Algebra und Zahlentheorie
Kurzskript

A. Martin-Pizarro

Albert-Ludwigs-Universität Freiburg
Wintersemester 2022/2023

pizarro@math.uni-freiburg.de

6. März 2023

Anmerkungen

Dieses Kurzskript ist zu der im Wintersemester 2022/2023 an der Albert-Ludwigs-Universität Freiburg gehaltenen Vorlesung „Algebra und Zahlentheorie“ entstanden und stark geprägt von den Skripten meiner Kollegin Annette Huber-Klawitter sowie meiner Kollegen Stefan Kebekus und Martin Ziegler. Deren Einflüsse sind nicht zu trennen und können nicht einzeln dargelegt werden.

Zu meinem eigenen Beitrag gehören sicherlich die zahlreichen Fehler, die es im Skript definitiv geben wird. Ich bin sehr dankbar für die Mitteilung solcher Fehler und Ungenauigkeiten. Insbesondere bedanke ich mich bei Herrn Michael Lösch und Herrn Christoph Brackenhofer für ihr aufmerksames Korrekturlesen und ihre Geduld.

Inhaltsverzeichnis

Kapitel 0

Einleitung

✪ Konstruktionen mit Zirkel und Lineal

Notation. In diesem Abschnitt arbeiten wir im Körper der *komplexen Zahlen* $\mathbb{C}$, welchen wir in diesem Abschnitt folgenderweise mit $\mathbb{R}^2$ identifizieren: Die komplexe Zahl $z = a+ib$ mit *Realteil* a und *Imaginärteil* b identifizieren wir mit dem Paar (a, b) aus $\mathbb{R}^2$. Mit dieser Identifikation ist jede reelle Zahl r (als Element von $\mathbb{C}$) *gleich* dem Paar $(r, 0)$.

Mit den Operationen

$$(a + ib) + (c + id) = a + c + i(b + d) \text{ und } (a + ib) \cdot (c + id) = ac - bd + i(ad + bc)$$

ist die Menge der komplexen Zahlen ein Körper (den Begriff kennen wir bereits aus der Vorlesung *Lineare Algebra I*), denn für $(a, b) \neq (0, 0)$ ist

$$(a + ib)^{-1} = \frac{a}{a^2 + b^2} + i\frac{-b}{a^2 + b^2} = \frac{a - ib}{a^2 + b^2},$$

wobei das Element $\bar{z} = a - ib$ das *komplex Konjugierte* von $z = a + bi$ ist.

Definition ✪.1. Eine komplexe Zahl $z = a + ib$ ist *konstruktibel* (mit Zirkel und Lineal), falls z sich durch Iteration folgender Operationen aus den Punkten $1_{\mathbb{R}} = 1_{\mathbb{C}}$ und $0_{\mathbb{R}} = 0_{\mathbb{C}}$ gewinnen lässt:

(a) Gegeben zwei bereits konstruierte verschiedene Punkte, können wir die gesamte Gerade durch diese zwei Punkte bilden.

(b) Gegeben drei bereits konstruierte Punkte P, Q und R (möglicherweise nicht alle verschieden), können wir den gesamten Kreis mit Mittelpunkt P und Radius der Abstand zwischen Q und R bilden, falls Q und R verschieden sind.

(c) Falls zwei bereits konstruierte Geraden sich schneiden, ist der Schnitt wiederum konstruktibel.

(d) Falls zwei bereits konstruierte Kreise sich schneiden, sind die Schnittpunkte wiederum konstruktibel.

(e) Falls eine bereits konstruierte Gerade einen bereits konstruierten Kreis schneidet, sind die Schnittpunkte (oder der Schnittpukt, wenn die Gerade den Kreis nur tangential berührt) wiederum konstruktibel.

Bemerkung ✪.2. Mit Hilfe der Operation (a) entsteht sofort die x-Achse. Mit Hilfe der Operationen (a), (b), (d) und (e) bekommen wir die y-Achse.

Des Weiteren können wir durch jeden konstruktiblen Punkt die zu den Achsen parallelen Geraden bilden. Mit Hilfe der Operation (b) können wir Punkte transportieren. Insbesondere sind der Real- und der Imaginärteil eines konstruktiblen Punktes wiederum konstruktibel. Wenn also die beiden reellen Zahlen $a = (a, 0)$ und $b = (b, 0)$ konstruktibel sind, so ist die komplexe Zahl ib konstruktibel und somit dann auch $z = a+ib$. Wir hätten also eine äquivalente Definition angeben können, indem wir nur die Konstruktibilität reeller Zahlen betrachten.

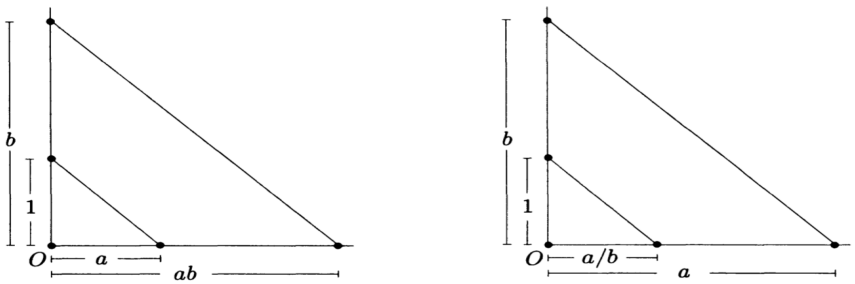
Lemma ✪.3. *Die Menge* Konst *aller konstruktiblen komplexen Zahlen bildet einen Teilkörper von* $\mathbb{C}$. *Das heißt,*

- *die Menge* Konst *ist unter Summen sowie Produkten abgeschlossen und enthält sowohl das additiv neutrale Element* $0_{\mathbb{C}}$ *sowie das multiplikativ neutrale Element* $1_{\mathbb{C}}$.
- *Für jedes Element* z *aus* Konst *liegt das additive Inverse* $-z$ *wiederum in* Konst. *Des Weiteren liegt das multiplikative Inverse* z^{-1} *in* Konst, *falls* $z \neq 0_{\mathbb{C}}$.

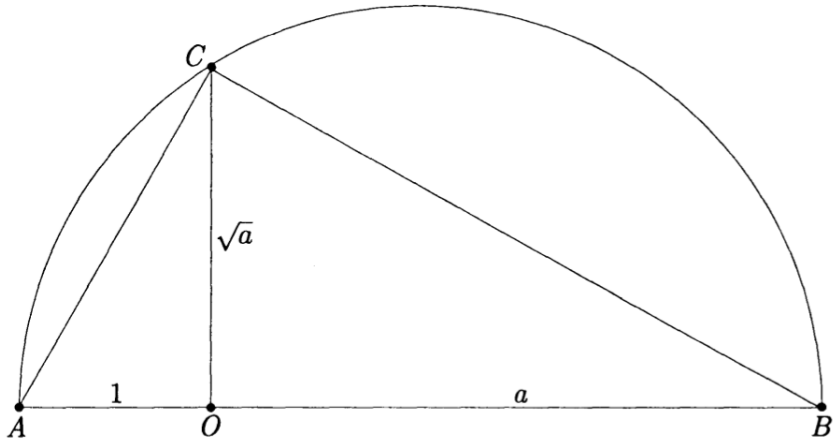
Ferner, wenn z *konstruktibel ist, so ist auch* $\sqrt{z}$ *konstruktibel. Insbesondere, wenn* z *Nullstelle eines nicht-trivialen Polynoms vom Grad* 2 *mit Koeffizienten aus* Konst *ist, so liegt* z *in* Konst.

Beweis. Weil die Summe zweier komplexer Zahlen durch die Summe ihrer reellen und imaginären Teile bestimmt wird, genügt es für die Abgeschlossenheit von Konst unter der Summe zu zeigen, dass die Summe von zwei rellen konstruktiblen Zahlen a und b wiederum konstruktibel ist, was sofort mit Hilfe der Operationen (b) und (e) folgt. Mit Hilfe der Spiegelung am Nullpunkt bekommen wir, dass das additive Inverse $-z = -a - ib$ der komplexen Zahl $z = a + ib$ aus Konst wiederum in Konst liegt. Klarerweise ist $0_{\mathbb{C}}$ in Konst und somit ist Konst eine additive Untergruppe von $\mathbb{C}$.

Die Multiplikation zweier komplexer Zahlen wird durch geeignete Summen von Produkten der reellen und imaginären Teilen definiert. Des Weiteren ist $(a+bi)^{-1} = \frac{a-bi}{a^2+b^2}$, also müssen wir für die Abgeschlossenheit von Konst unter Multiplikation und Division (mit Elementen ungleich Null) nur zeigen, dass das Produkt ab von zwei reellen konstruktiblen Zahlen a und b sowie der Quotient a/b (falls $b \neq 0$) wiederum konstruktibel ist, was sofort aus dem Strahlensatz folgt:



Wir zeigen nun, dass der Teilkörper Konst unter quadratischen Wurzeln abgeschlossen ist. Mit Hilfe der Polarkoordinaten der komplexen Zahl z genügt es zu zeigen, dass die quadratische Wurzel jeder positiven reellen konstruktiblen Zahl a wiederum konstruktibel ist (weil wir Winkel mit Zirkel und Linear halbieren können!). Betrachte nun folgendes Diagramm:



Wir müssen nur noch zeigen, dass der Abstand OC in der Tat $\sqrt{a}$ ist. Bezeichne mit h den Abstand OC sowie mit r den Abstand AC und mit s den Abstand CB. Klarerweise folgen aus dem Satz von Pythagoras folgende Gleichungen:

$$r^2 = 1^2 + h^2 = 1 + h^2 \text{ und } s^2 = h^2 + a^2;$$

$$1^2 + h^2 + h^2 + a^2 = r^2 + s^2 = (a+1)^2 = a^2 + 1 + 2a.$$

Also $2(a - h^2) = 0$ und somit ist $h = \sqrt{a}$, wie gewünscht.

Wenn z Nullstelle des Polynoms $P(T) = z_2T^2 + z_1T + z_0$ vom Grad 2 ist, wobei die Koeffizienten z_i konstruktibel sind, können wir aus dem Obigen annehmen, dass P normiert ist (also $z_2 = 1$). Setze $T = U - \frac{z_1}{2}$ und beachte, dass z genau dann konstruktibel ist, wenn $z - \frac{z_1}{2}$ es ist. Mit diesem Variablenwechsel ist

$$T^2 + z_1T + z_0 = U^2 + (z_0 - \frac{z_1^2}{4}).$$

Das Element $z_0 - \frac{z_1^2}{4}$ ist konstruktibel und somit ist auch $z - \frac{z_1}{2}$ konstruktibel, weil der Teilkörper Konst unter quadratischen Wurzeln abgeschlossen ist. Somit ist auch z konstruktibel, wie gewünscht. □

Definition ❂.4. Sei $n \geq 3$ eine natürliche Zahl. Das regelmäßige n-Eck ist *konstruktibel*, wenn wir das im Einheitskreis einbeschriebene regelmäßige n-Eck konstruieren können.

Aufgabe. Ist das regelmäßige Dreieck konstruktibel? Und das regelmäßige Hexagon (Sechseck)?

Bemerkung ❂.5. Sei z eine komplexe Zahl, welche aus einer der Operationen (c), (d) oder (e) entstanden ist. Wir nehmen an, dass die geometrischen Informationen der entsprechenden Operation über einem Teilkörper K von $\mathbb{C}$ definiert sind. Zeige, dass z Nullstelle eines nichttrivialen Polynoms vom Grad höchstens 2 mit Koeffizienten aus K ist.

Bemerkung ❂.6. Sei die komplexe Zahl z Nullstelle eines normierten Polynoms $P(T)$ vom Grad 2 mit Koeffizienten aus einem Teilkörper K von $\mathbb{C}$. Weil $\mathbb{C}$ algebraisch abgeschlossen ist, lässt sich jedes Polynom als Produkt von Linearfaktoren schreiben, das heißt

$$P(T) = T^2 + z_1T + z_0 = (T - z)(T - w)$$

für eine komplexe Zahl w. Beachte, dass w sich schreiben lässt als $az + b$ für geeignete a und b aus K.

Gegeben a, b, c und d aus K berechne in der einfachsten Form das Produkt $(az+b)(cz+d)$. Des Weiteren berechne $(az + b)(aw + b)$. Schließe daraus, dass die Menge $\{az + b \mid a, b \text{ aus } K\}$ einen Teilkörper von $\mathbb{C}$ bildet, welchen wir mit $K(z)$ bezeichnen. Zeige weiterhin, dass $K(z)$ der kleinste (bezüglich Inklusion) Teilkörper von $\mathbb{C}$ ist, welcher die Menge $K \cup \{z\}$ enthält.

Korollar ✪.7. *Eine komplexe Zahl z ist genau dann konstruktibel, wenn es eine Kette (oder einen* Turm*) von Teilkörpern*

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

von $\mathbb{C}$ derart gibt, dass z in K_r liegt und für jedes $i \geq 0$ der Körper K_{i+1} der Form $K_i(z_i)$ für eine komplexe Zahl z_i ist, welche Nullstelle eines nicht-trivialen normierten Polynoms $P(T)$ vom Grad 2 mit Koeffizienten aus dem Teilkörper K_i ist (siehe obige Bemerkung).

Beweis. ($\Rightarrow$) : Diese Richtung folgt sofort aus der Bemerkung ✪.5 induktiv über die Anzahl der Operationen, welche wir durchführen müssen, um die konstruktible Zahl z zu gewinnen.

($\Leftarrow$) : Wir beweisen induktiv über die Länge $r + 1$ des Turms, dass K_r eine Teilmenge von Konst ist (und somit z auch konstruktibel ist). Für $r = 0$ ist $K_0 = \mathbb{Q}$, welche klarerweise in Konst liegt, da Konst ein Teilkörper von $\mathbb{C}$ ist. Wir nehmen nun an, dass K_{r-1} in Konst liegt und dass das Element z aus K_r kommt, wobei $K_r = K_{r-1}(z_r)$ für eine Nullstelle z_r eines nicht-trivialen normierten Polynomes $P(T)$ vom Grad 2 mit Koeffizienten aus dem Teilkörper K_{r-1}. Aus dem Lemma ✪.3 folgt, dass z_r in Konst liegt und somit auch K_r wegen der Bemerkung ✪.6. □

Das obige Korollar liefert ein Kriterium, um zu bestimmen, ob eine komplexe Zahl konstruktibel ist. Um diese Charakterisierung besser untersuchen zu können, benötigen wir ein fundamentales Objekt, die *Galoisgruppe*, welche zu gewissen Körpererweiterungen wie $K \subset K(z)$ assoziiert werden kann und zahlreiche Informationen über die Struktur dieser Körpererweiterung liefert. Hierfür müssen wir mit Konstruktibilität erstmal aufhören und uns mit klassischen algebraischen Objekten wie Gruppen, Ringen und Körpern beschäftigen, bevor wir uns im Abschnitt 3.6 erneut der Konstruktibilität widmen können.

Kapitel 1

Einführung in die Gruppentheorie

1.1 Gruppen, Untergruppen und Gruppenwirkungen

Notation. Eine *Verknüpfung* $*$ auf einer Menge S ist eine binäre Operation $* : S \times S \to S$. Wir schreiben $a * b$ für das Element $*(a, b)$, das heißt, das Bild in S vom Paar (a, b) aus $S \times S$ unter der Verknüpfung $*$.

Definition 1.1. Ein *Monoid* $(S, *)$ ist eine Halbgruppe mit einem neutralen Element e in S, das heißt, die Menge S besitzt eine assoziative Verknüpfung $*$, es gilt also

$$a * (b * c) = (a * b) * c \text{ für alle } a, b \text{ und } c \text{ aus } S,$$

derart, dass für alle a aus S

$$a = e * a = a * e.$$

Das Monoid ist *kommutativ* (oder *abelsch*), falls je zwei Elemente miteinander *kommutieren*, das heißt,

$$a * b = b * a, \text{ für alle } a \text{ und } b \text{ aus } S.$$

In einem Monoid müssen wir wegen der Assoziativität nicht mehr auf die Klammerung langer Produkte achten und schreiben $a * b * c$ anstatt $a * (b * c)$, usw.

