu einer Einbettung $\tilde{j} : K(\alpha_1, \dots, \alpha_n) \hookrightarrow M$, im Diagramm*

$$\begin{array}{ccc} K & \xrightarrow{\quad} & K(\alpha_1, \dots, \alpha_n) \\ & \searrow & \downarrow \\ & & M \end{array}$$

Beweis. Mit der Proposition 3.8.9 über das Ausdehnen auf primitive Erweiterungen sehen wir, daß das Einschränken eine Kette von Surjektionen der Gestalt

$$\text{Ring}^K(K, M) \leftarrow \text{Ring}^K(K(\alpha_1), M) \leftarrow \dots \leftarrow \text{Ring}^K(K(\alpha_1, \dots, \alpha_n), M)$$

liefert. \square

3.8.13. Man beachte, daß es in obigem Satz nicht ausreicht, nur zu fordern, daß die Minimalpolynome $\text{Irr}(\alpha_\nu, K)$ jeweils eine Nullstelle in M haben: Dann könnten wir zwar den ersten Schritt in obigem Argument noch gehen, aber das Minimalpolynom von α_2 über $K(\alpha_1)$ ist im allgemeinen nur noch ein Teiler des Minimalpolynoms $\text{Irr}(\alpha_2, K)$ von α_2 über K , und auch wenn $\text{Irr}(\alpha_2, K)$ eine Nullstelle in M hat, muß das für $\text{Irr}(\alpha_2, K(\alpha_1))$ noch lange nicht gelten – man denke zum Beispiel an $K = \mathbb{Q}$, $M = \mathbb{R}$, $\alpha_1 = \sqrt[3]{2}$ und $\alpha_2 = \exp(2\pi i/3)\sqrt[3]{2}$. Zerfällt jedoch $\text{Irr}(\alpha_2, K)$ vollständig in M , so auch $\text{Irr}(\alpha_2, K(\alpha_1))$, und zerfällt allgemeiner $\text{Irr}(\alpha_i, K)$ vollständig in M , so auch $\text{Irr}(\alpha_i, K(\alpha_1, \dots, \alpha_{i-1}))$.

Vorschau 3.8.14. Diese Proposition wird auch unmittelbar aus der allgemeineren und vielleicht etwas „glatteren“ Aussage 3.11.7 über Einbettungen in den algebraischen Abschluß folgen: Mit 3.11.3.2 dürfen wir M algebraisch über K annehmen. Nach 3.11.7 läßt sich M dann über K in einen algebraischen Abschluß \bar{K} von K einbetten. Wieder nach 3.11.7 können wir auch $K(\alpha_1, \dots, \alpha_n)$ über K in \bar{K} einbetten, und nach Annahme liegt sein Bild dann notwendig im Bild von M .

Beweis der Eindeutigkeit von Zerfällungskörpern 3.8.2. Proposition 3.8.12 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. \square

Satz 3.8.15 (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*

$$|\text{Kring}^K(L, M)| \leq [L : K]$$

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 3.8.9 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 . \square

Zweiter Beweis. Seien $\sigma_1, \dots, \sigma_r$ paarweise verschiedene K -lineare Körperhomomorphismen $L \rightarrow M$. Wäre $\lambda_1, \dots, \lambda_s$ ein Erzeugendensystem des K -Vektorraums L mit weniger Elementen $s < r$, so gäbe es $a_1, \dots, a_r \in M$ nicht alle Null mit $\sum_i a_i \sigma_i(\lambda_j) = 0$ für alle j . Dann aber wäre $\sum_i a_i \sigma_i$ die Nullabbildung im Widerspruch zu Satz 3.8.16 über die lineare Unabhängigkeit der Charaktere $\sigma_1, \dots, \sigma_r$ im M -Vektorraum $\text{Ens}(L^\times, M)$. \square

Satz 3.8.16 (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.

3.8.17. 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 $\text{Grp}(G, M^\times)$ eine linear unabhängige Teilmenge des M -Vektorraums $\text{Ens}(G, M)$ ist. Sei in der Tat sonst

$$a_1\chi_1 + a_2\chi_2 + \dots + a_n\chi_n = 0$$

eine nichttriviale lineare Relation kürzestmöglicher Länge mit $a_i \in M$ und $\chi_i : G \rightarrow M^\times$ 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 $g \in G$ die Gleichungen

$$\begin{aligned} a_1\chi_1(g)\chi_1 + a_2\chi_2(g)\chi_2 + a_n\chi_n(g)\chi_n &= 0 \\ a_1\chi_1(g)\chi_1 + a_2\chi_1(g)\chi_2 + a_n\chi_1(g)\chi_n &= 0 \end{aligned}$$

und deren Differenz wäre eine kürzere und wegen $\chi_1(g) \neq \chi_2(g)$ nichttriviale Linearkombination im Widerspruch zu unserer Annahme. \square

Definition 3.8.18. Eine Körpererweiterung heißt **algebraisch**, wenn alle Elemente der Erweiterung algebraisch sind über dem Grundkörper.

3.8.19. Jede endliche Körpererweiterung ist also nach 3.4.7 auch algebraisch. Genauer ist nach 3.4.7 eine Körpererweiterung algebraisch genau dann, wenn sie eine Vereinigung von Teilerweiterungen ist, die jeweils endlich sind über dem Grundkörper.

Definition 3.8.20. 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.

3.8.21 (**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 3.8.22. $\mathbb{Q}(\sqrt{2})$ 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 3.8.23 (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. $1 \Rightarrow 2$. Ist L normal über K und erzeugt von $\alpha_1, \dots, \alpha_r$, so ist L ein Zerfällungskörper für das Produkt der Minimalpolynome $\text{Irr}(\alpha_i, K)$ 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 weiteren Körper M haben alle Fortsetzungen von j zu Einbettungen $\varphi, \psi : L \hookrightarrow M$ dasselbe Bild, in Formeln $\varphi(L) = \psi(L) \quad \forall \varphi, \psi \in \text{Kring}^K(L, M)$.

Jetzt zeigen wir $2 \Rightarrow 3 \Rightarrow 1$ und beginnen mit $2 \Rightarrow 3$. 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 $3 \Rightarrow 1$. 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 $L = K(\alpha, \beta_1, \dots, \beta_n)$. Dann wählen wir für M eine Körpererweiterung von L , in der sowohl das Minimalpolynom von α als auch die Minimalpolynome aller β_i vollständig in Linearfaktoren zerfallen. Für jede Nullstelle $\alpha_\nu \in M$ von P können wir unsere Einbettung $K \hookrightarrow M$ zunächst nach 3.8.9 fortsetzen zu einer Einbettung $K(\alpha) \hookrightarrow M$ mit $\alpha \mapsto \alpha_\nu$ und dann nach 3.8.12 weiter zu einer Einbettung $\varphi_\nu : L \hookrightarrow M$. Jede Nullstelle von P in M liegt also in $\varphi_\nu(L)$ für geeignetes φ_ν , und da alle diese Bilder $\varphi_\nu(L)$ nach Annahme übereinstimmen, in Formeln $\varphi_\nu(L) = L$ für alle φ_ν , zerfällt unser Polynom P schon über L vollständig in Linearfaktoren. □

Proposition 3.8.24 (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 $\alpha_1, \dots, \alpha_r$ 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 . \square

Übungen

Übung 3.8.25. Man zeige, daß eine algebraische Körpererweiterung eines unendlichen Körpers stets dieselbe Kardinalität hat wie der Ausgangskörper. Diese Erkenntnis wird bei einer Konstruktion des algebraischen Abschlusses benötigt werden.

Übung 3.8.26. 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 $[L : K] \leq n!$.

Übung 3.8.27. 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 3.8.28. Man formuliere präzise und zeige, daß es bis auf nichteindeutigen Isomorphismus genau ein minimales N wie in Proposition 3.8.24 gibt. Dies N heißt die **normale Hülle von L über K** .

Übung 3.8.29. Jede endliche Körpererweiterung von \mathbb{R} ist isomorph im Sinne von 3.8.5 zu \mathbb{R} oder \mathbb{C} . Hinweis: \mathbb{C} ist bekanntlich algebraisch abgeschlossen.

Ergänzende Übung 3.8.30. 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 3.8.31. 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 3.8.32. 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 $\mathbb{Q}(\zeta) \rightarrow \mathbb{Q}(\zeta)$ mit $\zeta \mapsto \xi$. Hinweis: Irreduzibilität des p -ten Kreisteilungspolynoms 2.8.4.

3.9 Vielfachheit von Nullstellen

3.9.1. Unter einer **mehrfachen Nullstelle** eines Polynoms mit Koeffizienten in einem Körper oder allgemeiner einem kommutativen Integritätsbereich verstehen wir eine Nullstelle mit der Vielfachheit Zwei oder mehr. Sagen wir, ein Polynom habe in irgendeinem vorgegebenen Körper „mehrfache Nullstellen“, so ist gemeint, daß es mindestens eine mehrfache Nullstelle haben soll. Eigentlich wäre es gemäß unserer allgemeinen Konventionen [GR] 2.4.3 präziser, zu sagen, es habe „eine mehrfache Nullstelle“, aber das ist unüblich: Hier fürchtet man offensichtlich das Mißverständnis „genau eine“ mehr als in anderen mathematischen Zusammenhängen und zieht es vor, den Fall genau einer mehrfachen Nullstelle gedanklich in den Plural „mehrfache Nullstellen“ mit einzuschließen. Möglicherweise rührt diese Sprechweise auch daher, daß man eine mehrfache Nullstelle gerne denkt als „mehrere Nullstellen, die zusammenfallen“. Das Nullpolynom hat mehrfache Nullstellen, bei ihm haben ja sogar alle Nullstellen die Vielfachheit ∞ .

Satz 3.9.2 (Irreduzible Polynome haben selten mehrfache Nullstellen). *Seien $K \subset L$ Körper. Gilt $\text{char } K = 0$ oder ist K endlich, so hat ein K -irreduzibles Polynom $P \in K[X]$ keine mehrfachen Nullstellen in L .*

3.9.3. Wir werden in 3.9.15 und 3.9.21 sogar noch etwas allgemeinere Aussagen zeigen. Das braucht jedoch einige Vorbereitungen.

Beispiel 3.9.4 (Ein irreduzibles Polynom mit mehrfachen Nullstellen). Über Körpern positiver Charakteristik können auch irreduzible Polynome mehrfache Nullstellen haben. Um ein Beispiel anzugeben, beachten wir zunächst, daß für K ein Körper positiver Charakteristik $\text{char } K = p > 0$ 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 irreduziblen Faktoren das Minimalpolynom $\text{Irr}(\sqrt[p]{T}, K)$ sein muß, so daß unser Polynom notwendig eine Potenz dieses Minimalpolynoms ist. Das läßt aber wegen p prim nur die Möglichkeit $X^p - T = \text{Irr}(\sqrt[p]{T}, K)$ offen. Dies Polynom ist also irreduzibel über K und hat in seinem Zerfällungskörper mehrfache Nullstellen, genauer eine einzige Nullstelle $\sqrt[p]{T}$ der Vielfachheit p .

Definition 3.9.5. Für ein Polynom $P = a_n X^n + \dots + a_2 X^2 + a_1 X + a_0$ mit Koeffizienten in einem beliebigen Ring R definieren wir seine **Ableitung** oder genauer seine **formale Ableitung** $P' \in R[X]$ durch die Vorschrift

$$P' := n a_n X^{n-1} + \dots + 2 a_2 X + a_1$$

Lemma 3.9.6 (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 $P = X^i$ und $Q = X^j$ zurückziehen, in dem man die Formel leicht explizit prüft. \square

Lemma 3.9.7 (Ableitung und mehrfache Nullstellen). Ist K ein Körper, $g \in K[X]$ ein Polynom und $\alpha \in K$ eine Nullstelle von g , so ist α genau dann eine mehrfache Nullstelle von g , wenn auch die Ableitung g' von g bei α verschwindet.

Beispiel 3.9.8. Unser Polynom $X^p - T$ mit Koeffizienten in $\mathbb{F}_p(T)$ hat nach 3.9.4 in seinem Zerfällungskörper $\mathbb{F}_p(\sqrt[p]{T})$ nur eine einzige Nullstelle der Vielfachheit p . In der Tat verschwindet dort auch seine Ableitung, die ist nämlich schlicht das Nullpolynom.

Beweis. Ist $g = (x - \alpha)^2 f$, so folgt mit der Produktregel 3.9.6 leicht $g'(\alpha) = 0$. Gilt umgekehrt $g(\alpha) = g'(\alpha) = 0$ und schreiben wir $g = (x - \alpha)h$, so folgt wieder mit der Produktregel 3.9.6 aus $g'(\alpha) = 0$ schon $h(\alpha) = 0$. \square

3.9.9. Gegeben eine Menge von Polynomen in einer Veränderlichen mit Koeffizienten einem Körper, nicht alle Null, besitzt das von unserer Menge erzeugte Ideal genau einen normierten Erzeuger. Er ist offensichtlich unter allen normierten gemeinsamen Teilern aller Polynome unserer Menge derjenige von größtmöglichem Grad. Wir nennen ihn den **normierten größten gemeinsamen Teiler** unserer Menge von Polynomen. Man kann ihn, analog wie in [LA1] 3.4.18 im Fall der ganzen Zahlen erklärt, mit dem euklidischen Algorithmus auch unschwer explizit berechnen.

Proposition 3.9.10 (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 größte gemeinsame Teiler von f und g in $K[X]$ ist auch der normierte größte gemeinsame Teiler von f und g in $L[X]$.

Beweis. 1. Schreiben wir $f = qg + r$ mit $\text{grad } r < \text{grad } g$, 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 bzw. d_L der normierte größte gemeinsame Teiler von f und g in $K[X]$ bzw. in $L[X]$ nach 3.9.9. Natürlich ist d_K auch ein gemeinsamer Teiler in $L[X]$, also gilt $d_K | d_L$. 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 $d_L = d_K$. \square

3.9.11. Ich erinnere an unsere Definition [LA1] 4.2.16: Zwei Elemente eines Krings oder allgemeiner die Elemente einer beliebigen Teilmenge eines Krings heißen **teilerfremd**, wenn sie außer Einheiten keine gemeinsamen Teiler haben.

Lemma 3.9.12 (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.

3.9.13. Bei der Bedingung „teilerfremd“ kommt es wegen 3.9.10 nicht darauf an, ob wir sie in unserem ursprünglichen Polynomring oder im Polynomring mit Koeffizienten in einem beliebigen Erweiterungskörper verstehen.

Beweis. Sei K unser Körper und $P \in K[X] \setminus 0$ 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 von P und P' in $L[X]$ und es folgt $\langle P, P' \rangle \neq \langle 1 \rangle$.

3 \Rightarrow 1. Wir betrachten wir den Zerfällungskörper M des Produkts PP' beziehungsweise im Fall $P' = 0$ den Zerfällungskörper M von P . 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 3.9.7. \square

3.9.14. 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 3.9.15 (Irreduzible Polynome mit mehrfachen Nullstellen). *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 $\text{char } K = p > 0$ 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 3.9.12 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 3.9.7 eine mehrfache Nullstelle unseres Polynoms.

$4 \Rightarrow 1$. Das scheint mir offensichtlich. □

Definition 3.9.16. Ein Element α eines Körpers L heißt **separabel über einem Teilkörper** $K \subset L$, wenn es algebraisch und eine einfache Nullstelle seines Minimalpolynoms ist. Eine Körpererweiterung L/K heißt **separabel**, wenn jedes Element von L separabel ist über K .

3.9.17. Nach 3.9.15 ist in anderen Worten ein Element eines Körpers separabel über einem Teilkörper genau dann, wenn es über diesem algebraisch ist mit separablem Minimalpolynom.

Beispiel 3.9.18. In Charakteristik Null ist jede algebraische Körpererweiterung separabel nach 3.9.15. Jede algebraische Körpererweiterung eines endlichen Körpers ist separabel nach 3.9.19 und 3.9.21. Nicht separabel ist $\mathbb{F}_p(\sqrt[p]{T})$ über $\mathbb{F}_p(T)$.

Definition 3.9.19. Ein Körper heißt **vollkommen**, wenn er entweder die Charakteristik Null hat oder aber für $p = \text{char } K > 0$ die Abbildung $x \mapsto x^p$ eine Surjektion $K \rightarrow K$ ist. Zum Beispiel ist jeder endliche Körper vollkommen, denn jeder Körperhomomorphismus ist injektiv.

Ergänzung 3.9.20. Für „vollkommen“ sagt man in diesem Zusammenhang auf Englisch **perfect** und auf Französisch **parfait**.

Satz 3.9.21 (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 $\text{char } K = 0$ haben wir bereits durch 3.9.2 oder besser 3.9.15 erledigt. Sei also ohne Beschränkung der Allgemeinheit $\text{char } K = p > 0$ und $P \in K[X]$ irreduzibel. Wäre P nicht separabel, so hätte P nach 3.9.15 die Form $P = b_n(X^p)^n + \dots + b_1X^p + b_0$. Nehmen wir aber nun $a_n, \dots, a_0 \in K$ mit $a_i^p = b_i$ und betrachten $Q = a_nX^n + \dots + a_0$, so folgt $P = Q^p$ im Widerspruch zur Irreduzibilität von P . \square

Satz 3.9.22 (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 $|\text{Kring}^K(L, N)| = [L : K]$;
4. Es gibt mindestens eine Körpererweiterung N/K von K mit der Eigenschaft $|\text{Kring}^K(L, N)| = [L : K]$.

Beweis. Zeigen wir $1 \Leftrightarrow 2$ für endliche Erweiterungen, so folgt es mit 3.2.6 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 3.8.9 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 3.8.9 für jedes N weniger als $[K(\alpha) : K]$ Ausdehnungen von $K \hookrightarrow N$ zu einer Einbettung $K(\alpha) \hookrightarrow N$ und damit nach Satz 3.8.15 über die maximal mögliche Zahl von Ausdehnungen notwendig auch weniger als $[L : K]$ Ausdehnungen von $K \hookrightarrow N$ zu einer Einbettung $L \hookrightarrow N$. \square

Ergänzung 3.9.23 (Die Diskriminante als Determinante). Ich behaupte für die $a_i \in \mathbb{Z}[\zeta_1, \dots, \zeta_n]$, die gegeben werden durch die Identität $T^n + a_1T^{n-1} + \dots + a_n = (T + \zeta_1) \dots (T + \zeta_n)$, daß die Determinante der nebenstehenden Matrix M gegeben wird durch die Formel

$$\det M = \prod_{i \neq j} (\zeta_i - \zeta_j)$$

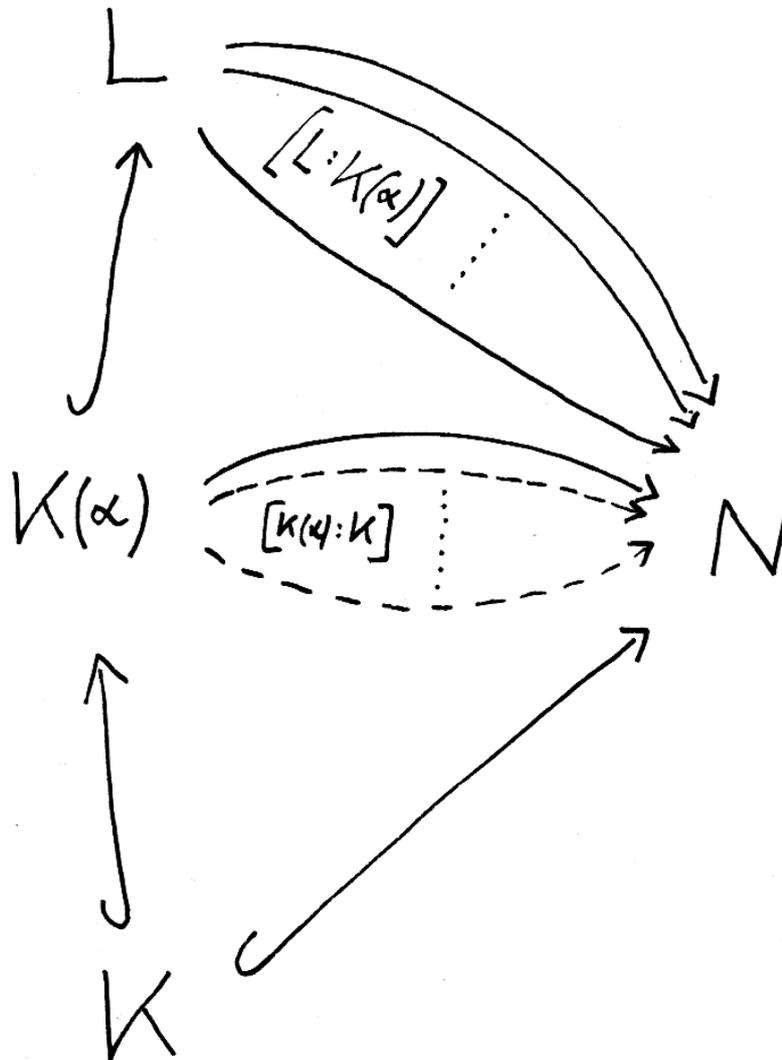


Illustration zum Beweis von 3.9.22, Implikation $2 \Rightarrow 3$. Die durchgezogenen Pfeile ganz oben sollen mögliche Erweiterungen des durchgezogenen Pfeils in der Mitte andeuten. Jeder andere der $[K(\alpha) : K]$ Pfeile in der Mitte besitzt ganz genauso $[L : K(\alpha)]$ Erweiterungen nach ganz oben, nur sind diese nicht eingezeichnet.

und folglich genau unsere Diskriminante aus 2.9.14 ist. Um das zu zeigen, beachten wir zunächst, daß beide Seiten symmetrische Polynome sind und daß zumindest in $\mathbb{Q}[\zeta_1, \dots, \zeta_n]$ alle $(\zeta_i - \zeta_j)$ nach 3.9.12 und [LA1] 4.4.5 und 2.10.10 das Polynom $(\det M)$ teilen müssen. 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 [LA1] 4.4.5 folglich ein weiteres Mal durch $(\zeta_i - \zeta_j)$ teilbar sein. Mithin ist $\det M$ in $\mathbb{Q}[\zeta_1, \dots, \zeta_n]$ 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 ζ_2, \dots, ζ_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 $(T + \zeta_1) \dots (T + \zeta_n) = T^n - 1$ 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 $(t^n - 1)/(t - 1) = t^{n-1} + \dots + t + 1$. 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 3.9.24 (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 [AN1] 5.3.10.

Ergänzende Übung 3.9.25. Seien P, Q nicht konstante Polynome mit Koeffizienten in einem algebraisch abgeschlossenen Körper k der Charakteristik Null. Man

$$\begin{pmatrix}
 1 & a_1 & \dots & a_m & & \\
 & 1 & a_1 & \dots & a_m & \\
 & & & 1 & a_1 & \dots & a_m \\
 n & (n-1)a_1 & \dots & a_{n-1} & & & \\
 & n & (n-1)a_1 & \dots & a_{n-1} & & \\
 & & & & & n & (n-1)a_1 & \dots & a_{n-1}
 \end{pmatrix}$$

Die Determinante dieser Matrix stimmt überein mit der Diskriminante des Polynoms $T^n + a_1 T^{n-1} + \dots + a_n$, wie sie in 2.9.15 für jedes normierte Polynom erklärt wird. Im übrigen ist diese Determinante im wesentlichen die Resultante unseres Polynoms und seiner Ableitung.

zeige: Haben unsere beiden Polynome dieselben Nullstellen und dieselben „Einstellen“, gelten also in Formeln für die zugehörigen Abbildungen $P, Q : k \rightarrow k$ die Gleichheiten $P^{-1}(0) = Q^{-1}(0)$ und $P^{-1}(1) = Q^{-1}(1)$ von Teilmengen von k , so folgt $P = Q$. Hinweis: Für d das Maximum der Grade unserer Polynome zeige man $d \geq |P^{-1}(1) \cup P^{-1}(0)|$. Es folgt, daß P' viele Nullstellen haben muß.

Übung 3.9.26. Man zeige: 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 3.9.27. Seien $M \supset L \supset K$ Körper. Man zeige: 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 3.9.22, insbesondere $4 \Rightarrow 1$, mit N einer Vergrößerung von M zu einer normalen Erweiterung von K .

Ergänzende Übung 3.9.28. Man zeige: 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 3.9.27.

Übung 3.9.29. 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: 3.9.15.

Ergänzende Übung 3.9.30. 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 3.9.27.

Vorschau 3.9.31. 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 4.1.30.

Übung 3.9.32. Man zeige für jede rein inseparable algebraische Körpererweiterung L/K und jede weitere Körpererweiterung N/K die Abschätzung

$$|\text{Kring}^K(L, N)| \leq 1$$

Ergänzende Übung 3.9.33. Gegeben eine algebraische Körpererweiterung L/K erklärt man ihren **Separabilitätsgrad** als $[L : K]_s := [S : K]$ für $S \subset L$ den separablen Abschluß von K in L .

1. Gegeben eine endliche Körpererweiterung L/K zeige man

$$[L : K]_s := \sup_{N/K} |\text{Kring}^K(L, N)|$$

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: [3.9.30](#) und [3.9.32](#).

2. Man zeige, daß der Separabilitätsgrad im Fall endlicher Körpererweiterungen multiplikativ ist, daß also für $M/L/K$ endliche Erweiterungen gilt

$$[M : K]_s = [M : L]_s [L : K]_s$$

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 $[L : K]_s = |\text{Kring}^K(L, N)|$.

Übung 3.9.34 (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 $r \in \mathbb{N}$ isomorph zur Körpererweiterung $k(X)/k(T)$ gegeben durch $X \mapsto T^{p^r}$. 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 3.9.35. Gegeben ein Körper k induzieren die Einbettungen $k[X] \hookrightarrow k[[X]] \hookrightarrow k((X))$ einen Ringhomomorphismus und nach [\[LA1\] 4.6.5](#) eine Einbettung $k(X) \hookrightarrow k((X))$. Man zeige, daß diese Einbettung im Fall $\text{char } k = 0$ 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.

3.10 Satz vom primitiven Element

Lemma 3.10.1 (Überdeckung durch affine Teilräume). *Ein Vektorraum oder allgemeiner ein affiner Raum über einem unendlichen Körper kann nicht durch endlich viele echte affine Teilräume überdeckt werden.*

Ergänzung 3.10.2. Unser Argument zeigt allgemeiner: Ein affiner Raum über einem Körper \mathbb{F} mit mehr als n Elementen, in Formeln $|\mathbb{F}| > n$, kann nie die Vereinigung von n echten affinen Teilräumen sein.