Beachte, dass das neutrale Element e eindeutig ist.

Beispiel 1.2. Die Kollektion X^X aller Abbildungen $X \to X$ bildet ein Monoid bezüglich der (umkehrten) Komposition von Abbildungen

$$f * g = f \circ g \text{ für } f \text{ und } g \text{ aus } X^X$$

mit neutralem Element die Identitätsabbildug $\mathbf{Id}_X$. Dieses Monoid ist nicht kommutativ, sobald X mehr als ein Element besitzt.

Gegeben $n \geq 1$, bildet die Menge $\mathcal{M}_{n\times n}(K)$ aller quadratischen $n \times n$-Matrizen über einem Körper K ein Monoid bezüglich der Matrixmultiplikation mit neutralem Element die Identitätsmatrix $\mathbf{E}_n$. Das Monoid ist nicht kommutativ, sobald $n \geq 2$.

Definition 1.3. Sei $(M, *)$ ein Monoid mit neutralem Element e. Wenn

$$a * b = e,$$

dann ist a ein *Linksinverses* von b und b ist ein *Rechtsinverses* von a.

Wenn das Element a des Monoides $(M, *)$ sowohl ein Linksinverses b als auch ein Rechtsinverses c besitzt, dann ist $b = c$, weil

$$b = b * e = b * (a * c) = (b * a) * c = e * c = c.$$

In diesem Fall reden wir über das *Inverse* von a und bezeichnen es mit a^{-1}, weil es eindeutig ist, wenn es existiert. Wenn das Monoid additiv geschrieben wird (nur wenn M abelsch ist!), schreiben wir das Inverse von a als $-a$.

Definition 1.4. Eine *Gruppe* ist ein Monoid $(G, \cdot)$ mit neutralem Element 1_G, in welchem jedes Element ein Inverses hat: für jedes a aus G gibt es ein Element b derart, dass

$$a \cdot b = b \cdot a = 1_G.$$

Insbesondere ist das Element b eindeutig bestimmt und wir bezeichnen es mit a^{-1}.

Bemerkung 1.5. Aus der Eindeutigkeit des Inversen folgt, dass in einer Gruppe G

$$(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$$

gilt. Allgemein definiere für n aus $\mathbb{Z}$

$$a^n = \begin{cases} 1_G, \text{ für } n = 0 \\ \underbrace{a \cdot \dots \cdot a}_{n}, \text{ für } n > 0 \\ (a^{-n})^{-1}, \text{ für } n < 0. \end{cases}$$

Bemerkung 1.6. Ein Monoid $(S, *)$ ist genau dann eine Gruppe, wenn für alle a und b aus S die Gleichungen $a * x = b$ und $y * a = b$ eindeutig lösbar sind.

Beispiel 1.7. In X^X bildet die Teilmenge aller *Permutationen* (das heißt, Bijektionen $X \to X$) eine Gruppe bezüglich Komposition, genannt die *symmetrische Gruppe* von X. Wir bezeichnen es mit $\mathrm{Sym}(X)$. Die Gruppe aller Permutationen der Menge $\{1, \dots, n\}$ wird mit S_n bezeichnet.

Jede endliche Teilmenge $\{x_1, \dots, x_k\}$ paarweise verschiedener Elemente aus $\{1, \dots, n\}$ definiert folgenderweise eine eindeutige Permutation aus S_n:

$$\begin{array}{rcl} \{1, \dots, n\} & \to & \{1, \dots, n\} \\ x & \mapsto & \begin{cases} x, \text{ falls } x \notin \{x_1, \dots, x_k\} \\ x_{i+1}, \text{ falls } x = x_i \text{ mit } 1 \le i \le k-1 \\ x_1, \text{ falls } x = x_k \end{cases} \end{array}$$

Wir bezeichnen die obige zyklische Permutation als den *Zyklus* $(x_1 \dots x_k)$ (beachte, dass wir keine Kommas benutzen). Zum Beispiel: der Zyklus (12) permutiert 1 und 2 und lässt sonst alle anderen Elemente fest. Wenn der *Träger* $\{x_1, \dots, x_k\}$ leer ist, benutzen wir nicht die Notation $()$, sondern schreiben $\mathbf{Id}_{\{1,\dots,n\}}$. Beachte, dass $\mathbf{Id}_{\{1,\dots,n\}}$ gerade das neutrale Element 1_{S_n} ist. Ein Zyklus der Form $(x_i x_j)$ ist eine *Transposition*.

Die Verkettung der Zyklen σ und τ wird mit $\sigma\tau$ (anstatt $\sigma \circ \tau$) bezeichnet. Beachte, dass Zyklen mit disjunkten Trägern miteinander kommutieren.

Es lässt sich leicht induktiv über die Anzahl der nicht-fixierten Elemente zeigen, dass sich jede Permutation als Produkt disjunkter Zyklen schreiben lässt, wobei das leere Produkt das neutrale Element 1_{S_n} ist. Weil der Zyklus $(x_1 \dots x_k)$ sich als

$$(x_1 \dots x_k) = (x_1 x_k)(x_1 x_{k-1}) \cdots (x_1 x_2)$$

schreiben lässt, folgt nun, dass sich jede Permutation als Produkt von Transpositionen schreiben lässt.

Aufgabe. Gegeben einen Zyklus $(x_1 \dots x_k)$ aus S_n, zeige, dass $(x_1 \dots x_k)^{-1} = (x_k x_{k-1} \dots x_1)$.

Gegeben eine beliebige Permutation τ aus S_n, zeige, dass

$$\tau^{-1}(x_1 \dots x_k)\tau = (\tau^{-1}(x_1) \dots \tau^{-1}(x_k)).$$

Schließe daraus eine allgemeine Formel für $\tau^{-1}\sigma\tau$, wobei σ aus S_n beliebig ist.

Definition 1.8. Eine Teilmenge H einer Gruppe G ist eine *Untergruppe*, bezeichnet mit $H \leq G$, falls folgende Bedingungen gelten:

- Das neutrale Element 1_G von G liegt in H.
- Die Menge H ist unter der Verknüpfung $\cdot$ von G sowie der Inversenabbildung $g \mapsto g^{-1}$ abgeschlossen, oder äquivalent dazu, für alle g und h aus H liegt $g^{-1} \cdot h$ in H.

Wenn wir die Verknüpfung $\cdot$ auf H eingeschränkt betrachten, dann ist die Untergruppe H wiederum eine Gruppe mit neutralem Element gegeben durch 1_G.

Bemerkung 1.9. Für eine Teilmenge A der Gruppe G ist

$$\langle A \rangle = \bigcap_{A \subset H \leq G} H$$

die *von A erzeugte Untergruppe*. Beachte, dass $\langle A \rangle$ die kleinste Untergruppe ist, welche A enthält.

Aufgabe. Zeige, dass die Kollektion der Transpositionen $\{(i\ i+1)\}_{1 \leq i \leq n-1}$ die Gruppe S_n erzeugt.

Schließe daraus, dass die 2-elementige Menge $\{(1\ 2), (1\ 2 \cdots\ n)\}$ die Gruppe S_n erzeugt.

Beispiel 1.10. Die Menge $\{1_G\}$ ist eine Untergruppe der Gruppe G, genannt die *triviale* Untergruppe.

Gegeben ein Element a aus der Gruppe G, bildet die Menge $a^{\mathbb{Z}} = \{a^n\}_{n \in \mathbb{Z}}$ (siehe Bemerkung 1.5) eine Untergruppe. Beachte, dass $a^{\mathbb{Z}} = \langle \{a\} \rangle$. Eine Untergruppe H ist *zyklisch*, falls $H = a^{\mathbb{Z}}$ für ein a aus G.

Aufgabe. Sei H eine nicht-leere Teilmenge von G derart, dass $g \cdot h^{-1}$ in H liegt, für alle g und h aus H. Zeige, dass H eine Untergruppe ist.

Definition 1.11. Ein *Homomorphismus* vom Monoid M nach dem Monoid N ist eine Abbildung $F : M \to N$ derart, dass $F(e_M) = e_N$ und für alle a und b aus M

$$F(a * b) = F(a) * F(b),$$

wobei $a * b$ das Produkt in M und $F(a) * F(b)$ das Produkt in N ist.

Wenn M und N beides Gruppen sind, sagen wir dass der Homomorphismus F ein *Gruppenhomomorphismus* ist, wobei wir häufig nur von Homomorphismen reden, falls der Zusammenhang klar ist.

Bemerkung 1.12. Wenn $F : G \to H$ ein Gruppenhomomorphismus ist, so ist $F(g^{-1}) = F(g)^{-1}$ für g aus G, wobei die Inversen in der entsprechenden Gruppe zu verstehen sind.

Insbesondere ist das Bild $F(G)$ eine Untergruppe von H. Des Weiteren ist für jede Untergruppe K von H das Urbild $F^{-1}(K) = \{g \in G \mid F(g) \in K\}$ eine Untergruppe von G. Insbesondere ist $\mathrm{Ker}(F) = \{g \in G \mid F(g) = 1_H\}$ eine Untergruppe von G.

Definition 1.13. Ein Gruppenhomomorphismus $F : G \to H$ heißt

- *trivial*, falls das Bild $f(G)$ nur aus dem neutralen Element von H besteht, oder äquivalent dazu, wenn $\mathrm{Ker}(F) = G$;
- ein *Monomorphismus* (oder eine *Einbettung*), wenn F injektiv ist, oder äquivalent dazu, wenn $\mathrm{Ker}(F) = \{1_G\}$ (schreibe $G \overset{F}{\hookrightarrow} H$);
- ein *Epimorphismus*, wenn F surjektiv ist (schreibe $G \overset{F}{\twoheadrightarrow} H$);
- ein *Isomorphismus*, wenn F bijektiv ist (schreibe $G \overset{F}{\simeq} H$);
- ein *Endomorphismus*, wenn $G = H$ ist;
- ein *Automorphismus*, wenn $G = H$ und F ein Isomorphismus ist.

Beachte, dass F genau dann ein Isomorphismus ist, wenn es einen Gruppenhomomorphismus $F_1 : H \to G$ derart gibt, dass $F_1 \circ F = \mathbf{Id}_G$ und $F \circ F_1 = \mathbf{Id}_H$.

Definition 1.14. Eine (linke) *Gruppenwirkung* von G auf einer nicht-leeren Menge X ist eine binäre Operation $* : G \times X \to X$ mit folgenden Eigenschaften:

- $1_G * x = x$ für alle x aus X.
- $(g \cdot h) * x = g * (h * x)$ für alle g und h aus G sowie x aus X.

Beachte, dass $g^{-1} * y = x$, falls $g * x = y$.

Bemerkung 1.15. Die Existenz einer Gruppenwirkung von G auf X ist also äquivalent dazu, dass wir einen Gruppenhomomorphismus $F : G \to \mathrm{Sym}(X)$ (siehe Beispiel 1.7) haben. In der Tat, wenn F so ein Homomorphismus ist, setze $g * x = F(g)(x)$. Nun ist $F(1_g) = \mathbf{Id}_X$ also $1_G * x = x$. Ferner ist

$$(g \cdot h) * x = F(g \cdot h)(x) = \big(F(g) \circ F(h)\big)(x) = F(g)\big(F(h)(x)\big) = F(g)(h * x) = g * (h * x).$$

Gegeben nun eine Gruppenwirkung $* : G \times X \to X$, betrachte für g aus G die Abbildung

$$\begin{array}{rccc} F(g): & X & \to & X \\ & x & \mapsto & g * x \end{array}$$

Beachte zuerst, dass $F(g)$ eine Bijektion ist: die Abbildung $F(g)$ ist klarerweise injektiv, denn $g \star x = F(g)(x) = F(g)(x') = g \star x'$ impliziert, dass

$$x = 1_G \star x = (g^{-1} \cdot g) \star x = g^{-1} \star (g \star x) = g^{-1} \star (g \star x') = (g^{-1} \cdot g) \star x' = 1_G \star x' = x'.$$

Des Weiteren ist ein Urbild des Elementen y aus X durch $F(g)$ gleich $g^{-1} \star y$, so $F(g)$ ist surjektiv und somit eine Bijektion. Es folgt direkt aus der Definition 1.14, dass $F(g \cdot h) = F(g) \circ F(h)$. Somit ist F ein Gruppenhomomorphismus von G nach $\mathrm{Sym}(X)$.

Wir können auch *rechte Gruppenwirkungen* definieren als binäre Operationen $* : X \times G \to X$ mit den Eigenschaften:

- $x * 1_G = x$ für alle x aus X.
- $x * (g \cdot h) = (x * g) * h$ für alle g und h aus G sowie x aus X.

Dies ist äquivalent dazu, dass wir Homomorphismen von der Gruppe G nach der Gruppe $\mathrm{Sym}(X)^{\mathrm{op}}$ betrachten, deren Grundmenge die Kollektion aller Permutationen auf X ist mit Gruppengesetz $f * g = g \circ f$. Alle Begriffe und Aussagen in diesem Abschnitt lassen sich auf rechte Gruppenwirkungen verallgemeinern.

Definition 1.16. Die *Bahn* (auf Englisch *orbit*) des Elementes x aus X ist die Menge

$$\mathrm{orb}(x) = \{g * x\}_{g \in G}.$$

Eine Wirkung ist *transitiv*, wenn $X = \mathrm{orb}(x)$ für jedes x aus X.

Bemerkung 1.17. Gegeben ein y aus X, beachte, dass y genau dann in $\mathrm{orb}(x)$ liegt, wenn $\mathrm{orb}(y) = \mathrm{orb}(x)$. Insbesondere zerlegen die Bahnen die Menge X und bestimmen somit eine Äquivalenzrelation auf X.

Beachte, dass eine Wirkung G auf X genau dann transitiv ist, wenn $S = \mathrm{orb}(x)$ für ein Element x aus X.

Definition 1.18. Der *Stabilisator* des Elementes x aus X ist die Untergruppe

$$\mathrm{Stab}(x) = \{g \in G \mid g * x = x\}.$$

Die Wirkung ist

- *trivial*, wenn $\mathrm{Stab}(x) = G$ für jedes x aus X;
- *treu*, wenn 1_G das einzige Element in $\bigcap_{x \in S} \mathrm{Stab}(x)$ ist;
- *frei*, wenn $\mathrm{Stab}(x) = 1_G$ für jedes x aus X.

Klarerweise ist jede freie Wirkung treu. Die Rückwirkung gilt offensichtlich nicht: betrachte die Wirkung der invertierbaren Matrizen auf den n-dimensionalen K-Vektorraum K.

Beispiel 1.19. Für jede Gruppe und jede nicht-leere Menge kann man die triviale Gruppenwirkung definieren.

Jede Untergruppe H einer Gruppe G definiert zwei freie Wirkungen auf G: Für h aus H betrachte die Abbildungen

$$\lambda_h : \begin{array}{ccc} G & \to & G \\ g & \mapsto & h \cdot g \end{array} \quad \text{und} \quad \mu_h : \begin{array}{ccc} G & \to & G \\ g & \mapsto & g \cdot h. \end{array}$$

Die Abbildung λ_h entspricht also der Translation um h von links, während μ_h die rechte Translation ist. Die Abbildung $(h, g) \mapsto \lambda_h(g)$ definiert eine linke Gruppenwirkung von H auf G. Die Bahn des Elementes g aus G unter dieser Wirkung ist die *rechte Nebenklasse* $H \cdot g = \{h \cdot g\}_{h \in H}$ von H. Beachte, dass $H \cdot g = H \cdot g_1$ genau dann, wenn $g \cdot g_1^{-1}$ (oder äquivalent dazu $g_1 \cdot g^{-1}$) in H liegt.

Die Abbildung $(h, g) \mapsto \mu_h(g)$ ist eine rechte Gruppenwirkung von H auf G. Die Bahn eines Elementes g unter dieser Wirkung ist die *linke Nebenklasse* $g \cdot H = \{g \cdot h\}_{h \in H}$ von H. Nun sind $g \cdot H$ und $g_1 \cdot H$ genau dann gleich, wenn $g^{-1} \cdot g_1$ in H liegt.