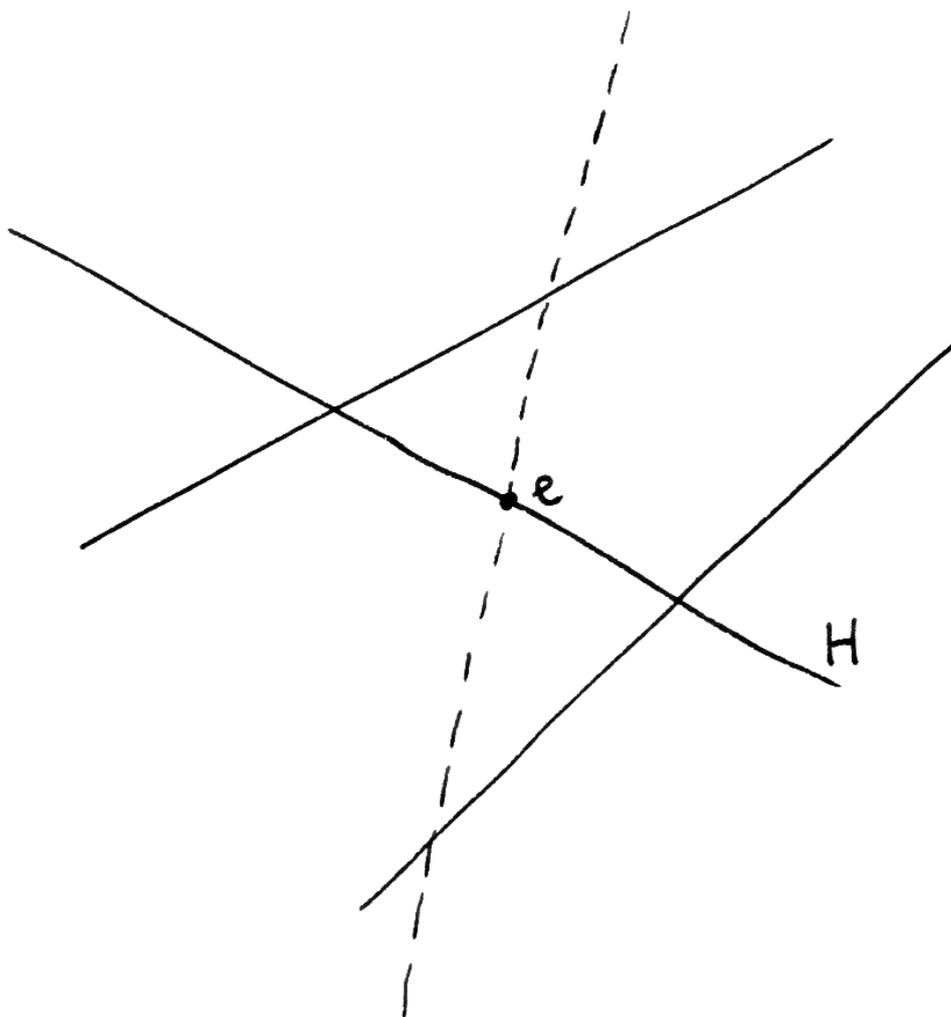


Illustration zum Beweis von [3.10.1](#)

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. \square

Lemma 3.10.3 (Überdeckung durch Untervektorräume). *Ein Vektorraum kann nie durch endlich viele Untervektorräume von unendlicher Kodimension überdeckt werden.*

Beweis. Sei sonst $V = U_1 \cup \dots \cup U_r$ ein Gegenbeispiel mit r kleinstmöglich. Natürlich gilt notwendig $r \geq 2$. Ganz allgemein liefern die offensichtlichen Abbildungen Isomorphismen $U_1/(U_1 \cap U_i) \xrightarrow{\sim} (U_1 + U_i)/U_i$. Wären diese beiden Räume für ein $i > 1$ endlichdimensional, so hätte mit U_i auch $U_1 + U_i$ unendliche Kodimension und wir hätten ein noch kleineres Gegenbeispiel gefunden. Das kann nicht sein, also haben auch alle $(U_1 \cap U_i)$ mit $i > 1$ unendliche Kodimension in U_1 und können, wieder wegen der Minimalität unseres Gegenbeispiels, U_1 nicht überdecken. In Formeln folgt

$$U_1 \not\subset \bigcup_{i>1} U_i$$

Wählen wir eine Ursprungsgerade G , so können aus demselben Grund auch die Untervektorräume $U_i + G$ für $i > 1$ nicht U_1 überdecken. Wählen wir nun G mit $G \cap U_1 = 0$ und $g \in G \setminus 0$, so können die $U_i + G$ für $i > 1$ den affinen Teilraum $g + U_1$ ebensowenig überdecken, und damit kann die Vereinigung aller U_i unmöglich ganz V sein. \square

Korollar 3.10.4 (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, und wir wissen bereits aus 3.10.1, daß ein \mathbb{Q} -Vektorraum nicht durch endlich viele echte Untervektorräume überdeckt werden kann. \square

Beweis im Fall eines endlichen Körpers. Ein endlicher Körper kann nicht durch echte Teilkörper überdeckt werden, da seine multiplikative Gruppe nach [LA2] 4.4.17 zyklisch ist. \square

Beweis im Fall eines unendlichen Körpers 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 unserem Lemma 3.10.3, nach dem ein

Vektorraum nicht durch endlich viele Untervektorräume von unendlicher Kodimension überdeckt werden kann. \square

Proposition 3.10.5 (Unterscheidung von Körperhomomorphismen). *Gegeben Körpererweiterungen L/K und M/K desselben Grundkörpers K und endliche viele paarweise verschiedene Homomorphismen $\sigma_1, \dots, \sigma_r \in \text{Kring}^K(L, M)$ 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 ist für $i \neq j$ ist L_{ij} sogar ein echter Teilkörper von L . Da ein Körper nach 3.10.4 nicht durch endlich viele echte Teilkörper überdeckt werden kann, gibt es stets ein $\alpha \in L \setminus \bigcup_{i \neq j} L_{ij}$. \square

Korollar* 3.10.6 (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 3.10.4 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

$$\left\{ \begin{array}{l} \text{Zwischenkörper } M, \\ K \subset M \subset K(\alpha) \end{array} \right\} \rightarrow \left\{ \begin{array}{l} \text{Normierte Teiler in } L[X] \\ \text{des Minimalpolynoms } \text{irr}(\alpha, K) \end{array} \right\}$$

$$M \quad \mapsto \quad \text{irr}(\alpha, M)$$

Es reicht zu zeigen, daß sie injektiv ist. In der Tat wird aber M über K bereits von den Koeffizienten des Minimalpolynoms $\text{irr}(\alpha, M)$ erzeugt, denn für den von diesen Koeffizienten über K erzeugten Teilkörper $M' \subset M$ gilt $[L : M'] = \text{grad}(\text{Irr}(\alpha, M)) = [L : M]$. Da jedes Polynom nur endlich viele normierte Teiler besitzt, folgt die Behauptung. \square

Satz* 3.10.7 (vom primitiven Element). *Ist L/K eine endliche separable Körpererweiterung, so gibt es ein Element $\alpha \in L$ mit $L = K(\alpha)$.*

Beweis. Nach 3.8.24 können wir L vergrößern zu einer normalen Erweiterung N von K . Wegen der Separabilität von L/K gibt es dann nach 3.9.22 genau $[L : K]$ Körperhomomorphismen über K von L nach N , in Formeln

$$|\text{Kring}^K(L, N)| = [L : K]$$

Nach 3.10.5 gibt es Elemente $\alpha \in L$ derart, daß die $\sigma(\alpha)$ für $\sigma \in \text{Kring}^K(L, N)$ paarweise verschieden sind. Gegeben solch ein α liefert die Restriktion eine Injektion $\text{Kring}^K(L, N) \hookrightarrow \text{Kring}^K(K(\alpha), N)$, 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

$$[L : K] = |\text{Kring}^K(L, N)| \leq |\text{Kring}^K(K(\alpha), N)| \leq [K(\alpha) : K] \leq [L : K] \quad \square$$

Lemma* 3.10.8 (Überdeckung durch Nebenklassen). *Eine abelsche Gruppe kann nicht durch endlich viele Nebenklassen zu Untergruppen von unendlichem Index überdeckt werden.*

Ergänzung 3.10.9. Dies Lemma ist eine gemeinsame Verallgemeinerung unserer beiden Lemmata 3.10.1 und 3.10.3 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 $H_0, H_1, \dots, H_n \subset G$ unsere überdeckenden Nebenklassen. Die zugehörigen Untergruppen notieren wir $\vec{H}_0, \vec{H}_1, \dots, \vec{H}_n$. 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 $g + \vec{H}_0 \subset H_1 \cup H_2 \cup \dots \cup H_n$ alias

$$\vec{H}_0 \subset \bigcup_{i=1}^n \left((H_i - g) \cap \vec{H}_0 \right)$$

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, und dieser Widerspruch zeigt das Lemma. \square

3.11 Algebraischer Abschluß*

3.11.1. 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 das Zorn'sche Lemma [LA1] 1.9.8 benötigt, dessen Herleitung aus dem a priori anschaulich besser motivierten Auswahlaxiom nicht ganz einfach ist. Um die Entwicklung der Grundlagen der Algebra von diesen 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.

3.11.2. Ich erinnere daran, daß eine Körpererweiterung nach 3.8.18 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 3.11.3 (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 $L = K(\alpha_1, \dots, \alpha_n)$. Sind alle α_i algebraisch über K , so sind sie erst recht algebraisch über $K(\alpha_1, \dots, \alpha_{i-1})$. Wir betrachten die Körperkette

$$K \subset K(\alpha_1) \subset K(\alpha_1, \alpha_2) \subset \dots \subset K(\alpha_1, \dots, \alpha_n) = L$$

Da hier alle Schritte endlich sind nach 3.4.7, ist auch L/K endlich nach der Multiplikativität des Grades 3.4.11.

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 3.4.7.

3. Für $\alpha \in M$ betrachten wir die Koeffizienten $\beta_0, \dots, \beta_r \in L$ seines Minimalpolynoms über L . Dann ist α sogar algebraisch über $K(\beta_0, \dots, \beta_r)$. Der Turm von endlichen Körpererweiterungen

$$K \subset K(\beta_0, \dots, \beta_r) \subset K(\beta_0, \dots, \beta_r, \alpha)$$

zeigt damit, daß α algebraisch ist über K . □

Definition 3.11.4. Ein **algebraischer Abschluß** eines Körpers ist eine algebraische Erweiterung unseres Körpers durch einen algebraisch abgeschlossenen Körper.

Satz 3.11.5 (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.*

3.11.6. 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 [LA1] 3.1.4 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 [GR] 3.4.14 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. 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 Menge Ω , deren Kardinalität echt größer ist als die Kardinalität jeder algebraischen Erweiterung von K in dem Sinne, 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 $L \rightarrow \Omega$ stünde damit im Widerspruch zu [GR] 2.3.36, wonach es keine Surjektion $K[X] \times \mathbb{N} \rightarrow \mathcal{P}(K[X] \times \mathbb{N})$ 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 Körperhomomorphismus $\varphi : K \rightarrow M$, bezüglich dessen M algebraisch ist über K . Nach dem Zorn'schen Lemma [LA1] 1.9.8 existiert bezüglich der offensichtlichen Ordnungsrelation ein maximales derartiges Tripel, und bei solch einem maximalen Tripel ist M notwendig algebraisch abgeschlossen: Sonst könnten wir nämlich mit der Kronecker-Konstruktion 3.7.7 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 noch einmal 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 3.11.7 über Ausdehnungen von Körpereinbettungen, die wir im Anschluß beweisen, läßt sich die Identität auf K fortsetzen zu einem Körperhomomorphismus $\varphi : \bar{K} \rightarrow E$. Er ist natürlich 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. \square

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 [KAG] 1.10.3 und [KAG] 1.10.6. Sei K unser Körper. Wir betrachten die Menge $S = K[X] \setminus K$ 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 3.7.4, 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

$$\begin{aligned} \varphi : R &\rightarrow L \\ X_f &\mapsto \alpha_f \end{aligned}$$

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 [KAG] 1.10.3 ein maximales Ideal $\mathfrak{m} \supset \mathfrak{a}$. Dann ist $K_1 = R/\mathfrak{m}$ nach [KAG] 1.10.6 ein Körper, und jedes nichtkonstante Polynom $f \in K[X] \setminus K$ hat eine Nullstelle in K_1 , nämlich die Nebenklasse von X_f . Iterieren wir diese Konstruktion, so erhalten wir ein Kette von Körpern

$$K = K_0 \hookrightarrow K_1 \hookrightarrow K_2 \hookrightarrow \dots$$

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. 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 [TS] 7.1.1 in voller Allgemeinheit kennenlernen können. \square

Proposition 3.11.7 (Ausdehnung von Körpereinbettungen). *Eine Einbettung eines Körpers in einen algebraisch abgeschlossenen Körper läßt sich auf jede algebraische Erweiterung unseres ursprünglichen Körpers ausdehnen.*

3.11.8. 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 $\text{Irr}(\alpha, K)$ 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 $\alpha \in L \setminus M$, und dies α wäre algebraisch über M , mit Minimalpolynom $f \in M[X]$. Die Minimalpolynom hätte eine Nullstelle $\beta \in F$, und nach Proposition 3.8.9 über das Ausdehnen auf primitive Erweiterungen könnten wir dann $M \hookrightarrow F$ fortsetzen zu einer Einbettung $M(\alpha) \rightarrow F$, $\alpha \mapsto \beta$ im Widerspruch zur Maximalität von M . \square

3.11.9. Der algebraische Abschluß des Körpers \mathbb{Q} der rationalen Zahlen ist abzählbar nach 3.8.25.

Beispiel 3.11.10 (Algebraischer Abschluß endlicher Körper). Einen algebraischen Abschluß eines endlichen Primkörpers \mathbb{F}_p können wir wie folgt konstruieren: Wir wählen eine Folge $r(0), r(1), \dots$ von natürlichen Zahlen so, daß jeweils gilt $r(i) | r(i+1)$ und daß jede natürliche Zahl eines unserer Folgenglieder teilt. Dann haben wir nach 3.7.13 Einbettungen $\mathbb{F}_{p^{r(i)}} \hookrightarrow \mathbb{F}_{p^{r(i+1)}}$ und die aufsteigende Vereinigung

$$\bar{\mathbb{F}}_p = \bigcup_{i=0}^{\infty} \mathbb{F}_{p^{r(i)}}$$

ist 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 3.11.5 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.

3.11.11. Ich erinnere an dem Körper $\mathbb{C}((t))$ der formalen Laurentreihen mit komplexen Koeffizienten aus [LA1] 4.3.41.

Satz 3.11.12 (Algebraischer Abschluß des Laurentreihenkörpers). *Der in hoffentlich offensichtlich 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 $\mathbb{C}((t)) = \text{Quot } \mathbb{C}[[t]]$.

3.11.13. 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 3.11.15. \square

3.11.14. 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 von Mengen“ aus [TS] 7.1.8 stützen.

Lemma 3.11.15 (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 $\lambda + t^{1/\gamma}k[[t^{1/\gamma}]]$.*

3.11.16. 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

$$P(X) = a_0 + a_1X + \dots + a_nX^n + \dots + a_NX^N$$

mit $a_0, \dots, a_{n-1} \in tk[[t]]$ und $a_n \in k^\times + tk[[t]]$. Wir verwenden nun die Bewertung $v : k[[t]] \rightarrow \mathbb{N} \sqcup \{\infty\}$, die jeder Potenzreihe a den Grad ihres Terms niedrigster Ordnung $v(a) := \sup\{\nu \mid t^\nu \mid a\}$ zuordnet. Im Spezialfall $v(a_0) = 1$ alias $a_0 \in k^\times t + t^2 k[[t]]$ führt für unsere Nullstelle der Ansatz

$$\mu_1 t^{1/n} + \mu_2 t^{2/n} + \dots$$

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

$$(\mu_1 t^{1/n} + h)^n = \mu_1 t + (n \mu_1^{n-1} t^{(n-1)/n}) h + \dots$$

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 $v(a_0), \dots, v(a_{n-1})$, 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 $a \in k[[t]] \setminus 0$. 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

$$\mu_1 t^\alpha + \mu_2 t^{\alpha+1/(n-k)} + \mu_3 t^{\alpha+2/(n-k)} + \dots$$

für eine Nullstelle mit $\mu_2, \mu_3, \dots \in k$ 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, \dots, l angenommen, und müssen „in erster Näherung“ eine Lösung der Gleichung

$$\tilde{a}_i t^{v(a_i)} X^i + \tilde{a}_j t^{v(a_j)} X^j + \dots + \tilde{a}_l t^{v(a_l)} X^l + \tilde{a}_n X^n = 0$$

finden. Wegen $v(a_i) + i\alpha = v(a_j) + j\alpha = \dots = v(a_l) + l\alpha = n\alpha$ 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

$$\mu_1 t^\alpha + \mu_2 t^{\alpha+1/\gamma} + \mu_3 t^{\alpha+2/\gamma} + \dots$$

und induktiv zu bestimmen $\mu_2, \mu_3, \dots \in k$ zum Erfolg. □

Definition 3.11.17. Seien K ein Körper und $\mathcal{P} \subset K[X] \setminus 0$ eine 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 3.11.18. Man zeige, daß eine Körpererweiterung L/K normal ist genau dann, wenn sie der Zerfällungskörper einer Menge von Polynomen $\mathcal{P} \subset K[X] \setminus 0$ ist. Hinweis: Man kopiere den Beweis von 3.8.23. Bei Punkt 3 dort reicht es, für M einen algebraischen Abschluß von K zu betrachten.

Übung 3.11.19. 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 3.11.20. 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 3.11.21. 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 $M \supset K$.

3.12 Schiefkörper über den reellen Zahlen*

3.12.1. 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 [LA1] ?? einen Ring R , der nicht der Nullring ist, und in dem alle von Null verschiedenen Elemente Einheiten sind.

Proposition 3.12.2 (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 [LA1] 4.7.4.*

Ergänzung 3.12.3. 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 3.3.12 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 $\mathbb{R} \rightarrow K$, 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 $\alpha \in K \setminus \mathbb{R}$ 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 $\mathbb{R}[\alpha]$ notwendig eine echte algebraische Körpererweiterung von \mathbb{R} und muß nach 3.8.29 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 $i \in \mathbb{C}$ von rechts wird dann ein \mathbb{C} -linearer Endomorphismus $J \in \text{End}_{\mathbb{C}} K$ mit $J^2 = -\text{id}_K$. Als Endomorphismus endlicher Ordnung [LA2] 3.3.15 oder einfacher als Endomorphismus der Ordnung vier ist er diagonalisierbar nach [LA2] 3.3.14 und liefert wegen $J^2 = -\text{id}$ eine Zerlegung $K = K^+ \oplus K^-$ mit $K^\pm = \{a \in K \mid ia = \pm ai\}$. Nun ist K^+ ein endlichdimensionaler Schiefkörper über \mathbb{C} mit \mathbb{C} im Zentrum, woraus sofort 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 Quadrat -1 . Setzen wir $j = \beta + \alpha$ an mit $\beta \in K^-$ und $\alpha \in \mathbb{R}$, so folgt $-1 = j^2 = \beta^2 + 2\alpha\beta + \alpha^2$ mit dem ersten und letzten Term in K^+ und dem mittleren Term in K^- . Damit folgt $2\alpha\beta = 0$ und dann $\alpha = 0$ und man erkennt $j \in K^-$. Für jedes von Null verschiedene $j \in K^-$ induziert aber die Multiplikation mit j von rechts einen Isomorphismus $K^+ \xrightarrow{\sim} K^-$. Der Rest des Arguments kann dem Leser überlassen bleiben. \square

Ergänzung 3.12.4. Eine **Kompositionsalgebra** ist ein reeller endlichdimensionaler euklidischer Vektorraum V zusammen mit einer bilinearen Abbildung $\mu : V \times V \rightarrow V$ derart, daß gilt $\|\mu(v, w)\| = \|v\| \cdot \|w\| \quad \forall v, w \in V$. Topologische Methoden zeigen, daß die Dimension eine Bijektion

$$\left\{ \begin{array}{l} \text{Kompositionsalgebren mit Einselement,} \\ \text{bis auf Isomorphismus} \end{array} \right\} \xrightarrow{\sim} \{0, 1, 2, 4, 8\}$$

liefert. 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 [LA1] 4.7.7 den dort ausgezeichneten Isomorphismus $\mathbb{H} \xrightarrow{\sim} \mathbb{H}^{\text{opp}}$, $q \mapsto \bar{q}$ und setzen $\mathbb{O} := \mathbb{H} \times \mathbb{H}$ mit der nicht-assoziativen Multiplikation $(a, b)(x, y) = (ax - \bar{y}b, b\bar{x} + ya)$. Mehr dazu findet man etwa bei [E+92].

Übungen

Ergänzende Übung 3.12.5. Man zeige mit Hilfe der Oktaven: Sind zwei natürliche Zahlen jeweils eine Summe von acht Quadraten, so auch ihr Produkt.

4 Galoistheorie

4.1 Galoiserweiterungen

Definition 4.1.1. 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** $\text{Gal}(L/K)$ der Körpererweiterung L/K .

4.1.2. Sprechen wir von der Galoisgruppe eines Polynoms oder genauer von der Galoisgruppe über einem Körper K eines Polynoms $P \in K[T]$, so meinen wir die Galoisgruppe seines Zerfällungskörpers L/K .

Ergänzung 4.1.3. 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 $\text{Gal}(L/K) = (\text{Ring}^K)^{\times}(L)$ und im Fall einer endlichen Erweiterung als $\text{Gal}(L/K) = \text{Ring}^K(L, L)$, da dann alle Körperhomomorphismen über K von L in sich selber bereits Isomorphismen sind.

Beispiele 4.1.4. $\text{Gal}(\mathbb{C}/\mathbb{R})$ 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 $\text{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ nur aus der Identität, denn jeder Körperhomomorphismus $\mathbb{Q}(\sqrt[3]{2}) \rightarrow \mathbb{Q}(\sqrt[3]{2})$ muß die einzige Lösung der Gleichung $x^3 = 2$ in diesem Körper auf sich selbst abbilden.

Lemma 4.1.5. *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*

$$|\text{Gal}(L/K)| \leq [L : K]$$

Beweis. Das folgt sofort aus Satz 3.8.15, nach dem sogar die Zahl der Körperhomomorphismen über K von L in einen beliebigen weiteren Körper M über K beschränkt ist durch der Erweiterungsgrad, $|\text{Ring}^K(L, M)| \leq [L : K]$. \square

Vorschau 4.1.6. Aus dem im Anschluß bewiesenen Satz 4.1.12 folgt unmittelbar, daß für den Fall einer endlichen Körpererweiterung die Kardinalität der Galoisgruppe sogar den Grad der Körpererweiterung teilen muß, in Formeln

$$|\text{Gal}(L/K)| \mid [L : K]$$

Proposition 4.1.7. *Ist q eine Primzahlpotenz und $r \geq 1$, so ist die Galoisgruppe $\text{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$ eine zyklische Gruppe der Ordnung r , erzeugt vom **Frobenius-Homomorphismus***

$$F : \mathbb{F}_{q^r} \xrightarrow{\sim} \mathbb{F}_{q^r}, \quad a \mapsto a^q$$

4.1.8. In [LA1] 4.2.36 hatten wir bereits einen Frobenius-Homomorphismus eingeführt. Der Frobenius-Homomorphismus 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 4.1.5 hat die Galoisgruppe jedoch höchstens r Elemente. \square

Definition 4.1.9. Eine Körpererweiterung L/K heißt eine **Galoiserweiterung** oder kurz **Galois**, wenn sie **normal** und **separabel** ist.

4.1.10. Gegeben eine endliche Galoiserweiterung L/K gilt für die Kardinalität der Galoisgruppe die Identität

$$|\text{Gal}(L/K)| = [L : K]$$

In der Tat gibt es nach (3.9.22, 1 \Rightarrow 3) für L endlich, separabel und normal über K genau $[L : K]$ Körperhomomorphismen $L \rightarrow L$ über K . Als Körperhomomorphismen sind diese natürlich injektiv, und wegen der Gleichheit der K -Dimensionen sind sie dann auch surjektiv. In 4.1.14 werden wir im übrigen zeigen, daß umgekehrt eine endliche Körpererweiterung L/K mit $|\text{Gal}(L/K)| = [L : K]$ auch notwendig bereits Galois ist.

4.1.11. 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 4.1.12 (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

$$\text{Irr}(\alpha, L^G) = \prod_{\beta \in G\alpha} (X - \beta)$$

2. Die Körpererweiterung L/L^G ist eine endliche Galoiserweiterung vom Grad $[L : L^G] = |G|$ mit Galoisgruppe $\text{Gal}(L/L^G) = G$.

Beweis. Wir setzen $L^G = K$. 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 $\text{Irr}(\alpha, K)$, da es bei α verschindet. Es wird aber auch von fraglichem Minimalpolynom geteilt, da ja mit α auch alle $\sigma(\alpha)$ für $\sigma \in G$ Nullstellen des besagten Minimalpolynoms sein müssen. 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

$$[L : K] = |G|$$

Zunächst bemerken wir dazu, daß es nach Proposition 3.10.5 über die Unterscheidung von Körperhomomorphismen, ein $\alpha \in L$ gibt mit $|G\alpha| = |G|$. Unsere Beschreibung des Minimalpolynoms von α über K zeigt $[K(\alpha) : K] = |G|$. Für $\beta \in L$ ist aber auch $K(\alpha, \beta)$ eine endliche separable Erweiterung von K und nach dem Satz vom primitiven Element 3.10.7 gibt es γ mit $K(\alpha, \beta) = K(\gamma)$. Aus $\text{grad}(\text{Irr}(\gamma, K)) \leq |G|$ 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 $G = \text{Gal}(L/K)$ ohne weitere Schwierigkeiten aus der Ungleichungskette

$$|G| \leq |\text{Gal}(L/K)| \leq [L : K] = |G|$$

Hier kommt die mittlere Ungleichung von 4.1.5 her und wir müssen unsere Erkenntnis 4.1.10, daß sie im Fall endlicher Galois-Erweiterungen sogar eine Gleichheit ist, gar nicht bemühen. \square

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 $\sigma_1, \dots, \sigma_r$ und es gebe in L eine um Eins größere über $K := L^G$ linear unabhängige Familie x_0, \dots, 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, \dots, y_r in L nicht alle Null mit $\sum_j y_j \sigma_i(x_j) = 0 \forall i$. Durch Ummummern der x_j dürfen wir hier ohne Beschränkung der Allgemeinheit $y_0 \neq 0$ annehmen, und indem wir von y_0, \dots, y_r zu yy_0, \dots, 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 dem Satz über die lineare Unabhängigkeit von Charakteren 3.8.16, angewandt auf

die Homomorphismen $\sigma_i : L^\times \rightarrow L^\times$, gibt es jedoch ein $z \in L^\times$ mit $\sum_i \sigma_i^{-1}(z) \neq 0$, und das ist der gesuchte Widerspruch. \square

Ergänzung 4.1.13. Ist L/K eine endliche Galois-Erweiterung, so ist $\alpha \in L$ nach dem ersten Beweis von 4.1.12 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“ 6.1.5. Diese schärfere Aussage stimmt keineswegs für jedes primitive Element, wie das Beispiel $L = \mathbb{C}$, $K = \mathbb{R}$, $\alpha = i$ zeigt.

Satz 4.1.14 (Charakterisierung endlicher Galois-Erweiterungen). *Seien L/K eine endliche Körpererweiterung und $G = \text{Gal}(L/K)$ ihre Galoisgruppe. So sind gleichbedeutend:*

1. L/K ist eine Galois-Erweiterung;
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. $1 \Rightarrow 2$ war 4.1.10. Die Implikation $2 \Rightarrow 3$ folgt daraus, daß wir $|G| = [L : L^G]$ ja bereits nach 4.1.12 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 $3 \Rightarrow 1$ folgt direkt aus 4.1.12. \square

Ergänzung 4.1.15. 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 4.1.33, und die andere aus 3.11.8.

Beispiel 4.1.16. Unter der Voraussetzung $\text{char } K \neq 2$ ist jede quadratische Körpererweiterung L von K Galois mit Galoisgruppe $\mathbb{Z}/2\mathbb{Z}$, und die Elemente $\alpha \in L \setminus K$ 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 4.1.17. Eine Wirkung einer Gruppe auf einer Menge heißt **treu**, englisch **faithful**, französisch **fidèle**, wenn nur das neutrale Element jedes Element der Menge festhält.

4.1.18. Wir erinnern aus [LA2] 5.1.5.??, 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 4.1.19 (Operation der Galoisgruppe auf Nullstellen). Gegeben K ein Körper, $P \in K[X]$ ein irreduzibles Polynom und L/K sein Zerfällungskörper operiert die Galoisgruppe $\text{Gal}(L/K)$ auf der Menge $\{\alpha \in L \mid P(\alpha) = 0\}$ der Nullstellen von P in L treu und transitiv.

Beweis. Treu ist die Operation, da besagte Zerfällungserweiterung per definitionem bereits von den Nullstellen des besagten Polynoms erzeugt wird. Transitiv ist sie, da es für je zwei Nullstellen α, β von P nach unserer Proposition 3.8.9 über das Ausdehnen auf primitive Erweiterungen einen Körperhomomorphismus $K(\alpha) \rightarrow L$ über K gibt mit $\alpha \mapsto \beta$, der sich dann nach 3.8.12 weiter ausdehnen läßt zu einem Körperhomomorphismus $L \rightarrow L$ über K . \square

4.1.20 (**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 auch die **Galoisgruppe unseres irreduziblen Polynoms**. Hierzu gebe ich gleich drei Beispiele.

Beispiel 4.1.21 (Ein kubisches Polynom mit Galoisgruppe 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 $\text{Gal}(L/\mathbb{Q}) \cong S_3$. In der Tat ist L/\mathbb{Q} normal als Zerfällungskörper und sogar Galois, da in Charakteristik Null jede Körpererweiterung separabel ist. Damit folgt insbesondere $[L : \mathbb{Q}] = |\text{Gal}(L/\mathbb{Q})|$. 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 $\zeta = \exp(2\pi i / 3)$ 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 $|\text{Gal}(L/\mathbb{Q})| = 6$. Die Operation von $\text{Gal}(L/\mathbb{Q})$ auf der Menge $\{\sqrt[3]{2}, \zeta \sqrt[3]{2}, \zeta^2 \sqrt[3]{2}\}$ definiert nun nach 4.1.19 eine Einbettung $\text{Gal}(L/\mathbb{Q}) \hookrightarrow S_3$, und da beide Seiten gleichviele Elemente haben, muß diese Einbettung ein Isomorphismus sein.

Beispiel 4.1.22 (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 $\text{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$. In der Tat können wir mit $\zeta = \exp(2\pi i/7)$ 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 [LA1] 4.3.39 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 4.7.9 geben wir im übrigen ein Kriterium an, das es erlaubt, die Galoisgruppe einer kubischen Gleichung ganz mechanisch zu bestimmen.

Beispiel 4.1.23 (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.

Proposition 4.1.24 (Quotientenkörper eines Invariantenrings). *Operiert eine endliche Gruppe G auf einem kommutativen Integritätsbereich R , so definiert die offensichtliche Einbettung einen Isomorphismus*

$$\text{Quot}(R^G) \xrightarrow{\sim} (\text{Quot } R)^G$$

des Quotientenkörpers seines Invariantenrings mit den Invarianten seines Quotientenkörpers.

Beweis. Jeden Bruch $f/h \in (\text{Quot } R)^G$ können wir mit $\prod_{\sigma \in G \setminus 1} \sigma(h)$ erweitern zu einem Bruch, dessen Nenner in 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 nur dann G -invariant sein, wenn auch sein Zähler in R^G liegt. \square

Beispiel 4.1.25. Für jeden Körper k ist nach 4.1.12 und 4.1.24 in den Notationen von 2.9.6 die Erweiterung

$$k(\prime s_1, \dots, s_n) = k(\prime X_1, \dots, X_n)^{S_n} \subset k(\prime X_1, \dots, X_n)$$

eine Galoiserweiterung mit Galoisgruppe S_n . Unsere Erweiterung ist natürlich auch ein Zerfällungskörper der **allgemeinen Gleichung**

$$T^n + s_1 T^{n-1} + \dots + s_{n-1} T + s_n$$

wo wir die s_i schlicht als algebraisch unabhängige Variablen des Funktionenkörpers $k(s_1, \dots, s_n)$ über k auffassen. 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 4.1.12 irreduzibel, da ja alle ihre Wurzeln einfach sind und zueinander konjugiert unter der Galoisgruppe. Die Irreduzibilität dieses Polynoms kann aber auch bereits aus 2.7.20 abgeleitet werden.