Weil die Bahnen der Wirkung durch Translation mit Elementen aus der Untergruppe H eine Zerlegung der Gruppe G definieren, folgern wir sofort folgende Bemerkung.

Korollar 1.20. *Zwei linke (bzw. rechte) Nebenklassen einer Untergruppe H sind entweder disjunkt oder gleich.*

Korollar 1.21. (*Der Satz von Cayley*) *Jede treue Wirkung von G auf X induziert einen Gruppenmonomorphismus $G \hookrightarrow \mathrm{Sym}(X)$.*

Insbesondere ist jede Gruppe ist isomorph zu einer Untergruppe einer Permutationsgruppe.

Beweis. Aus der Bemerkung 1.15 folgt, dass eine Wirkung von G auf X einen Gruppenhomomorphismus

$$\begin{array}{rccc} F: & G & \to & \mathrm{Sym}(X) \\ & g & \mapsto & F(g) \end{array} \quad \text{mit} \quad \begin{array}{rccc} F(g): & X & \to & X \\ & x & \mapsto & g * x \end{array}$$

induziert. Wir müssen also nur noch zeigen, dass die Abbildung F injektiv ist, oder äquivalent dazu, dass $\mathrm{Ker}(F) = \{1_G\}$. Wenn g aus G im Kern von F liegt, so ist $F(g)$ die Identitätsabbildung auf X, so $g \star x = F(g)(x) = x$ für jedes x aus X. Das bedeutet, dass g in $\mathrm{Stab}(x)$ für jedes x aus X liegt, so $g = 1_G$, weil die Wirkung treu ist.

Nun ist die Wirkung von G auf G durch Translation von links eine freie transitive Wirkung. Sei also für g aus G die Abbildung

$$\begin{array}{rccc} \lambda_g: & G & \to & \mathrm{Sym}(G) \\ & h & \mapsto & g \cdot h \end{array}$$

aus dem Beispiel 1.19. Klarerweise ist die Bahn des Elementen 1_G gleich G, so die Wirkung ist transitiv. Des Weiteren, falls das Element g in $\mathrm{Stab}(h)$ liegt, bedeutet es, dass $g \cdot h = h$, so g muss 1_G sein aus der Bemerkung 1.6. Es folgt somit, dass die Wirkung frei, und insbesondere treu, ist. Wir schließen, dass $G \hookrightarrow \mathrm{Sym}(G)$, wie gewünscht. □

Beispiel 1.22. Ein weiteres klassisches Beispiel einer rechten Gruppenwirkung von G auf sich selbst wird durch *Konjugation* gegeben:

$$\begin{array}{rcl} G \times G & \to & G \\ (g, h) & \mapsto & h^g = g^{-1} \cdot h \cdot g \end{array}.$$

Beachte, dass in der Literatur häufig die Notation h^g für das Produkt $g \cdot h \cdot g^{-1}$ verwendet wird (in diesem Fall definiert die obige Abbildung eine linke Gruppenwirkung).
Die Konjugationswirkung ist genau dann trivial, wenn G abelsch ist. Allgemein ist der *Zentralisator* des Elementes h der Stabilisator von h bezüglich der Konjugationswirkung, also

$$C_G(h) = \{g \in G \mid h^g = h\} = \{g \in G \mid h \cdot g = g \cdot h\}.$$

Das *Zentrum* von G ist der Durchschnitt aller Zentralisatoren

$$Z(G) = \bigcap_{h \in G} C_G(h) = \{g \in G \mid h \cdot g = g \cdot h \text{ für alle } h \text{ aus } G\}.$$

Eine Gruppe G ist also genau dann abelsch, wenn $G = Z(G)$. Wir bezeichnen die Bahn eines Elementes g aus G unter der Konjugationswirkung mit $h^G = \{h^g\}_{g \in G}$. Beachte, dass die Bahn h^G eines Elementes h aus genau dann G *trivial* ist (das heißt, sie besteht nur aus h, also $h^G = \{h\}$), wenn das Element h zentral ist.

Bemerkung 1.23. Gegeben eine Untergruppe H von der Gruppe G und ein Element g aus G, so ist

$$H^g = \{h^g\}_{h\in H} = \{g^{-1} \cdot h \cdot g\}_{h\in H}$$

wiederum eine Gruppe, welche *durch g zu H konjugiert* ist.

Definition 1.24. Ein *Normalteiler* der Gruppe G ist eine Untergruppe N, welche unter der Konjugationswirkung von Elementen aus G abgeschlossen ist, das heißt, für g aus G ist $N^g = N$ oder äquivalent dazu, für h aus N ist h^g in N. Wenn N ein Normalteiler von G ist, schreiben wir $N \trianglelefteq G$.

Bemerkung 1.25. Sei H die von der Teilmenge A von G erzeugte Untergruppe. Falls die Menge A *unter Konjugation invariant* ist, das heißt

$$a^g \text{ liegt in } A \text{ für alle } a \text{ aus } A \text{ und } g \text{ aus } G,$$

so ist H ein Normalteiler von G.

Aufgabe. Zeige, dass jede Untergruppe des Zentrums $Z(G)$ einer Gruppe G sowie die trivialen Untergruppen $\{1_G\}$ und G immer Normalteiler sind.

Wenn $F : G \to H$ ein Gruppenhomomorphismus ist, so ist $F^{-1}(K) \trianglelefteq G$ falls $K \trianglelefteq H$. Insbesondere ist $\mathrm{Ker}(F)$ ein Normalteiler von G.

Bemerkung 1.26. Beachte, dass eine Untergruppe H genau dann ein Normalteiler ist, wenn für jedes g aus G die linken und rechten Nebenklassen (als Mengen) übereinstimmen, also $H \cdot g = g \cdot H$.

Bemerkung 1.27. Sei $\mathrm{Links}(H)$, bzw. $\mathrm{Rechts}(H)$, die Kollektion aller linken (bzw. rechten) Nebenklassen der Untergruppe H von G. Die Abbildung

$$\begin{array}{rccc} \varphi: & \mathrm{Links}(H) & \to & \mathrm{Rechts}(H) \\ & g \cdot H & \mapsto & H \cdot g^{-1} \end{array}$$

ist wohldefiniert und eine Bijektion. Insbesondere definieren wir den *Index* $(G : H)$ von H in G als die Anzahl der Nebenklassen (links oder rechts) von H in G.

Beweis. Angenommen, dass $g \cdot H = g_1 \cdot H$, so ist $g_1 = g \cdot h$ für ein h aus H. Somit liegt $g_1^{-1} = h^{-1} \cdot g^{-1}$ in $H \cdot g^{-1}$. Insbesondere ist $H \cdot g^{-1} = H \cdot g_1^{-1}$ wegen des Korollars 1.20, was zeigt, dass φ wohldefiniert ist. Die Abbildung φ ist klarerweise surjektiv, also müssen wir nur zeigen, dass φ injektiv ist. Falls $H \cdot g^{-1} = H \cdot g_1^{-1}$, schreibe $g_1^{-1} = h \cdot g^{-1}$ für ein h aus H. Nun liegt $g_1 = g \cdot h^{-1}$ in $g \cdot H$, also $g \cdot H = g_1 \cdot H$, wie gewünscht. □

Bemerkung 1.28. Jede Untergruppe von G mit Index 2 ist ein Normalteiler, das folgt aus der Bemerkung 1.26.

Falls die Gruppe G endlich ist, so ist

$$|G| = |H|(G : H)$$

für jede Untergruppe H von G, weil je zwei Nebenklassen dieselbe Anzahl von Elementen haben. Insbesondere teilt $|H|$ immer die Mächtigkeit der Gruppe G.

Korollar 1.29. *Gegeben Untergruppen $H \leq K$ der endlichen Gruppe G, so ist der Index* multiplikativ*:*

$$(G : H) = (G : K)(K : H)$$

Bemerkung 1.30. Die Untergruppen von $(\mathbb{Z}, +)$ sind zyklisch und genau der Form

$$m\mathbb{Z} = \{n \in \mathbb{Z} |\ n = km \text{ für ein } k \text{ aus } \mathbb{Z}\}$$

mit m aus $\mathbb{N}$. Der Index von $m\mathbb{Z}$ in $\mathbb{Z}$ ist m.

Beweis. Klarerweise ist $m\mathbb{Z}$ eine Untergruppe von $(\mathbb{Z}, +)$ mit Index m, weil jedes Element genau zu einer der Zahlen $0, 1, \ldots, m-1$ modulo m kongruent ist (und diese Elemente sind alle in verschiedenen Nebenklassen).

Sei nun H eine Untergruppe von $\mathbb{Z}$. Wenn H trivial ist, dann ist $H = 0\mathbb{Z}$. Sonst gibt es eine kleinste positive natürliche Zahl m in H (weil H unter Inversen abgeschlossen ist). Da H eine Gruppe ist, ist $m\mathbb{Z}$ eine Teilmenge von H, denn

$$km = \underbrace{m + \cdots + m}_{k}.$$

Sei nun h aus H beliebig. Mit Hilfe von Division mit Rest (in $\mathbb{Z}$), schreibe $h = km + r$ mit $0 \leq r \leq m-1$. Da H eine Untergruppe ist und m kleinstmöglich gewählt wurde, folgt, dass $r = 0$ sein muss, was die Inklusion $H \subset m\mathbb{Z}$ liefert. □

Bemerkung 1.31. Gegeben ein Element a aus einer Gruppe G sei H die von a erzeugte Untergruppe. Die Abbildung

$$\begin{array}{rccc} \varphi: & (\mathbb{Z}, +) & \to & H \\ & n & \mapsto & a^n \end{array}$$

ist klarerweise ein Gruppenhomomorphismus, siehe Bemerkung 1.5. Wegen der Bemerkung 1.12 ist $\mathrm{Ker}(\varphi)$ eine Untergruppe von $(\mathbb{Z}, +)$ und lässt sich somit als $m\mathbb{Z}$ für eine natürliche Zahl m schreiben. Wenn $m = 0$ sagen wir, dass a *unendliche Ordnung hat*. Ansonsten ist die *Ordnung* von a gleich m. Beachte, dass $m = |H|$: Klarerweise ist $m \neq 0$ minimal mit $a^m = 1_G$, also sind die Elemente $\{1_G, \ldots, a^{m-1}\}$ paarweise verschieden. Jede weitere Potenz a^n von a aus H lässt sich somit schreiben als

$$a^n = a^{km+r} = (a^m)^k \cdot a^r = 1_G^k \cdot a^r = a^r$$

für $0 \leq r \leq m-1$. Insbesondere ist $|H|$ gleich der Ordnung des erzeugenden Elements a.

Aufgabe. Sei G eine Gruppe derart, dass jedes Element Ordnung höchstens 2 hat, das heißt, dass $a^2 = 1_G$ für alle a aus G. Zeige, dass G abelsch ist.

Mit Hilfe der Bemerkung 1.27 folgt, dass die Ordnung von a immer die Mächtigkeit $|G|$ von G teilt, falls G endlich ist.

Korollar 1.32. *Falls die Gruppe G endlich ist, so gilt $a^{|G|} = 1_G$ für jedes a aus G.*

Wir zeigen als letztes die Konjugationsklassengleichung als Korollar einer allgemeineren Beobachtung über die Größe einer Bahn in einer Gruppenwirkung.

Satz 1.33. (*Konjugationsklassengleichung*) *Sei G eine Gruppe, welche auf der Menge X links wirkt. Gegeben ein Element x aus X ist die Mächtigkeit seiner Bahn* $\mathrm{orb}(x)$ *gleich dem Index von* $\mathrm{Stab}(x)$ *in G (wenn einer dieser Zahlen unendlich ist, dann ist es auch die andere Zahl).*

Insbesondere, wenn die Gruppe G endlich und $(a_i)_{1\leq i\leq m}$ ein Repräsentantensystem der nicht-trivialen Konjugationsklassen (siehe Beispiel 1.22) ist, das heißt, jedes Element aus G liegt entweder in $Z(G)$ oder in der Konjugationsklasse a_i^G für ein einziges $1 \leq i \leq m$, dann ist

$$|G| = |Z(G)| + \sum_{i=1}^{m} (G : C_G(a_i)).$$

Beweis. Sei $\mathrm{Links}(\mathrm{Stab}(x))$ die Kollektion aller linken Nebenklassen von $\mathrm{Stab}(x)$. Wegen der Bemerkung 1.27 müssen wir für die erste Behauptung nur zeigen, dass die Abbildung

$$\begin{array}{rccc} \varphi: & \mathrm{Links}(\mathrm{Stab}(x)) & \to & \mathrm{orb}(x) \\ & g \cdot \mathrm{Stab}(x) & \mapsto & g * x \end{array}$$

eine Bijektion ist. Beachte, dass diese Abbildung wohldefiniert ist, denn $(g \cdot h) * x = g * (h * x) = g * x$, falls h aus $\mathrm{Stab}(x)$ kommt. Die Abbildung φ ist klarerweise surjektiv, also müssen wir nur die Injektivität überprüfen. Falls

$$\varphi(g \cdot \mathrm{Stab}(x)) = g * x = g_1 * x = \varphi(g_1 \cdot \mathrm{Stab}(x)),$$

folgt, dass $g^{-1} \cdot g_1$ in $\mathrm{Stab}(x)$ liegt, wie gewünscht.

Wir nehmen nun an, dass die Gruppe G endlich ist und wählen ein Repräsentantensystem $(a_i)_{1\leq i\leq m}$ der nicht-trivialen Konjugationsklassen. Weil die Bahnen durch Konjugation eine Zerlegung der Menge G bilden, ist G die disjunkte Vereinigung

$$G = Z(G) \cup \bigcupdot_{i=1}^{n} a_i^G.$$

Aus der vorigen Diskussion folgt $|a_i^G| = [G : C_G(a_i)]$, was die gewünschte Identität liefert. □

1.2 Isomorphiesätze

Analog zu der Definition des Quotientenraumes in der Linearen Algebra bilden die Nebenklassen eines Normalteilers wiederum eine Gruppe.

Proposition 1.34. *Sei N ein Normalteiler der Gruppe G. Die Menge G/N aller linken Nebenklassen von N in G ist wiederum eine Gruppe bezüglich der Verknüpfung*

$$\begin{array}{rcc} G/N \times G/N & \to & G/N \\ (g \cdot N, h \cdot N) & \mapsto & (g \cdot h) \cdot N \end{array}$$

mit neutralem Element die Nebenklasse $1_G \cdot N$ und Inversen $(g \cdot N)^{-1} = g^{-1} \cdot N$.

Des Weiteren ist die Projektion

$$\begin{array}{rccc} \pi_N: & G & \to & G/N \\ & g & \mapsto & g \cdot N \end{array}$$

ein Gruppenepimorphismus mit $\mathrm{Ker}(\pi_N) = N$.

Beweis. Wir zeigen zuerst, dass die obige Verknüpfung wohldefiniert ist: Angenommen $g \cdot N = g_1 \cdot N$ und $h \cdot N = h_1 \cdot N$, so liegen $a = g^{-1} \cdot g_1$ und $b = h^{-1} \cdot h_1$ in N. Nun liegt

$$(g \cdot h)^{-1} \cdot (g_1 \cdot h_1) = h^{-1} \cdot (g^{-1} \cdot g_1) \cdot h_1 = h^{-1} \cdot a \cdot h_1 = h^{-1} \cdot a \cdot h \cdot b = a^h \cdot b$$

wiederum in N, weil a^h und b beide in N liegen, da $N \trianglelefteq G$.

Die Verknüpfung ist klarerweise assoziativ, weil das Gruppengesetz von G assoziativ ist. Des Weiteren ist die Nebenklasse $1_G \cdot N$ das neutrale Element (links und rechts) dieser Verknüpfung, direkt aus der Definition. Dementsprechend ist

$$g \cdot N \cdot g^{-1} \cdot N = (g \cdot g^{-1}) \cdot N = 1_G \cdot N = 1_{G/N} = g^{-1} \cdot N \cdot g \cdot N,$$

also ist $g^{-1} \cdot N$ das Inverse der Nebenklasse $g \cdot N$, wie gewünscht.

Aus der Definition des Gruppengesetzes folgt, dass

$$\pi_N(g \cdot h) = (g \cdot h) \cdot N = (g \cdot N) \cdot (h \cdot N) = \pi_N(g) \cdot \pi_N(h),$$

also ist π_N ein Gruppenhomomorphismus, welcher klarerweise surjektiv ist. Schließlich liegt ein Element g aus G genau dann in $\mathrm{Ker}(\pi_N)$, wenn $g \cdot N = 1_G \cdot N$, das heißt, wenn g aus N kommt. □

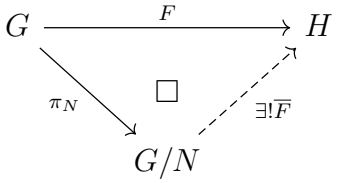
Notation. Um die Notation zu vereinfachen, werden wir ab jetzt die Nebenklasse vom Element g bezüglich der Gruppe N mit gN anstatt mit $g \cdot N$ bezeichnen.

Beispiel 1.35. Weil die Gruppe $\mathbb{Z}$ abelsch ist, ist jede Untergruppe ein Normalteiler. Der Quotientenraum $\mathbb{Z}/n\mathbb{Z}$ der Kongruenzklassen modulo $n \geq 1$ (siehe Proposition 1.34) ist eine abelsche Gruppe bezüglich der Operation

$$\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \ , \\ (\overline{x}, \overline{y}) & \mapsto & \overline{x+y} \end{array}$$

wobei $\overline{x}$ die Nebenklasse $x + n\mathbb{Z}$ bezeichnet. Ein mögliches Repräsentantensystem der Mengen der Nebenklassen von $n\mathbb{Z}$ wird durch die Menge $\{0, \ldots, n-1\}$ gegeben, wobei das neutrale Element von $\mathbb{Z}/n\mathbb{Z}$ genau die Klasse $\bar{0}$ ist. Beachte, dass das additive Inverse von $\bar{k}$, für $0 \leq k \leq n-1$, gleich $\overline{n-k}$ ist.

Satz 1.36. *Für jeden Homomorphismus $F : G \to H$ und jeden Normalteiler N von G mit $N \subset \mathrm{Ker}(F)$, gibt es einen eindeutigen* von F induzierten *Homomorphismus $\overline{F} : G/N \to H$ derart, dass $\overline{F} \circ \pi_N = F$, das heißt, das Diagramm*



kommutiert (wir kennzeichnen dies mit dem Zeichen □). Ferner gilt $\mathrm{Im}(F) = \mathrm{Im}(\overline{F})$ *und somit ist F genau dann surjektiv, wenn $\overline{F}$ es ist.*

Des Weiteren ist $\mathrm{Ker}(\overline{F}) = \{gN \in G/N \mid g \in \mathrm{Ker}(F)\}$*, also ist $\overline{F}$ genau dann injektiv, wenn $N = \mathrm{Ker}(F)$.*

Beweis. Wenn eine Abbildung $\overline{F} : G/N \to H$ derart existiert, dass das obige Diagramm kommutiert, muss sie erfüllen, dass $\overline{F}(gN) = \overline{F} \circ \pi_N(g) = F(g)$. Daher setzen wir

$$\begin{array}{rccc} \overline{F}: & G/N & \to & H \\ & gN & \mapsto & F(g) \end{array}$$

und überprüfen, dass $\overline{F}$ wohldefiniert ist und die gewünschten Eigenschaften besitzt. Wenn $gN = g_1N$, so ist $a = g^{-1} \cdot g_1$ in N und somit ist $F(a) = 1_H$. Nun ist

$$\overline{F}(g_1N) = F(g_1) = F(g \cdot a) = F(g) \cdot F(a) = F(g) = \overline{F}(gN),$$

also ist $\overline{F}$ wohldefiniert. Des Weiteren ist $\overline{F}$ ein Gruppenhomomorphismus, weil

$$\overline{F}(gN \cdot g_1N) = \overline{F}((g \cdot g_1)N) = F(g \cdot g_1) = F(g) \cdot F(g_1) = \overline{F}(gN) \cdot \overline{F}(g_1N).$$

Die Eindeutigkeit des Homomorphismus $\overline{F}$ ist offensichtlich. Klarerweise ist $\mathrm{Im}(F) = \mathrm{Im}(\overline{F})$ und $\overline{F} \circ \pi_N = F$. Nun ist die Nebenklase gN genau dann in $\mathrm{Ker}(\overline{F})$, wenn $F(g) = \overline{F}(gN) = 1_H$. Dies bedeutet, dass g in $\mathrm{Ker}(F)$ liegt, wie gewünscht. Somit folgern wir, dass $\overline{F}$ genau dann injektiv ist, wenn $N = \mathrm{Ker}(F)$. □

Da jeder Homomorphismus eine Surjektion auf seinem Bildbereich induziert, folgt folgender Satz:

Korollar 1.37. (*Noetherscher Isomorphiesatz*) *Jeder Homomorphimus $F : G \to H$ induziert einen Isomorphimus $\overline{F} : G/\mathrm{Ker}(F) \to \mathrm{Im}(F)$.*

Mit Hilfe des Korollars 1.32 und des Noetherschen Isomorphiesatzes gewinnen wir folgendes Korollar.

Korollar 1.38. *Wenn die endliche Gruppe G Mächtigkeit p hat, wobei p eine Primzahl ist, so ist $G \simeq \mathbb{Z}/p\mathbb{Z}$.*

Satz 1.39. (*Diamantsatz*) *Sei G eine Gruppe mit Untergruppen H und N, wobei N Normalteiler von G ist.*

- *Die Abbildung π_N induziert eine Korrespondenz zwischen den Untergruppen von G/N und den Untergruppen von G, welche N enthalten.*
- *Die Normalteiler von G/N sind genau in Korrespondenz mit den Normalteilern von G, welche N enthalten.*
- *Die kleinste Untergruppe von G, welche N und H enthält, ist gerade $H \cdot N = \{h \cdot n \mid n \in N, h \in H\}$.*
- *Die Untergruppe $H \cap N$ ist ein Normalteiler von H und es gibt einen natürlichen Isomorphismus $H/(H \cap N) \simeq (H \cdot N)/N$.*

Insbesondere, wenn N in einem Normalteiler N_1 von G enthalten ist, so haben wir die Isomorphie $G/N_1 \simeq (G/N)/(N_1/N)$.

Beweis. Klarerweise folgt die letzte Behauptung aus den vorigen mit dem noetherschen Isomorphiesatz, denn N_1/N ist ein Normalteiler von G/N: Wegen des Satzes 1.36 induziert der Homomorphismus $\pi_{N_1} : G \to G/N_1$ mit $\mathrm{Ker}(p_{N_1}) = N_1$ einen Epimorphismus $\overline{\pi_{N_1}} : G/N \to G/N_1$ mit Kern N_1/N, also folgt

$$(G/N)/(N_1/N) \simeq G/N_1$$

aus dem Korollar 1.37.

Die Korrespondenz zwischen den Untergruppen von G/N und den Untergruppen von G, welche N enthalten, wird definiert durch $V \mapsto \pi_N^{-1}(V)$. Wenn K eine Untergruppe von G ist, welche N enthält ist, so ist $K/N = \{kN\}_{k\in K}$ eine Untergruppe von G/N, aus der Definition des Gruppengesetzes in G/N. Ferner liegt g in $\pi_N^{-1}(K/N)$ genau dann, wenn $gN = kN$ für ein k aus K, oder äquivalent dazu, wenn g in K liegt, da $N \subset K$.

Klarerweise ist das Urbild eines Normalteilers wiederum normal in G. Da π_N surjektiv ist, folgt, dass für jeden Normalteiler K von G, welcher N enthält, K/N ein Normalteiler von G/N ist.

Wenn wir zeigen, dass die Menge $H \cdot N$ eine Untergruppe von G ist, dann ist sie klarerweise die kleinste Untergruppe von G, welche H und N enthält. Da $1_G = 1_G \cdot 1_G$, müssen wir also nur zeigen, dass $x^{-1} \cdot y$ in $H \cdot N$ liegt für $x = h \cdot n$ und $y = h_1 \cdot n_1$ aus $H \cdot N$. Nun ist

$$x^{-1} \cdot y = (h \cdot n)^{-1} \cdot h_1 \cdot n_1 = n^{-1} \cdot h^{-1} \cdot h_1 \cdot n_1 = h^{-1} \cdot h_1 \cdot \tilde{n} \cdot n_1,$$

für ein $\tilde{n}$ aus N, weil $N(h^{-1} \cdot h_1) = (h^{-1} \cdot h_1)N$ wegen der Bemerkung 1.26.

Die Untergruppe $H \cap N$ von H ist ein Normalteiler von H, weil ein Konjugiertes x^h von x aus $H \cap N$ mit h aus H offensichtlich sowohl in H als auch in N liegt.

Wir zeigen als Letztes, dass $H/(H \cap N)$ und $H \cdot N/N$ isomorph sind. Betrachte hierfür die Inklusionsabbildung $i_H : H \to G$ als Gruppenhomomorphismus. Insbesondere ist die Abbildung $F = \pi_N \circ i_H : H \to G/N$ ein Gruppenhomomorphismus mit Bild

$$\{hN \mid h \in H\} = (H \cdot N)/N = \pi_N(H \cdot N).$$

Ein Element h liegt genau dann in $\mathrm{Ker}(F)$, wenn $hN = N$, oder äquivalent dazu, wenn h in N liegt. Insbesondere ist $\mathrm{Ker}(F) = H \cap N$ und das Korollar 1.37 liefert den gewünschten Isomorphismus zwischen $H/(H \cap N)$ und $(H \cdot N)/N$. □

Definition 1.40. Der *Normalisator* einer Untergruppe H von G ist

$$N_G(H) = \{g \in G \mid gH = Hg\}.$$

Bemerkung 1.41. Der Normalisator $N_G(H)$ ist eine Untergruppe von G, welche H entält. Es ist nämlich die größte Untergruppe von G, welche H enthält und derart ist, dass H ein Normalteiler davon ist.

Falls $K \leq N_G(H)$, dann ist die kleinste Untergruppe von G, welche H und K enthält, gleich der Menge $K \cdot H = \{k \cdot h \mid h \in H, k \in K\}$.

Definition 1.42. Eine Gruppe G heißt *einfach*, falls die trivialen Untergruppen $\{1_G\}$ und G die einzigen Normalteiler von G sind.

Gewisse Kongruenzgruppen sind einfach. Dafür müssen wir die Identität von Bézout benutzen.

Proposition 1.43. *Sei d der größte gemeinsame Teiler der ganzen Zahlen a und b, die beide ungleich Null sein sollen. Dann lässt sich die Zahl d als Linearkombination*

$$d = ax + by$$

mit x und y aus $\mathbb{Z}$ schreiben.

Beweis. Betrachte die Menge $S(a, b)$ aller echt positiven natürlichen Zahlen n, welche sich als $\mathbb{Z}$-Linearkombination von a und b schreiben lassen. Klarerweise ist $S(a, b)$ nicht leer, weil sie $|a|$ und $|b|$ enthält.

Wähle n in $S(a, b)$ minimal (weil $S(a, b) \subset \mathbb{N}$), also $n = ax + by$. Insbesondere ist n ein Vielfaches von d. Wir müssen also nur noch zeigen, dass n die Zahl d teilt, oder äquivalent dazu, dass n sowohl a als auch b teilt. Da beide Beweise analog laufen, genügt es, wenn wir zeigen, dass n die Zahl a teilt. Da $n > 0$ schreibe $a = n \cdot m + r$ mit $0 \leq r < n$. Nun ist

$$r = a - nm = a - m(ax + by) = a(1 - mx) + b(-y),$$

also ist r eine $\mathbb{Z}$-Linearkombination von a und b. Weil n minimal in $S(a, b)$ gewählt wurde, folgt $r = 0$, was den gewünschten Beweis liefert. □

Korollar 1.44. *Die Kongruenzgruppe $\mathbb{Z}/n\mathbb{Z}$ ist genau dann einfach, wenn $n = 1$ oder n eine Primzahl ist.*

Beweis. Aus dem Satz 1.39 folgt, dass die Untergruppen von $\mathbb{Z}/n\mathbb{Z}$ in Korrespondenz sind mit den Untergruppen von $\mathbb{Z}$, welche $n\mathbb{Z}$ enthalten. Weil $\mathbb{Z}$ und $\mathbb{Z}/n\mathbb{Z}$ abelsch sind, ist jede Untergruppe sofort ein Normalteiler. Wenn n weder 1 noch eine Primzahl ist, gibt es klarerweise echte Untergruppen H mit $n\mathbb{Z} \subsetneq H \subsetneq \mathbb{Z}$.

Wir nehmen also nun an, dass $n = 1$ oder eine Primzahl ist. Falls $n = 1$, müssen wir nichts zeigen, denn die Gruppe $\mathbb{Z}/n\mathbb{Z}$ ist trivial. Sei also $n = p$ eine Primzahl. Angenommen es gäbe eine Obergruppe $H \supsetneq p\mathbb{Z}$, dann wähle a aus $H \setminus p\mathbb{Z}$. Nun ist 1 der größte gemeinsame Teiler von a und p (weil p prim ist!), also schreibe $1 = ax + py$ für x und y aus $\mathbb{Z}$ mit Hilfe der Proposition 1.43. Weil H eine Obergruppe von $p\mathbb{Z}$ ist, folgt, dass 1 in H liegt, also $H = \mathbb{Z}$, wie gewünscht. □

Proposition 1.45. *Die Gruppe S_n aller Permutationen der Menge $\{1, \ldots, n\}$ (siehe Beispiel 1.7) ist nicht einfach, falls $n \geq 3$. Die Menge A_n aller Permutationen, welche sich als Produkt einer geraden Anzahl von Transpositionen schreiben lassen, bildet einen echten Normalteiler von S_n vom Index 2.*

Beweis. Wir müssen also zeigen, dass A_n ein nicht-trivialer Normalteiler ist. Hierfür sagen wir, dass die 2-elementige Menge $\{i, j\}$ ein *Fehlstand* der Permutation σ aus S_n ist, falls σ die Ordnung invertiert, d. h. $i < j$ aber $\sigma(i) > \sigma(j)$ (oder andersherum). Definiere nun das *Vorzeichen* als

$$\begin{array}{rccl} \text{sign}: & S_n & \to & H \\ & \sigma & \mapsto & (-1_{\mathbb{Z}})^{\text{Anzahl der Fehlstände von } \sigma} \end{array}$$

wobei H die Untergruppe $\{-1, 1\}$ von $(\mathbb{Q} \setminus \{0\}, \cdot)$ ist. Beachte, dass H isomorph zu $\mathbb{Z}/2\mathbb{Z}$ ist.

Wenn wir zeigen, dass sign ein Homomorphismus ist, folgt sofort, dass $A_n = \text{Ker}(\text{sign})$, weil das Vorzeichen der Transposition (ij) gerade -1 ist. Aus der Bemerkung 1.28 schließen wir

dann, dass A_n ein Normalteiler ist. Des Weiteren ist der Index $(S_n : A_n)$ genau 2 ist, aus dem Korollar 1.37.