Übungen

Übung 4.1.26. 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 4.1.27. Man zeige, daß sich jede endliche Erweiterung eines vollkommenen Körpers zu einer endlichen Galoiserweiterung vergrößern läßt. Man zeige, daß sich wie in [LA2] 3.3.2 behauptet jeder Endomorphismus x eines endlichdimensionalen Vektorraums über einem vollkommenen Körper auf genau eine Weise zerlegen läßt als $x = x_s + x_n$ mit x_s halbeinfach, x_n nilpotent und $x_s x_n = x_n x_s$.

Übung 4.1.28. 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 4.1.29. 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 4.1.30. Jede normale Körpererweiterung mit trivialer Galoisgruppe ist rein inseparabel im Sinne von 3.9.29. Für jede normale Körpererweiterung K/k mit Galoisgruppe G ist K^G/k rein inseparabel. Hinweis: 3.9.15. Im Fall unendlicher Erweiterungen verwende man 3.11.7.

Ergänzende Übung 4.1.31 (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 3.10.7 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 3.9.29.

Übung 4.1.32. Man bestimme die Galoisgruppe des Zerfällungskörpers des Polynoms $X^4 - 5$ über \mathbb{Q} und über $\mathbb{Q}[i]$.

Ergänzende Übung 4.1.33. Ist L/K eine algebraische, aber nicht notwendig endliche Körpererweiterung und $G \subset \text{Gal}(L/K)$ 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 $\text{Gal}(\mathbb{F}_p/\mathbb{F}_p)$, aber der Fixkörper seines Erzeugnisses ist dennoch \mathbb{F}_p .

4.2 Anschauung für die Galoisgruppe*

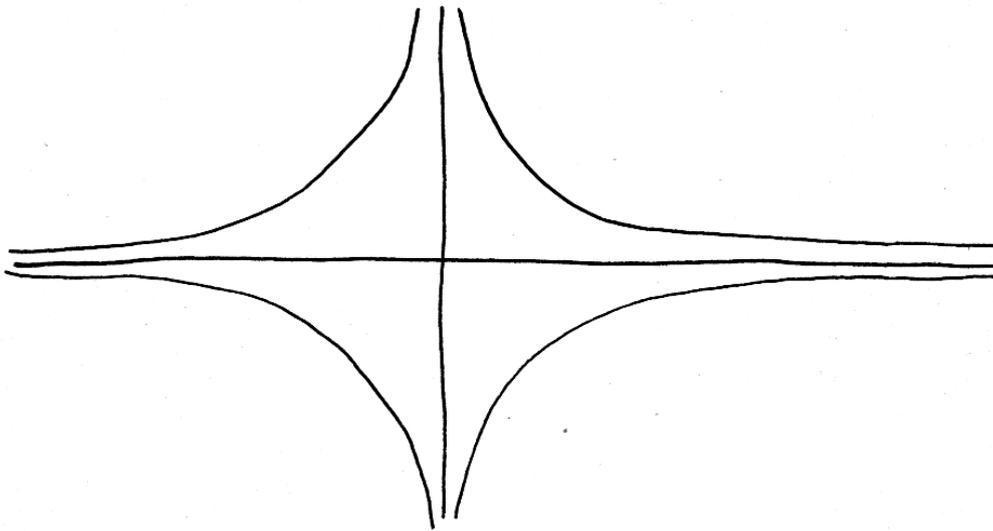
4.2.1. Formal ist der nun folgende Abschnitt für die logische Kohärenz dieser Vorlesung nicht von Belang. Es wird darin auch nichts bewiesen. Ich denke jedoch, daß die im folgenden erklärten Ideen bei der historischen Entwicklung der Theorie von zentraler Bedeutung waren und hoffe, daß sie Ihnen beim Verständnis helfen.

4.2.2 (**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 $\mathbb{R}(t) = \text{Quot } \mathbb{R}[t]$ über dem Körper der reellen Zahlen. Sei $E \subset \mathbb{R}$ die endliche Menge aller Punkte, an denen mindestens ein Koeffizient von P eine Polstelle hat. An jeder anderen Stelle $\lambda \in \mathbb{R} \setminus E$ können wir die Koeffizienten von P bei $t = \lambda$ auswerten und erhalten so ein Polynom $P_\lambda \in \mathbb{R}[X]$. Die reellen Nullstellen dieser Polynome P_λ hängen dann von λ ab, und eine bildliche Darstellung der Menge

$$\mathcal{Z}(P) := \{(\lambda, \alpha) \in \mathbb{R}^2 \mid \lambda \notin E, P_\lambda(\alpha) = 0\}$$

als Teilmenge der Ebene vermittelt eine gewisse Anschauung für diese Abhängigkeit. Ist etwa $P = X^2 - 1/t$, so besteht die Ausnahmemenge E aus dem Nullpunkt, $E = \{0\}$, und wir haben $\mathcal{Z}(P) = \{(\lambda, \alpha) \mid \lambda \neq 0, \alpha^2 - 1/\lambda = 0\}$.

4.2.3 (**Komplexe Nullstellen einer Familie komplexer Polynome**). Nun betrachten wir analog ein normiertes Polynom $P \in \mathbb{C}(t)[X]$ mit Koeffizienten im Funktionenkörper $\mathbb{C}(t) = \text{Quot } \mathbb{C}[t]$ über dem Körper der komplexen Zahlen. Sei wieder $E \subset \mathbb{C}$ die endliche Menge aller Punkte, an denen mindestens ein Koeffizient von P eine Polstelle hat. An jeder anderen Stelle $\lambda \in \mathbb{C} \setminus E$ können wir die Koeffizienten von P bei $t = \lambda$ auswerten und erhalten so ein Polynom $P_\lambda \in \mathbb{C}[X]$. Die



Graphische Darstellung der Menge $\{(\lambda, \alpha) \mid \lambda \neq 0, \alpha^2 - 1/\lambda = 0\}$

komplexen Nullstellen dieses Polynoms P_λ hängen dann von λ ab, und wir bilden die Menge

$$\mathcal{Z}(P) := \{(\lambda, \alpha) \in \mathbb{C}^2 \mid \lambda \notin E, P_\lambda(\alpha) = 0\}$$

Ist etwa zur Abwechslung diesmal $P = X^2 - t$, so ist die Ausnahmemenge E leer und wir haben $\mathcal{Z}(P) = \{(\lambda, \alpha) \mid \alpha^2 - \lambda = 0\}$.

4.2.4. Gegeben eine stetige Abbildung $p : Z \rightarrow C$ von metrischen oder auch von topologischen Räumen verstehen wir unter einer **Decktransformation von p** eine stetige Abbildung $f : Z \rightarrow Z$ mit $p \circ f = p$.

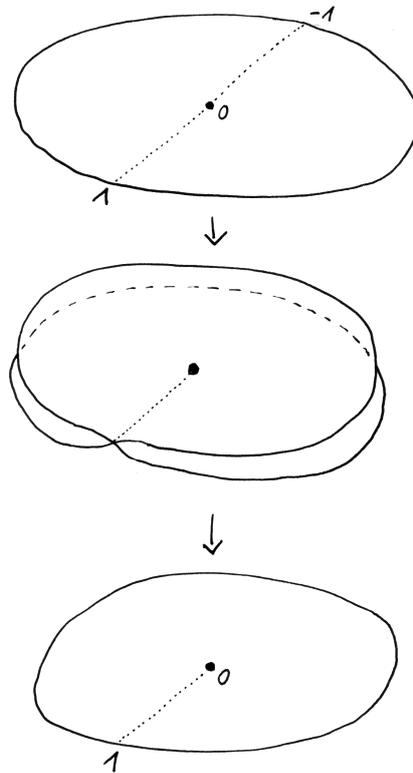
Satz 4.2.5 (Anschauung für die Galoisgruppe). Sei $P \in \mathbb{C}(t)[X]$ ein normiertes irreduzibles Polynom und $L/\mathbb{C}(t)$ die Körpererweiterung von $\mathbb{C}(t)$, die durch die Adjunktion einer Nullstelle von P entsteht. Bezeichne weiter

$$\mathcal{Z}(P) := \{(\lambda, z) \in \mathbb{C}^2 \mid P_\lambda \in \mathbb{C}[X] \text{ ist definiert bei } t = \lambda \text{ und } P_\lambda(z) = 0\}$$

die simultane Nullstellenmenge. So ist die Galoisgruppe $\text{Gal}(L/\mathbb{C}(t))$ isomorph zum Monoid aller Decktransformationen der Projektion $\text{pr}_1 : \mathcal{Z}(P) \rightarrow \mathbb{C}$.

4.2.6. Hier meint $\text{pr}_1 : \mathbb{C}^2 \rightarrow \mathbb{C}$ die Projektion auf die erste Komponente alias die erste Koordinate und Stetigkeit ist für die von \mathbb{C}^2 induzierte Metrik gemeint. Wir werden den vorhergehenden Satz im Rahmen dieser Vorlesung weder beweisen noch verwenden, ihn aber in 4.2.10 noch präzisieren, indem wir einen Isomorphismus der Galoisgruppe mit unserem Monoid von Decktransformationen explizit angeben. Der Satz vom primitiven Element 3.10.7 sagt uns im übrigen, daß jede endliche Körpererweiterung von $\mathbb{C}(t)$ primitiv ist, also durch Adjunktion eines einzigen Elements erhalten werden kann.

4.2.7 (**Hilfen zur graphischen Darstellung**). Die Abbildung $\text{pr}_1 : \mathcal{Z}(P) \rightarrow \mathbb{C}$ hat endliche Fasern. Ist P nicht konstant, so sind die Fasern über Punkten $\lambda \notin E$ auch nie leer. Ist weiter P irreduzibel oder allgemeiner teilerfremd zu seiner Ableitung, so ist seine Diskriminante nicht die Null von $\mathbb{C}(t)$, und bezeichnet $F \subset \mathbb{C}$ die endliche Menge aller Null- und Polstellen dieser Diskriminante, so hat jede Faser von $\text{pr}_1 : \mathcal{Z}(P) \rightarrow \mathbb{C}$ über Punkten $\lambda \in \mathbb{C} \setminus (E \cup F)$ genau $\text{grad } P$ Elemente. Indem wir nun um jeden Punkt aus $E \cup F$ in der komplexen Zahlenebene einen Kreis zeichnen, der keinen anderen Punkt von $E \cup F$ umläuft, und alle diese Kreise durch sich nicht kreuzende Wege mit einem festen Punkt verbinden, und weiter das Urbild eines solchen Gebildes in $\mathcal{Z}(P)$ zeichnen, erhalten wir eine gewisse Anschauung für die Abbildung $\text{pr}_1 : \mathcal{Z}(P) \rightarrow \mathbb{C}$ und das Monoid ihrer Decktransformationen: Bezeichnet genauer $S \subset \mathbb{C}^2$ unser Gebilde, so liefert die Restriktion auf $\text{pr}_1^{-1}(S)$ eine Bijektion zwischen dem Monoid der Decktransformationen von $\text{pr}_1 : \mathcal{Z}(P) \rightarrow \mathbb{C}$ und dem Monoid der Decktransformationen von $\text{pr}_1 : \text{pr}_1^{-1}(S) \rightarrow S$.



Dies Bild kam bereits in [LA1] 3.1.6 vor als Illustration für die Abbildung $z \mapsto z^2$ der komplexen Zahlenebene auf sich selbst. Für die durch Adjunktion einer Quadratwurzel aus t entstehende Erweiterung L des Funktionenkörpers $\mathbb{C}(t)$ ist nun $P = X^2 - t$ das Minimalpolynom eines Erzeugers und wir erhalten eine stetige Bijektion $\mathbb{C} \xrightarrow{\sim} Z(P)$ mit stetiger Umkehrung mittels der Vorschrift $z \mapsto (z^2, z)$. Die Komposition $\mathbb{C} \xrightarrow{\sim} Z(P) \rightarrow \mathbb{C}$ mit der Projektion auf die erste Koordinate ist also gerade unsere Abbildung $z \mapsto z^2$. Wir sehen so anschaulich, daß die Galoisgruppe von $L/\mathbb{C}(t)$ 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 $\mathbb{C}(\sqrt[n]{t})/\mathbb{C}(t)$ notierten Körpererweiterung gerade $\mathbb{Z}/n\mathbb{Z}$ sein sollte, was Sie bereits als Übung 4.1.26 formal bewiesen haben.

Vorschau 4.2.8. Betrachten wir in der Situation der vorhergehenden Bemerkung 4.2.7 eine beliebige endliche Teilmenge $H \subset \mathbb{C}$, die $E \cup F$ umfaßt, und bilden $\mathcal{Z}_H(P) := \{(\lambda, \alpha) \in \mathcal{Z}(P) \mid \lambda \notin H\}$, so induziert die Projektion sogar eine Überlagerung $\text{pr}_1 : \mathcal{Z}_H(P) \rightarrow \mathbb{C} \setminus H$ im Sinne von [TF] 3.1.1 und die Restriktion liefert einen Isomorphismus des Monoids der Decktransformationen von $\text{pr}_1 : \mathcal{Z}(P) \rightarrow \mathbb{C}$ mit der Deckbewegungsgruppe besagter Überlagerung im Sinne von [TF] 3.4.4.

4.2.9. Ich will zum Abschluß noch genauer erklären, wie in Satz 4.2.5 die Galoisgruppe mit unserem Monoid von Decktransformationen identifiziert werden kann. Für jede Menge Z und jeden Ring k erklären wir den Ring $\text{Ensf}(Z, k)$ der **fast überall definierten Funktionen auf Z mit Werten in k** als den Quotient des Rings $\text{Ens}(Z, k)$ nach dem Ideal aller Funktionen, die nur an endlich vielen Stellen einen von Null verschiedenen Wert annehmen. Für jede Abbildung $f : Y \rightarrow Z$ mit endlichen Fasern liefert das Vorschalten von f einen Ringhomomorphismus $(\circ f) : \text{Ensf}(Z, k) \rightarrow \text{Ensf}(Y, k)$ in die Gegenrichtung, das **Zurückholen** fast überall definierter Funktionen.

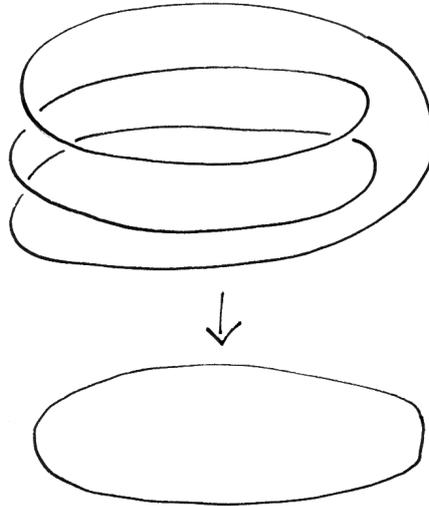
4.2.10 (**Decktransformationen als Körperautomorphismen**). Seien nun ein normiertes Polynom $P \in \mathbb{C}(t)[X]$ gegeben und sei $Z = \mathcal{Z}(P) \subset \mathbb{C}^2$ wie oben erklärt. Die Restriktion von Polynomen in zwei Variablen zu Funktionen auf Z liefert offensichtlich einen Ringhomomorphismus $\mathbb{C}[t, X] \rightarrow \text{Ens}(Z, \mathbb{C})$ in den Ring der komplexwertigen Funktionen auf Z . Dieser Ringhomomorphismus besitzt genau eine Fortsetzung zu einem Ringhomomorphismus $\mathbb{C}(t)[X] \rightarrow \text{Ensf}(Z, \mathbb{C})$, der hinwiederum über einen Ringhomomorphismus

$$\mathbb{C}(t)[X]/\langle P \rangle \hookrightarrow \text{Ensf}(Z, \mathbb{C})$$

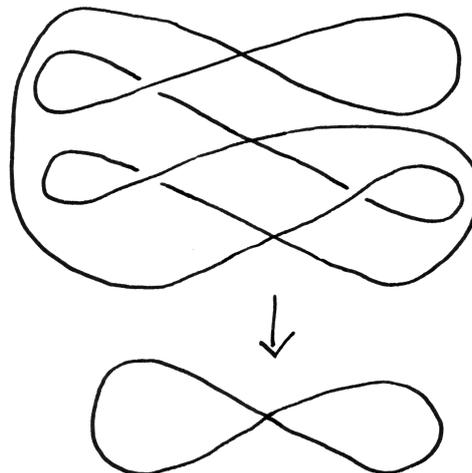
faktoriisiert. Letzterer Ringhomomorphismus ist notwendig injektiv, da er von einem Körper startet und in einem vom Nullring verschiedenen Ring landet. Unser Satz 4.2.5 über die anschauliche Bedeutung der Galoisgruppe läßt sich nun dahingehend präzisieren, daß die offensichtliche Operation „durch Vorschalten“ des Monoids D der Decktransformationen von $\text{pr}_1 : Z \rightarrow \mathbb{C}$ auf dem Ring $\text{Ensf}(Z, \mathbb{C})$ das Bild der obigen Einbettung $\mathbb{C}(t)[X]/\langle P \rangle \hookrightarrow \text{Ensf}(Z, \mathbb{C})$ stabilisiert, und daß die so induzierte Operation unseres Monoids auf $L = \mathbb{C}(t)[X]/\langle P \rangle$ einen Isomorphismus $D \xrightarrow{\sim} \text{Gal}(L/\mathbb{C}(t))$ unseres Monoids mit der fraglichen Galoisgruppe liefert. Auch diese Präzisierung soll hier nicht bewiesen und im weiteren Verlauf nicht verwendet werden.

4.3 Galois-Korrespondenz

Satz 4.3.1 (Galois-Korrespondenz). *Gegeben eine endliche Galois-erweiterung L/K mit Galoisgruppe $G = \text{Gal}(L/K)$ liefern das Bilden der Galoisgruppe*



Anschauung für die durch Adjunktion einer dritten Wurzel aus t entstehende Körpererweiterung des Funktionenkörpers $\mathbb{C}(t)$ nach 4.2.7. 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.

$M \mapsto \text{Gal}(L/M)$ und das Bilden des Fixpunktkörpers $H \mapsto L^H$ zueinander inverse Inklusionsumkehrende Bijektionen

$$\left\{ \begin{array}{l} \text{Zwischenkörper } M \\ \text{unserer Körpererweiterung} \\ K \subset M \subset L \end{array} \right\} \overset{\sim}{\leftrightarrow} \left\{ \begin{array}{l} \text{Untergruppen } H \\ \text{ihrer Galoisgruppe} \\ H \subset G \end{array} \right\}$$

$$\begin{array}{ccc} M & \xrightarrow{\phi} & \text{Gal}(L/M) \\ L^H & \xleftarrow{\psi} & H \end{array}$$

Unter dieser Bijektion entsprechen die Normalteiler H von G genau denjenigen Zwischenkörpern M , die normal sind über K , und in diesen Fällen definiert das Einschränken von Elementen der Galoisgruppe einen Isomorphismus von Gruppen $G/H \xrightarrow{\sim} \text{Gal}(L^H/K)$ alias eine kurze exakte Sequenz

$$\text{Gal}(L/M) \hookrightarrow \text{Gal}(L/K) \twoheadrightarrow \text{Gal}(M/K)$$

Vorschau 4.3.2. In der Sprache der Kategorientheorie nimmt dieser Satz die folgende Form an: Ist L/K eine endliche Galoiserweiterung mit Galoisgruppe G , so liefert Funktor $\text{Kring}^K(_, L)$ der K -linearen Körperhomomorphismen nach L eine Äquivalenz von Kategorien

$$\left\{ \begin{array}{l} \text{Körpererweiterungen von } K, \\ \text{die sich in } L \text{ einbetten lassen} \end{array} \right\} \overset{\sim}{\rightarrow} \{\text{transitive } G\text{-Mengen}\}^{\text{opp}}$$

Beweis. Nach Eigenschaft 3.8.27 der Normalität und der Definition der Separabilität 3.9.16 ist für jeden Zwischenkörper M auch L/M normal und separabel, also Galois, und damit folgt $\psi \circ \phi = \text{id}$ aus unserer Erkenntnis 4.1.14, daß bei einer endlichen Galoiserweiterung der Grundkörper gerade der Fixkörper der Galoisgruppe ist. Ohne alle Schwierigkeiten folgt $\phi \circ \psi = \text{id}$ aus unserer Erkenntnis 4.1.12, 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 $g \in G$. 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 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 $G \rightarrow \text{Gal}(L^H/K)$ über G/H und liefert eine Injektion $G/H \hookrightarrow \text{Gal}(L^H/K)$, die mit einem Abzählargument bijektiv sein muß. \square

Beispiel 4.3.3. Nach 4.1.7 ist für jede Potenz $q = p^r$ mit $r \geq 1$ einer Primzahl p die Galoisgruppe $\text{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ 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 [LA2] 4.3.20 genau die Gruppen $\mathbb{Z}d/\mathbb{Z}r$ für Teiler d von r . Das liefert im Licht der Galoiskorrespondenz 4.3.1 einen neuen Beweis unserer Klassifikation 3.7.13 aller Unterkörper eines endlichen Körpers.

Definition 4.3.4. Sei $\text{char } K \neq 2$. Eine Körpererweiterung L/K heißt **biquadratisch**, wenn sie den Grad $[L : K] = 4$ hat und erzeugt ist von zwei Elementen $L = K(\alpha, \beta)$ für $\alpha, \beta \in L$ mit $\alpha^2, \beta^2 \in K$.

Beispiel 4.3.5. $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ 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 4.3.6. Jede biquadratische Erweiterung ist Galois, und ihre Galoisgruppe ist die Klein'sche Vierergruppe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Beweis. Für die nichttrivialen Elemente $\sigma \in \text{Gal}(L/K(\alpha))$, $\tau \in \text{Gal}(L/K(\beta))$ haben wir

$$\sigma : \begin{cases} \alpha \mapsto \alpha \\ \beta \mapsto -\beta \end{cases} \quad \tau : \begin{cases} \alpha \mapsto -\alpha \\ \beta \mapsto \beta \end{cases}$$

und wir haben $\{\text{id}, \sigma, \tau, \sigma\tau\} \subset \text{Gal}(L/K)$. Das muß dann aber schon die ganze Galois-Gruppe sein. \square

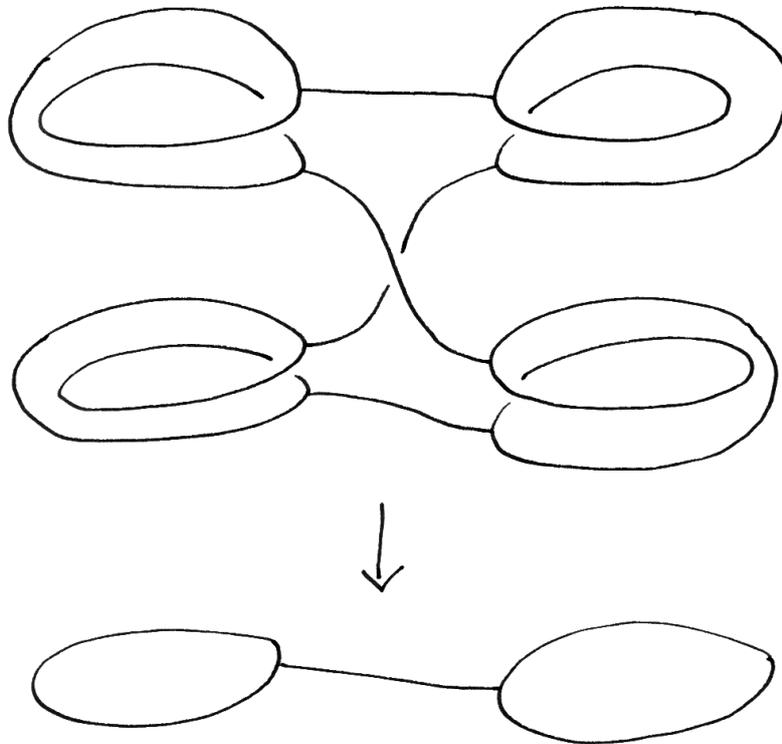
4.3.7. Die Klein'sche Vierergruppe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{F}_2^2$ hat fünf Untergruppen: Den Nullpunkt, drei Geraden, und die ganze Gruppe. Sie entsprechen in unserer biquadratischen Erweiterung aus 4.3.6 den Unterkörpern

$$L \supset K(\alpha), K(\beta), K(\alpha\beta) \supset K$$

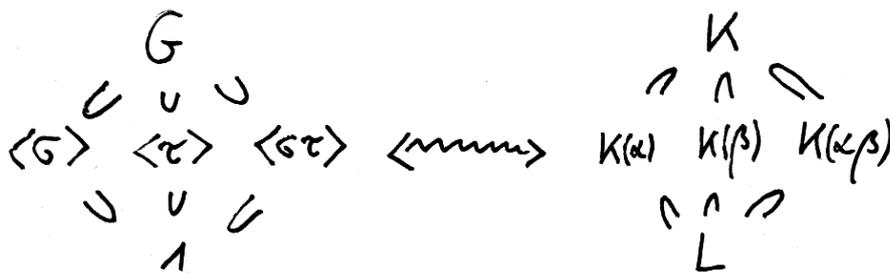
Eine K -Basis von L besteht aus $1, \alpha, \beta, \alpha\beta$, wie die simultane Eigenraumzerlegung von L unter σ und τ zeigt. Hier ist $\alpha + \beta$ ein primitives Element, da es von keinem nichttrivialen Element der Galoisgruppe festgehalten wird.

Satz 4.3.8 (Fundamentalsatz der Algebra). Der Körper der komplexen Zahlen ist algebraisch abgeschlossen.

4.3.9. Alternative Beweise diskutieren wir in [LA1] 4.3.25. 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.



Dies Bild ist wie in 4.2.7 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 Galois Korrespondenz entsprechenden fünf Zwischenkörper einer biquadratischen Erweiterung.

Beweis. Sei $[L : \mathbb{R}]$ eine endliche normale Erweiterung von \mathbb{R} . Sei $G = \text{Gal}(L/\mathbb{R})$ 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 aus $\mathbb{R}[X]$ von ungeradem Grad nach dem Zwischenwertsatz [ANI] 2.2.15 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 1.3.9 über die Struktur von p -Gruppen und unter Zuhilfenahme der Galoiskorrespondenz und Übung 4.3.10 die Körpererweiterung L aus \mathbb{R} durch sukzessive Körpererweiterungen vom Grad 2, also nach 3.4.9 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 $L = \mathbb{C}$. \square

Übungen

Übung 4.3.10. 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: 4.1.10, 3.4.11, [LA2] 4.1.5, 4.3.1.

Übung 4.3.11. Man drücke $\sqrt{3}$ aus als Polynom in $\sqrt{3} + \sqrt{5}$ mit rationalen Koeffizienten: Das muß möglich sein, da dies Element nach 4.3.7 primitiv ist in $\mathbb{Q}(\sqrt{3}, \sqrt{5})$.

Ergänzung 4.3.12. In der algebraischen Zahlentheorie können Sie lernen, warum ganz allgemein für paarweise teilerfremde natürliche Zahlen a_1, \dots, a_n die Körpererweiterung $\mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_n})$ über \mathbb{Q} die Galoisgruppe $(\mathbb{Z}/2\mathbb{Z})^n$ hat. Daß es sich dabei um eine Galoiserweiterung handelt, sollten Sie jedoch auch hier bereits unmittelbar einsehen können.

Übung 4.3.13. 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 $\text{Gal}(K_1K_2/K) \xrightarrow{\sim} \text{Gal}(K_1/K) \times \text{Gal}(K_2/K)$ mittels der Restriktionen.

Ergänzende Übung 4.3.14. Sei L/K eine endliche Galoiserweiterung mit Galoisgruppe G und sei $H \subset G$ eine Untergruppe. Man konstruiere einen Isomorphismus zwischen $\text{Gal}(L^H/K)$ und dem Quotienten N/H nach H des **Normalisators** $N = N_G(H) := \{g \in G \mid gHg^{-1} = H\}$ von H in G .

Übung 4.3.15. Für jeden Körper k , dessen Charakteristik kein Teiler von n ist, hat der Zerfällungskörper des Polynoms

$$T^n + a_2T^{n-2} + \dots + a_{n-1}T + a_n$$

mit Koeffizienten im Funktionenkörper $k(a_2, \dots, a_n)$ in $n - 1$ algebraisch unabhängigen Veränderlichen als Galoisgruppe die volle symmetrische Gruppe \mathcal{S}_n . Hinweis: Man gehe aus von 4.1.25; 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 $\text{Gal}(L/K) = \text{Gal}(L(X)/K(X))$. Die Irreduzibilität folgt bereits aus 2.7.20.

Ergänzung 4.3.16. Bei der Behandlung kubischer Gleichungen in 4.7.4 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.