Wir zeigen also nun, dass sign ein Homomorphismus ist: für festes $i < j$ sowie Permutationen σ und τ sei $(i_1, j_1) = (\tau(i), \tau(j))$ sowie $(i_2, j_2) = (\sigma(i_1), \sigma(j_1))$. Bezeichne mit x die Anzahl von Paaren $i < j$ derart, dass $i_1 > j_1$ aber $i_2 < j_2$. Analog ist y die Anzahl von Paaren $i < j$ mit $i_1 > j_1$ und $i_2 > j_2$, sowie z die Anzahl von Paaren $i < j$ mit $i_1 < j_1$, aber $i_2 > j_2$. Es folgt, dass $x + y$ die Anzahl der Fehlstände von τ ist. Die Anzahl der Fehlstände von σ ist $x + z$ und die Anzahl der Fehlstände von $\sigma \circ \tau$ ist $y + z$. Also,

$$\operatorname{sign}(\sigma \circ \tau) = (-1)^{y+z} = (-1)^{2x} \cdot (-1)^{y+z} = (-1)^{x+z} \cdot (-1)^{x+y} = \operatorname{sign}(\sigma) \cdot \operatorname{sign}(\tau),$$

wie gewünscht. □

1.3 Direkte Produkte

Definition 1.46. Das *direkte Produkt* $G \times H$ zweier Gruppen G und H ist das kartesische Produkt $G \times H$ mit koordinatenweiser Multiplikation

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 \cdot g_2, h_1 \cdot h_2).$$

Diese Verknüpfung definiert eine Gruppenoperation auf $G \times H$ mit neutralem Element $(1_G, 1_H)$ und Inversen $(g, h)^{-1} = (g^{-1}, h^{-1})$.

Bemerkung 1.47. Beachte, dass die Abbildungen

$$\begin{array}{rccc} i_G : & G & \to & G \times H \\ & g & \mapsto & (g, 1_H) \end{array} \quad \text{und} \quad \begin{array}{rccc} i_H : & H & \to & G \times H \\ & h & \mapsto & (1_G, h) \end{array}$$

Gruppenmonomorphismen derart definieren, dass G zu der Untergruppe $G \times \{1_H\}$ von $G \times H$ isomorph ist und $H \simeq \{1_G\} \times H$, wegen des Korollars 1.37.

Klarerweise sind $G \times \{1_H\}$ und $\{1_G\} \times H$ beides Normalteiler in $G \times H$ mit $G \times H = (G \times \{1_H\}) \cdot (\{1_G\} \times H)$ aus dem Satz 1.39.

Die obige Bemerkung begründet folgende Verallgemeinerung:

Definition 1.48. Eine Gruppe G ist das *innere direkte Produkt* der Untergruppen H und K, falls $G = H \cdot K$ mit $H \cap K = \{1_G\}$ und H sowie K beides Normalteiler von G sind.

Notation. Wenn die abelsche Gruppe G ein inneres direktes Produkt der Untergruppen H und K ist, sagen wir, dass G eine *innere direkte Summe* von H und K ist und bezeichnen es mit $G \simeq H \oplus K$.

Lemma 1.49. *Die Gruppe G ist genau dann das innere direkte Produkt der Untergruppen H und K, wenn folgende Bedingungen gleichzeitig gelten:*

- *Jedes Element g aus G lässt sich eindeutig als ein Produkt $h \cdot k$ schreiben, mit h aus H und k aus K.*

- *Die Untergruppen H und K kommutieren miteinander:*

$$h \cdot k = k \cdot h$$

für alle h aus H und k aus K.

Beweis. Wir nehmen zuerst an, dass G das innere direkte Produkt der Normalteiler H und K ist. Weil $G = H \cdot K$, lässt sich jedes g aus G als ein Produkt $h \cdot k$ schreiben, mit h aus H und k aus K. Wenn $g = h \cdot k = h_1 \cdot k_1$, dann ist $h^{-1} \cdot h_1 = k \cdot k_1^{-1}$ sowohl in H als auch in K, also $h = h_1$ und $k = k_1$, was zeigt, dass die Darstellung eindeutig ist.

Des Weiteren müssen H und K miteinander kommutieren: Das Produkt $k \cdot h$ muss sich eindeutig in der Form $h_1 \cdot k_1$ schreiben lassen. Nun ist

$$1_G \cdot k_1 = k_1 = h_1^{-1} \cdot k \cdot h = (h_1^{-1} \cdot h) \cdot k^h.$$

Da K Normalteiler ist, liegt k^h in K. Aus der Eindeutigkeit der Darstellung folgt, dass $h_1 = h$ (und $k^h = k_1$). Analog ist

$$h \cdot 1_G = h = k \cdot h \cdot k_1^{-1} = h^{k^{-1}} \cdot (k \cdot k_1^{-1}),$$

also folgern wir, dass $k = k_1$ und somit $k \cdot h = h \cdot k$, wie gewünscht.

Wir nehmen nun an, dass die Untergruppen H und K miteinander kommutieren und dass wir jedes Element g aus G eindeutig darstellen können als $h \cdot k$. Insbesondere ist $H \cap K = \{1_G\}$ wegen der Eindeutigkeit der Darstellung. Wenn wir zeigen, dass H und K beides Normalteiler sind, folgt, dass $G = H \cdot K$, wie gewünscht. Wir zeigen nur, dass K ein Normalteiler ist, weil der Beweis für H analog geht. Gegeben g aus G beliebig, müssen wir zeigen, dass $Kg = gK$. Schreibe $g = h \cdot k$ mit h aus H und k aus K. Nun ist $g = k \cdot g$, so

$$Kg = K \cdot (k \cdot h) = Kh = \{k_1 \cdot h\}_{k_1 \in K} = \{h \cdot k_1 1\}_{k_1 \in K} = hK = (h \cdot k) \cdot K = gK,$$

wie gewünscht. □

Korollar 1.50. *Wenn G ein inneres direktes Produkt der Normalteiler H und K ist, dann ist $G \simeq H \times K$.*

Induktiv können wir innere direkte Produkte einer beliebigen Familie $(H_i)_{i \in I}$ von Untergruppen definieren.

Definition 1.51. Eine Gruppe G ist das *innere direkte Produkt* der Familie $(H_i)_{i \in I}$ von Normalteilern, falls $G = \langle \bigcup_{i \in I} H_i \rangle$ und für jedes i aus I der Durchschnitt $H_i \cap \langle \bigcup_{i \neq j \in I} H_j \rangle = \{1_G\}$. Oder äquivalent dazu, die Untergruppen H_i und H_j mit $i \neq j$ kommutieren miteinander:

$$H_i \subset C_G(H_j) = \bigcap_{h \in H_j} C_G(h)$$

und jedes Element g aus G sich eindeutig als ein Produkt $h_{i_1} \cdots h_{i_n}$, mit n aus $\mathbb{N}$ und h_{i_k} aus H_{i_k}, schreiben lässt.

Satz 1.52. (*Der chinesische Restsatz*)
Gegeben paarweise teilerfremde natürliche Zahlen $m_1, \ldots, m_k$, so gilt

$$\mathbb{Z}/M\mathbb{Z} \simeq \mathbb{Z}/m_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/m_k\mathbb{Z},$$

wobei $M = \prod_{i=1}^{k} m_k$.

Beweis. Weil M von jedem m_i geteilt wird, ist die Abbildung

$$\begin{array}{rccl} \varphi: & \mathbb{Z}/M\mathbb{Z} & \to & \mathbb{Z}/m_1\mathbb{Z} \times \ldots \times \mathbb{Z}/m_k\mathbb{Z} \\ & r + M\mathbb{Z} & \mapsto & (r + m_1\mathbb{Z}, \ldots, r + m_k\mathbb{Z}) \end{array}$$

wohldefiniert. Ferner ist φ ein Gruppenhomomorphismus. Um zu beweisen, dass φ ein Isomorphismus ist, genügt es zu zeigen, dass die Abbildung injektiv ist, weil beide endlichen Gruppen dieselbe Mächtigkeit M haben. Sei r eine ganze Zahl mit $\varphi(r) = (\overline{0}, \ldots, \overline{0})$. Dies bedeutet $r \equiv \overline{0}$ mod m_i für jedes $i \leq k$, das heißt, m_i teilt r. Da die Zahlen $m_1, \ldots, m_k$ paarweise teilerfremd sind, folgt, dass $M = \prod_{i=1}^{k} m_k$ das Element r teilt. Somit ist $\overline{r} = \overline{0}$ in $\mathbb{Z}/M\mathbb{Z}$, wie gewünscht. □

Korollar 1.53. *Wenn die natürliche Zahl $M \geq 2$ sich als $M = \prod_{i=1}^{k} p_i^{e_i}$ faktorisieren lässt, so ist*

$$\mathbb{Z}/M\mathbb{Z} \simeq \mathbb{Z}/p_1^{e_1}\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/p_k^{e_k}\mathbb{Z}.$$

Wir werden nun eine vollständige Beschreibung aller endlichen abelschen Gruppen liefern. Hierfür brauchen wir einige Grundbegriffe:

Definition 1.54. Eine Gruppe ist:

- eine *Torsionsgruppe*, falls jedes Element endliche Ordnung hat.
- eine *p-Gruppe* für eine Primzahl p, falls die Ordnung jedes Elements g eine p-Potenz p^e ist. Beachte, dass e von g abhängt.
- *torsionsfrei*, wenn kein Element außer der Identität 1_G endliche Ordnung besitzt.

Eine Torsionsgruppe hat *Exponenten* n, falls die Ordnung jedes Elementes n teilt und es ein Element mit Ordnung genau n gibt.

Klarerweise ist jede p-Gruppe eine Torsionsgruppe. Mit Hilfe der binomischen Formel lässt sich leicht zeigen, dass in einer abelschen Gruppe die Menge der *Torsionselemente* (das heißt, die Elemente endlicher Ordnung) eine Untergruppe bildet.

Aufgabe. Zeige, dass eine abelsche Gruppe vom Exponenten p eine kanonische Struktur als Vektorraum über dem Körper $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ besitzt.

Proposition 1.55. *Jede abelsche p-Gruppe vom Exponenten p^e, mit e aus $\mathbb{N}$, ist eine innere direkte Summe zyklischer Gruppen.*

Beweis. Der *Sockel* S der abelschen p-Gruppe G vom Exponenten p^e ist die Menge

$$S = \{a \in G \mid p \cdot a = 0_G\}$$

der Elemente der Ordnung höchstens p. Beachte, dass S ein $\mathbb{F}_p$-Vektorraum ist. In S finden wir eine Kette

$$S_e = \{0_G\} \subset S_{e-1} \subset \cdots \subset S_1 \subset S_0 = S$$

von Unterräumen $S_i = S \cap p^i(G)$, wobei $p^i : G \to G$ den Homomorphismus gegeben durch Multiplikation mit p^i bezeichnet, mit p^0 gleich der Identitätsabbildung. Wir wählen eine Vektorraumbasis $B = B_0 \cup \cdots \cup B_{e-1}$ von S derart, dass die Nebenklassen von Elementen aus B_i eine Basis des Quotientenraumes S_i/S_{i+1} bilden.

Nun sind die Elemente aus S_i in G durch p^i teilbar, also wähle für s aus B_i ein $g(s)$ aus G mit $p^i g(s) = s$. Weil die Elemente aus dem Sockel Ordnung höchstens p haben, ist die erzeugte Untergruppe $H_s = \langle\{g_s\}\rangle$, mit s aus B_i, zyklisch der Ordnung p^{i+1}.

Wir müssen somit nur zeigen, dass $G = \bigoplus_{s\in B} H_s$. Klarerweise liegt der Sockel S in dieser direkten Summe (weil s in H_s liegt). Sei nun a aus G beliebig. Wenn die Ordnung von a höchstens p ist, liegt a im Sockel und daher in der direkten Summe. Falls die Ordnung von a der Form p^i ist, liegt $p^{i-1}a$ in $S \cap p^{i-1}G = S_{i-1}$, also lässt es sich als Linearkombination von Elementen aus $B_{i-1} \cup \cdots \cup B_{e-1}$ schreiben. Jeder dieser Basisvektoren ist durch p^{i-1} in $\bigoplus_{s\in B} H_s$ teilbar (denn $p^k g(s) = s$) und somit ist auch $p^{i-1}a$ durch p^{i-1} in $\bigoplus_{s\in B} H_s$ teilbar. Schreibe also $p^{i-1}a = p^{i-1}h$ für ein h aus $\oplus_{s\in B} H_s$. Es folgt, dass $(a-h)$ Ordnung höchstens p^{i-1} hat und induktiv folgern wir, dass $a-h$ in $\bigoplus_{s\in B} H_s$ liegt. Somit liegt auch a in $\bigoplus_{s\in B} H_s$, wie gewünscht.

Wir müssen nur noch zeigen, dass die Darstellung von a aus G als Summe eindeutig ist, oder äquivalent dazu, dass

$$\sum_{s\in B} h_s = 0_G \quad \Rightarrow \quad h_s = 0 \text{ für jedes } s \text{ aus } B.$$

Beachte, dass

$$\sum_{s\in B} h_s = \sum_{s\in B_0} h_s + \cdots + \sum_{s\in B_k} h_s$$

für ein k maximal derart, dass die entsprechenden h_s nicht alle Null sind. Für s aus B_k schreibe $h_s = \lambda_s g(s)$ mit $0 \le \lambda_s \le p^{k+1} - 1$. Nun ist

$$0 = p^{k-1} \sum_{s\in B} h_s = \sum_{s\in B_k} \lambda_s p^{k-1} g(s) = \sum_{s\in B_k} \lambda_s s$$

und somit jedes λ_s durch p teilbar (weil die Elemente aus B linear unabhängig über $\mathbb{F}_p$ sind). Schreibe also $\lambda_s = p\lambda'_s$ mit $0 \le \lambda_s \le p^k - 1$. Nun ist

$$0 = p^{k-2} \sum_{s\in B} h_s = \sum_{s\in B_{k-1}} p^{k-2} h_s + \sum_{s\in B_k} \lambda'_s s = \sum_{s\in B_{k-1}} \mu_s s + \sum_{s\in B_k} \lambda'_s s$$

für geeignete μ_s's zwischen 0 und $p^k - 1$. Wir schließen analog, dass jedes λ'_s wiederum durch p teilbar ist. Wir iterieren dieses Verfahren $k+1$-mal und bekommen, dass λ_s durch p^{k+1} teilbar ist. Jedes λ_s und somit auch jedes h_s mit s aus B_k ist also Null, was der Maximalität von k widerspricht. □

Satz 1.56. *Jede abelsche Torsionsgruppe ist innere direkte Summe ihrer p-Gruppen.*

Insbesondere ist jede endliche abelsche Gruppe isomorph zu einer direkten Summe zyklischer Gruppen der Form $\mathbb{Z}/p^e Z$ mit p eine Primzahl. Die Summanden sind bis auf Permutation eindeutig bestimmt.

Beweis. Sei G eine abelsche Torsionsgruppe. Gegeben eine Primzahl p, bezeichne mit G_p die Untergruppe aller Elemente von G, welche als Ordnung eine p-Potenz haben. Wenn a aus G mit Ordnung n ist, dann ist $\langle\{a\}\rangle \simeq \mathbb{Z}/n\mathbb{Z}$, was wiederum isomorph zu einer direkten Summe zyklischer Gruppen der Form $\mathbb{Z}/p^e Z$ ist, mit p einem Faktor von n. Es folgt, dass a eine Summe von Elementen aus den entsprechenden G_p's ist.

Wir müssen also nur zeigen, dass der Durchschnitt $G_p \cap \langle \bigcup_{q \neq p} G_q \rangle$ trivial ist: Wenn das Element a aus G sich als $b_{q_1} + \cdots + b_{q_r}$ schreiben lässt mit b_{q_j} der Ordnung $q_j^{e_j}$, so teilt die Ordnung von a das Produkt $q_1 \cdots q_r$.

Für die zweite Behauptung sei nun G eine endliche abelsche Gruppe. Aus der ersten Behauptung folgt, dass G innere direkte Summe ihrer p-Gruppen ist, welche wiederum endlich sind und somit vom Exponenten p^e für ein gewisses e (wobei p^e höchstens die größte p-Potenz ist, welche $|G|$ teilt, wegen des Korollars 1.32). Es folgt nun aus der Proposition 1.55, dass jede der p-Gruppen innere direkte Summe zyklischer Gruppen ist und somit auch G, wie gewünscht.