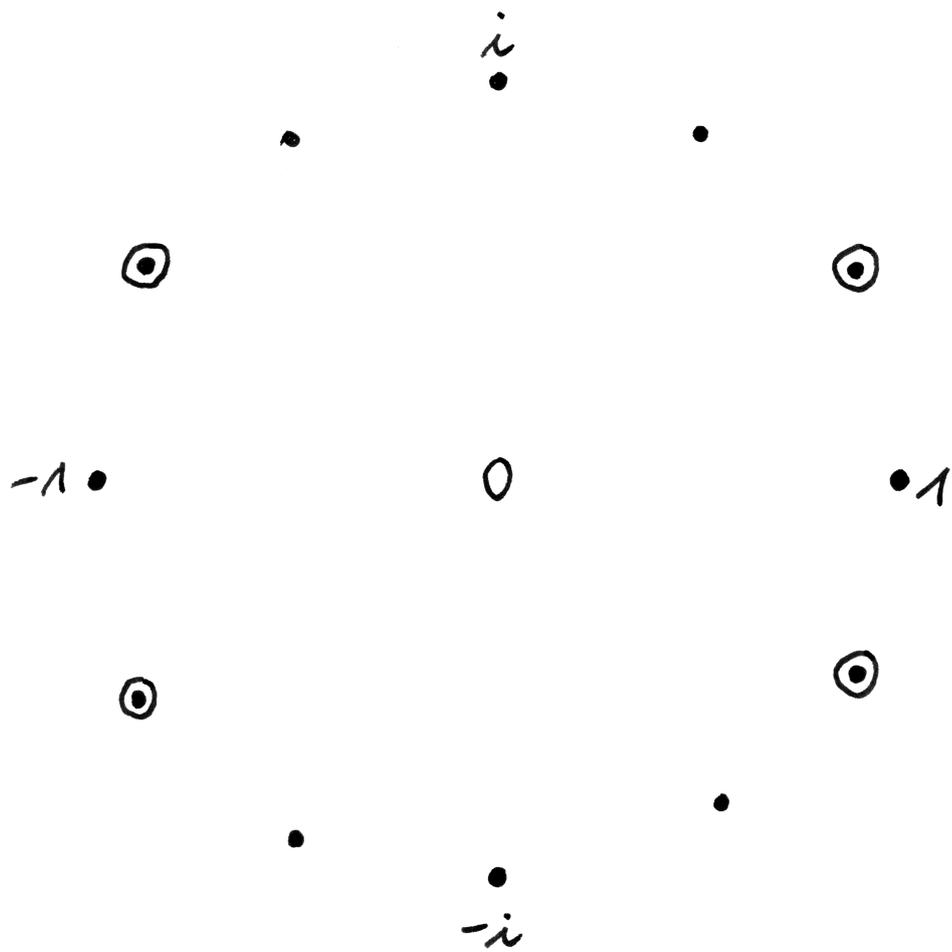
4.4 Galoisgruppen von Kreisteilungskörpern

4.4.1. Gegeben $n \geq 1$ interessieren wir uns nun für den Zerfällungskörper über \mathbb{Q} des Polynoms $X^n - 1$. Dieser Zerfällungskörper 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 $\zeta = e^{2\pi i/n}$. Auch ohne Rückgriff auf den Körper der komplexen Zahlen wissen wir nach [LA2] 4.4.17, 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 2.8.1 sind sie gerade die Nullstellen des n -ten Kreisteilungspolynoms

$$\Phi_n = \prod_{\text{ord } \zeta = n} (X - \zeta)$$

Wir hatten schon in 2.8.1 mit Induktion über n gezeigt, daß dieses Polynom Koeffizienten in \mathbb{Q} und sogar in \mathbb{Z} hat, und 2.8.4 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 2.7.11 ist das ganz allgemein für normierte Polynome in $\mathbb{Z}[X]$ gleichbedeutend dazu, irreduzibel zu sein in $\mathbb{Z}[X]$.

Satz 4.4.2 (Galoisgruppen der Kreisteilungskörper). 1. Die Kreisteilungspolynome $\Phi_n(X)$ sind irreduzibel in $\mathbb{Q}[X]$;



Die zwölften Einheitswurzeln in \mathbb{C} , eingekringelt die vier primitiven zwölften Einheitswurzeln

2. Bezeichnet μ_n die Gruppe der n -ten Einheitswurzeln im n -ten Kreisteilungskörper $\mathbb{Q}(\sqrt[n]{1})$ und $\text{Aut}(\mu_n)$ ihre Automorphismengruppe, so liefern die offensichtlichen Abbildungen Isomorphismen

$$\text{Gal}(\mathbb{Q}(\sqrt[n]{1})/\mathbb{Q}) \xrightarrow{\sim} \text{Aut}(\mu_n) \xleftarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^\times$$

Auf diese Weise erhalten wir einen ausgezeichneten Isomorphismus zwischen der Galoisgruppe des n -ten Kreisteilungskörpers und der Einheitsengruppe des Restklassenrings $\mathbb{Z}/n\mathbb{Z}$;

3. Gegeben zwei primitive n -te Einheitswurzeln $\zeta, \xi \in \mathbb{Q}(\sqrt[n]{1})$ existiert genau ein Körperhomomorphismus $\sigma : \mathbb{Q}(\sqrt[n]{1}) \rightarrow \mathbb{Q}(\sqrt[n]{1})$ mit $\sigma(\zeta) = \xi$.

4.4.3. Die Irreduzibilität der Kreisteilungspolynome für prime Einheitswurzeln haben wir bereits in 2.8.4 gezeigt. In diesem Fall vereinfacht sich der Beweis entsprechend.

4.4.4. 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 $e^{2\pi i/n}$ 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.

4.4.5. Ich schicke dem Beweis einige allgemeine Betrachtungen zu zyklischen Gruppen voraus. Für $n \geq 1$ liefert ja sicher die Multiplikation einen Isomorphismus $(\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\sim} \text{Aut}(\mathbb{Z}/n\mathbb{Z})$ zwischen der Einheitengruppe unseres Restklassenrings und der Automorphismengruppe seiner zyklischen Gruppe, das Inverse 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 $(\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\sim} \text{Aut}(C)$ 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 $(\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\sim} \text{Aut}(\mu)$ 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 irreduzibel. 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 ζ eine Nullstelle von f und p prim mit $p \nmid n$ und $g(\zeta^p) = 0$. Nach 3.3.3.2 teilt dann f das Polynom $g(X^p)$, 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 3.9.12 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 3.3.3

$$[\mathbb{Q}(\sqrt[n]{1}) : \mathbb{Q}] = \deg \Phi_n = |(\mathbb{Z}/n\mathbb{Z})^\times|$$

Sicher liefert die Operation der Galoisgruppe auf den n -ten Einheitswurzeln weiter eine Einbettung $\text{Gal}(\mathbb{Q}(\sqrt[n]{1})/\mathbb{Q}) \hookrightarrow \text{Aut}(\mu_n)$ und nach [LA2] 5.3.3 haben wir einen kanonischen Isomorphismus $(\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\sim} \text{Aut}(\mu_n)$. Da diese drei Gruppen alle gleichviele Elemente haben, folgt der Satz. \square

4.4.6. Man erklärt die **Euler'sche φ -Funktion** $\varphi : \mathbb{Z}_{\geq 1} \rightarrow \mathbb{Z}_{\geq 1}$ durch die Vorschrift

$$\begin{aligned} \varphi(n) &= \text{Zahl der zu } n \text{ teilerfremden } d \in \mathbb{N} \text{ mit } 1 \leq d \leq n \\ &= \text{Zahl der Erzeuger der Gruppe } \mathbb{Z}/n\mathbb{Z} \\ &= |\{x \in \mathbb{Z}/n\mathbb{Z} \mid \text{ord}(x) = n\}| \\ &= |(\mathbb{Z}/n\mathbb{Z})^\times| \end{aligned}$$

Wir haben etwa $\varphi(1) = \varphi(2) = 1$, $\varphi(3) = \varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$ und so weiter. Nach 4.4.2 haben wir auch $\varphi(n) = \deg \Phi_n = [\mathbb{Q}(\sqrt[n]{1}) : \mathbb{Q}]$.

Satz 4.4.7 (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 3.6.4. Ist $\varphi(n)$ eine Zweierpotenz, so ist $G = \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ eine 2-Gruppe. Nach 1.3.9 oder einfacher induktiv nach [LA2] 4.3.18 gibt es dann in G eine Kette von Normalteilern von G der Gestalt

$$G = G_r \supset G_{r-1} \supset \dots \supset G_0 = 1$$

mit $G_i/G_{i-1} \cong \mathbb{Z}/2\mathbb{Z}$ für $1 \leq i \leq r$. Deren Fixkörper bilden eine Kette

$$\mathbb{Q} = K_r \subset K_{r-1} \subset \dots \subset K_0 = \mathbb{Q}(\zeta)$$

von Teilkörpern mit $[K_{i-1} : K_i] = 2$ für $1 \leq i \leq r$. Diese Kette hinwiederum zeigt mit 3.6.2, daß ζ konstruierbar ist. \square

Lemma 4.4.8 (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

$$\varphi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1) \quad \square$$

4.4.9 (Diskussion der Zahlen n mit $\varphi(n)$ eine Zweierpotenz). Damit $\varphi(n)$ eine Zweierpotenz ist, darf nach den eben erklärten Rechenregeln 4.4.8 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

$$(1 - X^t) = (1 - X)(1 + X + \dots + X^{t-1})$$

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 4.4.10. 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 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 2009 mit Zitat in Wikipedia gelesen.

Ergänzung 4.4.11. 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 [LA2] 4.3.8 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 4.4.12. 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 $\varphi(d) = |\{x \in \mathbb{Z}/n\mathbb{Z} \mid \text{ord}(x) = d\}|$. In der Tat definiert 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 4.4.13. Man zeige, daß man aus einem regelmäßigen 7-Eck mit Zirkel und Lineal ein regelmäßiges 35-Eck konstruieren kann. Hinweis: Man verwende [3.6.10](#).

Übung 4.4.14. Wieviele zu 140000 teilerfremde Zahlen a mit $1 \leq a \leq 140000$ gibt es?

Übung 4.4.15 (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 4.4.16. 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.

4.5 Quadratisches Reziprozitätsgesetz

4.5.1. 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 nicht a priori 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.

4.5.2 (**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 [LA2] 4.3.11. Nach dieser Bemerkung werden wir uns bei der Untersuchung unserer ursprünglichen Frage auf den Fall beschränken, daß b eine 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.

4.5.3 (**Reduktion auf a teilerfremd zu $b = p^n$**). Sei nun also b eine 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 nur unter der Annahme r gerade ganzzahlig 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 Primzahlpotenz ist und zusätzlich a teilerfremd zu b .

4.5.4 (**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 [LA2] 4.4.31 oder besser seinem Beweis, wo Sie gezeigt haben, daß die Projektion $(\mathbb{Z}/p^n\mathbb{Z})^\times \rightarrow (\mathbb{Z}/p\mathbb{Z})^\times$ faktorisiert über einen Isomorphismus mit der Projektion als zweitem Pfeil in der Form

$$(\mathbb{Z}/p^n\mathbb{Z})^\times \xrightarrow{\sim} \mathbb{Z}/p^{n-1}\mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^\times \rightarrow (\mathbb{Z}/p\mathbb{Z})^\times$$

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 .

4.5.5 (**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 [LA2] 4.4.31 oder besser seinem Beweis, daß sich die offensichtliche Surjektion $(\mathbb{Z}/2^n\mathbb{Z})^\times \rightarrow (\mathbb{Z}/8\mathbb{Z})^\times$ als rechte Vertikale in ein kommutatives Diagramm

$$\begin{array}{ccccc} (\mathbb{Z}/2^n\mathbb{Z})^\times & \xrightarrow{\sim} & \mathbb{Z}/2^{n-2}\mathbb{Z} \times (\mathbb{Z}/4\mathbb{Z})^\times & \xrightarrow{\sim} & \mathbb{Z}/2^{n-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \\ \downarrow & & \downarrow & & \downarrow \\ (\mathbb{Z}/8\mathbb{Z})^\times & \xrightarrow{\sim} & \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/4\mathbb{Z})^\times & \xrightarrow{\sim} & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \end{array}$$

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.

4.5.6. 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 [LA1] 4.3.35, 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 4.5.17 erklären wir, wie diese Frage für endliche Primkörper durch das Zusammenwirken von quadratischem Reziprozitätsgesetz 4.5.7 und Ergänzungssatz 4.5.16 effizient gelöst werden kann.

Satz 4.5.7 (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 4.5.8. 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.

4.5.9. Wir schicken dem Beweis einige allgemeine Überlegungen voraus. Ich erinnere zunächst daran, daß nach [LA2] 4.4.25 jede nichttriviale zyklische Gruppe G gerader Ordnung $2n$ genau eine Untergruppe mit zwei Elementen und genau eine Untergruppe vom Index Zwei hat. Für den in additiver Notation geschriebenen Gruppenhomomorphismus

$$(n\cdot) : G \rightarrow G$$

ist das Bild die einzige Untergruppe mit zwei Elementen und der Kern die einzige Untergruppe vom Index Zwei. Für den in additiver Notation geschriebenen Gruppenhomomorphismus

$$(2\cdot) : G \rightarrow G$$

ist dahingegen das Bild die einzige Untergruppe vom Index Zwei und der Kern die einzige Untergruppe mit zwei Elementen.

4.5.10. Im Fall der additiven Gruppe $\mathbb{Z}/2n\mathbb{Z}$ ist zum Beispiel $\{\bar{0}, \bar{n}\} = n\mathbb{Z}/2n\mathbb{Z}$ die einzige zweielementige Untergruppe und $2\mathbb{Z}/2n\mathbb{Z}$ die einzige Untergruppe vom Index Zwei.

4.5.11. 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 Zwei und das Potenzieren mit $(p-1)/2$ ist ein surjektiver Gruppenhomomorphismus $\mathbb{F}_p^\times \rightarrow \{1, -1\}$ 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

$$\left(\frac{a}{p}\right) := \begin{cases} 0 & a \text{ ist ein Vielfaches von } p; \\ 1 & a \text{ ist kein Vielfaches von } p, \text{ aber ein Quadrat modulo } p; \\ -1 & \text{sonst,} \end{cases}$$

Für p eine ungerade Primzahl erhalten wir damit die Identität

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

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.

Beweis des quadratischen Reziprozitätsgesetzes. Wir betrachten den p -ten Kreisteilungskörper $\mathbb{Q}(\sqrt[p]{1})$ mit $\sqrt[p]{1} = \zeta$ einer primitiven p -ten Einheitswurzel. Darin betrachten wir den Teiltring $\mathbb{Z}[\zeta]$ und darin das Element

$$\alpha := \sum_{a \in \mathbb{F}_p^\times} \left(\frac{a}{p} \right) \zeta^a$$

Ich erkläre im Anschluß, wie man mit Galoistheorie auf diesen Ansatz kommt und warum dann $\alpha^2 \in \mathbb{Q}$, ja sogar $\alpha^2 \in \mathbb{Z}$ eh klar ist. Hier machen wir einfach eine explizite Rechnung und erhalten sogar genauer die Formel

$$\alpha^2 = (-1)^{\frac{p-1}{2}} p$$

In der Tat, beachten wir $\left(\frac{ab^2}{p} \right) = \left(\frac{a}{p} \right)$, 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 $\left(\frac{-1}{p} \right) (p-1)$. Bei $a \neq -1$ beachten wir, daß für $\eta = \zeta^{a+1}$ wie für jede primitive p -te Einheitswurzel die Relation

$$1 + \eta + \eta^2 + \dots + \eta^{p-1} = 0$$

erfüllt ist, so daß die Summanden mit $a \neq -1$ jeweils den Beitrag $-\left(\frac{a}{p} \right)$ liefern. Da nun die Summe der $\left(\frac{a}{p} \right)$ über alle $a \in \mathbb{F}_p^\times$ verschwindet, liefern alle Summanden mit $a \neq -1$ zusammen den Beitrag $\left(\frac{-1}{p} \right)$ und mit **4.5.10** folgern wir

$$\alpha^2 = \left(\frac{-1}{p} \right) p = (-1)^{\frac{p-1}{2}} p$$

Ist p eine ungerade Primzahl und ζ eine primitive p -te Einheitswurzel, so besitzt demnach $(-1)^{\frac{p-1}{2}} p$ die Quadratwurzel $\alpha \in \mathbb{Z}[\zeta]$. Das quadratische Reziprozitätsgesetz ergibt sich nun, indem wir für unsere zweite Primzahl q den Körperhomomorphismus $\sigma_q : \mathbb{Q}(\zeta) \rightarrow \mathbb{Q}(\zeta)$ mit $\zeta \mapsto \zeta^q$ aus **3.8.32** oder alternativ **4.4.2** betrachten, und das Vorzeichen, mit dem er aus α wirkt, auf zwei Weisen berechnen. Ein Vergleich der Resultate zeigt dann das Reziprozitätsgesetz. Einerseits erhalten wir durch Umsummieren

$$\sigma_q(\alpha) = \left(\frac{q}{p} \right) \alpha$$

Andererseits erhalten für beliebiges $\alpha = \sum c_i \zeta^i \in \mathbb{Z}[\zeta] := R$ mit der Notation \equiv für die Gleichheit im Restklassenring R/qR unter Verwendung des Frobeniushomomorphismus

$$\sigma_q(\alpha) = \sigma_q\left(\sum c_i \zeta^i\right) = \sum c_i \zeta^{qi} \equiv \sum c_i^q \zeta^{qi} \equiv \alpha^q \pmod{qR}$$

Beide Formeln zusammen liefern für unser spezielles α dann

$$\left(\frac{q}{p}\right) \alpha \equiv \alpha^q \pmod{qR}$$

Unser Ring R ist nun offensichtlich eine endlich erzeugte torsionsfreie abelsche Gruppe, insbesondere gilt für unsere Primzahl q notwendig $qR \neq \mathbb{Z}[\zeta]$ und damit $1 \notin qR$ und damit $qR \cap \mathbb{Z} = q\mathbb{Z}$. Da $\alpha^2 = (-1)^{\frac{p-1}{2}} p$ und damit auch α invertierbar sind in R/qR , folgt

$$\left(\frac{q}{p}\right) \equiv (\alpha^2)^{\frac{q-1}{2}} \equiv p^{\frac{q-1}{2}} (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \equiv \left(\frac{p}{q}\right) (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \pmod{qR}$$

mit 4.5.10 im letzten Schritt. Hier sind jedoch beide Seiten ganze Zahlen, also gilt diese Kongruenz auch modulo $q\mathbb{Z}$. Am Anfang und am Ende dieser Kette von Kongruenzen stehen weiter die Zahlen ± 1 zur Auswahl, folglich gilt dort sogar Gleichheit. Man überzeugt sich aber mühelos anhand der Definitionen, daß diese Gleichheit gerade bedeutet, was wir in Worten als quadratisches Reziprozitätsgesetz formuliert hatten. \square

4.5.12 (Der Beweis des Reziprozitätsgesetzes im Licht der Galoistheorie). Wir haben für p eine ungerade Primzahl und ζ eine primitive p -te Einheitswurzel in 4.4.2 einen Isomorphismus $\mathbb{F}_p^\times \xrightarrow{\sim} \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ konstruiert. Er zeigt daß diese Galoisgruppe eine zyklische Gruppe von gerader Ordnung ist. Sie hat also genau eine Untergruppe vom Index Zwei und nach der Galois-Korrespondenz hat dann auch $\mathbb{Q}(\zeta)$ genau einen Unterkörper, der eine quadratische Erweiterung von \mathbb{Q} ist. Bezeichnet $G := \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ die Galoisgruppe in additiver Notation, so sind die Elemente dieser quadratischen Erweiterung genau die Fixpunkte der Untergruppe $2G$ und diejenigen Elemente unserer quadratischen Erweiterung außerhalb von \mathbb{Q} , deren Quadrat in \mathbb{Q} liegt, sind darin die Eigenvektoren zum Eigenwert (-1) jedes Elements von G , das nicht in $2G$ liegt. Das sind nun genau alle von Null verschiedenen Elemente der Gestalt

$$\alpha = \sum_{\sigma \in 2G} \sigma(\gamma) - \sum_{\sigma \notin 2G} \sigma(\gamma)$$

für beliebiges $\gamma \in \mathbb{Q}(\zeta)$. Unser α aus obigem Beweis ist nun genau dieses α im Fall $\gamma = \zeta$. Es war also eh klar, daß wir $\alpha^2 \in \mathbb{Q}$ finden mußten. Daß wir sogar

$\alpha^2 \in \mathbb{Z}$ finden mußten, liegt an der Identität $\mathbb{Q} \cap \mathbb{Z}[\zeta] = \mathbb{Z}$. In der Tat ist $\mathbb{Z}[\zeta]$ eine endlich erzeugte abelsche Gruppe, der Schnitt ist also auch eine endlich erzeugte abelsche Gruppe, andererseits aber auch ein Teilring von \mathbb{Q} , und diese beiden Eigenschaften zusammen zeigen nach Übung 2.2.8 bereits, daß unser Schnitt \mathbb{Z} sein muß.

4.5.13. Versteckt im Beweis des quadratischen Reziprozitätsgesetzes ist die Aussage, daß für jede ungerade Primzahl p die Zahl $(-1)^{\frac{p-1}{2}} p$ im p -ten Kreisteilungskörper eine Wurzel besitzt. Die durch Adjunktion einer solchen Wurzel entstehende quadratische Erweiterung von \mathbb{Q} ist also unsere eindeutig bestimmte quadratische Erweiterung von \mathbb{Q} im p -ten Kreisteilungskörper. Explizit prüft man für eine von Null verschiedene dritte Einheitswurzel ζ leicht $(\zeta - \zeta^2)^2 = -3$ und damit $\pm\sqrt{-3} \in \mathbb{Q}(\sqrt[3]{1})$ und die Beziehung zwischen regelmäßigem Fünfeck und dem goldenen Schnitt [AN2] ?? zeigt $\sqrt{5} \in \mathbb{Q}(\sqrt[5]{1})$.

Vorschau 4.5.14. Vom höheren Standpunkt aus betrachtet mögen Sie, falls Sie sich weiter mit Zahlentheorie beschäftigen, die beim Beweis des Reziprozitätsgesetzes gegebene Argumentation wie folgt einordnen: Man kann die Frage nach der Lösbarkeit polynomialer Gleichungen in ganzen Zahlen, sogenannter **diophantischer Gleichungen**, oft uminterpretieren als Frage nach dem „Verzweigungsverhalten“ endlicher algebraischer Erweiterungen des Körpers der rationalen Zahlen. Allgemeiner als im analogen Fall der Riemann’schen Flächen kann sich der Grad der Erweiterung lokal auf drei Weisen bemerkbar machen: (1) Verzweigung, (2) mehrere Stellen über einer gegebenen lokalen Stelle und (3) Erweiterung des Restklassenkörpers. Erster zu untersuchender Fall ist natürlich a priori der Fall quadratischer Erweiterungen, und speziell der Fall der Adjunktion der Wurzel aus einer Primzahl oder auch aus dem Negativen einer Primzahl. Als viel einfacher erweist sich jedoch der Fall der Kreisteilungskörper, in dem alles explizit ausgerechnet werden kann. Und nun basiert der im folgenden gegebene Beweis des quadratischen Reziprozitätsgesetzes im wesentlichen auf dem Trick, den durch Adjunktion der Quadratwurzel einer Primzahl, genauer den durch Adjunktion der Quadratwurzel aus $(-1)^{\frac{p-1}{2}} p$ für eine ungerade Primzahl p , entstehenden Körper als Teilkörper des p -ten Kreisteilungskörpers zu realisieren und besagte Frage im Fall quadratischer Erweiterungen auf diesem Wege zu lösen.

4.5.15. Wann 2 ein Quadrat ist modulo einer ungeraden Primzahl p , das sagt uns der folgende „Ergänzungssatz zum quadratischen Reziprozitätsgesetz“.

Proposition 4.5.16 (Ergänzungssatz). *Für jede ungerade Primzahl q gilt*

$$\left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}} = \begin{cases} 1 & \text{für } q \equiv \pm 1 \pmod{8}; \\ -1 & \text{für } q \equiv \pm 3 \pmod{8}. \end{cases}$$

Beweis. Wir betrachten die primitive achte Einheitswurzel $\zeta = \exp(\pi i/4)$. Wir prüfen $\zeta + \zeta^{-1} = \sqrt{2}$. Bezeichne σ_q das Element der Galoisgruppe mit $\zeta \mapsto \zeta^q$.

Sei ε_q das Vorzeichen mit $\sigma_q(\sqrt{2}) = \varepsilon_q\sqrt{2}$. Wir rechnen im Ring $R := \mathbb{Z}[\zeta]$ und erhalten

$$\varepsilon_q\sqrt{2} = \sigma_q(\sqrt{2}) = \zeta^q + \zeta^{-q} \equiv (\zeta + \zeta^{-1})^q \equiv (\sqrt{2})^q \pmod{qR}$$

Es folgt $\varepsilon_q \equiv (\sqrt{2})^{q-1} \equiv 2^{\frac{q-1}{2}} \pmod{q}$ und damit $\varepsilon_q = \left(\frac{2}{q}\right)$. Für das Vorzeichen ε_q prüft man andererseits anhand der Formel $\varepsilon_q(\zeta + \zeta^{-1}) = \zeta^q + \zeta^{-q}$ leicht explizit, daß es durch die im Ergänzungssatz behauptete Formel gegeben wird. \square

Ergänzung 4.5.17. 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 $n = p_1 p_2 \dots p_r$ das Jacobi-Symbol als Produkt von Legendre-Symbolen

$$\left(\frac{a}{n}\right) := \left(\frac{a}{p_1}\right) \left(\frac{a}{p_2}\right) \dots \left(\frac{a}{p_r}\right)$$

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

$$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right) \left(\frac{b}{n}\right)$$

Schließlich folgt aus dem quadratischen Reziprozitätsgesetz 4.5.7, daß allgemeiner für je zwei ungerade Zahlen $m, n > 1$ 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 $n > 1$ folgt schließlich aus dem Ergänzungssatz 4.5.16 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

$$\begin{aligned} \left(\frac{1231}{1549}\right) &= \left(\frac{1549}{1231}\right) = \left(\frac{318}{1231}\right) = \left(\frac{2}{1231}\right) \left(\frac{159}{1231}\right) = \left(\frac{159}{1231}\right) = -\left(\frac{1231}{159}\right) = -\left(\frac{118}{159}\right) = \\ &= -\left(\frac{2}{159}\right) \left(\frac{59}{159}\right) = -\left(\frac{59}{159}\right) = -\left(\frac{159}{59}\right) = -\left(\frac{41}{59}\right) = -\left(\frac{59}{41}\right) = -\left(\frac{18}{41}\right) = \\ &= -\left(\frac{2}{41}\right) \left(\frac{9}{41}\right) = -\left(\frac{9}{41}\right) = -\left(\frac{41}{9}\right) = -\left(\frac{5}{9}\right) = -\left(\frac{9}{5}\right) = -\left(\frac{4}{5}\right) = -\left(\frac{2}{5}\right)^2 = -1 \end{aligned}$$

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 4.5.18. 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 4.5.19. Im Fall $a = -1$ kennen wir das das Resultat der vorhergehenden Übung 4.5.18 im Übrigen bereits aus 2.6.6. 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 4.5.20. 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 4.5.21. 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 4.5.22. Ist 283 ein quadratischer Rest modulo 397? Hinweis: 397 ist eine Primzahl.

Übung 4.5.23. Gibt es eine Quadratzahl, deren Darstellung im Dezimalsystem mit der Ziffernfolge 39 endet? Für welche Ziffern $a, b \in \{0, 1, \dots, 9\}$ gibt es eine Quadratzahl, die mit der Ziffernfolge ab endet?

4.6 Radikalerweiterungen

Definition 4.6.1. Eine Galoiserweiterung mit zyklischer Galoisgruppe heißt eine **zyklische Erweiterung**. Eine Galoiserweiterung mit abelscher Galoisgruppe heißt eine **abelsche Erweiterung**.

4.6.2. 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 4.6.3 (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:*

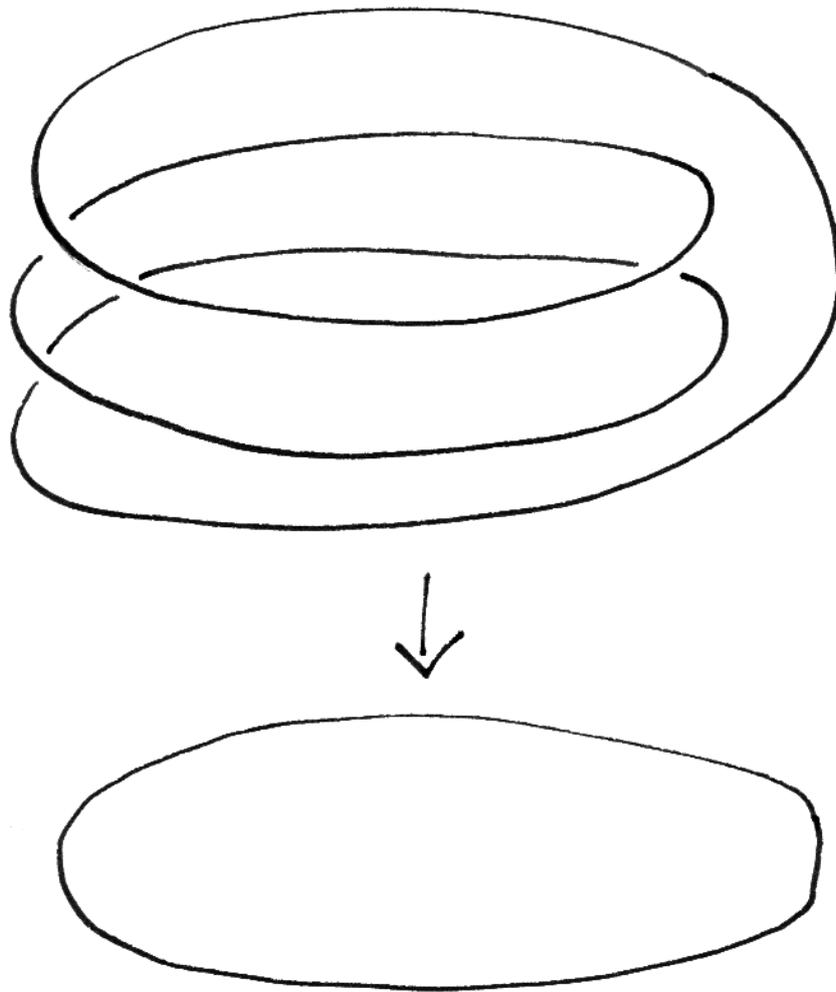
1. *Alle zyklischen Erweiterungen von K vom Grad n entstehen durch die Adjunktion einer n -ten Wurzel;*
2. *Adjungieren wir zu K eine n -te Wurzel, so erhalten wir eine zyklische Erweiterung, deren Grad n teilt.*

4.6.4. Der Beweis beschreibt im Fall einer zyklischen Erweiterung vom Grad n sogar die Elemente genauer, deren n -te Potenz im Grundkörper liegt und die unsere Erweiterung erzeugen: Es handelt sich genau um alle Eigenvektoren eines beliebigen Erzeugers der Galoisgruppe mit einer primitiven n -ten Einheitswurzel als Eigenwert.