Wir müssen also nur zeigen, dass die Darstellung als innere direkte Summe zyklischer Gruppen eindeutig ist. Ohne Beschränkung der Allgemeinheit schreibe

$$G = \bigoplus_{p,e} (\mathbb{Z}/p^e\mathbb{Z})^{n(p,e)}.$$

Wie in der Proposition 1.55 sei $S(G)_p$ der p-Sockel von G, das heißt,

$$S_p = \{a \in G \mid pa = 0\}.$$

Es folgt direkt aus dem Beweis der Proposition 1.55, dass die Anzahl der Summanden der Form $\mathbb{Z}/p^e\mathbb{Z}$ genau der Dimension des Quotienten $S(G)_p \cap p^{e-1}G / S(G)_p \cap p^e G$ als $\mathbb{F}_p$-Vektorraum entspricht. Diese Information hängt nur von der Gruppe G sowie von der Primzahl p und von der natürlicher Zahl e ab. In der Tat, wenn

$$G = \bigoplus_{p,e} (\mathbb{Z}/p^e\mathbb{Z})^{n(p,e)},$$

so ist

$$S(G)_p \cap p^{e-1}G = \bigoplus e(p^{e-1}\mathbb{Z}/p^e)^{n(p,e)} \text{ und } S(G)_p \cap p^e G = \bigoplus r > e(p^{r-1}\mathbb{Z}/p^r)^{n(p,r)},$$

was die gewünschte Gleichheit

$$n(p,e) = \dim_{\mathbb{F}_p} S(G)_p \cap p^{e-1}G / S(G)_p \cap p^e G$$

liefert. □

1.4 Sylow- und auflösbare Gruppen

Die Sylowsätze liefern in vielen Situationen eine hilfreiche Methode, die Struktur (bis auf Isomorphie) einer endlichen Gruppe zu bestimmen. Wir werden in diesem Abschnitt sehen, wie wir mit Hilfe der Sylowsätze einen Beweis gewinnen können, dass die Gruppe A_5 (siehe Proposition 1.45) der geraden Permutationen aus S_5 einfach ist.

In diesem Abschnitt sei p eine feste Primzahl.

Lemma 1.57. (*Cauchys Lemma*) *Wenn die Primzahl p die Mächtigkeit der endlichen Gruppe G teilt, so besitzt G ein Element der Ordnung p.*

Beweis. Wir beweisen das Lemma induktiv über die Mächtigkeit $|G|$ der endlichen Gruppe G. Aus der Konjugationsklassengleichung 1.33 folgt, dass p die Mächtigkeit des Zentrums $Z(G)$ teilt oder es eine nicht-triviale Konjugationsklasse a^G derart gibt, dass p den Index $[G : C_G(a)]$ nicht teilt. Im zweiten Fall folgt aus der Bemerkung 1.28, dass p die Mächtigkeit der echten Untergruppe $C_G(a)$ teilt. Wir folgern induktiv, dass $C_G(a)$ (und somit auch G) ein Element der Ordnung p besitzt.

Wenn p die Mächtigkeit der abelschen Untergruppe $Z(G)$ teilt, dann folgt aus dem Satz 1.56, dass $Z(G)$ einen Summanden besitzen muss, welcher zu $\mathbb{Z}/p^e\mathbb{Z}$, mit $e \neq 0$, isomorph ist. Klarerweise hat dieser Summand ein Element der Ordnung p, wie gewünscht. □

Korollar 1.58. *Sei p eine Primzahl. Jede endliche p-Gruppe G mit $|G| = p^n$ besitzt für jedes $0 \leq e \leq n$ einen Normalteiler mit Index p^e.*

Beweis. Falls $e = 0$ wähle G selbst als Normalteiler. Falls $e = n$ wähle also die triviale Untergruppe $\{1_G\}$ als Normalteiler. Wir können also annhemen, dass $1 \leq e \leq n - 1$. Wir beweisen die Aussage per Induktion über n. Für $n = 1$ gibt es nichts zu zeigen. Ohne Beschränkung der Allgemeinheit ist $n \geq 2$. Beachte, dass p wegen der Konjugationsklassengleichung 1.33 die Mächtigkeit des Zentrums $Z(G)$ teilen muss. Insbesondere folgt aus dem Lemma von Cauchy 1.57, dass $Z(G)$ ein Element a der Ordnung p besitzt. Setze $H = \langle a \rangle$ die von a erzeugte Untergruppe, welche klarerweise ein Normalteiler von G ist. Die Quotientengruppe G/H ist eine p-Gruppe der Mächtigkeit p^{n-1}, also besitzt sie einen Normalteiler mit Index p^e. Wegen des Diamantsatzes 1.39 gibt es einen Normalteiler von G mit Index p^e, welcher H enthält, wie gewünscht. □

Definition 1.59. Eine Untergruppe S der endlichen Gruppe G ist *p-Sylow*, falls $|S| = p^e$ und $|G| = p^e m$, mit p und m teilerfremd.

Lemma 1.60. *Wenn p die Mächtigkeit $|G|$ der endlichen Gruppe teilt, so besitzt G eine p-Sylow-Untergruppe.*

Beweis. Wir beweisen das Lemma induktiv über die Mächtigkeit $|G|$ der endlichen Gruppe G. Schreibe also $|G| = p^e m$, mit p und m teilerfremd. Aus unserer Annahme ist $e > 0$.

Wie im Beweis des Lemmas 1.57 teilt p entweder die Mächtigkeit des Zentrums $Z(G)$ oder es gibt eine nicht-triviale Konjugationsklasse a^G derart, dass p den Index $(G : C_G(a))$ nicht teilt. Im zweiten Fall muss also p^e die Mächtigkeit vom Zentralisators $C_G(a)$ teilen. Beachte, dass jede p-Sylow-Untergruppe des Zentralisators $C_G(a)$ eine p-Sylow-Untergruppe von G ist. Weil $C_G(a)$ eine echte Untergruppe ist, folgern wir die Existenz induktiv über ihre Mächtigkeit.

Ansonsten teilt p also die abelsche Untergruppe $Z(G)$. Wegen des Satzes 1.56 besitzt jede abelsche Gruppe eine p-Sylow-Untergruppe S_1, nämlich die p-Gruppe aller Torsionselemente deren Ordnung eine p-Potenz ist. Wenn S_1 eine p-Sylow-Untergruppe von G ist, dann sind wir fertig. Sonst betrachte die Quotientengruppe G/S_1, da S_1 ein Normalteiler von G ist. Die Primzahl p teilt also die Mächtigkeit der Quotientengruppe G/S_1. Induktiv finden wir eine p-Sylow-Untergruppe von G/S_1, welche der Form S/S_1, mit $S_1 \leq S \leq G$, sein muss, wegen des Satzes 1.39. Klarerweise ist S eine p-Sylow-Untergruppe von G, siehe Bemerkung 1.28. □

Proposition 1.61. *Wenn p die Mächtigkeit $|G|$ der endlichen Gruppe teilt, so gelten folgende Aussagen:*

(a) Jede p-Untergruppe von G ist in einer p-Sylow-Untergruppe enthalten.

(b) Die Gruppe G wirkt transitiv durch Konjugation auf der Kollektion der p-Sylow-Untergruppen. Insbesondere sind je zwei p-Sylow-Untergruppen zueinander konjugiert.

(c) Schreibe $|G| = p^e m$ mit m und p teilerfremd. Die Anzahl m_p der verschiedenen p-Sylow-Untergruppen von G teilt m und ist kongruent zu 1 modulo p.

Beweis. Sei S eine beliebige p-Sylow-Untergruppe von G, welche wegen des Lemmas 1.60 existiert. Beachte, dass jede zu S konjugierte Untergruppe S^g wiederum eine p-Sylow-Untergruppe von G ist. Wir zeigen zuerst, dass jede p-Untergruppe H von G in einer p-Sylow-Untergruppe der Form S^g enthalten ist. Insbesondere ist somit die Wirkung durch Konjugation von G auf der Kollektion der p-Sylow-Untergruppen transitiv.

Die Untergruppe H wirkt von links auf der Kollektion der linken Nebenklassen von S durch

$$h \star gS = (h \cdot g)S.$$

Es genügt also zu zeigen, dass es eine Nebenklasse gS derart geben muss, dass die entsprechende Bahn unter der obigen Wirkung aus dem einzigen Element gS besteht, denn

$$h \star gS = (h \cdot g)S = gS \iff (h \cdot g) \in gS \iff h \in S^{g^{-1}}$$

und somit $H \leq S^{g^{-1}}$, wie gewünscht. Nun muss die Mächtigkeit der Bahn von gS unter der Wirkung von H eine p-Potenz sein, wegen des Satzes 1.33. Wenn alle Bahnen mehr als ein Element besitzen würden, wäre die Anzahl der linken Nebenklassen von S in G durch p teilbar, was der Bemerkung 1.28 widerspricht. Somit finden wir eine Nebenklasse gS mit

$$h \star gS = (h \cdot g)S = gS \text{ für alle } h \text{ aus } H,$$

wie gewünscht.

Wenn wir den obigen Fall für $H = S$ betrachten, ist die Anzahl $(G : S)$ der linken Nebenklassen von S in G die Mächtigkeit der Vereinigung der Bahnen $S \star bS$ mit b aus G. Beachte, dass eine Bahn $S \star bS$ genau dann aus der Nebenklasse bS besteht, wenn b in $N_G(S)$ liegt: Eine Richtung ist klar, denn $Sb = bS$. Wenn $abS = bS$ für alle a aus S, so liegt ab in bS für alle a aus S und somit ist $Sb = bS$, wie gewünscht. Es folgt aus dem Satz 1.33 und aus dem Korollar 1.29, dass

$$(G : N_G(S))(N_G(S) : S) = (G : S) = (N_G(S) : S) + \text{Vielfaches von } p,$$

also muss

$$(G : N_G(S))(N_G(S) : S) - (N_G(S) : S) = (N_G(S) : S)\big((G : N_G(S)) - 1\big)$$

durch p teilbar sein. Weil $(G : S)$ teilerfremd zu p ist, folgt, dass $(G : N_G(S))$ kongruent zu 1 modulo p ist. Wir müssen also zeigen, dass die Anzahl m_p der p-Sylow-Untergruppen gleich $(G : N_G(S))$ ist. Hierfür betrachte nun die Wirkung von G durch Konjugation auf den p-Sylow-Untergruppen. Weil die Wirkung transitiv ist, ist die Anzahl m_p der p-Sylow-Untergruppen gleich der Mächtigkeit der Bahn von S. Aus dem Satz 1.33 folgt, dass m_p genau dem Index vom Normalisator $N_G(S)$ in G entspricht, also ist m_p kongruent zu 1 modulo p, wie gewünscht. Mit Hilfe des Korollars 1.29 folgt sofort, dass $m_p = (G : N_G(S))$ die Zahl $m = (G : S)$ teilt. □

Definition 1.62. Ein *Kommutator* in der Gruppe G ist ein Element der Form

$$[h, g] = h^{-1} \cdot h^g = h^{-1} \cdot g^{-1} \cdot h \cdot g.$$

Die *Kommutatorgruppe* $G' = [G, G]$ ist die von der Menge aller Kommutatoren erzeugte Untergruppe. Allgemein definieren wir die n-te *derivierte* Untergruppe $G^{(n)}$ als die Kommutatorgruppe $G^{(n)} = [G^{(n-1)}, G^{(n-1)}]$.

Beachte, dass $[g, h] = [h, g]^{-1}$. Des Weiteren ist $[h, g]^{g_1} = [h^{g_1}, g^{g_1}]$.

Bemerkung 1.63. Zwei Elemente g und h kommutieren genau dann miteinander, wenn ihr Kommutator $[h, g] = 1_G$.

Weil die Menge aller Kommutatoren unter Konjugation abgeschlossen ist, ist die Kommutatorgruppe ein Normalteiler von G wegen der Bemerkung 1.25. Beachte, dass G/G' abelsch ist. Ferner ist G' der kleinste Normalteiler N von G derart, dass G/N abelsch ist.

Beachte, dass jede n-te derivierte Untergruppe $G^{(n)}$ sogar ein Normalteiler von G ist.

Definition 1.64. Eine Gruppe G ist *auflösbar*, wenn $G^{(n)}$ trivial ist für ein n aus $\mathbb{N}$, oder äquivalent dazu, wenn es eine aufsteigende Kette (oder *Normalreihe*)

$$\{1_G\} = N_0 \trianglelefteq N_1 \trianglelefteq \cdots N_{m-1} \trianglelefteq N_m = G,$$

von Untergruppen derart gibt, dass die Quotientengruppen N_{k+1}/N_k abelsch sind für jedes $0 \leq k \leq m - 1$.

Beachte, dass in einer Normalreihe

$$\{1_G\} = N_0 \trianglelefteq N_1 \trianglelefteq \cdots N_{m-1} \trianglelefteq N_m = G$$

die Untergruppe N_k nicht zwingend ein Normalteiler von N_{k+2} ist.

Folgendes Lemma gewinnen wir direkt aus dem Satz 1.39.

Lemma 1.65. *Jede Untergruppe einer auflösbaren Untergruppe ist wiederum auflösbar. Gegeben einen Epimorphismus $\varphi : G \to H$ mit G auflösbar, so ist H wiederum auflösbar.*

Gegeben einen Normalteiler N einer beliebigen Gruppe G, so folgt, dass die Gruppe G genau dann auflösbar ist, wenn N und G/N beide auflösbar sind.

Klarerweise ist jede abelsche Gruppe auflösbar.

Aufgabe. Zeige, dass die Gruppe S_3 auflösbar, aber nicht abelsch ist.

Nicht jede endliche Gruppe ist auflösbar, wie folgende Proposition zeigt.

Proposition 1.66. *Die Gruppe A_5 aller geraden Permutationen ist einfach. Insbesondere ist die Gruppe S_5 aller Permutationen nicht auflösbar.*

Beweis. Die letzte Behauptung folgt sofort aus der Einfachheit der Untergruppe A_5, denn A_5 ist klarerweise nicht abelsch und somit nicht auflösbar. Wenn S_5 auflösbar wäre, so wäre es aber auch A_5 nach Lemma 1.65, was den gewünschten Widerspruch liefert.

Beachte, dass die Mächtigkeit von A_5 gleich $|A_5| = |S_5|/2 = 5!/2 = 60 = 2^2 \cdot 3 \cdot 5$ ist, wegen der Proposition 1.45. Sei also $\{1_{A_5}\} \neq N \triangleleft A_5$. Wir müssen nur zeigen, dass $N = A_5$. Aus der Bemerkung 1.28 folgt, dass die Mächtigkeit von N die Zahl 60 teilt. Falls $|N| = 2$

wäre, würde N von einer Permutation der Ordnung 2 erzeugt werden. Da jede Permutation sich eindeutig als ein Produkt disjunkter Zyklen schreiben lässt, folgt, dass $N = \langle (ij)(kl) \rangle$ für eine 4-elementige Teilmenge $\{i, j, k, l\}$ von $\{1, \ldots, 5\}$ (weil das erzeugende Element eine gerade Anzahl von Produkten von Transpositionen sein muss). Wähle r aus $\{1, \ldots, 5\} \setminus \{i, j, k, l\}$ und beachte, dass das Element

$$(ijr)^{-1}(ij)(kl)(ijr) = (rji)(ij)(ijr)(kl) = (ir)(kl)$$

nicht in N liegen darf, denn j wird fixiert aber r wird bewegt, also ist N kein Normalteiler.

Wenn N Mächtigkeit 4 hätte, wäre N eine 2-Sylow-Untergruppe von A_5. Da N ein Normalteiler ist und alle 2-Sylow-Untergruppen wegen der Proposition 1.61 konjugiert zu N sind, ist N die einzige 2-Sylow-Untergruppe. Jedes Element der Ordnung 2 muss in N liegen, aber es gibt mindestens 5 solche Elemente, was einen Widerspruch liefert.

Es folgt also, dass die Mächtigkeit von N durch 3 oder durch 5 teilbar sein muss. Das bedeutet, dass N eine 3-Sylow oder eine 5-Sylow-Untergruppe (und somit alle, weil N ein Normalteiler ist) von A_5 enthält.