4.6.5 (**Adjunktion von Einheitswurzeln und anderen Wurzeln, 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 Einfachheit halber Charakteristik Null voraus, so ist im ersten Fall nach 4.4.2 und 4.6.10 die Ordnung der Galois-Gruppe ein Teiler von $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$, im zweiten Fall jedoch 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 $a = \alpha^n$, so sind die Wurzeln des Polynoms $X^n - a$ die $\zeta\alpha$ mit ζ den n -ten Einheitswurzeln, folglich ist unsere Erweiterung Galois. Weiter erhalten wir eine Injektion der Galois-Gruppe in die Gruppe μ_n der n -ten Einheitswurzeln, indem wir jedem $\sigma \in \text{Gal}(L/K)$ diejenige Einheitswurzel ζ zuordnen mit $\sigma(\alpha) = \zeta\alpha$, also die Einheitswurzel $\sigma(\alpha)/\alpha$. Da nach [LA2] 4.4.17 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 $\sigma \neq \text{id}$ ein Erzeuger der Galoisgruppe. Wir fassen σ auf als eine K -lineare Abbildung $\sigma : L \rightarrow L$. Da gilt $\sigma^n = \text{id}$ 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 4.6.6 diagonalisierbar und seine



Anschauung für die durch Adjunktion einer dritten Wurzel aus T entstehenden Körpererweiterung des Funktionenkörpers $\mathbb{C}(T)$. Am zweiten Bild zu ?? 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.

Eigenwerte sind n -te Einheitswurzeln. Da aus $\sigma(\alpha) = \zeta\alpha$ und $\sigma(\beta) = \eta\beta$ für n -te Einheitswurzeln ζ, 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 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 $\alpha, \alpha^2, \dots, \alpha^n$ sind linear unabhängig über K als Eigenvektoren zu paarweise verschiedenen Eigenwerten von σ . Es folgt $[K(\alpha) : K] = n$ und damit $L = K(\alpha)$. \square

Proposition 4.6.6. *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 $Q = (X - \lambda_1) \dots (X - \lambda_r)$ von P kleinstmöglichen Grades r mit $Q(f) : v \mapsto 0$. Dann ist $E := \langle v, f(v), f^2(v), \dots, f^{r-1}(v) \rangle$ ein unter f stabiler Untervektorraum von V . Andererseits ist $(f - \lambda_2) \dots (f - \lambda_r)v$ 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 $\lambda_2, \dots, \lambda_r$. Da Eigenvektoren zu paarweise verschiedenen Eigenwerten linear unabhängig sind nach [LA1] 5.6.18, ist damit $f|_E$ diagonalisierbar und v eine Summe von Eigenvektoren von f . Die Proposition folgt. \square

Zweiter Beweis. Der chinesische Restsatz liefert einen Ringisomorphismus

$$K[X]/\langle P \rangle \xrightarrow{\sim} K[X]/\langle X - \lambda_1 \rangle \times \dots \times K[X]/\langle X - \lambda_n \rangle$$

für λ_i die Nullstellen von P . Ist $1 = e_1 + \dots + e_n$ 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 $v = e_1v + \dots + e_nv$ eine Zerlegung mit $e_iv \in \text{Eig}(f; \lambda_i)$. \square

Korollar 4.6.7 (Adjunktion primer Wurzeln). *Seien p eine Primzahl und K ein Körper einer Charakteristik $\text{char } K \neq p$, 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 4.6.3. \square

Definition 4.6.8. Sind in einem Körper Ω zwei Teilkörper $K, L \subset \Omega$ gegeben, so bezeichnet $(KL) \subset \Omega$ den von K und L erzeugten Teilkörper. Man nennt diesen Körper das **Kompositum von K und L** .

4.6.9 (**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 [GR] 3.1.3 a priori nur die Menge aller Produkte bedeutet und man oft runde Klammern als Symbol für die „Erzeugung als Körper“ verwendet.

Satz 4.6.10 (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*

$$\text{Gal}((KL)/K) \xrightarrow{\sim} \text{Gal}(L/K \cap L)$$

4.6.11. 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 4.6.12. 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 6.2.2.

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 4.1.14 der Fixkörper der Galoisgruppe, in Formeln gilt also $K = (KL)^G$ für $G = \text{Gal}((KL)/K)$. Da L normal ist über $(K \cap L)$, stabilisieren alle Körperautomorphismen von (KL) über K den Unterkörper L , und die durch Restriktion gegebene Abbildung $\text{res} : \text{Gal}((KL)/K) \rightarrow \text{Gal}(L/(K \cap L))$ zwischen den Galoisgruppen ist offensichtlich injektiv. Der Fixkörper des Bildes von res ist aber genau $K \cap L$, und das zeigt mit unserem Satz 4.1.12 über Galoiserweiterungen durch Gruppenoperationen die Bijektivität von res . \square

Korollar 4.6.13. *Sind in einem großen 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*

$$\text{Gal}((TM)/(SM)) \hookrightarrow \text{Gal}(T/S)$$

Beweis. Mit $T \supset S$ ist ja erst recht $T \supset (T \cap (SM))$ Galois, also nach dem Translationsatz 4.6.10 auch $(TM) = (T(SM)) \supset (SM)$, und diese beiden Erweiterungen haben nach dem Translationsatz auch dieselbe Galoisgruppe. \square

Definition 4.6.14. Sei L/K eine Körpererweiterung. Wir nennen L eine **Radikalerweiterung von K** , wenn es eine Körperkette

$$K = K_0 \subset K_1 \subset K_2 \subset \dots \subset K_r = L$$

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 $K_i = K_{i-1}(\alpha_i)$.

4.6.15. 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 4.6.16. 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 4.6.17. 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 4.6.18. Seien K ein Körper und $P \in K[X]$ ein Polynom. Wir sagen, die Gleichung $P(X) = 0$ läßt sich **aufösen durch Radikale**, wenn sich alle Nullstellen des Polynoms P in seinem Zerfällungskörper durch Radikale über K darstellen lassen. Ist unser Polynom irreduzibel, so ist es offensichtlich auch gleichbedeutend, daß sich eine Nullstelle durch Radikale über K darstellen läßt.

4.6.19. Ich erinnere, daß eine Gruppe G nach 1.3.10 **auflösbar** heißt, wenn es eine Folge von Untergruppen $G = G_0 \supset G_1 \supset G_2 \supset \dots \supset G_r = 1$ gibt mit G_i normal in G_{i-1} und G_{i-1}/G_i abelsch für $1 \leq i \leq r$.

Satz 4.6.20 (Auflösbarkeit von Gleichungen durch Radikale). Seien K ein Körper der Charakteristik $\text{char } K = 0$ und $P \in K[X]$ ein 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 der anschließenden Proposition 4.6.21 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 $\text{Gal}(L/K)$ ein Quotient der Galoisgruppe $\text{Gal}(M/K)$ ist, und da nach 1.3.16 Quotienten auflösbarer Gruppen auflösbar sind, ist das auch gleichbedeutend dazu, daß L selbst eine auflösbare Galoisgruppe hat. \square

Proposition 4.6.21. *Sei K ein Körper der Charakteristik $\text{char } K = 0$ 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. Nun, es gilt zu zeigen, daß sich jede Radikalerweiterung einbetten läßt in eine endliche Galoiserweiterung mit auflösbarer Galoisgruppe und umgekehrt, daß sich jede endliche Galoiserweiterung mit auflösbarer Galoisgruppe einbetten läßt in eine Radikalerweiterung. Wir beginnen mit letzterem.

$2 \Rightarrow 1$. Sei L/K eine endliche Galoiserweiterung mit auflösbarer Galoisgruppe $G = \text{Gal}(L/K)$. So gibt es eine Folge von Untergruppen

$$G = G_0 \supset G_1 \supset \dots \supset G_r = 1$$

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

$$K = K_0 \subset K_1 \subset \dots \subset K_r = L$$

Adjungieren wir eine primitive $|G|$ -te Einheitswurzel ζ , so erhalten wir nach dem Translationsatz 4.6.10 oder besser seinem Korollar 4.6.13 wieder eine Kette

$$K = K_0 \subset K_0(\zeta) \subset K_1(\zeta) \subset \dots \subset K_r(\zeta) = L(\zeta)$$

von Galoiserweiterungen. Nach unserem Satz über Adjunktion primer Wurzeln 4.6.7 entsteht 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

$$K = K_0 \subset K_1 \subset K_2 \subset \dots \subset K_r = L$$

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

$$K = K_0 \subset K_0(\zeta) \subset K_1(\zeta) \subset \dots \subset K_r(\zeta) = L(\zeta)$$

jeder Schritt eine abelsche Erweiterung: Das folgt, indem wir den Translationsatz der Galoistheorie oder besser 4.6.13 im ersten Schritt auf die nach 4.4.2 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 betrachten darin das Kompositum $M \subset N$ aller $\varphi(L(\zeta))$ mit $\varphi \in \text{Ring}^K(L(\zeta), N)$, also die normale Hülle von $L(\zeta)$, so ist M eine Galoiserweiterung von K und es gibt einen Körperturm

$$K = M_0 \subset M_1 \subset M_2 \subset \dots \subset M_t = M$$

in dem jede Stufe eine abelsche Erweiterung ist: Um solch einen Körperturm anzugeben, zählen wir unsere φ auf als $\varphi_1, \dots, \varphi_m$, beginnen mit $M_1 = M_0(\zeta)$ und adjungieren der Reihe nach $\varphi_1(\alpha_1), \varphi_1(\alpha_2), \dots, \varphi_1(\alpha_r), \varphi_2(\alpha_1), \varphi_2(\alpha_2), \dots, \varphi_2(\alpha_r), \dots, \varphi_m(\alpha_1), \varphi_m(\alpha_2), \dots, \varphi_m(\alpha_r)$. Die Galoiskorrespondenz zeigt dann, daß die Galoisgruppe $\text{Gal}(M/K)$ auflösbar ist. \square

Proposition 4.6.22. *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 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 1.4.8 ein $g \in G$ von der Ordnung $\text{ord } g = 5$. Man sieht etwa mit [LA1] 5.1.10, daß g und τ schon ganz S_5 erzeugen. \square

Beispiel 4.6.23. 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 2.8.2. Seine Galoisgruppe ist nach 4.6.22 folglich nicht auflösbar, und damit kann nach 4.6.20 die Gleichung $X^5 - 16X + 2 = 0$ nicht durch Radikale gelöst werden.

Beispiel 4.6.24. Das Polynom $X^5 - 2$ in $\mathbb{Q}[X]$ ist irreduzibel nach dem Eisensteinkriterium 2.8.2. Es ist jedoch durchaus auflösbar durch Radikale.

Übungen

Übung 4.6.25. Seien p, q Primzahlen. So ist die Galoisgruppe des Zerfällungskörpers 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 .

Übung 4.6.26. 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 Galoisweiterungen, so ist auch $(KL) \supset (K \cap L)$ eine endliche Galoisweiterung und die Restriktionen liefern einen Gruppenisomorphismus

$$\text{Gal}((KL)/K \cap L) \xrightarrow{\sim} \text{Gal}(K/K \cap L) \times \text{Gal}(L/K \cap L)$$

4.7 Lösung kubischer Gleichungen

4.7.1. 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 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 4.7.2. *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.

4.7.3. 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 4.7.6 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 $\zeta u = v$, damit das Verschwinden der Diskriminante $27q^2 + 4p^3$, und damit gibt es auch nur höchstens zwei Lösungen nach 2.9.13. 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 $y = 0$. \square

4.7.4. 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. Sei dazu k ein Körper einer von Zwei und Drei verschiedenen Charakteristik $\text{char } k \neq 2, 3$, der eine nichttriviale dritte Einheitswurzel $\zeta = \sqrt[3]{1} \in k$ enthalten möge. Wir bilden den Funktionenkörper

$$K = k(p, q) = \text{Quot } k[p, q]$$

in zwei über k algebraisch unabhängigen Veränderlichen p und q . Unser Polynom $Y^3 + pY + q$ ist dann irreduzibel in $K[Y]$, denn nach 2.7.11 muß jede Faktorisierung von einer Faktorisierung im Polynomring $k[p, q, Y]$ herkommen, in der wir $p = q$ setzen könnten und so einen Widerspruch zum Eisensteinkriterium für faktorielle Ringe 2.8.3 erhielten. Ist L/K ein Zerfällungskörper unseres Polynoms, so schreiben wir

$$Y^3 + pY + q = (Y - \alpha)(Y - \beta)(Y - \gamma)$$

mit $\alpha, \beta, \gamma \in L$ und erhalten

$$\begin{aligned} \alpha + \beta + \gamma &= 0 \\ \alpha\beta + \beta\gamma + \gamma\alpha &= p \\ -\alpha\beta\gamma &= q = \alpha^2\beta + \beta^2\alpha \end{aligned}$$

Da die Diskriminante $4p^3 + 27q^2$ aus 2.9.13 in unserem Fall nicht verschwindet, sind die drei Nullstellen paarweise verschieden und unsere Erweiterung ist Galois. Die Galoisgruppe von L/K muß treu und transitiv operieren als eine Gruppe von Permutationen der Menge $\{\alpha, \beta, \gamma\}$ der drei Wurzeln. Damit kommen für diese Galoisgruppe nur die Gruppe \mathcal{S}_3 aller Permutationen und die Gruppe A_3 aller geraden Permutationen in Betracht. Der Fixkörper des Normalteilers A_3 der geraden Permutationen enthält das Element

$$E = (\alpha - \beta)(\beta - \gamma)(\gamma - \alpha) = -2\alpha^3 - 3\alpha^2\beta + 3\alpha\beta^2 + 2\beta^3$$

Nach 2.9.13 oder auch elementarer Rechnung ist sein Quadrat bis auf ein Vorzeichen die Diskriminante, genauer gilt

$$E^2 = -4p^3 - 27q^2$$

Hier sei gleich die Formel $(\zeta^2 - \zeta)^2 = -3$ bemerkt, das Quadrat von $(\zeta^2 - \zeta)E/18$ ist also genau der Ausdruck, von dem in der Cardano'schen Formel die Quadratwurzel zu ziehen war. Ist die Charakteristik unseres Körpers nicht gerade Zwei, so ist $-4p^3 - 27q^2$ nach 2.7.19 in $K = k(p, q)$ kein Quadrat und wir folgern $[K(E) : K] = 2$. Da nun unsere Erweiterung L/K höchstens Grad 6 haben kann und da L über dem Fixkörper der geraden Permutationen notwendig Grad drei hat, muß $K(E)$ bereits dieser Fixkörper sein und $L/K(E)$ ist eine Galoiserweiterung mit der Galoisgruppe A_3 . Sei nun $\sigma \in G$ der Erzeuger dieser Galoisgruppe mit $\sigma(\alpha) = \beta$, $\sigma(\beta) = \gamma$ und $\sigma(\gamma) = \alpha$. Nach 4.6.4 entsteht dann L aus $K(E)$ durch Adjunktion eines Eigenvektors von σ zu einem von 1 verschiedenen Eigenwert. Hier benötigen wir unsere Voraussetzung, daß es in k nichttriviale dritte Einheitswurzeln gibt, und damit ist insbesondere auch der Fall der Charakteristik drei ausgeschlossen. Die dritte Potenz eines solchen Eigenvektors liegt in $K(E)$, so daß L aus $K(E)$ entsteht durch Adjunktion einer Kubikwurzel. Ist $\zeta \in k$ eine nichttriviale dritte Einheitswurzel, so liegt zum Beispiel

$$\begin{aligned} u &= \alpha + \zeta\sigma(\alpha) + \zeta^2\sigma^2(\alpha) \\ &= (1 - \zeta^2)\alpha + (\zeta - \zeta^2)\beta \end{aligned}$$

im Eigenraum $\text{Eig}(\sigma; \zeta^2)$ und ist nicht Null, da sonst gälte $\beta \in k\alpha$ im Widerspruch zu $\sigma(\alpha) = \beta \neq \alpha$. Ebenso erzeugt

$$\begin{aligned} v &= \alpha + \zeta^2\sigma(\alpha) + \zeta\sigma^2(\alpha) \\ &= (1 - \zeta)\alpha + (\zeta^2 - \zeta)\beta \end{aligned}$$

den Eigenraum $\text{Eig}(\sigma; \zeta)$ als $K(E)$ -Vektorraum und die 1 erzeugt als $K(E)$ -Vektorraum den Eigenraum $\text{Eig}(\sigma; 1)$. Die drei Elemente $u, v, 1$ bilden also eine $K(E)$ -Basis von L und wir müssen unsere drei Wurzeln linear aus ihnen kombinieren können. In der Tat erhalten wir unmittelbar $u + v = 3\alpha$ und dann durch Teilen durch Drei und Anwenden von σ

$$\alpha = \frac{u}{3} + \frac{v}{3} \quad \beta = \zeta^2 \frac{u}{3} + \zeta \frac{v}{3} \quad \gamma = \zeta \frac{u}{3} + \zeta^2 \frac{v}{3}$$

Die dritten Potenzen von u und von v müssen nun wie gesagt in $K(E)$ liegen, also als K -Linearkombinationen von 1 und E zu schreiben sein. Um besagte dritte Potenzen explizit darzustellen, zerlegen wir sie unter dem Element τ der Galoisgruppe, das α und β vertauscht, in Eigenvektoren: Schreiben wir $2v^3 =$

$(v^3 + \tau(v^3)) + (v^3 - \tau(v^3))$, so muß offensichtlich der erste Summand zu K gehören und der zweite zu KE . Nun können wir ja unsere obige Gleichung auch umformen zu $v = (1 - \zeta)(\alpha - \zeta\beta)$. Packen wir der Einfachheit der Rechnung halber den Faktor $(1 - \zeta)$ noch auf die andere Seite und setzen $\tilde{v} := (1 - \zeta)^{-1}v = \alpha - \zeta\beta$, so erhalten wir

$$\begin{aligned}\tilde{v}^3 &= +\alpha^3 - 3\zeta\alpha^2\beta + 3\zeta^2\alpha\beta^2 - \beta^3 \\ \tau(\tilde{v})^3 &= -\alpha^3 + 3\zeta^2\alpha^2\beta - 3\zeta\alpha\beta^2 + \beta^3 \\ \tilde{v}^3 + \tau(\tilde{v})^3 &= 3(\zeta^2 - \zeta)(\alpha^2\beta + \alpha\beta^2) &&= 3(\zeta^2 - \zeta)q \\ \tilde{v}^3 - \tau(\tilde{v})^3 &= 2\alpha^3 - 3(\zeta + \zeta^2)\alpha^2\beta + 3(\zeta + \zeta^2)\alpha\beta^2 - 2\beta^3 \\ &= 2\alpha^3 + 3\alpha^2\beta - 3\alpha\beta^2 - 2\beta^3 &&= -E\end{aligned}$$

und damit $2\tilde{v}^3 = 3(\zeta^2 - \zeta)q - E$ und wegen $(1 - \zeta)^3 = 3(\zeta^2 - \zeta)$ und $(\zeta^2 - \zeta)^2 = \zeta + \zeta^2 - 2 = -3$ schließlich

$$\left(\frac{v}{3}\right)^3 = -\frac{q}{2} + \frac{(\zeta - \zeta^2)E}{18}$$

Genauso liefert Ersetzen von ζ durch ζ^2 in obiger Rechnung auch

$$\left(\frac{u}{3}\right)^3 = -\frac{q}{2} - \frac{(\zeta - \zeta^2)E}{18}$$

und es folgt, daß die beiden Ausdrücke

$$-\frac{q}{2} \pm \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}$$

genau $\left(\frac{v}{3}\right)^3$ und $\left(\frac{u}{3}\right)^3$ liefern. Unsere Lösung α hat also die Gestalt

$$\alpha = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$

Wenn wir andererseits die beiden kubischen Wurzeln so ziehen, daß ihr Produkt gerade $-p/3$ ist, so erhalten wir auch stets Lösungen.

4.7.5. Haben wir statt dem Funktionenkörper $K = k(p, q)$ einen beliebigen Körper K einer Charakteristik $\text{char } K \neq 2, 3$ mit nichttrivialen dritten Einheitswurzeln vor uns, so kann obiges Argument in verschiedener Weise zusammenbrechen: Unser Polynom muß nicht irreduzibel sein, und wenn es irreduzibel ist, könnte seine Galoisgruppe nur aus den drei geraden Permutationen der drei Nullstellen bestehen. In diesen Fällen funktioniert das obige Argument nur noch in mehr oder

weniger stark modifizierter Form. Es scheint mir jedoch einigermaßen klar, daß unsere für allgemeines p, q hergeleiteten Formeln ihre Gültigkeit behalten sollten, „was immer man für p und q einsetzt, solange dabei nicht Nullen in Nennern auftreten“. In unserem Fall haben wir das ja sogar in 4.7.3 bereits explizit geprüft. Für eine formale Begründung muß ich Sie auf spezialisiertere Vorlesungen verweisen.

4.7.6 (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 keine zum Koeffizientenkörper $K := \mathbb{Q}(p, q) \subset \mathbb{R}$ gehört, etwa unsere Gleichung $X^3 - 16X + 2 = 0$ aus 4.6.23. Wir zeigen, daß es dann nicht möglich ist, eine Kette

$$K = K_0 \subset K_1 \subset \dots \subset K_r \subset \mathbb{R}$$

von Teilkörpern von \mathbb{R} so zu finden, daß unser Polynom in K_r 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 2.9.13 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, und für seinen Zerfällungskörper $Z \subset \mathbb{R}$ über K gilt $Z \supset K_1$ und $\text{Gal}(Z/K_1) \cong \mathbb{Z}/3\mathbb{Z}$ nach 4.7.9 und insbesondere $[Z : K_1] = 3$. Gegeben eine Wurzel $\alpha \in \mathbb{R}$ unseres kubischen Polynoms mit $\alpha \notin K_s$ ist 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 $K_r = K_{r-1}(\sqrt[l_r]{a_r})$ mit $a_r = a_r$ und $l_r = l_r$ prim muß aber nach 4.7.7 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**.

4.7.7 (Ziehen primter Wurzeln). Ist K ein Körper und l eine Primzahl, so ist für $a \in K$ das Polynom $X^l - a$ entweder irreduzibel oder es besitzt eine Nullstelle. In

der Tat zerfällt unser Polynom in seinem Zerfällungskörper als $X^l - a = \prod_{\nu} (X - \zeta^{\nu} b)$ für eine l -te Einheitswurzel ζ . Zerfällt es also in K als $X^l - a = fg$ mit $0 < \text{grad } f < l$, so muß der konstante Term c von f die Gestalt $c = \xi b^d$ haben für eine l -te Einheitswurzel ξ . Es folgt $c^l = b^{dl} = a^d$. Damit führt der Ansatz $(c^n a^m)^l = a$ zur Gleichung $a^{nd+ml} = a$ alias $nd + ml = 1$ und damit zu einer l -ten Wurzel von a in K .

Übungen

Ergänzende Übung 4.7.8. 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 4.7.9. Ein irreduzibles Polynom dritten Grades der Gestalt $Y^3 + pY + q$ mit Koeffizienten in einem Körper k der Charakteristik $\text{char } k \neq 2$ 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 4.7.10. Das Polynom $X^3 - 2$ hat nach 4.1.21 oder 4.7.9 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 4.6.3. 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 $(\zeta - \zeta^{-1})^2 = -3$.

4.8 Einheitswurzeln und reelle Radikale*

4.8.1. 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 [AN2] ?? 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 4.8.2. 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

$$R = \text{rad}(F \subset E)$$

Beispiel 4.8.3. 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 4.8.4. 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

$$Q = \text{quad}(F \subset E)$$

4.8.5. Den Quadratwurzelabschluß der rationalen Zahlen in den komplexen Zahlen haben wir bereits in 3.6.2 betrachtet und gezeigt, daß er genau aus allen konstruierbaren Zahlen besteht.

Satz 4.8.6 (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*

$$\text{rad}(\mathbb{Q} \subset \mathbb{R}) \cap \mathbb{Q}(\sqrt[n]{1}) \subset \text{quad}(\mathbb{Q} \subset \mathbb{R})$$

Ergänzung 4.8.7. Für jeden Teilkörper $K \subset \mathbb{R}$ und jedes $n \geq 1$ gilt allgemeiner $\text{rad}(K \subset \mathbb{R}) \cap K(\sqrt[n]{1}) \subset \text{quad}(K \subset \mathbb{R})$. Der Beweis ist im wesentlichen derselbe.

4.8.8. 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 4.1.22 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} .

4.8.9. 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 $\text{rad}(\mathbb{Q} \subset \mathbb{R})$ der rationalen in den reellen Zahlen, so folgt $\sin(\pi/n) \in \text{quad}(\mathbb{Q} \subset \mathbb{R})$ aus dem Satz 4.8.6 von Rost. Damit ist $\sin(\pi/n)$ aber nach 3.6.2 konstruierbar und damit dann unschwer auch das regelmäßige n -Eck. Der Beweis der Gegenrichtung bleibe dem Leser überlassen.

Beweis des Satzes von Rost 4.8.6. Wir halten eine natürliche Zahl $n \geq 1$ für den folgenden Beweis fest und vereinbaren die Abkürzung $Q := \text{quad}(\mathbb{Q} \subset \mathbb{R})$ 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

$$R \cap E \subset Q \Rightarrow R(x) \cap E \subset Q$$

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 Galoisweiterung, denn das sind beides Zwischenkörper einer endlichen abelschen Erweiterung. Nach dem Translationsatz 4.6.10 ist dann auch $((R(x) \cap E)R)/R$ eine nichttriviale Galoisweiterung. Da $R(x)/R$ Primzahlgrad hat, folgt $((R(x) \cap E)R) = R(x)$, und $R(x)/R$ ist mithin selbst eine Galoisweiterung vom Grad p . Das Polynom $X^p - a$ ist dann notwendig das Minimalpolynom von x über R , und da jede Galoisweiterung 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} . \square

5 Verallgemeinerungen ins Unendliche*

5.1 Ordinalzahlen

Definition 5.1.1. Eine Anordnung einer Menge heißt eine **Wohlordnung**, wenn jede nichtleere Teilmenge ein kleinstes Element besitzt.

Beispiel 5.1.2. Die Menge der natürlichen Zahlen \mathbb{N} ist wohlgeordnet mit ihrer üblichen Anordnung aus [LA1] 3.2.10, wie wir in 5.2.2 formal zeigen werden. Die Menge der rationalen Zahlen ist nicht wohlgeordnet mit ihrer üblichen Anordnung.

5.1.3. Gegeben eine partiell geordnete Menge X versteht man unter einem **unmittelbaren Nachfolger** oder kurz **Nachfolger** eines Elements $x \in X$ das kleinste Element „oberhalb von x “, also in Formeln das kleinste Element der Menge $\{y \in X \mid y > x\}$, wenn es denn existiert. Jedes Element hat höchstens einen unmittelbaren Nachfolger. Ebenso versteht man unter einem **unmittelbaren Vorgänger** oder kurz **Vorgänger** eines Elements $x \in X$ das größte Element „unterhalb von x “, in Formeln also das größte Element der Menge $\{y \in X \mid y < x\}$, wenn es denn existiert. Jedes Element hat höchstens einen unmittelbaren Vorgänger.

5.1.4. Jede nichtleere wohlgeordnete Menge besitzt ein kleinstes Element, das wir meist mit 0 bezeichnen. In einer wohlgeordneten Menge (Ω, \leq) hat weiter jedes Element a außer dem größten, wenn denn ein größtes Element existiert, einen unmittelbaren Nachfolger, nämlich das kleinste Element von $\Omega_{>a}$. Wir notieren diesen unmittelbaren Nachfolger

$$S(a)$$

für englisch „successor“. Manche Elemente besitzen auch unmittelbare Vorgänger, aber keineswegs alle.

Definition 5.1.5. Eine Teilmenge A einer wohlgeordneten Menge Ω heißt ein **Anfangsstück**, wenn A mit einem Element von Ω auch alle kleineren Elemente von Ω enthält.

5.1.6. Jedes von der ganzen Menge verschiedene Anfangsstück A einer wohlgeordneten Menge Ω ist von der Gestalt $A = \Omega_{<a}$ für genau ein $a \in \Omega$, nämlich für a das kleinste Element des Komplements $\Omega \setminus A$.

Definition 5.1.7. Eine Abbildung $f : X \rightarrow Y$ von geordneten Mengen heißt ein **Morphismus von geordneten Mengen**, wenn gilt $x \leq x' \Rightarrow f(x) \leq f(x')$. Ein **Isomorphismus von geordneten Mengen** oder auch **Ordnungsisomorphismus** ist ein bijektiver Morphismus von geordneten Mengen, dessen Inverses auch ein Morphismus von geordneten Mengen ist. Zwei geordnete Menge heißen **ordnungsisomorph**, wenn es zwischen ihnen einen Ordnungsisomorphismus gibt.

Satz 5.1.8 (Vergleich von wohlgeordneten Mengen). 1. Gegeben wohlgeordnete Mengen (Ω, \leq) und (Ω', \leq') gibt es höchstens einen Isomorphismus von (Ω, \leq) mit einem Anfangsstück von (Ω', \leq') ;

2. Gegeben wohlgeordnete Mengen (Ω, \leq) und (Ω', \leq') ist mindestens eine von beiden ordnungsisomorph zu einem Anfangsstück der anderen.

5.1.9. Insbesondere sind zwei Anfangsstücke einer wohlgeordneten Menge nur dann ordnungsisomorph, wenn sie gleich sind als Teilmengen.

Beweis. 1. Gegeben zwei verschiedene derartige Isomorphismen f, g gäbe es ein kleinstes Element $b \in \Omega$, auf dem sie verschiedene Werte annähmen. Dies Element müßte jedoch sowohl unter f als auch unter g auf das kleinste Element von $\Omega' \setminus f(\Omega_{<b}) = \Omega' \setminus g(\Omega_{<b})$ abgebildet werden. Widerspruch!

2. Wir betrachten das Mengensystem aller Anfangsstücke $A \subset \Omega$, die zu einem Anfangsstück von Ω' ordnungsisomorph sind. Die Vereinigung über dieses Mengensystem ist offensichtlich das größte Anfangsstück $A_{\max} \subset \Omega$, das zu einem Anfangsstück von Ω' ordnungsisomorph ist. Gilt $A_{\max} = \Omega$ oder $A_{\max} \cong \Omega'$, so sind wir fertig. Sonst aber wäre A_{\max} vereinigt mit dem kleinsten Element außerhalb auch ordnungsisomorph zum Bild von A_{\max} in Ω' vereinigt mit dem kleinsten Element außerhalb, im Widerspruch zur Maximalität von A_{\max} . \square

Lemma 5.1.10. Auf jeder Menge existiert eine Wohlordnung.

Beweis. Sei X unsere Menge. Wir betrachten die Menge \mathcal{W} aller Paare (Ω, \leq) mit $\Omega \subset X$ einer Teilmenge und \leq einer Wohlordnung auf Ω . Auf dieser Menge \mathcal{W} erklären wir eine partielle Ordnung durch die Vorschrift $(\Omega, \leq) \leq (\Omega', \leq')$ genau dann, wenn (Ω, \leq) ein Anfangsstück von (Ω', \leq') ist. Das Zorn'sche Lemma liefert die Existenz eines maximalen Paares $(\Omega_{\max}, \leq_{\max}) \in \mathcal{W}$. Für solch ein Paar gilt $\Omega_{\max} = X$, da wir sonst $(\Omega_{\max}, \leq_{\max})$ noch vergrößern könnten, indem wir ein weiteres Element von X hinzunehmen und die Anordnung dahingehend erweitern, daß es das größte Element der dadurch neu entstehenden Menge wird. \square

5.1.11. Unter einer **Ordinalzahl** versteht man eine Isomorphieklasse von wohlgeordneten Mengen. Gegeben zwei Ordinalzahlen ω und ω' nennen wir ω kleinergleich ω' , wenn ω isomorph ist zu einem Anfangsstück von ω' . Wir schreiben dann

$$\omega \leq \omega'$$

Der zweite Teil des Satzes 5.1.8 bedeutet, daß je zwei Ordinalzahlen vergleichbar sind, wohingegen der zweite Teil bedeutet, daß gegeben eine durch eine wohlgeordnete Menge (Ω, \leq) repräsentierte Ordinalzahl die angeordnete Klasse aller

Ordinalzahlen, die echt kleiner sind als diese, isomorph ist als angeordnete Klasse zur angeordneten Menge (Ω, \leq) selber. Jede Ordinalzahl besitzt einen unmittelbaren Nachfolger. Diejenigen Ordinalzahlen, die keinen unmittelbaren Vorgänger besitzen, heißen **Limeszahlen**. In diesem Sinne ist 0 also auch eine Limeszahl. Problematisch ist hierbei allerdings, daß wir uns mit unserem Begriff einer Isomorphieklasse in die „Klasse aller Mengen“ begeben, die schon am Rande des Gebietes liegt, in dem ich mich mit dem alleinigen Rüstzeug der naiven Mengenlehre noch sicher fühle. Man kann jedoch auch alternativ kanonische Repräsentanten wählen und mit von Neumann eine Ordinalzahl definieren als eine wohlgeordnete Menge Ω mit der Eigenschaft, daß jedes ihrer Elemente mit der Menge der kleineren Elemente, zusammenfällt, in Formeln

$$a = \{b \in \Omega \mid b < a\} \quad \forall a \in \Omega$$

Ergänzung 5.1.12. Man definiert die **Addition** von Ordinalzahlen als das Hintereinandersetzen von wohlgeordneten Mengen. Sie ist sicher assoziativ. Es gilt jedoch zu beachten, daß diese Addition nicht kommutativ ist, zum Beispiel haben wir für die durch die wohlgeordnete Menge \mathbb{N} repräsentierte Ordinalzahl ω die Formeln $1 + \omega = \omega \neq \omega + 1$. Wieder eine andere Ordinalzahl wäre etwa $\omega + \omega$. Man erklärt das **Produkt** zweier Ordinalzahlen als das kartesische Produkt von wohlgeordneten Mengen, versehen mit der lexikographischen Ordnung, und hätte für ω wie eben etwa

$$\omega \cdot \omega = \omega + \omega + \dots$$

in hoffentlich verständlicher Schreibweise. Dieses Produkt ist sicher assoziativ, aber nicht kommutativ, zum Beispiel gilt $2 \cdot \omega = \omega + \omega \neq \omega = \omega \cdot 2$.

5.2 Wohlordnung und natürliche Zahlen

5.2.1. Ich erinnere an [LA1] 3.2.1. 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 Mengenlehre, wir nennen es kurz das **Unendlichkeitsaxiom**.

Satz 5.2.2 (Charakterisierung der natürlichen Zahlen). *Die Menge der natürlichen Zahlen mit ihrer Anordnung aus [LA1] 3.2.10 ist die bis auf eindeutigen Ordnungsisomorphismus eindeutig bestimmte kleinste unendliche wohlgeordnete Menge.*

5.2.3. Insbesondere ist jede endliche wohlgeordnete Menge isomorph zu genau einem Anfangsstück der Menge der natürlichen Zahlen. Um welches Anfangsstück es sich dabei handelt, kann noch nicht einmal von der gewählten Wohlordnung

abhängen, denn verschiedene Möglichkeiten würden schnell zu einer injektiven nicht surjektiven Selbstabbildung unserer Menge führen, die es ja wegen der Endlichkeit nicht geben kann. Insbesondere ist jede endliche Menge X in Bijektion zu einer Menge der Gestalt $\{n \in \mathbb{N} \mid n < a\}$ für genau ein $a \in \mathbb{N}$. Diese natürliche Zahl nennen wir dann ihre **Kardinalität** und schreiben $|X| = a$.

Beweis. Nach 5.1.10 und 5.1.8 können wir „die kleinste unendliche Ordinalzahl“ bilden: Dazu wählen wir mithilfe des Unendlichkeitsaxioms 5.2.1 eine unendliche Menge, erklären darauf mithilfe von 5.1.10 eine Wohlordnung, vereinigen disjunkt mit einem weiteren Element, und erweitern unsere Wohlordnung so, daß das neue Element das Größte wird. In der so entstehenden unendlichen wohlgeordneten Menge (Ω, \leq) mit einem größten Element betrachten das kleinste b derart, daß $\Omega_{<b}$ unendlich ist. Dieses $\omega = \Omega_{<b}$ ist dann die kleinste unendliche wohlgeordnete Menge in dem Sinne, daß sie in jeder unendlichen wohlgeordneten Menge als Anfangsstück auftritt. Zwischen je zwei derartigen wohlgeordneten Mengen gibt es nach 5.1.8 genau einen Ordnungsisomorphismus. Es gilt nun zu zeigen, daß ω ordnungsisomorph ist zu unserer in [LA1] 3.2.10 beschriebenen angeordneten Menge \mathbb{N} . Die Menge ω hat sicher kein größtes Element, denn ein solches könnten wir ihr wegnehmen und so ein unendliches echtes Anfangsstück erhalten. Mithin hat in ω jedes Element einen Nachfolger. Die Abbildung $S : \omega \rightarrow \omega$, die jedem Element seinen Nachfolger zuordnet, ist injektiv, denn haben zwei Elemente x und y denselben Nachfolger, so führen beide Annahmen $x < y$ und $x > y$ leicht zum Widerspruch. Offensichtlich gehört auch das kleinste Element $o \in \omega$ nicht zum Bild von S . Um zu zeigen, daß das Tripel (ω, o, S) die definierenden Eigenschaften der natürlichen Zahlen nach [LA1] 3.2.4 hat, müssen wir nur noch prüfen, daß es keine echte S -stabile Teilmenge $Z \subsetneq \omega$ gibt mit $o \in Z$. Gegeben eine echte Teilmenge $Z \subsetneq \omega$ gäbe es aber in $\omega \setminus Z$ ein kleinstes Element b . Gilt zusätzlich $o \in Z$, so folgt $b \neq o$. Jedes Element von ω außer der Null hat aber einen Vorgänger, denn für jedes $b \in \omega$ ist $\omega_{<b}$ endlich und im Fall $b \neq o$ nicht leer und hat damit als nichtleere endliche angeordnete Menge nach [LA1] 3.2.3 ein größtes Element a . Aus $a \in Z$ folgt dann aber sofort $S(a) = b \in Z$, und das ist der gesuchte Widerspruch. \square

5.3 Dimension als Kardinalität

Definition 5.3.1. Gibt es zwischen zwei Mengen eine Bijektion, so sagt man auch, sie seien **gleichmächtig**.

Vorschau 5.3.2. Unter einer **Kardinalzahl** versteht man eine Äquivalenzklasse in der Klasse aller Mengen unter der Äquivalenzrelation, die durch die Existenz einer Bijektion erklärt wird. Die Äquivalenzklasse einer Menge heißt dann ihre

Kardinalität. Hier rede ich sehr vorsichtig von der „Klasse“ aller Mengen, da wir ja bereits aus [GR] 2.2.18 wissen, daß es nicht sinnvoll ist, von der „Menge aller Mengen“ zu reden. Die Gesamtheit aller Kardinalitäten ist dann auch keine Menge mehr, und wir stoßen hier wieder an die Grenze dessen, was im Rahmen der naiven Mengenlehre noch sinnvoll behandelt werden kann. Die Gesamtheit aller Kardinalitäten von Mengen, die Elemente eines gegebenen Universums [LA2] 8.10.3 sind, ist aber durchaus noch eine wohldefinierte Teilmenge besagten Universums.

5.3.3. Nach [GR] 2.3.36 ist keine Menge gleichmächtig zu ihrer Potenzmenge.

Satz 5.3.4 (Kardinalitäten von Basen). *Zwischen je zwei Basen ein- und desselben Vektorraums gibt es eine Bijektion.*

Beweis. Nach dem Austauschlemma 5.3.5 gibt es eine Injektion von jeder Basis in jede andere Basis. Die Behauptung folgt dann mit dem Satz von Schröder-Bernstein 5.3.6. \square

Lemma 5.3.5 (Austauschlemma). *Ist V ein Vektorraum, $E \subset V$ ein Erzeugendensystem und $L \subset V$ eine linear unabhängige Teilmenge, so gibt es eine Injektion $\varphi : L \hookrightarrow E$ derart, daß auch $(E \setminus \varphi(L)) \cup L$ ein Erzeugendensystem von V ist.*

Beweis. In [LA1] 1.8.2 hatten wir das für L endlich bereits gezeigt. Wir erweitern nun unseren Beweis und betrachten die „durch Einschränkung“ angeordnete Menge aller „partiellen Austauschungen“ (L', φ') bestehend aus einer Teilmenge $L' \subset L$ und einer dazu gegebenen Injektion $\varphi' : L' \hookrightarrow E$ mit der Eigenschaft, daß auch $(E \setminus \varphi'(L')) \cup L'$ ein Erzeugendensystem von V ist. Dann zeigen wir, daß gegeben ein angeordnetes System \mathcal{L} von partiellen Austauschungen auch die Vereinigung L° mit dem darauf durch Fortsetzung definierten φ° eine partielle Austauschung ist, daß also $(E \setminus \varphi^\circ(L^\circ)) \cup L^\circ$ ein Erzeugendensystem ist. Aber wählen wir für einen Vektor von V unter allen Darstellung als Linearkombination von Vektoren aus einem $(E \setminus \varphi'(L')) \cup L'$ mit $(L', \varphi') \in \mathcal{L}$ eine Darstellung aus, für die wir so wenig Vektoren aus $E \setminus \varphi'(L')$ wie möglich brauchen, so ist leicht zu sehen, daß dabei diese Vektoren bereits alle zu $E \setminus \varphi^\circ(L^\circ)$ gehören. Nach dem Zorn'schen Lemma gibt es also eine maximale partielle Ausdehnung $(L_{\max}, \varphi_{\max})$, und es bleibt zu zeigen $L_{\max} = L$. Sonst gäbe es aber einen Vektor $w \in L \setminus L_{\max}$, und nach [LA1] 1.8.4 könnten wir den auch noch in unser Erzeugendensystem hereintauschen alias φ_{\max} ausdehnen auf $L_{\max} \cup \{w\}$, im Widerspruch zur Maximalität. \square

Satz 5.3.6 (Schröder-Bernstein). *Seien X und Y zwei Mengen. Gibt es eine Injektion $f : X \hookrightarrow Y$ und eine Injektion $g : Y \hookrightarrow X$, so gibt es auch eine Bijektion zwischen X und Y .*

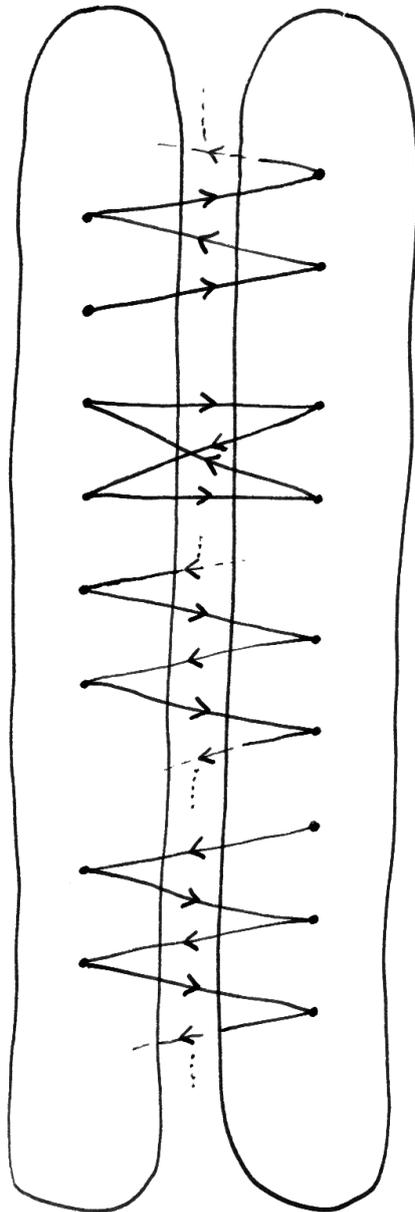


Illustration der vier Typen von Äquivalenzklassen im Beweis des Satzes von Schröder-Bernstein

Beweis. Wir dürfen unsere beiden Mengen X und Y als disjunkt annehmen, indem wir sie andernfalls etwa durch $X \times \{0\}$ und $Y \times \{1\}$ ersetzen. Wir betrachten auf der Vereinigung $X \cup Y$ nun die Äquivalenzrelation \sim , die erzeugt wird von $x \sim f(x)$ und $y \sim g(y)$, und interessieren uns für deren Äquivalenzklassen. Besitzt in einer derartigen Äquivalenzklasse A ein Element $x \in A \cap X$ kein Urbild unter g , so hat unsere Äquivalenzklasse die Gestalt „einer in X beginnenden Kette“

$$A = \{x, f(x), gf(x), fgf(x), \dots\}$$

Besitzt ein Element $y \in A \cap Y$ kein Urbild unter f , so hat unsere Äquivalenzklasse die Gestalt „einer in Y beginnenden Kette“

$$A = \{y, g(y), fg(y), ffg(y), \dots\}$$

Sind wir in keinem der beiden vorhergehenden Fälle und ist unsere Äquivalenzklasse endlich, so hat sie die Gestalt „einer geschlossenen Kette“

$$A = \{x, f(x), gf(x), fgf(x), \dots, (gf)^i(x) = x\}$$

für ein $i \geq 1$ und jedes $x \in A \cap X$. Sind wir schließlich in keinem der drei vorhergehenden Fälle, so hat unsere Äquivalenzklasse die Gestalt „einer nach beiden Seiten unendlichen Kette“

$$A = \{x_i, y_i \mid i \in \mathbb{Z}\}$$

mit x_i und y_i paarweise verschieden und $f(x_i) = y_i, g(y_i) = x_{i+1} \forall i \in \mathbb{Z}$. Man überzeugt sich nun leicht, dass für jede Äquivalenzklasse entweder f oder g oder beide eine Bijektion zwischen den Elementen aus X in unserer Äquivalenzklasse und den Elementen aus Y in unserer Äquivalenzklasse liefern. Im Zweifelsfall wählen wir hier f und erhalten auf diese Weise eine wohlbestimmte Bijektion zwischen X und Y . \square

5.3.7 (Vergleichbarkeit von Kardinalitäten). Gegeben zwei Mengen X, Y gibt es stets entweder eine Inklusion $X \hookrightarrow Y$ oder eine Inklusion $Y \hookrightarrow X$. In der Tat, betrachten wir auf der Menge aller Tripel (X', f, Y') mit $X' \subset X, Y' \subset Y$ und $f : X' \xrightarrow{\sim} Y'$ einer Bijektion die offensichtliche partielle Ordnung, so können wir das Zorn'sche Lemma anwenden und ein maximales Tripel finden, für das dann offensichtlich entweder $X' = X$ oder $Y' = Y$ gilt. Wir schreiben $|X| \leq |Y|$ falls es eine Inklusion $X \hookrightarrow Y$ gibt. Mit dem Satz von Schröder-Bernstein 5.3.6 sehen wir, daß $|X| \leq |Y| \leq |X|$ bereits $|X| = |Y|$ impliziert.

Ergänzung 5.3.8. Es liegt nun nahe, auf der Gesamtheit aller möglichen Kardinalitäten, etwa von Mengen eines gegebenen Universums, eine Ordnungsrelation einzuführen durch die Vorschrift $|X| \leq |Y|$ genau dann, wenn eine Injektion $X \hookrightarrow Y$ existiert. Daß diese Ordnungsrelation total ist, daß also darunter je zwei Kardinalitäten vergleichbar sind, folgt dann aus 5.3.7.

Satz 5.3.9 (Multiplikationssatz der Mengenlehre). Für jede unendliche Menge ist ihr kartesisches Quadrat gleichmächtig zur Menge selber; in Formeln

$$|M \times M| = |M|$$

Beweis. Wir zeigen zunächst eine schwächere Aussage.

Lemma 5.3.10. Für jede unendliche Menge M gilt $|\mathbb{N} \times M| = |M|$.

Beweis. Um dies Lemma zu zeigen, müssen wir nach Schröder-Bernstein 5.3.6 nur die Existenz einer Injektion $\mathbb{N} \times M \hookrightarrow M$ nachweisen. Dazu betrachten wir die Menge aller Paare (A, φ) mit $A \subset M$ und $\varphi : \mathbb{N} \times A \hookrightarrow A$ einer Injektion. Sie ist in offensichtlicher Weise induktiv geordnet und besitzt folglich ein maximales Element $(A_{\max}, \varphi_{\max})$. Gilt $|A_{\max}| = |M|$, so haben wir schon gewonnen. Sonst gilt nach 5.3.7 jedoch $|A_{\max}| \neq |M|$ und wir finden nach 5.3.12 eine abzählbare unendliche Menge $Z \subset M \setminus A_{\max}$. Dann aber können wir unsere Injektion zu einer Injektion $\mathbb{N} \times (A_{\max} \cup Z) \hookrightarrow A_{\max} \cup Z$ ausdehnen, indem wir eine Injektion $\mathbb{N} \times Z \xrightarrow{\sim} Z$ wählen. Widerspruch! \square

Nun zeigen wir den Multiplikationssatz. Wir betrachten dazu die Menge aller Paare (A, φ) mit $A \subset M$ und $\varphi : A \times A \hookrightarrow A$ einer Injektion. Sie ist in offensichtlicher Weise induktiv geordnet und besitzt folglich ein maximales Element $(A_{\max}, \varphi_{\max})$. Sicher ist dann A_{\max} unendlich. Im Fall $|A_{\max}| = |M|$ haben wir schon gewonnen. Sonst gilt $|A_{\max}| < |M|$ nach 5.3.7 und dann nach Lemma 5.3.10 sogar $|\mathbb{N} \times A_{\max}| < |M|$. Wir finden also eine Einbettung $\psi : \mathbb{N} \times A_{\max} \hookrightarrow M$, von der wir sogar $\psi(0, a) = a$ fordern dürfen. Wählen wir nun eine Injektion $\xi : \mathbb{N} \times \mathbb{N} \hookrightarrow \mathbb{N}$ mit $\xi(0, 0) = 0$, können wir die Injektion

$$\begin{aligned} (\mathbb{N} \times A_{\max}) \times (\mathbb{N} \times A_{\max}) &\hookrightarrow (\mathbb{N} \times A_{\max}) \\ ((i, a), (j, b)) &\mapsto (\xi(i, j), \varphi_{\max}(a, b)) \end{aligned}$$

bilden. Vermittels ψ erhalten wir eine Injektion $(\text{im } \psi) \times (\text{im } \psi) \hookrightarrow (\text{im } \psi)$, die φ_{\max} fortsetzt. Widerspruch zur Maximalität von $(A_{\max}, \varphi_{\max})$! \square

Ergänzung 5.3.11. Gegeben Mengen X, Y mit $2 \leq |X| \leq |Y|$ und Y unendlich kann man zeigen, daß gilt $|\text{Ens}(Y, X)| = |\text{Ens}(Y, \{0, 1\})| = |\text{Pot}(Y)|$. Im allgemeinen ist die Frage nach der Kardinalität einer Menge von Abbildungen $\text{Ens}(Y, X)$ nicht so leicht zu beantworten.

Übungen

Übung 5.3.12. Lassen wir aus einer unendlichen Menge endlich viele Elemente weg, so erhalten wir eine gleichmächtige Menge.

Übung 5.3.13. Gegeben ein von Null verschiedener Vektorraum abzählbarer Dimension über einem unendlichen Körper zeige man, daß der Vektorraum dieselbe Kardinalität hat wie der Grundkörper. Gegeben ein Vektorraum unendlicher Dimension über einem abzählbaren Körper zeige man, daß die Kardinalität jeder seiner Basen übereinstimmt mit der Kardinalität des ganzen Vektorraums. Jede algebraische Körpererweiterung eines unendlichen Körpers hat dieselbe Kardinalität wie besagter Körper. Hinweis: 5.3.10.

Übung 5.3.14. Gegeben ein unendlichdimensionaler Vektorraum zeige man, daß sein Dualraum stets eine im Sinne von Kardinalitäten echt größere Dimension hat. Hinweis: Man beginne mit der Betrachtung von Vektorräumen über dem Körper mit zwei Elementen und verwende 5.3.13 sowie [GR] 2.3.36.

Übung 5.3.15. Jede unendliche Menge ist gleichmächtig zur Menge ihrer endlichen Teilmengen. Gegeben eine surjektive Abbildung mit endlichen Fasern zwischen unendlichen Mengen sind unsere beiden Mengen gleichmächtig.

5.4 Anwendungen in der Analysis*

5.4.1 (**Die kleinste überabzählbare Ordinalzahl**). Wir können nach 5.1.10 und 5.1.8 insbesondere auch „die kleinste überabzählbare Ordinalzahl“ bilden: Dazu wählen wir mit 5.1.10 eine Wohlordnung auf einer überabzählbaren Menge, etwa auf \mathbb{R} , und betrachten in der so entstehenden überabzählbaren wohlgeordneten Menge (Ω, \leq) das kleinste b derart, daß $\Omega_{<b}$ überabzählbar ist. Dieses $\omega = \Omega_{<b}$ ist dann die kleinste überabzählbare wohlgeordnete Menge in dem Sinne, daß sie in jeder überabzählbaren wohlgeordneten Menge als Anfangsstück auftritt. Aber versuchen sie bloß nicht, eine derartige kleinste überabzählbare wohlgeordnete Menge explizit anzugeben! Bereits einen Repräsentanten für die „kleinste unendliche Ordinalzahl“ schreiben wir zwar leichthin auf's Papier als $\mathbb{N} = \{0, 1, 2, \dots\}$, aber ob das eigentlich eine explizite Darstellung ist, scheint mir bei näherem Hinsehen auch schon recht fragwürdig.

5.4.2. Die kleinste überabzählbare Ordinalzahl (ω, \leq) besitzt kein größtes Element, denn ein solches könnten wir ihr leicht wegnehmen. Die **Alexandroff'sche Halbgerade** wird erklärt, indem man $\omega \times [0, 1)$ lexikographisch anordnet und mit der Topologie versieht, die von allen Teilmengen $\{x \mid x > y\}$ und $\{x \mid x < y\}$ für y aus unserer lexikographisch angeordneten Menge erzeugt wird. Läßt man aus $\omega \times [0, 1)$ das kleinste Element weg, so entsteht eine nicht parakompakte wegzusammenhängende eindimensionale Mannigfaltigkeit, wie wir im folgenden zeigen werden. Zunächst zeigen wir, daß wir so eine wegzusammenhängende eindimensionale Mannigfaltigkeit erhalten. Genauer behaupten wir, daß $\omega_{<a} \times [0, 1)$ homöomorph ist zu $[0, 1)$ für alle $a \in \omega$: Ist sonst b kleinstmöglich mit $\omega_{<b} \times [0, 1)$ nicht homöomorph zu $[0, 1)$, so könnte b keinen direkten Vorgänger haben, wäre

also eine Limeszahl, wir fänden also eine streng monoton wachsende Folge mit Supremum b , und abzählbar viele $[0, 1)$ zu verkleben ist unproblematisch. Daß unser Raum nicht parakompakt ist, zeigen wir nach einer Vorbemerkung als 5.4.4.

Lemma 5.4.3. *Eine Selbstabbildung einer überabzählbaren wohlgeordneten Menge, die das kleinste Element auf sich selbst abbildet und jedes andere Element auf ein echt Kleineres, hat mindestens eine überabzählbare Faser.*

Beweis. Sei Ω unsere überabzählbare wohlgeordnete Menge und $f : \Omega \rightarrow \Omega$ unsere Selbstabbildung, von der wir in Formeln ausgedrückt fordern $f(0) = 0$ und $f(a) < a \quad \forall a \neq 0$. Es gilt zu zeigen, daß ein $b \in \Omega$ existiert mit $f^{-1}(b)$ überabzählbar. Nun muß für alle $a \in \Omega$ die Menge $\{f^n(a) \mid n \geq 0\}$ ein kleinstes Element besitzen, und das kann nur das kleinste Element 0 unserer wohlgeordneten Menge Ω sein. In anderen Worten gibt es für alle $a \in \Omega$ ein $n \in \mathbb{N}$ mit $f^n(a) = 0$. Wären nun alle Fasern von f abzählbar, so wären auch die Mengen $(f^n)^{-1}(0)$ abzählbar für alle $n \in \mathbb{N}$ und Ω wäre abzählbar als die Vereinigung all dieser abzählbar vielen abzählbaren Mengen. Widerspruch! \square

Lemma 5.4.4. *Die Alexandroff'sche Halbgerade aus 5.4.2 ist nicht parakompakt. Dasselbe gilt auch für das Komplement des kleinsten Elements der Alexandroff'schen Halbgerade.*

Beweis. Wir betrachten für jedes $a \in \omega$ das offene Intervall U_a aller Punkte, die kleiner sind als mindestens ein Punkt von $\{a\} \times [0, 1)$. Sicher bilden diese U_a eine offene Überdeckung, und ich behaupte, daß diese Überdeckung keine lokal endliche Verfeinerung zuläßt. In der Tat kann man für jede Verfeinerung eine Abbildung $f : \omega \rightarrow \omega$ finden mit $f(0) = 0$ und $f(a) < a$ falls $a \neq 0$ derart, daß für $a \neq 0$ jeweils ein $t_a \in (0, 1)$ existiert, für das das Intervall $[(f(a), t_a), (a, 0)]$ ganz in einer offenen Menge unserer Verfeinerung enthalten ist. Diese Abbildung f hat nun nach 5.4.3 eine überabzählbare Faser. Ist etwa $f^{-1}(b)$ überabzählbar, so hat $f^{-1}(b)$ keine obere Schranke in ω , aber es gibt natürlich ein kleinstes Element $c \in f^{-1}(b)$. Wir erkennen nun, daß $(c, 0)$ zu unendlich vielen offenen Mengen unserer Verfeinerung gehört, denn für alle $a \in f^{-1}(b)$ gibt es eine offene Menge unserer Verfeinerung, die $(a, 0)$ und $(c, 0)$ beide enthält. \square

Lemma 5.4.5. *Seien gegeben eine Menge X und darin ein System von Teilmengen $\mathcal{E} \subset \mathcal{P}(X)$.*

1. *Hat \mathcal{E} eine Kardinalität $\leq |\mathbb{R}|$, so hat auch die davon erzeugte σ -Algebra $\mathcal{M}(\mathcal{E})$ eine Kardinalität $\leq |\mathbb{R}|$, in Formeln*

$$|\mathcal{E}| \leq |\mathbb{R}| \quad \Rightarrow \quad |\mathcal{M}(\mathcal{E})| \leq |\mathbb{R}|$$

2. Hat \mathcal{E} eine Kardinalität $\geq |\mathbb{R}|$, so hat die davon erzeugte σ -Algebra $\mathcal{M}(\mathcal{E})$ dieselbe Kardinalität wie \mathcal{E} , in Formeln

$$|\mathcal{E}| \geq |\mathbb{R}| \Rightarrow |\mathcal{M}(\mathcal{E})| = |\mathcal{E}|$$

5.4.6 (Vergleich von Lebesgue-Mengen und Borel-Mengen). Die σ -Algebra der Borelmengen in \mathbb{R} kann von einem abzählbaren Mengensystem erzeugt werden, mithin gilt nach unserem Satz 5.4.5 die Abschätzung $|\text{Borel}(\mathbb{R})| \leq |\mathbb{R}|$. Dahingegen hat die Cantormenge [AN3] 1.2.39 dieselbe Kardinalität wie \mathbb{R} und alle ihre Teilmengen sind Lebesgue-meßbar. Folglich stimmt wieder nach 5.4.5 die Kardinalität der σ -Algebra der Lebesgue-Mengen in \mathbb{R} überein mit der Kardinalität von $\mathcal{P}(\mathbb{R})$.