Wenn N alle 5-Sylow-Untergruppen enthält, folgt, dass $|N| \geq 25$: In der Tat wird jede 5-Sylow-Untergruppe durch ein Element der Ordnung 5 erzeugt. In S_5 ist ein Element der Ordnung 5 genau ein 5-Zyklus (beachte, dass jeder 5-Zyklus in A_5 liegt). Es gibt genau

$$\frac{5 \cdot 4 \cdots 2 \cdot 1}{5} = 24$$

solche Elemente und sie müssen alle in N liegen aus der Proposition 1.61. Insbesondere enthält N mindestens $1 + 24 = 25$ Elemente. Weil $|N|$ die Zahl $|A_5| = 60$ teilen muss, folgt, dass $|N| = 30$ oder $N = A_5$. Wir müssen also zeigen, dass $|N| \neq 30$. Sonst enthält N auch alle 3-Sylow-Untergruppen von A_5, welche jeweils isomorph zu $\mathbb{Z}/3\mathbb{Z}$ sind. Jede 3-Sylow-Untergruppe ist der Form

$$H = \{1_{A_5}, \sigma, \sigma^2\},$$

wobei σ ein Zyklus der Länge 3 ist (beachte, dass σ in A_5 liegt!). Ein solcher Zyklus fixiert genau 2 Punkte aus $\{1, \ldots, 5\}$ (und dementsprechend auch σ^2). Für jede 2-elementige Teilmenge von $\{1, \ldots, 5\}$ finden wir eine 3-Sylow-Untergruppe, deren nicht-trivialen Elemente genau diese Teilmenge fixieren. Es gibt 10 verschiedene 2-elementige Teilmengen von $\{1, \ldots, 5\}$, also es gibt mindestens $2 \cdot 10$ Elemente der Ordnung 3 in A_5. Aus dem Korollar 1.32 können diese neuen Elemente (bis auf die Identität) nicht in einer der vorigen 5-Sylow-Untergruppen liegen. Das bedeutet, dass N mindestens $1 + 24 + 10 \cdot 2 = 45$ viele Elemente enthält, also $|N| \neq 30$, wie gewünscht.

Wenn N dagegen alle 3-Sylow-Untergruppen enthält, folgt aus dem obigen Paragraphen, dass N mindestens $1 + 10 \cdot 2 \geq 21$ Elemente enthält, also $N = A_5$ oder $|N| = 30$. Wenn $|N| = 30$ ist, bekommen wir aus dem obigen den gewünschten Widerspruch. □

Kapitel 2

Ringe und Körper

2.1 Ringe und Ideale

Definition 2.1. Ein *Ring (mit Eins)* besteht aus einer Menge R zusammen mit zwei Verknüpfungen $+$ und $\cdot$ derart, dass:

- $(R, +)$ eine abelsche Gruppe mit neutralem Element 0_R ist.
- $(R, \cdot)$ ein Monoid mit neutralem Element 1_R, genannt die *Eins* von R, ist.
- Die Distributivitätsgesetze für alle a, b und c aus R gelten:

$$a \cdot (b + c) = a \cdot b + a \cdot c \text{ und } (a + b) \cdot c = a \cdot c + b \cdot c.$$

Ein Ring ist *kommutativ*, falls das Monoid $(R, \cdot)$ kommutativ ist. In diesem Fall sind beide Distributivitätsgesetze äquivalent!

Der *triviale* Ring ist der Ring, welcher nur aus dem Element 0 besteht.

Notation. In einem Ring benutzen wir die additive Notation für die Summe und die multiplikative Notation für das Produkt: Insbesondere ist $-a$ das Inverse des Elements a bezüglich der Verknüpfung $+$, wobei a^{-1} das Inverse (falls es überhaupt existiert) des Elements a bezüglich der Verknüpfung $\cdot$ bezeichnet.

Die multiplikative Verknüpfung $\cdot$ wird häufig aus dem Kontext implizit so verwendet, dass wir ab anstatt $a \cdot b$ schreiben.

Bemerkung 2.2. In jedem Ring R gelten folgende Identitäten für alle Elemente a und b aus R :

- $a0_R = 0_R = 0_R a$.
- $a(-b) = -ab = (-a)b$.

Insbesondere ist ein Ring genau dann trivial, wenn $0_R = 1_R$ ist, denn

$$a1_R = a0_R = 0_R \text{ für alle } a \text{ aus } R.$$

Beispiel 2.3. Die bekannten Strukturen $\mathbb{Z}$, $\mathbb{Q}$, sowie $\mathbb{R}$ und $\mathbb{C}$ sind kommutative Ringe mit den Standardoperationen.

Für eine abelsche Gruppe A bildet die Menge $\mathrm{End}(A)$ aller Endomorphismen von A in sich selbst ein Ring bezüglich der elementenweisen Addition als Summe und der Komposition als Multiplikation. Dieser Ring muss nicht unbedingt kommutativ sein, z. B. wenn $A = \mathbb{Q} \oplus \mathbb{Q}$, denn ein Endomorphismus dieser Gruppe ist genau ein Endomorphismus als $\mathbb{Q}$-Vektorraum.

Definition 2.4. Eine Teilmenge S eines Ringes R ist ein *Teilring*, falls S eine additive Untergruppe von R ist, die Eins 1_R enthält und unter Multiplikation abgeschlossen ist.

Der Teilring S ist wiederum ein Ring, wenn wir die Einschränkung der Operationen auf S betrachten.

Definition 2.5. Eine Teilmenge I eines Ringes R ist ein *Linksideal*, falls I eine additive Untergruppe von R derart ist, dass

$$ra \text{ in } I \text{ liegt für alle } a \text{ aus } I \text{ und } r \text{ aus } R.$$

Ein *Rechtsideal* I ist eine additive Untergruppe von R mit

$$ar \text{ in } I \text{ für alle } a \text{ aus } I \text{ und } r \text{ aus } R.$$

Ein *Ideal* ist ein Linksideal, welches auch ein Rechtsideal ist.

Beispiel 2.6. Das Nullideal $(0_R) = \{0_R\}$ sowie der Ring selbst sind Ideale eines Ringes R, genannt die *trivialen Ideale*. Ein Ideal ist *echt*, falls $I \subsetneq R$ oder äquivalent dazu, wenn 1_R nicht in I liegt.

Die Ideale des Ringes $\mathbb{Z}$ sind genau der Form $n\mathbb{Z}$ für ein n aus $\mathbb{N}$.

Aufgabe. Gegeben zwei Ideale I und J von dem Ring R, zeige, dass $I \cap J$ sowie

$$I + J = \langle I \cup J \rangle = \{z \in R \mid z = a + b \text{ mit } a \in I \text{ und } b \in J\}$$

wiederum Ideale von R sind. Beachte, dass $I \cap J \subset I \subset I + J$ (und analog für J).

Allgemein ist das von der Teilmenge A *erzeugte Ideal*

$$(A) = \bigcap_{\substack{A \subset I \subset R \\ I \, Ideal}} I$$

das kleinste Ideal (bezüglich Inklusion), welches A enthält. Beachte, dass (A) genau aus allen endlichen Summen der Form

$$\sum_{i=1}^{n} r_i a_i s_i \text{ mit } n \text{ aus } \mathbb{N},\ a_i \text{ aus } A \text{ sowie } r_i, s_i \text{ aus } R$$

besteht. Wenn der Ring kommutativ ist, dann ist das von der Einermenge $\{a\}$ erzeugte Ideal

$$(a) = \{ra\}_{r \in R}.$$

Definition 2.7. Ein *Ringhomomorphismus* $F : R \to S$ ist ein additiver Gruppenhomomorphismus von $(R, +)$ nach $(S, +)$ mit $F(1_R) = 1_S$, welcher mit dem Produkt kompatibel ist:

$$F(ab) = F(a)F(b) \text{ für alle } a \text{ und } b \text{ aus } R.$$

Analog zu der Definition 1.11, werden wir häufig nur von Homomorphismen reden, falls der Zusammenhang klar ist.

Bemerkung 2.8. Wenn $F : G \to H$ ein Gruppenhomomorphismus ist, so ist das Bild $F(R)$ ein Teilring von S. Des Weiteren ist für jedes Linksideal I von S das Urbild $F^{-1}(I) = \{r \in R \mid F(r) \in I\}$ ein Linksideal von R (und analog falls I ein Rechtsideal ist). Insbesondere ist $\mathrm{Ker}(F)$ ein Ideal von R.

Proposition 2.9. *Sei I ein Ideal des Ringes R. Die Menge R/I aller additiven Nebenklassen von I in R ist wiederum ein Ring bezüglich der Verknüpfung*

$$\begin{array}{rcl} R/I \times R/I & \to & R/I \\ (a+I, b+I) & \mapsto & ab+I \end{array}$$

mit Eins die Nebenklasse $1_R + I$. Des Weiteren ist die Projektion

$$\begin{array}{rccl} \pi_I : & R & \to & R/I \\ & r & \mapsto & r+I \end{array}$$

ein Ringepimorphismus mit $\mathrm{Ker}(\pi_I) = I$. Die Ideale J/I von R/I sind in Korrespondenz mit den Idealen J aus R, welche I enthalten.

Beweis. Beachte, dass die obige Verknüpfung wohldefiniert ist: Angenommen, dass $a'+I = a+I$ und $b'+I = b+I$, so liegen $a-a'$ und $b-b'$ in I. Insbesondere sind

$$(a'-a)b' = a'b' - ab' \text{ und } a(b'-b) = ab' - ab$$

beide in I. Es folgt, dass $a'b' + I = ab' + I = ab + I$, wie gewünscht.

Weil die Multiplikation auf R ein Monoid mit Eins bestimmt, ist R/I ein Monoid mit Eins die Nebenklasse $1_R + I$. Des Weiteren gelten die Distributivitätsgesetze in R/I, weil sie von R geerbt werden. Klarerweise ist π_I ein Ringhomomorphismus mit Kern das Ideal I.

Aus der Bemerkung 2.8 folgt, dass das Urbild eines Ideales von R/I ein Ideal von R definiert, welches I enthält. Sei nun $J \supset I$ ein Ideal von R. Das Bild

$$J/I = \pi_I(J) = \{a + I \mid a \in J\}$$

ist eine additive Untergruppe von R/I. Seien nun $r+I$ aus R/I und $a+I$ aus J/I mit a aus J. Beachte, dass ra und ar beide in J liegen, also sind

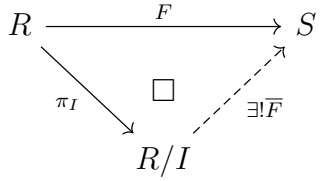
$$(a+I)(r+I) = ar + I \text{ und } (r+I)(a+I) = ra + I$$

beide in J/I, wie gewünscht. □

Korollar 2.10. *Die Menge $\mathbb{Z}/n\mathbb{Z}$ bildet einen kommutativen Ring mit Eins.*

Folgendes lässt sich analog zum Satz 1.36 beweisen.

Satz 2.11. *Für jeden Homomorphismus $F : R \to S$ und jedes Ideal I von R mit $I \subset \mathrm{Ker}(F)$ gibt es einen eindeutigen* von F induzierten *Homomorphismus $\overline{F} : R/I \to S$ derart, dass $\overline{F} \circ \pi_I = F$:*



Ferner gilt $\mathrm{Im}(F) = \mathrm{Im}(\overline{F})$ *und somit ist* F *genau dann surjektiv, wenn* $\overline{F}$ *es ist. Des Weiteren ist* $\mathrm{Ker}(\overline{F}) = \{a + I \in R/I \mid a \in \mathrm{Ker}(F)\}$ *und somit ist* $\overline{F}$ *genau dann injektiv, wenn* $I = \mathrm{Ker}(F)$*. In diesem Fall ist* $\overline{F} : R/\mathrm{Ker}(F) \to F(R)$ *ein Ringisomorphismus.*

Definition 2.12. Ein Ring R ist *nullteilerfrei*, falls das Produkt $a \cdot b$ zweier von Null verschiedener Elemente a und b aus R wiederum nicht Null ist. Ein kommutativer nullteilerfreier nicht-trivialer Ring ist ein *Integritätsbereich*.

Ein echtes Ideal I des Ringes R ist ein *Primideal*, falls

$$ab \in I \Longrightarrow a \in I \text{ oder } b \in I,$$

oder äquivalent dazu, wenn der Quotientenring R/I *nullteilerfrei* ist.

Bemerkung 2.13. Die einzigen Primideale des Ringes $\mathbb{Z}$ sind $\{0\}$ und die Ideale der Form $(p) = p\mathbb{Z}$ mit p eine Primzahl.

Definition 2.14. Die *Charakteristik* eines nicht-trivialen Ringes R wird folgenderweise definiert: Falls

$$n \cdot 1_R = \underbrace{1_R + \cdots + 1_R}_{n} \neq 0_R \text{ für alle } n \neq 0,$$

so ist die Charakteristik gleich Null. Ansonsten gibt es eine kleinste positive natürliche Zahl $m \neq 0$ mit $m \cdot 1_R = 0_R$ und dann sagen wir, dass R *endlicher Charakteristik* gleich m ist.

Bemerkung 2.15. Beachte, dass ein nicht-trivialer Ring R genau dann der Charakteristik n ist, wenn $\mathbb{Z}/n\mathbb{Z}$ sich in R durch

$$\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \to & R \\ \bar{k} & \mapsto & k \cdot 1_R \end{array}$$

einbetten lässt. Des Weiteren gilt $n \cdot r = 0_R$ für alle r aus R.

Die Charakteristik eines Integritätsbereiches ist entweder Null oder eine Primzahl.

Definition 2.16. Zwei Ideale I und J eines Rings R heißen *teilerfremd* (oder *relativ prim zueinander*), falls $I + J = R$.

Wir liefern nun einen allgemeineren Beweis des Korollars 1.53.

Proposition 2.17. (*Der chinesische Restsatz für kommutative Ringe*) *Gegeben paarweise teilerfremde Ideale* $I_1, \ldots, I_n$ *des kommutativen Ringes* R*, setze* $I = \bigcap_{k=1}^{n} I_k$*. Dann sind die Quotientenringe* R/I *und* $R/I_1 \times \cdots \times R/I_n$ *isomorph.*

Das kartesische Produkt $R/I_1 \times \cdots \times R/I_n$ ist klarerweise ein Ring bezüglich der koordinatenweisen Operationen.

Beweis. Es folgt aus dem Satz 2.11, dass die Abbildung

$$\begin{array}{rccc} \overline{\varphi}: & R/I & \to & R/I_1 \times \cdots \times R/I_n \\ & a + I & \mapsto & (a + I_1, \ldots, a + I_n) \end{array}$$

ein Ringmonomorphismus ist, denn $I = \bigcap_{k=1}^{n} I_k$. Wir müssen also nur zeigen, dass $\overline{\varphi}$ surjektiv ist. Für $1 \leq k \neq m \leq n$ ist $I_k + I_m = R$. Wähle also $e_k(m)$ aus I_k und $e_m(k)$ aus I_m derart, dass $e_k(m) + e_m(k) = 1_R$. Nun ist

$$e(k) = \prod_{m \neq k} e_m(k) \equiv 1_R \mod I_k,$$

aber $e(k)$ liegt in I_m für $m \neq k$, also $e(k) \equiv 0_R \mod I_m$.

Gegeben ein beliebiges Tupel $(r_1 + I_1, \ldots, r_n + I_n)$ aus $R/I_1 \times \cdots \times R/I_n$, betrachte nun $a = \sum_{1 \leq k \leq n} r_k e(k)$ aus R. Klarerweise ist

$$\pi_{I_k}(a) = r_k + I_k,$$

also $\overline{\varphi}(a) = (r_1 + I_1, \ldots, r_n + I_n)$, wie gewünscht. □

Korollar 2.18. (*Der chinesische Restsatz für $\mathbb{Z}/M\mathbb{Z}$ als Ring*)
Gegeben paarweise teilerfremde natürliche Zahlen $m_1, \ldots, m_k$, so sind die Ringe

$$\mathbb{Z}/M\mathbb{Z} \simeq \mathbb{Z}/m_1\mathbb{Z} \times \ldots \times \mathbb{Z}/m_k\mathbb{Z}$$

isomorph wobei $M = \prod_{i=1}^{k} m_k$.