Beweis. Die von einem Mengensystem $\mathcal{E} \subset \mathcal{P}(X)$ erzeugte σ -Algebra $\mathcal{M}(\mathcal{E})$ kann wie folgt beschrieben werden: Wir beginnen mit der kleinsten überabzählbaren Ordinalzahl ω und behaupten zunächst die Existenz und Eindeutigkeit zweier Abbildungen $[0, \omega] \rightarrow \mathcal{P}(\mathcal{M}(\mathcal{E}))$, $\alpha \mapsto \Pi_\alpha$ und $\alpha \mapsto \Sigma_\alpha$ mit der Eigenschaft $\Pi_0 = \Sigma_0 = \mathcal{E}$ und so, dass für $\alpha > 0$ gilt

$$\Pi_\alpha = \left\{ \begin{array}{l} \text{abzählbare Schnitte von Mengen aus} \\ \text{irgendwelchen } \Sigma_\beta \text{ mit } \beta < \alpha \end{array} \right\}$$

$$\Sigma_\alpha = \left\{ \begin{array}{l} \text{abzählbare Vereinigungen von Mengen} \\ \text{aus irgendwelchen } \Pi_\beta \text{ mit } \beta < \alpha \end{array} \right\}$$

Sowohl die Existenz als auch die Eindeutigkeit dieser Abbildungen folgt leicht durch „transfinite Induktion“, d.h. man betrachtet das kleinste α , für das Π_α oder Σ_α nicht mehr mit diesen Eigenschaften definiert werden kann oder für das es verschiedene Möglichkeiten gibt und kommt sofort zu einem Widerspruch. Wir behaupten nun $\Pi_\omega = \Sigma_\omega = \mathcal{M}(\mathcal{E})$. Hier folgt offensichtlich die zweite Gleichung aus der ersten, denn alle unsere Π_α sind stabil unter abzählbaren Schnitten und alle unsere Σ_α sind stabil unter abzählbaren Vereinigungen. Nun haben wir aber $\Pi_\alpha \subset \Sigma_{\alpha+1}$ und $\Sigma_\alpha \subset \Pi_{\alpha+1}$ per definitionem. Ein $M \in \Pi_\omega$ alias eine abzählbare Vereinigung

$$M_1 \cup M_2 \cup \dots$$

mit $M_i \in \Pi_{\alpha(i)}$ und $\alpha(i) < \omega$ gehört also wegen $\alpha(i) + 1 < \omega$ auch zu Σ_ω und die umgekehrte Inklusion $\Sigma_\omega \subset \Pi_\omega$ zeigt man ähnlich. Geht man speziell von einem Mengensystem der Kardinalität $|\mathcal{E}| \leq |\mathbb{R}|$ aus, so haben alle unsere Π_α und Σ_α auch höchstens die Kardinalität $|\mathbb{R}|$ und es folgt $|\mathcal{M}(\mathcal{E})| \leq |\mathbb{R}|$. Geht man dahingegen von einem Mengensystem der Kardinalität $|\mathcal{E}| \geq |\mathbb{R}|$ aus, so haben alle unsere Π_α und Σ_α dieselbe Kardinalität wie \mathcal{E} und es folgt $|\mathcal{M}(\mathcal{E})| = |\mathcal{E}|$. \square

Übungen

Ergänzende Übung 5.4.7. Die Alexandroff'sche Halbgerade ist folgenkompakt, aber nicht überdeckungskompakt.

Übung 5.4.8. Sei $\Omega = \Omega_\alpha$ die kleinste wohlgeordnete Menge einer vorgegebenen unendlichen Kardinalität α und $X \subset \Omega$ eine Teilmenge einer echt kleineren Kardinalität. So gibt es $\omega \in \Omega$ mit $X \subset \Omega_{<\omega}$. Hinweis: Eine Vereinigung einer Familie von höchstens α Mengen einer Kardinalität höchstens α hat auch selbst nur höchstens die Kardinalität α nach dem Multiplikationssatz der Mengenlehre [5.3.9](#).

6 Ergänzungen zur Körpertheorie*

6.1 Tensorprodukte von Körpern

6.1.1 (**Tensorprodukte von Körpern sind im allgemeinen keine Körper**). Gegeben Körpererweiterungen L/K und M/K muß $L \otimes_K M$ keineswegs wieder ein Körper sein, wie bereits das Beispiel $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ zeigt. Solch ein Tensorprodukt kann sogar von Null verschiedene nilpotente Elemente enthalten: Für ein Beispiel sei k ein Körper positiver Charakteristik $\text{char } k = p > 0$. Betrachten wir nun den Funktionenkörper $K = k(T)$ und seine Erweiterung $L = k(\sqrt[p]{T}) = K[X]/\langle X^p - T \rangle$, so ergibt sich $L \otimes_K L \cong L[X]/\langle X^p - T \rangle$ und in diesem Ring ist $X - \sqrt[p]{T}$ nilpotent und von Null verschieden. Ist jedoch L/K eine endliche separable Körpererweiterung und M/K eine beliebige Körpererweiterung, so ist $L \otimes_K M$ stets ein Produkt von Körpern. Ist genauer $\alpha \in L$ ein primitives Element und $P \in K[X]$ sein Minimalpolynom, so entsprechen die Faktoren von $L \otimes_K M$ den irreduziblen Faktoren $P = Q_1 \dots Q_r$ von P in $M[X]$, denn wir haben ja natürliche Isomorphismen

$$L \otimes_K M \xrightarrow{\sim} (K[X]/PK[X]) \otimes_K M \xrightarrow{\sim} M[X]/PM[X] \xrightarrow{\sim} \prod_{i=1}^r M[X]/Q_i M[X]$$

Für den letzten Schritt verwendet man den chinesischen Restsatz und braucht dazu, daß die Q_i paarweise teilerfremd sind. Das folgt jedoch aus der Separabilität von P .

6.1.2 (**Endomorphismenring einer endlichen Galoiserweiterung**). Gegeben eine Körpererweiterung L/K mit Galoisgruppe Γ liefert der Satz über die lineare Unabhängigkeit von Charakteren 3.8.16 eine L -lineare Einbettung

$$L\Gamma \hookrightarrow \text{Hom}_K(L, L)$$

Hierbei soll die Operation von L auf dem Hom-Raum durch Nachschalten geschehen, also $(lf)(x) = lf(x)$. Verstehen wir hier $L\Gamma$ als getwisteten Gruppenring $L\Gamma = L^\times \langle \Gamma \rangle$ im Sinne von [NAS] 1.4.4 mit der Multiplikation charakterisiert durch $\gamma \cdot l = \gamma(l) \cdot \gamma$, so wird unsere Einbettung ein Ringhomomorphismus $L^\times \langle \Gamma \rangle \hookrightarrow \text{End}_K(L)$. Ist schließlich unsere Körpererweiterung auch noch endlich und Galois, so ist unsere Einbettung wegen der Gleichheit der Dimensionen sogar ein Ringisomorphismus

$$L^\times \langle \Gamma \rangle \xrightarrow{\sim} \text{End}_K L$$

6.1.3 (**Tensorquadrat einer endlichen Galoiserweiterung**). Für jede Körpererweiterung L/K mit Galoisgruppe Γ haben wir einen Ringhomomorphismus

$$\begin{aligned} L \otimes_K L &\rightarrow \text{Ens}(\Gamma, L) \\ x \otimes y &\mapsto (\sigma \mapsto x\sigma(y)) \end{aligned}$$

Der Ring der Abbildungen von Γ nach L ist hierbei schlicht mit der punktweisen Multiplikation zu verstehen. Im Fall einer Galoiserweiterung ist unser Ringhomomorphismus injektiv, wie wir aus der linearen Unabhängigkeit von Charakteren folgern werden. Sind genauer $x_1, \dots, x_r \in L$ linear unabhängig über K , so können wir sie zu einer K -Basis einer endlichen Galoiserweiterung $E \subset L$ von K ergänzen durch geeignete x_{r+1}, \dots, x_s . Bilden dann $\sigma_1, \dots, \sigma_s \in \Gamma$ ein Repräsentantensystem von $G := \text{Gal}(E/K)$, so hat die Matrix der $(\sigma_i(x_j))$ vollen Rang wegen der linearen Unabhängigkeit von Charakteren. Für $y_j \in L$ folgt aus $\sum_j y_j \sigma_i(x_j) = 0$ für alle i also $y_1 = \dots = y_s = 0$. Im Fall einer endlichen Galoiserweiterung entlarvt damit ein Dimensionsvergleich unseren Homomorphismus sogar als Isomorphismus

$$L \otimes_K L \xrightarrow{\sim} \text{Ens}(\Gamma, L)$$

Ergänzung 6.1.4. Gegeben eine endliche Galoiserweiterung L/K mit Galoisgruppe Γ kann man zeigen, daß unsere Isomorphismen $L \otimes_K L \xrightarrow{\sim} \text{Ens}(\Gamma, L)$ und $L^\times \langle \Gamma \rangle \xrightarrow{\sim} \text{End}_K L$ einander entsprechen unter dem von der sogenannten „Spurform“ induzierten Isomorphismus $L \xrightarrow{\sim} \text{Hom}_K(L, K)$ und dem davon abgeleiteten Isomorphismus $L \otimes_K L \xrightarrow{\sim} \text{End}_K(L)$. Ich führe das hier nicht weiter aus.

Satz 6.1.5 (über die Normalbasis). *Gegeben eine endliche Galoiserweiterung L/K mit Galoisgruppe Γ ist L ein freier $K\langle \Gamma \rangle$ -Modul vom Rang Eins.*

Beweis. Nach 6.1.3 ist $L \otimes_K L$ für die Operation von Γ auf dem zweiten Tensorfaktor ein freier $K\langle \Gamma \rangle$ -Modul vom Rang $[L : K]$. Der Satz von Krull-Schmid [NAS] 5.2.4 zeigt jedoch, daß zwei endlichdimensionale $K\langle \Gamma \rangle$ -Moduln, die nach endlicher Erweiterung der Skalare isomorph werden, schon von Anfang an isomorph gewesen sein müssen, denn die Erweiterung der Skalare gefolgt von der Restriktion bedeutet schlicht, eine direkte Summe von $[L : K]$ Kopien des Moduls zu nehmen. \square

Ergänzung 6.1.6. Gegeben eine Erweiterung endlicher Körper kann man zeigen, daß jeder Erzeuger der multiplikativen Gruppe des großen Körpers zusammen mit seinen Bildern unter der Galoisgruppe eine Basis des großen Körpers über dem kleinen Körper bildet. Der Beweis soll hier nicht gegeben werden.

6.2 Allgemeiner Translationssatz

Satz 6.2.1 (Kompositum als Tensorprodukt). *Gegeben Unterkörper K, L eines gemeinsamen Körpers mit K normal über $K \cap L$ liefert die Multiplikation stets einen Isomorphismus mit dem Kompositum*

$$K \otimes_{K \cap L} L \xrightarrow{\sim} (KL)$$

Beweis. Da K algebraisch ist über $S := K \cap L$, fällt das Erzeugnis als Ring mit dem Erzeugnis als Körper zusammen, in Formeln $[KL] = (KL)$, und unser Homomorphismus ist schon mal surjektiv. Es reicht also, die Injektivität zu zeigen, und dazu können wir uns auf den Fall beschränken, daß L/S als Körpererweiterung endlich erzeugt ist. Mit einer offensichtlichen Induktion können wir uns weiter beschränken auf den Fall, daß L/S eine primitive Körpererweiterung ist, etwa $L = S(\alpha)$. Wir dürfen uns sogar auf drei Fälle beschränken: Erstens α transzendent über S , zweitens α eine p -te Wurzel eines Elements aus S für p die Charakteristik, und drittens α separabel über S . Diese drei Fälle gehen wir nun der Reihe nach durch. Ist α transzendent über S , so auch über K , und die Multiplikation liefert schon mal einen Ringisomorphismus

$$K \otimes_S S[\alpha] \xrightarrow{\sim} K[\alpha]$$

Damit erhalten wir für jedes von Null verschiedene Polynom $P \in S[\alpha] \setminus 0$ auch einen Isomorphismus $K \otimes_S P^{-1}S[\alpha] \xrightarrow{\sim} P^{-1}K[\alpha]$, und das zeigt die Injektivität der durch Multiplikation gegebenen Abbildung $K \otimes_S S(\alpha) \rightarrow K(\alpha)$ für den Fall, daß α transzendent ist über S . Ist α algebraisch über S mit $\alpha \notin S$, aber $\alpha^p \in S$ für $p > 0$ die Charakteristik, so folgt $[S(\alpha) : S] = p$ und $[K(\alpha) : K] = p$ und die Injektivität folgt durch Dimensionsvergleich. Ist schließlich α algebraisch und separabel über S , so können wir, indem wir notfalls unseren großen Körper noch weiter vergrößern, auch einen Unterkörper L' finden, der Zerfällungskörper über S des Minimalpolynoms von α über S ist. Betrachten wir nun das Diagramm

$$\begin{array}{ccccc}
 & & (KL) & & \\
 & & \parallel & & \\
 & K & \text{-----} & K(\alpha) & \text{-----} & (KL') \\
 & | & & | & & | \\
 K \cap L' & \text{-----} & (K \cap L')(\alpha) & \xrightarrow{G} & L' \\
 & | & & | & \\
 & G & & & \\
 K \cap L & \text{-----} & (K \cap L)(\alpha) & & \\
 & \parallel & & \parallel & \\
 & S & & L &
 \end{array}$$

von Teilkörpern unseres großen Körpers. Für jedes in unserem Diagramm enthaltene Rechteck steht in der Ecke oben rechts das Kompositum der Körper an den beiden benachbarten Ecken. Zusätzlich zu den beiden mit G bezeichneten Körpererweiterungen ist auch noch die ganze mittlere Horizontale $L'/(K \cap L')$ offensichtlich Galois. In den drei Rechtecken über diesen Galois-Erweiterungen

sind nach dem bereits bewiesenen Translationssatz für endliche Galoiserweiterungen [AL] 4.6.10 also gegenüberliegende Ecken jeweils Körpererweiterungen vom selben Grad, in Formeln

$$\begin{aligned} [(KL') : K(\alpha)] &= [L' : (K \cap L')(\alpha)] \\ [(K \cap L')(\alpha) : K \cap L'] &= [(K \cap L)(\alpha) : K \cap L] \\ [(KL') : K] &= [L' : K \cap L'] \end{aligned}$$

Aus der ersten und der letzten Gleichung für das obere große Rechteck und sein rechtes Quadrat folgt aber sofort die Identität

$$[K(\alpha) : K] = [(K \cap L')(\alpha) : K \cap L']$$

in seinem linken Quadrat, und zusammen mit der mittleren unserer drei Gleichungen aus dem unteren Quadrat ergibt sich schließlich

$$[K(\alpha) : K] = [(K \cap L)(\alpha) : K \cap L]$$

Mithilfe dieser Identität erhalten wir dann die Injektivität der Multiplikationsabbildung

$$K \otimes_{K \cap L} L \rightarrow (KL)$$

aus der Gleichheit der Dimensionen besagter K -Vektorräume. \square

Satz 6.2.2 (Translationssatz der Galoistheorie). *Seien in einem großen Körper zwei Teilkörper K, L gegeben. Ist $K \supset (K \cap L)$ eine Galoiserweiterung, so ist auch $(KL) \supset L$ eine Galoiserweiterung. Ist $K \supset (K \cap L)$ eine normale Erweiterung, so ist auch $(KL) \supset L$ eine normale Erweiterung. In beiden Fällen liefert die Restriktion einen Isomorphismus von Galoisgruppen*

$$\text{Gal}((KL)/L) \xrightarrow{\sim} \text{Gal}(K/K \cap L)$$

Beweis. Ist K Zerfällungskörper einer Familie separabler Polynome über $K \cap L$, so ist auch (KL) Zerfällungskörper derselben Familie separabler Polynome über L . Ist K Zerfällungskörper einer Familie von Polynomen über $K \cap L$, so ist auch (KL) Zerfällungskörper derselben Familie von Polynomen über L . Das zeigt die ersten Aussagen. Daß der von der Restriktion induzierte Homomorphismus auf den Galoisgruppen injektiv ist, scheint mir offensichtlich. Daß er auch surjektiv ist erkennt man, indem man den Isomorphismus

$$K \otimes_{K \cap L} L \xrightarrow{\sim} (KL)$$

aus 6.2.1 beachtet: Wir können mit seiner Hilfe nämlich eine Spaltung unseres Homomorphismus explizit angeben durch die Vorschrift $\sigma \mapsto \sigma \otimes \text{id}$. \square

Korollar 6.2.3. Sind $k \subset K \subset M$ Körper und ist K/k normal und $\alpha \in M$ algebraisch über k , so gilt für die Minimalpolynome von α die Identität

$$\text{Irr}(\alpha; k(\alpha) \cap K) = \text{Irr}(\alpha; K)$$

Beweis. Man wende 6.2.1 an auf $L = k(\alpha)$. □

6.3 Krull-Topologie

Definition 6.3.1. Gegeben eine algebraische Körpererweiterung L/K erklärt man auf der Galoisgruppe $\text{Gal}(L/K)$ die **Krull-Topologie** als die grösste Topologie mit der Eigenschaft, daß für jedes Element $a \in L$ die durch das Anwenden auf a gegebene Abbildung $\text{Gal}(L/K) \rightarrow L$ nach L mit seiner diskreten Topologie stetig ist.

6.3.2. Mit ihrer Krull-Topologie wird die Galoisgruppe jeder algebraischen Körpererweiterung L/K eine kompakte Hausdorff'sche topologische Gruppe, und ist L/K Galois, so liefern die Abbildungen der Galoiskorrespondenz eine eindeutige Entsprechung zwischen abgeschlossenen Untergruppen und Zwischenkörpern.

6.3.3 (**Nichtoffene Untergruppen von endlichem Index**). Untergruppen von endlichem Index in einer Galoisgruppe müssen für die Krulltopologie nicht abgeschlossen oder gleichbedeutend offen sein. Das folgende Beispiel habe ich von Franziska Jahnke gelernt: Man betrachtet die Galoiserweiterung von \mathbb{Q} , bei der man die Quadratwurzeln aller Primzahlen adjungiert, in Formeln die Erweiterung

$$\mathbb{Q}(\sqrt{p} \mid p \text{ prim})/\mathbb{Q}$$

Die Galoisgruppe dieser Erweiterung ist ein abzählbares Produkt von Kopien von $\mathbb{Z}/2\mathbb{Z}$. Diese Gruppe hat nur abzählbar viele offene Untergruppen, aber überabzählbar viele Untergruppen von endlichem Index. Da die Restriktionsabbildung ein offener Epimorphismus ist, gilt das auch für $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

Ergänzung 6.3.4. Eine Vermutung von Serre, nach der in jeder endlich erzeugten profiniten Gruppe jede Untergruppe von endlichem Index offen sein sollte, wurde 2007 von Segal und Nikolov gezeigt.

6.3.5. Gegeben eine Galoiserweiterung L/K mit Galoisgruppe Γ erhalten wir eine Bijektion

$$L \otimes_K L \xrightarrow{\sim} \text{Top}(\Gamma, L)$$

durch die Vorschrift $p \otimes q \mapsto (\sigma \mapsto p\sigma(q))$. Hierbei ist die Galoisgruppe mit ihrer Krulltopologie zu verstehen und L mit der diskreten Topologie. Das folgt aus dem Fall 6.1.3 einer endlichen Galoiserweiterung durch Übergang zum Kolimes.

6.4 Formen von Vektorräumen und Algebren

Definition 6.4.1. Seien K/k eine Galois-erweiterung und $\Gamma = \text{Gal}(K/k)$ ihre Galoisgruppe. Unter einer **abstrakten Galois-linearen Operation** von Γ auf einem K -Vektorraum V verstehen wir eine Operation $\rho : \Gamma \rightarrow \text{Ab}^\times V$ auf der zugrundeliegenden additiven Gruppe derart, daß für alle $v \in V, \lambda \in K$ gilt

$$\gamma(\lambda \cdot v) = \gamma(\lambda) \cdot \gamma(v)$$

Von einer **stetigen Galois-linearen Operation** oder auch kurz **galoislinearen Operation** fordern wir zusätzlich die Stetigkeit der zugehörigen Abbildung $\Gamma \times V \rightarrow V$ für die Krull-Topologie auf Γ und die diskrete Topologie auf V .

6.4.2. Oft ist für solch eine Operation auch die exponentielle Schreibweise $a^\gamma := \gamma^{-1}(a)$ praktisch. Das Invertieren sorgt dabei für die Identität $a^{(\gamma\sigma)} = (a^\gamma)^\sigma$.

Definition 6.4.3. Sei K/k eine Körpererweiterung. Eine **k -Form eines K -Vektorraums** V ist ein k -Untervektorraum $V_k \subset V$ derart, daß die Multiplikation einen Isomorphismus $K \otimes_k V_k \xrightarrow{\sim} V$ liefert. Gleichbedeutend ist die Forderung, daß V_k ganz V als K -Vektorraum erzeugt und daß jede über k linear unabhängige Teilmenge unseres Untervektorraums V_k auch über K linear unabhängig ist in V .

Proposition 6.4.4 (Formen und Galoiswirkungen bei Vektorräumen). *Seien K/k eine Galois-erweiterung und $\Gamma = \text{Gal}(K/k)$ ihre Galoisgruppe. Gegeben ein K -Vektorraum V mit einer galoislinearen Operation von Γ induziert die Multiplikation einen Isomorphismus*

$$K \otimes_k V^\Gamma \xrightarrow{\sim} V$$

6.4.5. Gegeben eine Galois-Erweiterung K/k mit Galoisgruppe Γ und ein K -Vektorraum V erhalten wir insbesondere zueinander inverse Bijektionen

$$\left\{ \begin{array}{l} k\text{-Formen} \\ V_k \subset V \end{array} \right\} \xleftrightarrow{\sim} \left\{ \begin{array}{l} \text{galoislineare Operationen} \\ \Gamma \times V \rightarrow V \end{array} \right\}$$

wie folgt: Jeder k -Form $V_k \subset V$ ordnen wir diejenige galoislineare Operation von Γ , die durch die Vorschrift $\gamma : a \otimes v \mapsto \gamma(a) \otimes v \quad \forall a \in K, v \in V_k$ gegeben ist, und umgekehrt jeder galoislinearen Operation $\Gamma \times V \rightarrow V$ ihre Fixpunktmenge $V_k = V^\Gamma$. Nach der Proposition ist offensichtlich, daß wir so zueinander inverse Bijektionen erhalten.

Beweis. Wir beginnen mit der Surjektivität. Gegeben $v \in V$ finden wir nach Annahme und der Definition der Krull-Topologie eine endliche Galois'sche Untererweiterung K_0/k derart, daß die Operation von Γ auf v über $\Gamma_0 := \text{Gal}(K_0/k)$

faktorisiert. Sind $\sigma, \tau, \dots, \rho$ die Elemente von Γ_0 und ist $a_\sigma, a_\tau, \dots, a_\rho$ eine Basis von K_0 über k , so ist nach dem Satz über die lineare Unabhängigkeit von Charakteren 3.8.16 die Matrix $(a_\tau^\sigma)_{\tau, \sigma \in \Gamma_0}$ invertierbar, deren Einträge wie angedeutet durch das Anwenden der Elemente $\sigma, \tau, \dots, \rho$ der Galoisgruppe Γ_0 auf die Elemente $a_\sigma, a_\tau, \dots, a_\rho$ des Körpers K_0 entstehen. Es gibt also Elemente $b_{\rho, \sigma} \in K$ mit $\sum_\sigma b_{\rho, \sigma} a_\sigma^\tau = \delta_{\rho\tau}$ für alle ρ, τ . Bilden wir nun die Vektoren

$$v_\sigma := \sum_{\tau \in \Gamma_0} (a_\sigma v)^\tau = \sum_{\tau \in \Gamma_0} a_\sigma^\tau v^\tau \in V^\Gamma, \quad \text{so erkennen wir} \quad \sum_\sigma b_{1, \sigma} v_\sigma = v$$

für $1 \in \Gamma_0$ das neutrale Element. Das zeigt die Surjektivität. Nun erfüllt der Kern \ker unserer Abbildung auch die Bedingung der Proposition, aus $\ker \neq 0$ folgt demnach mit dem, was wir schon wissen, sofort $\ker^\Gamma \neq 0$. Es bleibt also nur zu zeigen, daß die Γ -Invarianten in $K \otimes_k V^\Gamma$ mit dem Bild von $k \otimes_k V^\Gamma$ zusammenfallen. Dabei können wir uns leicht auf den Fall $V^\Gamma = k$ einschränken, und in diesem Fall ist es offensichtlich. \square

Definition 6.4.6. Gegeben ein K -Vektorraum mit einer k -Form $V \supset V_k$ heißt ein K -Untervektorraum $W \subset V$ **definiert über k** , wenn es einen k -Untervektorraum $W_k \subset V_k$ gibt derart, daß die Multiplikation einen Isomorphismus $K \otimes_k W_k \xrightarrow{\sim} W$ liefert.

6.4.7. Sei K/k eine Galoiserweiterung mit Galoisgruppe Γ und $V \supset V_k$ ein K -Vektorraum mit einer k -Form. Sei $\Gamma \times V \rightarrow V$ die zugehörige galoislineare Operation. Offensichtlich ist ein K -Untervektorraum $W \subset V$ genau dann definiert über k , wenn er unter Γ stabil ist, wenn also in Formeln gilt $\gamma(W) \subset W$ oder gleichbedeutend $\gamma(W) = W$ für alle $\gamma \in \Gamma$.

6.4.8 (**Formen und bepunktete Torsoren**). Sei K/k eine Galoiserweiterung, $\Gamma = \text{Gal}(K/k)$ ihre Galoisgruppe und V ein K -Vektorraum. Für jede k -Form $\hat{V} \subset V$ erhalten wir eine Rechtsoperation von Γ durch Konjugation auf der Gruppe $\text{Mod}_K^\times(V)$ der Automorphismen des K -Vektorraums V , in Formeln

$$p^\gamma := \hat{\gamma}^{-1} \circ p \circ \hat{\gamma}$$

für $\hat{\gamma} : V \rightarrow V$ unsere galoislineare Operation. Ich notiere unsere Automorphismengruppe dann $\text{Mod}_K^\times(\hat{V})$, um anzudeuten, daß die Γ -Operation von der Form \hat{V} abhängt. Versehen wir $\text{Mod}_K^\times(\hat{V})$ mit der Topologie, in der die Fixatoren endlicher Teilmengen von V eine Umgebungsbasis des neutralen Elements bilden, und versehen unsere Galoisgruppe Γ mit der Krull-Topologie, so ist unsere Rechtsoperation von Γ stetig. Gegeben eine weitere k -Form $\tilde{V} \subset V$ liefert die offensichtliche Identifikation

$$\text{Mod}_K^\times(\tilde{V} \otimes_k K, \hat{V} \otimes_k K) \xrightarrow{\sim} \text{Mod}_K^\times(V)$$

eine Rechtsoperation der Galoisgruppe Γ auf dieser Menge durch die Vorschrift $q^{(\gamma)} := \hat{\gamma}^{-1} \circ q \circ \tilde{\gamma}$. Mit ihrer offensichtlichen Operation $\text{Mod}_K^\times(\hat{V})$ -Linksoperation wird unsere Menge dann ein topologischer Γ -äquivarianter $\text{Mod}_K^\times(\hat{V})$ -Torsor im Sinne von ??, in Formeln gilt insbesondere

$$(pq)^{(\gamma)} = p^\gamma q^{(\gamma)}$$

Unser Torsor besitzt auch einen ausgezeichneten Punkt, die Identität auf V . Diese Konstruktion liefert sogar für jede feste k -Form $\hat{V} \subset V$ eine Bijektion

$$\left\{ \begin{array}{l} k\text{-Formen } \tilde{V} \subset V \\ \text{des } K\text{-Vektorraums } V \end{array} \right\} \xrightarrow{\sim} \left\{ \begin{array}{l} \text{Bepunktete topologische} \\ \Gamma\text{-äquivariante } \text{Mod}_K^\times(\hat{V})\text{-Torsoren,} \\ \text{bis auf Isomorphismus} \end{array} \right\}$$

Gemeint sind rechts Isomorphismen bepunkteter Torsoren, die also den ausgezeichneten Punkt in den ausgezeichneten Punkt überführen. Die Umkehrabbildung kann wie folgt beschrieben werden: Gegeben ein bepunkteter topologischer Γ -äquivarianter $\text{Mod}_K^\times(\hat{V})$ -Torsor (X, x) erhalten wir die zugehörige galoislineare Γ -Operation auf V , indem wir eine Abbildung $z : \Gamma \rightarrow \text{Mod}_K^\times(\hat{V})$ erklären durch die Identität $x^{(\gamma)} = z(\gamma)x$ und daraus eine galoislineare Γ -Wirkung auf V machen mittels der Vorschrift $\tilde{\gamma} := \hat{\gamma} \circ z(\gamma)$ und eben wieder $\tilde{V} \subset V$ definieren als deren Fixpunktmenge. Gegeben $\varphi \in \text{Mod}_K^\times(\hat{V})$ entspricht nun der bepunktete Torsor $(X, \varphi x)$ der k -Form $\varphi(\tilde{V}) \subset V$. Da aber je zwei k -Formen eines K -Vektorraums V durch einen Automorphismus von V auseinander hervorgehen, gibt es insbesondere, wenn wir keinen Basispunkt auszeichnen, bis auf Isomorphismus nur einen einzigen topologischen Γ -äquivarianten $\text{Mod}_K^\times(\hat{V})$ -Torsor. In der Sprache der Gruppenkohomologie gilt also $H_{\text{st}}^1(\Gamma; \text{Mod}_K^\times(\hat{V})) = 0$ und insbesondere

$$H_{\text{st}}^1(\Gamma; \text{GL}(n; K)) = 0$$

für die Gruppe $\text{GL}(n; K)$ mit ihrer offensichtlichen Γ -Operation. Diese Aussage wird meist zitiert als **Hilbert's Satz 90**. Hilbert selbst formuliert sie allerdings nur im Fall $n = 1$.

Definition 6.4.9. Sei K/k eine Körpererweiterung. Eine **k -Form einer K -Algebra** A ist eine k -Form $\hat{A} \subset A$ des Vektorraums A , die gleichzeitig eine k -Unteralgebra von A ist.

6.4.10 (**Formen von Algebren und galoislineare Operationen**). Gegeben eine Galoiserweiterung K/k mit Galoisgruppe Γ und eine K -Algebra A liefern die Bijektionen aus 6.4.5 auch zueinander inverse Bijektionen

$$\left\{ \begin{array}{l} k\text{-Formen} \\ \hat{A} \subset A \\ \text{der } K\text{-Algebra } A \end{array} \right\} \xleftrightarrow{\sim} \left\{ \begin{array}{l} \text{galoislineare Operationen} \\ \Gamma \times A \rightarrow A \\ \text{auf der } K\text{-Algebra } A \end{array} \right\}$$

Hier fordern wir von einer Operation auf einer Algebra zusätzlich, daß sie mit der Verknüpfung in unserer Algebra verträglich sein soll, in Formeln $\hat{\gamma}(a \cdot b) = \hat{\gamma}(a) \cdot \hat{\gamma}(b)$ für alle $a, b \in A$ und $\gamma \in \Gamma$.

6.4.11 (Formen von Algebren und Torsoren). Gegeben eine Galoiserweiterung K/k mit Galoisgruppe Γ und eine K -Algebra A mit einer ausgezeichneten k -Form $\hat{A} \subset A$ stabilisiert unsere Γ -Operation auf $\text{Mod}_K^\times(\hat{A})$ aus 6.4.8 die Untergruppe $\text{Alg}_K^\times(\hat{A})$ der Automorphismen von K -Algebren und unsere Bijektion aus 6.4.8 induziert eine Bijektion

$$\left\{ \begin{array}{l} k\text{-Formen } \tilde{A} \subset A \\ \text{der } K\text{-Algebra } A \end{array} \right\} \xrightarrow{\sim} \left\{ \begin{array}{l} \text{bepunktete topologische} \\ \Gamma\text{-äquivalente } \text{Alg}_K^\times(\hat{A})\text{-Torsoren,} \\ \text{bis auf Isomorphismus} \end{array} \right\}$$

$$\tilde{A} \quad \mapsto \quad \text{Alg}_K^\times(\tilde{A}, \hat{A})$$

Hier ist rechts zu verstehen, daß wir beim Übergang vom Fall der Vektorräume zum Fall der Algebren jedem bepunkteten $\text{Mod}_K^\times(\hat{A})$ -Torsor die $\text{Alg}_K^\times(\hat{A})$ -Bahn des ausgezeichneten Punktes zuordnen. Entspricht die k -Form $\tilde{A} \subset A$ dem bepunkteten Torsor (X, x) und ist $\varphi \in \text{Alg}_K^\times(\hat{A})$ ein Automorphismus von K -Algebren, so entspricht nun der bepunktete Torsor $(X, \varphi x)$ der k -Form $\varphi(\tilde{A}) \subset A$. Insbesondere induziert unsere Bijektion eine Bijektion

$$\left\{ \begin{array}{l} k\text{-Formen } \tilde{A} \subset A \\ \text{der } K\text{-Algebra } A, \\ \text{bis auf Isomorphismus} \\ k\text{-Algebren} \end{array} \right\} \xrightarrow{\sim} \left\{ \begin{array}{l} \text{topologische} \\ \Gamma\text{-äquivalente} \\ \text{Alg}_K^\times(\hat{A})\text{-Torsoren,} \\ \text{bis auf Isomorphismus} \end{array} \right\}$$

Vorschau 6.4.12. In der Sprache der Gruppenkohomologie ?? lesen sich die obigen Bijektionen als Bijektionen

$$\{k\text{-Formen der } K\text{-Algebra } A\} \xrightarrow{\sim} Z_{\text{st}}^1(\Gamma; \text{Alg}_K^\times(\hat{A}))$$

$$\{k\text{-Formen der } K\text{-Algebra } A\}_{/\cong_k} \xrightarrow{\sim} H_{\text{st}}^1(\Gamma; \text{Alg}_K^\times(\hat{A}))$$

Hier meint \cong_k , daß wir in der zweiten Zeile nur k -Formen bis auf Isomorphismus von k -Algebren betrachten, und der untere Index st erinnert jeweils daran, daß nur stetige Einskozykel zu betrachten sind.

6.4.13 (Innere Formen algebraischer Gruppen). Analoges gilt für Koalgebren und Bialgebren und überhaupt sehr allgemein für Vektorräume A mit einer Familie ausgezeichneter Homomorphismen zwischen Tensorpotenzen von A , etwa einem Homomorphismus $A \otimes A \rightarrow A$ und einem weiteren Homomorphismus $A \rightarrow A \otimes A$. Insbesondere gilt es für affine algebraische Gruppen G . In diesem

Fall induziert die Operation der Gruppe $G(K)$ durch Konjugation einen Gruppenhomomorphismus $\text{int} : G(K) \rightarrow \text{GrpVar}_K^\times(G)$. Ist \hat{G} eine k -Form von G , so trägt $\hat{G}(K) := \text{RAlg}_k(\mathcal{O}(\hat{G}), K)$ eine stetige Γ -Wirkung durch Nachschalten, die wir durch Invertieren zu einer Rechtsoperation machen können. Der Homomorphismus $\text{int} : \hat{G}(K) \rightarrow \text{GrpVar}_K^\times(\hat{G})$ ist verträglich mit der Rechtsoperation von Γ . Die k -Formen von G , die Kohomologieklassen im Bild der von int induzierten Abbildung

$$H_{\text{st}}^1(\Gamma; \hat{G}(K)) \rightarrow H_{\text{st}}^1(\Gamma; \text{GrpVar}_K^\times(\hat{G}))$$

entsprechen, heißen dann die **zu \hat{G} inneren k -Formen von G** . Gegeben ein Einszykel alias eine stetige Abbildung $z : \Gamma \rightarrow \hat{G}(K)$ mit $z(\gamma\beta) = z(\gamma)^\beta z(\beta)$ wie in ?? wird die Galoisoperation zur neuen Form also gegeben durch $\tilde{\gamma} := \hat{\gamma} \circ \text{int}(z(\gamma))$.

Ergänzung 6.4.14. Ich wollte mir überlegen, daß gegeben zwei Bilinearformen auf einem endlichdimensionalen k -Vektorraum, die über K isomorph werden, die zugehörigen Automorphismengruppen innere Formen voneinander sind. Ich wollte mir ferner überlegen, daß zueinander innere Formen isomorphe k -lineare Tensorkategorien endlichdimensionaler Darstellungen besitzen.

6.5 Kummer-Theorie

Definition 6.5.1. Sei $n \in \mathbb{N}$ eine natürliche Zahl. Eine Körpererweiterung L/K heißt eine **Kummer-Erweiterung durch n -te Wurzeln** oder kurz eine **n -Kummererweiterung**, wenn (1) unser n kein Vielfaches der Charakteristik unserer Körper ist, (2) der Körper K **alle n -ten Einheitswurzeln enthält** und (3) der Körper L über K erzeugt wird von n -ten Wurzeln von Elementen aus K , in Formeln

$$L = K(\alpha \mid \alpha \in L, \alpha^n \in K)$$

Nennen wir L/K eine Kummer-Erweiterung, so ist gemeint, daß es ein n gibt derart, daß L/K eine Kummer-Erweiterung durch n -te Wurzeln ist.

6.5.2. Für jedes multiplikativ notierte Monoid M vereinbaren wir die Notation $M^n = \{\alpha^n \mid \alpha \in M\}$. Der kleine Punkt vor dem n soll klar machen, daß nicht das kartesische Produkt von n Kopien der Menge M gemeint ist.

Satz 6.5.3 (Kummer-Theorie). Seien K ein Körper und $n \in \mathbb{N}$ kein Vielfaches der Charakteristik von K und K enthalte alle n -ten Einheitswurzeln. So gilt:

1. Genau dann ist eine Körpererweiterung L/K eine n -Kummererweiterung, wenn L/K eine Galois-Erweiterung ist mit abelscher Galois-Gruppe vom Exponenten n , also mit $g^n = 1$ für alle $g \in \text{Gal}(L/K)$;

2. Die Abbildungsvorschrift $L \mapsto \Delta(L) := ((L^\times)^n \cap K^\times) / (K^\times)^n$ liefert eine Bijektion

$$\left\{ \begin{array}{l} n\text{-Kummererweiterungen von } K \text{ in einem} \\ \text{festen algebraischen Abschluß } \bar{K} \text{ von } K \end{array} \right\} \xrightarrow{\sim} \left\{ \begin{array}{l} \text{Untergruppen von} \\ K^\times / (K^\times)^n \end{array} \right\}$$

Wir nennen $\Delta(L)$ die **Kummergruppe** unserer Kummererweiterung.

3. Ist L/K eine n -Kummererweiterung mit Kummergruppe $\Delta = \Delta(L)$ und Galoisgruppe $G := \text{Gal}(L/K)$ und bezeichnet μ_n die n -ten Einheitswurzeln von K , so erhalten wir eine wohldefinierte bilineare Abbildung

$$\begin{aligned} G \times \Delta &\rightarrow \mu_n \\ (g, a) &\mapsto g(\sqrt[n]{a}) / \sqrt[n]{a} \end{aligned}$$

4. Ist L/K eine n -Kummererweiterung, so liefert unsere bilineare Abbildung einen Isomorphismus

$$G \xrightarrow{\sim} \text{Hom}(\Delta, \mu_n)$$

Insbesondere haben wir für jede endliche Kummererweiterung einen unkanonischen Isomorphismus $G \cong \Delta$ zwischen ihrer Galoisgruppe und ihrer Kummergruppe;

5. Ist L/K eine n -Kummererweiterung, so liefert unsere bilineare Abbildung einen Isomorphismus

$$\Delta \xrightarrow{\sim} \text{Hom}^{\text{st}}(G, \mu_n)$$

Hierbei sind rechts stetige Gruppenhomomorphismen gemeint für die Krull-Topologie auf der Galoisgruppe und die diskrete Topologie auf μ_n .

6.5.4. Seien K ein Körper und \bar{K} ein algebraischer Abschluß von K . Da Kummererweiterungen per definitionem Galois sind, ist jede Kummererweiterung von K isomorph über K zu genau einem Unterkörper von \bar{K} , der K umfaßt.

Beweis. 3. Das ist klar.

1. Per definitionem ist jede Kummererweiterung ein Zerfällungskörper separabler Polynome und mithin Galois. Die in Teil 3 angegebene Paarung $G \times \Delta \rightarrow \mu_n$ liefert offensichtlich einen injektiven Gruppenhomomorphismus $G \hookrightarrow \text{Ens}(\Delta, \mu_n)$ und zeigt so, daß für jede n -Kummererweiterung die Galoisgruppe abelsch ist vom Exponenten n . Sei andererseits L/K eine Erweiterung mit abelscher Galoisgruppe vom Exponenten n . Jedes Element von L liegt schon in einem Zwischenkörper, der Galois und endlich ist über K . Ohne Beschränkung der Allgemeinheit dürfen wir also L/K endlich annehmen. Dann finden wir Untergruppen

$H_1, \dots, H_r \subset \text{Gal}(L/K)$ mit trivialem Schnitt $H_1 \cap \dots \cap H_r = 1$ und zyklischen Quotienten G/H_i , und die zugehörigen Unterkörper L_1, \dots, L_r erzeugen L und entstehen nach 4.6.3 jeweils durch Adjunktion einer n -ten Wurzel zu K . Damit ist auch 1 bewiesen.

4&5. Gegeben eine abelsche Gruppe G definieren wir ihre duale Gruppe oder Charaktergruppe als $\mathfrak{X}(G) := \text{Hom}(G, \mathbb{Q}/\mathbb{Z})$. Die offensichtliche Paarung $G \times \mathfrak{X}(G) \rightarrow \mathbb{Q}/\mathbb{Z}$ liefert dann eine natürliche Abbildung von G in sein Biduals. Für $G = \mathbb{Z}/m\mathbb{Z}$ prüft man $\mathfrak{X}(G) \cong \mathbb{Z}/m\mathbb{Z}$ und prüft sogar, daß die natürliche Abbildung von G in sein Biduals eine Bijektion ist. Dieselben Aussagen $\mathfrak{X}(G) \cong G$ und $G \xrightarrow{\sim} \mathfrak{X}(\mathfrak{X}(G))$ folgen dann für alle endlichen abelschen Gruppen G . Betrachten wir nur Gruppen mit Exponent n , so kann hier auch μ_n den Part von \mathbb{Q}/\mathbb{Z} übernehmen. Nun wissen wir bereits, daß unsere Paarung $G \times \Delta \rightarrow \mu_n$ eine Injektion

$$G \hookrightarrow \text{Hom}(\Delta, \mu_n)$$

induziert. Ebenso ist umgekehrt klar, daß sie eine Injektion

$$\Delta \hookrightarrow \text{Hom}(G, \mu_n)$$

induziert, denn für $a \in \Delta$ und $\alpha \in L^\times$ mit $\alpha^n = a$ folgt aus $g(\alpha) = \alpha \forall g \in G$ schon $\alpha \in K^\times$, also $a \in (K^\times)^n$. Im Fall einer endlichen n -Kummererweiterung zeigt die zweite Injektion, daß Δ endlich ist, und mit unserer Dualität folgt dann, daß unsere Injektionen beide Isomorphismen sein müssen. So erhalten wir 4 und 5 im Fall einer endlichen Kummererweiterung. Im allgemeinen folgt dann 4 durch Übergang zum Limes über alle endlichen Teilerweiterungen und 5 durch Übergang zum Kolimes über alle endlichen Teilerweiterungen.

2. Sei \bar{K} ein fester algebraischer Abschluß von K . Für eine beliebige Teilmenge $D \subset K^\times / (K^\times)^n$ können wir eine n -Kummererweiterung $E(D) \subset \bar{K}$ von K bilden, indem wir zu K alle n -ten Wurzeln von Repräsentanten in K^\times der Elemente aus D in \bar{K} adjungieren. Sicher erhalten wir dann für eine n -Kummererweiterung $L \subset \bar{K}$ von K unser L aus seiner Kummergruppe $\Delta(L)$ zurück als $L = E(\Delta(L))$. Es gilt nur noch umgekehrt zu zeigen, daß für jede Untergruppe $D \subset K^\times / (K^\times)^n$ auch gilt $D = \Delta(E(D))$. Offensichtlich ist hier $D \subset \Delta(E(D))$. Um Gleichheit zu zeigen, dürfen wir ohne Beschränkung der Allgemeinheit D endlich annehmen. Dann ist auch $E(D)/K$ endlich. Nun bezeichne man mit G die Galoisgruppe dieser Körpererweiterung. und betrachte das Diagramm

$$\begin{array}{ccc} G & \xrightarrow{\sim} & \text{Hom}(\Delta(E(D)), \mu_n) \\ \parallel & & \downarrow \\ G & \hookrightarrow & \text{Hom}(D, \mu_n) \end{array}$$

Die obere Horizontale ist bijektiv aufgrund der bereits bewiesenen Teile. Die untere Horizontale ist injektiv, da die n -ten Wurzeln der Repräsentanten der Elemente

von D bereits $E(D)$ erzeugen. Die rechte Vertikale ist surjektiv als duale Abbildung zu einer Injektion. Es folgt, daß die rechte Vertikale ein Isomorphismus sein muß. Dualisieren liefert schließlich $D = \Delta(E(D))$ wie gewünscht. \square

7 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, . . .

8 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 1.1 zu Fuß. Klassifikation der Gruppen F mit fünf Elementen durch Theorie: Untergruppen, Untergruppen von \mathbb{Z} nach ??, Nebenklassen ?? und Lagrange: F hat nur die beiden Untergruppen 1 und F . Bijektion $\text{Grp}(\mathbb{Z}, G) \xrightarrow{\sim} G$, $\varphi \mapsto \varphi(1)$ für jede Gruppe G . Also für $|G| = 5$ Surjektion $\mathbb{Z} \rightarrow G$ durch $1 \mapsto g$ mit $g \neq e$. Universelle Eigenschaft surjektiver Gruppenhomomorphismen.
- 21.10 Normalteiler ?? 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 1.2.5.
- 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 ??, ??.
- 4.11 Jeder Primteiler der Ordnung einer abelschen Gruppe ist die Ordnung eines Elements ??, ?? . 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

- [AL] *Skriptum Algebra und Zahlentheorie*;
- [AN1] *Skriptum Analysis 1*;
- [AN2] *Skriptum Analysis 2*;
- [AN3] *Skriptum Analysis 3*;
- [Art] Emil Artin, *Galois theory*.
- [E⁺92] Ebbinghaus et al., *Zahlen*, Springer, 1992.
- [GR] *Skriptum Grundlagen*;
- [KAG] *Skriptum Kommutative Algebra und Geometrie*;
- [LA1] *Skriptum Lineare Algebra 1*;
- [LA2] *Skriptum Lineare Algebra 2*;
- [Lan74] Serge Lang, *Algebra*, Addison-Wesley, 1974.
- [Lor96] Falko Lorenz, *Einführung in die Algebra I*, Spektrum, 1996.
- [NAS] *Skriptum Nichtkommutative Algebra und Symmetrie*;
- [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** (1987), no. 7, 279–280.
- [TF] *Skriptum Fundamentalgruppe und Überlagerungstheorie*;
- [TS] *Skriptum Singuläre Homologie*;
- [Wei74] André Weil, *Basic number theory*, Springer, 1974.

Index

- $K(X)$ Funktionenkörper, 78
- $R[X_1, \dots, X_n]$ Polynomring, 36
- $R[a_1, \dots, a_n]$ Teilring, 36
- $R[X_1, \dots, X_n]$ Polynomring, 36
- $[L : K]_s$ Separabilitätsgrad, 111
- \bar{K} algebraischer Abschluß, 118
- \times
 - semidirektes Produkt, 11
- $\langle T \rangle$ Ideal-Erzeugnis, 33
- $\langle ' \rangle$ Freiheitsstrichlein, 85
- $\langle () \rangle$ Erzeugung als Körper, 85
- $\langle \frac{a}{n} \rangle$ Jacobi-Symbol, 155
- $\langle \frac{a}{p} \rangle$ Legendre-Symbol, 151
- $\langle \dagger \rangle$ Mengenanzeiger bei Erzeugung, 85
- $\langle [] \rangle$ Erzeugung als Krings, 85
- $\langle \prime \rangle$ Freiheitsstrichlein, 85
- $\langle \rangle$ Erzeugung als Gruppe oder Modul, 84
- $\langle | \rangle$ Erzeugung als Ring, 85
- $\langle | \rangle$ Erzeugung als Monoid, 84
- abelsch
 - Körpererweiterung, 156
- Ableitung
 - formale, 103
- Abschluß
 - algebraischer, von Körper, 118
- Addition
 - von Ordinalzahlen, 175
- Adjunktion
 - einer Nullstelle, 92
- Alexandroff'sche Halbgerade, 181
- algebraisch
 - Abschluß, 118
 - in Körpererweiterung, 79
 - Körpererweiterung, 100
 - komplexe Zahl, 79
 - unabhängig, über Ring, 36
- allgemeine Gleichung, 131
- alternierende Gruppe, 7, 26
- Anfangsstück, 173
- antisymmetrisch
 - Polynom, 67
- auflösbar
 - Gruppe, 13, 161
- Auflösbarkeit von Gleichungen, 161
- Ausdehnbarkeitskriterium, 98
- Ausdehnung, 97
- Automorphismus
 - eines Körpers, 126
- Bewertung, 55
- Bézout
 - Schranke von, 68
- Binomialkoeffizienten
 - quantisierte, 62
- biquadratisch, 140
- Cardano'sche Formeln, 164
- casus irreducibilis, 168
- Cauchy
 - Satz von, 17
- Cayley'sche Zahlen, 124
- Charakteristik, 76
- Chinesischer Restsatz
 - abstrakter, 38
- cyclotomic polynomial, 60
- Darstellung durch Radikale, 161
- Decktransformation, 135
- Deli'sches Problem, 90
- deriviert
 - Gruppe, 14
- Dimension
 - eines Vektorraums, 177
- diophantische Gleichung, 154
- disjunkt, 24

Diskriminante, 66
 eines kubischen Polynoms, 66
 Doppeldreizykel, 27
 Doppeltransposition, 27
 duale Partition, 21
 echt
 Ideal, 46
 einfach
 Gruppe, 7
 Körpererweiterung, 81
 Einheitswurzel
 in \mathbb{C} , 60
 Eisensteinkriterium, 60
 Element
 primitives, 81
 elementarsymmetrische Polynome, 63
 endlich
 Körpererweiterung, 82
 Menge, 175
 endliche Körper, 91
 Ensf fast überall definierte Funktionen, 137
 Ergänzungssatz
 für Jacobi-Symbole, 155
 zum Reziprozitätsgesetz, 154
 Erweiterungskörper, 77
 erzeugt
 Teilring, 36
 euklidisch
 Ring, 45
 Euler'sche Kongruenz, 147
 φ , Euler'sche φ -Funktion, 146
 faithful, 129
 faktoriell, 41
 Feit-Thompson
 Satz von, 7
 Fermat'sche Zahlen, 147
 fidèle, 129
 Fixkörper, 127
 Form
 innere, 194
 von Algebra, 192
 von Vektorraum, 190
 Freiheitsstrichlein, 85
 Frobenius-Homomorphismus, 126
 $\text{Gal}(L/K)$ Galoisgruppe, 126
 Galois-linear
 Operation, abstrakte, 190
 Operation, stetige, 190
 Galoiserweiterung, 127
 Galoisgruppe, 126
 eines Polynoms, 130
 Galoiskorrespondenz, 137
 Gauß'sche Zahl, 45
 Gauß, Lemma von, 56
 Gilmer
 Satz von, 132
 gleichmächtig, 176
 $\text{grad}_K(\alpha)$ Grad von α über K , 82
 Grad
 einer Körpererweiterung, 82
 eines Polynoms
 in mehreren Veränderlichen, 68
 von Element in Körpererweiterung, 82
 Grundkörper, 77
 Gruppe
 einfache, 7
 Gruppentafel, 5
 Hauptideal, 34
 Hauptidealring, 43
 Hilbert's Satz 90, 192
 Hilbert'sche Probleme
 Nummer 12, 156
 homogen
 Polynom, 65
 homogene Komponente
 von Polynom, 65

Homomorphismus
 über Grundring, 97
 von Körpererweiterungen, 97
 von K -Kringen, 97

Ideal
 echtes, 46
 erzeugt von, 33
 maximales, 46
 von Ring, 32

innere Form, 194

inseparabel
 rein, Körpererweiterung, 111

Integritätsbereich, 41

Invariantenring, 62

irk Irreduziblenklassen, 50

$\text{Irr}(\alpha, K)$ Minimalpolynom, 79

irreduzibel
 k -irreduzibel, Polynom, 46
 Element eines Krings, 39
 Polynom, 46

Irreduziblenklasse, 50

isomorph
 Gruppen, 5

Isomorphismus
 von geordneten Mengen, 173
 von Körpererweiterungen, 97

Jacobi-Symbol, 155

Jordan-Hölder
 für endliche Gruppen, 10
 für Gruppen, 11

Kardinalität, 177
 einer endlichen Menge, 176

Kardinalzahl, 176

ker
 Kern von Ringhomomorphismus, 32

Klassengleichung, 12

Klassifikation
 der endlichen Gruppen, 5

Klein'sche Vierergruppe, 5

Körper
 vollkommener, 106
 körperendlich, 77
 Körpererweiterung, 77
 abelsche, 156
 algebraische, 100
 echte, 77
 einfache, 81
 endliche, 82
 im verallgemeinerten Sinne, 97
 normale, 100
 primitive, 81
 quadratische, 83
 separable, 106
 zyklische, 156

Kommutator
 in Gruppe, 14

Kompositionsalgebra, 124

Kompositionsfaktor
 von Gruppe, 10

Kompositionsreihe
 einer Gruppe, 10

Kompositum, 160

konjugiert
 Untergruppen, 15

konstruierbare Zahlen, 86
 aus Teilmenge, 91

Konstruierbarkeit, 86, 91

Konstruierbarkeit regelmäßiger n -Ecke,
 146

Kranzprodukt, 11

Kreisteilungskörper, 143

Kreisteilungspolynom, 60

A -Kring, 97

K -Kring, 97

Kronecker-Konstruktion, 93

Kronecker-Weber, Satz von, 156

Krull-Topologie, 189

kubische Gleichung, 164

Kummer-Erweiterung
 durch n -te Wurzeln, 194

Kummergruppe, 195
 Legendre-Symbol, 151
 lexikographische Ordnung, 64
 Limeszahl, 175
 logarithmische Ableitung
 formale, 109
 maximal
 echtes Ideal, 46
 Ideal, 46
 mehrfache Nullstelle, 103
 Mengenanzeiger, 85
 minimaler Zerfällungskörper, 96
 Minimalpolynom, 79
 Morphismus
 von geordneten Mengen, 173
 Multiplikationssatz
 der Mengenlehre, 180
 Multiplikativität
 des Grades, 83
 $N_G(H)$ Normalisator, 142
 Nachfolger, 173
 Neumann
 Lemma, 116
 Nikolov, 189
 nilpotent
 Gruppe, 13
 normal
 Körpererweiterung, 100
 normale Hülle, 102
 Normalisator
 von Untergruppe, 142
 normiert
 größter gemeinsamer Teiler, 104
 Nullstelle
 mehrfache, 103
 Oberkörper, 77
 Oktaven, 124
 Oktonionen, 124
 Ordinalzahl, 174
 ordnungsisomorph, 173
 Ordnungsisomorphismus, 173
 p -Gruppe, 12
 parfait, corps, 106
 Partition
 einer Zahl, 20
 perfect field, 106
 Polynom
 antisymmetrisches, 67
 symmetrisches, 62
 Polynominterpolation, 39
 prim, 44
 Primelement, 44
 primitiv
 Element von Körpererweiterung, 81
 Körpererweiterung, 81
 Polynom, 56
 primitive Einheitswurzel, 143
 primitives Element, 115
 Primkörper, 76
 Produkt
 von Ordinalzahlen, 175
 von Gruppen
 semidirektes, 11
 von Idealen, 37
 von Ringen, 37
 Produktring, 37
 Puiseux
 Satz von, 121
 Puiseux-Reihe, 121
 $\mathbb{Q}(\sqrt[n]{1})$ Kreisteilungskörper, 143
 quadratisch
 Körpererweiterung, 83
 quadratischer Rest, 148
 Quadratwurzelabschluß, 170
 Radikalabschluß
 in Körpererweiterung, 170
 Radikalerweiterung

eines Körpers, 161
 rein inseparabel, 111
 Restklassenring, 33
 Resultante, 72
 Reziprozitätsgesetz
 für Jacobi-Symbole, 155
 quadratisches, 150
 Ring, 31
 Ring(R, S) Ringhomomorphismen, 31
 Ringhomomorphismus, 31

 Schröder-Bernstein, 177
 semidirektes Produkt, 11
 separabel
 Element von Körpererweiterung, 106
 Körpererweiterung, 106
 Polynom, 105
 Separabilitätsgrad, 111
 separabler Abschluß
 eines Körpers, 118
 in Körpererweiterung, 111
 soluble, 13
 solvable, 13
 Subquotient
 einer Kompositionsreihe, 10
 Summe
 von Idealen, 37
 Sylow, 14
 Sylowsätze, 15
 Sylowuntergruppe, 14
 Sylvesterdeterminante, 75
 Symmetrie, 7
 Symmetriegruppe, 7
 symmetrisch
 Polynom, 62
 symmetrische Polynome, 63

 teilerfremd, 105
 Teilring, 36
 Totalgrad, 68
 Translationssatz der Galoistheorie
 allgemeiner Fall, 188
 endlicher Fall, 160
 Transposition, 24
 transzendent
 in Körpererweiterung, 79
 komplexe Zahl, 79
 treu
 Gruppenwirkung, 129

 überauflösbar, 14
 unendlich
 Menge, 175
 Unendlichkeitsaxiom, 175
 Unterkörper, 76
 erzeugt von Teilmenge, 76
 Untervektorraum
 definiert über, 191

 valuation, 55
 vollkommen
 Körper, 106
 Vorgänger, 173

 Wohlordnung, 173
 Würfelverdopplung, 90

 \times
 semidirektes Produkt, 11

 Young-Diagramm, 21

 $Z(G)$ Zentrum der Gruppe G , 11
 $Z_G(g)$ Zentralisator von g in G , 12
 Zentralisator
 von Element, 12
 Zentralreihe
 absteigende, 14
 Zentrum
 einer Gruppe, 11
 Zerfallungserweiterung
 eines Polynoms, 96
 Zerfallungskörper
 einer Menge von Polynomen, 123

eines Polynoms, 96
Zurückholen
 von fast überall definierten Funktionen, 137
Zykel
 in Permutationsgruppe, 24
Zykellängenabbildung, 23
Zykelschreibweise, 24
zyklisch
 Körpererweiterung, 156
zyklotomisches Polynom, 60