2.2 Maximale Ideale und Körper

In diesem Abschnitt sind alle Ringe kommutativ.

Definition 2.19. Ein Ideal M von dem Ring R ist *maximal*, falls $M \subsetneq R$ und es kein echtes Ideal I mit $M \subsetneq I \subsetneq R$ gibt.

Definition 2.20. Ein kommutativer Ring R mit Eins ist ein *Körper*, falls $1_R \neq 0_R$ und die multiplikative Untergruppe der *Einheiten*

$$\mathcal{U}(R) = \{r \in R \mid rs = 1_R \text{ für ein } s \text{ aus } R\}$$

gleich der Menge $R \setminus \{0_R\}$ ist, oder äquivalent dazu, wenn jedes Element $r \neq 0$ aus dem Körper ein multiplikatives Inverses r^{-1} besitzt.

Beachte, dass jeder Körper ein Integritätsbereich ist. Der kleine Satz von Wedderburn liefert die Rückrichtung im endlichen Fall.

Proposition 2.21. (*Der kleine Satz von Wedderburn*) *Jeder endliche Integritätsbereich ist ein Körper.*

Beweis. Weil R ein Integritätsbereich ist, ist die Abbildung

$$\begin{array}{rccc} \lambda_a : & R & \to & R \\ & b & \mapsto & a \cdot b \end{array}$$

genau dann injektiv, wenn $a \neq 0_R$. Nun ist eine injektive Abbildung zwischen endlichen Mengen gleicher Mächtigkeit immer surjektiv. Somit liegt also 1_R im Bildbereich von λ_a falls $a \neq 0_R$. Das bedeutet, dass das Element $a \neq 0_R$ ein multiplikatives Inverses a^{-1} besitzt. □

Lemma 2.22. *Ein kommutativer Ring R mit Eins ist genau dann ein Körper, wenn (0_R) das einzige echte Ideal ist.*

Beweis. Sei K ein Körper. Klarerweise ist (0_K) ein echtes Ideal, denn $1_K \neq 0_K$. Wir nehmen nun an, dass das Ideal $I \subset K$ ein Element $r \neq 0$ enthält. Dann liegt auch $1_K = r \cdot r^{-1}$ in I, also ist $I = K$ nicht echt.

Sei nun R ein kommutativer Ring mit Eins derart, dass (0_R) das einzige echte Ideal ist. Insbesondere ist (0_R) echt, also $1_R \neq 0_R$. Wir müssen nun zeigen, dass jedes Element $r \neq 0_R$ ein multiplikatives Inverses besitzt. Das Ideal (r) ist klarerweise nicht das triviale Ideal (0_R) und wir folgern, dass 1_R in (r) liegt. Schreibe $1_R = sr$, so ist s das multiplikative Inverse r^{-1} von r. □

Weil die Ideale des Quotientenringes R/I in Korrespondenz mit den Idealen aus R sind welche I enthalten, lässt sich folgendes Korollar sofort beweisen.

Korollar 2.23. *Sei M ein echtes Ideal des kommutativen Ringes R. Der Quotientenring R/M ist genau dann ein Körper, wenn M ein maximales Ideal ist.*

Weil Körper nullteilerfrei sind, schließen wir folgendes Korollar aus dem Lemma 2.22.

Korollar 2.24. *Jedes maximale Ideal ist ein Primideal.*

Mit Hilfe des Zorn'schen Lemmas im Appendix A können wir die Existenz maximaler Ideale zeigen.

Proposition 2.25. *Jedes echte Ideal I eines (nicht-trivialen) Ringes R liegt in einem maximalen Ideal.*

Insbesondere besitzt jeder nicht-triviale Ring maximale Ideale.

Beweis. Wir definieren auf der Kollektion

$$\mathcal{S} = \{J \underset{\text{Ideal}}{\subsetneq} R \mid I \subset J\}$$

eine partielle Ordnung durch *mengentheoretische Inklusion*

$$J_1 \leq J_2 \iff J_1 \subset J_2.$$

Wir wollen zeigen, dass $\mathcal{S}$ induktiv ist (siehe A.1). Sei Γ also eine linear geordnete Teilmenge von $\mathcal{S}$. Falls $\Gamma = \emptyset$, dann ist das Element I aus $\mathcal{S}$ bereits eine obere Schranke aus $\mathcal{S}$. Falls $\Gamma \neq \emptyset$, dann ist die Menge

$$J^* = \bigcup_{J \in \Gamma} J = \{r \in R \mid \text{ es gibt ein } J \text{ aus } \Gamma \text{ mit } r \in J\}$$

ein echtes Ideal, welches jedes I aus Γ enthält. Insbesondere enthält J^* das Ideal I, also liegt J^* in $\mathcal{S}$. Das Ideal J^* ist klarerweise eine obere Schranke für Γ.

Aus dem Zorn'schen Lemma A.3 folgt, dass ein maximales Element M in $\mathcal{S}$ existiert. Per Definition ist M ein echtes Ideal, welches I enthält. Wir müssen nur zeigen, dass M ein maximales Ideal ist, das heißt, dass es kein Ideal $J \subsetneq R$ so gibt, dass $M \subsetneq J$. Ein solches Ideal J wäre aber auch in $\mathcal{S}$, was der Maximalität von M in $\mathcal{S}$ widerspricht. □

Es folgt aus der Proposition 2.21, dass der Quotientenring $\mathbb{Z}/n\mathbb{Z}$ genau dann ein Körper ist, wenn n eine Primzahl ist. Somit können wir den berühmten kleinen Satz von Fermat zeigen:

Korollar 2.26. (*Der kleine Satz von Fermat*) *Gegeben eine Primzahl p, so ist a^{p-1} kongruent zu 1 modulo p, falls p die ganze Zahl a nicht teilt.*

Beweis. Weil $\mathbb{Z}/p\mathbb{Z}$ ein Körper ist, ist $\mathcal{U}(\mathbb{Z}/p\mathbb{Z}) = \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ eine Gruppe der Mächtigkeit $p-1$. Da p die Zahl a nicht teilt, ist ihre Restklasse $\bar{a} \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$, also $\overline{a^{p-1}} = \bar{a}^{p-1} = \bar{1}$ wegen des Korollars 1.32, wie gewünscht. □

2.3 Teilbarkeit

In diesem Abschnitt sind alle Ringe Integritätsbereiche.

Wir werden demnächst sehen, dass die Bemerkung im Beispiel 2.6 für mehr Ringe als nur $\mathbb{Z}$ gilt. Hierfür brauchen wir einige Definitionen.

Definition 2.27. Seien a und b zwei Elemente des Ringes R. Das Element a *teilt* das Element b, falls $b = ar$ für ein r aus R, oder äquivalent dazu, wenn $(b) \subset (a)$.

Der Integritätsbereich R ist ein *euklidischer Ring*, falls eine Betragsfunktion $|\cdot| : R \to \mathbb{N}$ mit folgenden Eigenschaften existiert:

- $|r| = 0 \iff r = 0_R$.
- **Division mit Rest:** Sei $a \neq 0_R$ aus R. Für jedes b aus R gibt es c und r aus R mit

$$b = ac + r \text{ und } |r| < |a|.$$

Beispiel 2.28. Der Ring $\mathbb{Z}$ ist ein euklidischer Ring bezüglich dem Standardabsolutbetrag.

Der Polynomring $K[T]$ mit Koeffizienten aus dem Körper K ist ein euklidischer Ring bezüglich dem Betrag $|P(T)| = 2^{\deg(P)}$, wobei der Grad $\deg(P)$ des Nullpolynoms gleich $-\infty$ und $|0| = 0$ gesetzt wird (siehe Satz B.5).

Beispiel 2.29. Der Ring der *gaußschen Zahlen* ist der Teilring

$$\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$$

der komplexen Zahlen mit der *Betragsfunktion* $|a + ib| = a^2 + b^2$ (beachte, dass diese Funktion das Quadrat des Standardabsolutbetrags $||\cdot||$ auf $\mathbb{C}$ ist!). Der Ring $\mathbb{Z}[i]$ ist auch ein euklidischer Ring. Gegeben $z_0 = a + ib \neq 0_{\mathbb{Z}[i]} = 0 + i0$ und z_1 suchen wir q und r aus $\mathbb{Z}[i]$ mit $z_1 = qz_0 + r$ und $|r| < |z_0$. Hierfür unterscheiden wir zwei Fälle: Wenn z_0 das Element z_1 in $\mathbb{Z}[i]$ bereits teilt, schreibe $z_1 = z_0 q$ mit q aus $\mathbb{Z}[i]$ und setze $r = 0$. Sonst liegt die komplexe Zahl $z_1/z_0 = \lambda + i\mu$ in $\mathbb{C} \setminus \mathbb{Z}[i]$. Beachte, dass λ und μ beide aus $\mathbb{Q}$ kommen, weil

$$\frac{z_1}{z_0} = \frac{z_1(a - ib)}{a^2 + b^2}.$$

Weil jede rationale Zahl höchstens Abstand $1/2$ zu einer ganzen Zahl hat, gibt es ganze Zahlen n und m mit

$$||\frac{z_1}{z_0} - (n + im)|| \leq \frac{1}{\sqrt{2}} < 1.$$

Setze $q = n + im$ und $r = z_1 - z_0 q$, dann ist $z_1 = z_0 q + r$ und $|r| < |z_0|$, wie gewünscht.

Beachte allerdings, dass es mehrere Möglichkeiten für q und r gibt, z. B. $105 + i0 = 105 = 2 \cdot 56 - 7 = 1 \cdot 56 + 49$.

Proposition 2.30. *Jeder euklidische Ring R ist ein* Hauptidealring*: Jedes Ideal I ist der Form $I = (a)$ für ein a aus R.*

Beweis. Sei I ein beliebiges Ideal des euklidischen Rings R. Wenn $R = (0)$, dann ist es klarerweise ein Hauptideal. Sonst gibt es ein Element $a \neq 0_R$ aus I mit kleinstmöglichem Betrag $|a|$. Wir müssen nur zeigen, dass $I \subset (a)$. Sei b aus I beliebig und schreibe $b = ac + r$ für c und r aus R mit $|r| < |a|$.

Nun liegt $r = b - ac$ wiederum in I. Also folgt aus der Minimalität des Betrags von a, dass $r = 0_R$, das heißt, das Element a teilt b, wie gewünscht. □

Korollar 2.31. *Jeder Hauptidealring R ist* noethersch*: Jede echte aufsteigende Kette*

$$I_0 \subsetneq I_1 \subsetneq \cdots$$

von Idealen ist endlich.

Beweis. Gegeben eine aufsteigende Kette $(I_n)_{n\in\mathbb{N}}$ von Idealen, so ist $I = \bigcup_{n\in\mathbb{N}} I_n$ wiederum ein Ideal, wie im Beweis der Proposition 2.25. Weil R ein Hauptidealring ist, ist $I = (a)$ für ein a aus R. Insbesondere liegt a in I_n für ein n aus $\mathbb{N}$. Somit ist $I \subset I_n \subset I_{n+1} \subset I$, also $I = I_n = I_{n+1}$, echte aufsteigende Kette muss endlich sein. □

Definition 2.32. Ein Element $p \neq 0_R$ aus dem Integritätsbereich R ist *irreduzibel*, falls p keine Einheit ist und folgende Eigenschaft besitzt: Wenn a das Element p teilt, so ist a eine Einheit oder p teilt a.

Bemerkung 2.33. Beachte, dass $p \neq 0_R$ genau dann irreduzibel ist, wenn p keine Einheit ist und jedes Mal, dass wir p als ein Produkt $p = a \cdot b$ schreiben, muss a oder b eine Einheit sein. Mit dieser Umformulierung können wir also irreduzible Elemente in einem nicht-kommutativen Ring definieren.

Ein Element p aus einem Hauptidealring ist genau dann irreduzibel, wenn (p) ein maximales Ideal ist. Insbesondere ist (p) ein Primideal, aus dem Korollar 2.24.

Proposition 2.34. *Jeder Hauptidealring R ist* faktoriell*: Jedes $r \neq 0_R$ aus $R \setminus \mathcal{U}(R)$ lässt sich als ein Produkt von Potenzen irreduzibler Elemente schreiben. Die Darstellung ist bis auf Permutation und Äquivalenz eindeutig, wobei zwei irreduzible Elemente p und q* äquivalent *sind, wenn $p = uq$ für u aus $\mathcal{U}(R)$.*

Beweis. Wir zeigen zuerst die Existenz der Darstellung: Angenommen, es gibt ein $r \neq 0_R$ aus $R \setminus \mathcal{U}(R)$ ohne Faktorisierung, dann ist r insbesondere nicht irreduzibel, also $r = ab$ und weder a noch b sind Einheiten. Beachte, dass a und b beide ungleich Null sein müssen. Wenn a und b Faktorisierungen haben, so hat r eine Faktorisierung, was unserer Wahl von r widerspricht. Wir finden also einen echten Teiler r_1 von $r = r_0$ ohne Faktorisierung. Wir iterieren dieses Verfahren und konstruieren eine Kette von Idealen

$$(r_0) \subset (r_1) \subset \cdots$$

Aus dem Korollar 2.31 folgt, dass dieses Verfahren stoppt, also $(r_n) = (r_{n+1})$ und somit ist r_{n+1} kein echter Teiler von r_n:

$$r_n = ar_{n+1} \text{ und } r_{n+1} = br_n,$$

also $r_n = abr_n$ und somit ist a eine Einheit, weil R ein Integritätsbereich ist. Dies widerspricht unserer Darstellung von r_n als Produkt mit r_{n+1} als Faktor.

Für die Eindeutigkeit der Darstellung nehmen wir an, dass das Element r aus $R \setminus \mathcal{U}(R)$ zwei verschiedene Faktorisierungen

$$r = p_1^{e_1} \cdots p_n^{e_n} = q_1^{d_1} \cdots q_m^{d_m}$$

besitzt. Ohne Beschränkung der Allgemeinheit gibt es keine Wiederholungen in den Produkten und alle Potenzen e_i und d_j sind positiv. Des Weiteren können wir annehmen, dass kein p_i oder q_j eine Einheit ist (denn sonst betrachten wir das äquivalente Produkt mit weniger Faktoren).

Wir beweisen die Eindeutigkeit induktiv über n. Falls $n = 1$, so liegt $p_1^{e_1}$ im Ideal (q_1), welches nach der Bemerkung 2.33 ein Primideal ist. Insbesondere liegt p_1 in (q_1) und somit gilt $(p_1) = (q_1)$ wegen der Maximalität. Es folgt, dass p_1 und q_1 äquivalent sind. Falls $e_1 \neq d_1$, folgern wir, dass q_1 eine Einheit wäre oder dass q_1 das Produkt $q_2^{d_2} \cdots q_m^{d_m})$, was unserer Annahme widerspricht. Also $e_1 = d_1$ und somit

$$u = (q_2^{d_2} \cdots q_m^{d_m}) \text{ für eine Einheit } u.$$

Es folgt, dass $d_1 = e_1$ und $m = 1$, nach unserer Annahme.

Falls $n > 1$, argumentieren wir wie oben und folgern, dass das Produkt $p_1^{e_1} \cdots p_n^{e_n}$ im Primideal (q_1) liegt. Bis auf Permutation folgern wir, dass p_1 und und q_1 äquivalent sind. Falls $d_1 < e_1$, so besitzt das Element

$$p_1^{e_1 - d_1} \cdots p_2^{e_2} \cdots p_n^{e_n} = u \cdot q_2^{d_2} \cdots q_m^{d_m} \text{ für eine Einheit } u,$$

zwei Faktorisierungen. Wir folgern analog, dass p_1 und q_2 (und somit auch q_1 und q_2) äquivalent sind, was unserer Annahme widerspricht. Also $e_1 \leq d_1$. Es folgt, dass

$$u \cdot p_2^{e_2} \cdots p_n^{e_n} = q_1^{d_1 - e_1} \cdot q_2^{d_2} \cdots q_m^{d_m} \text{ für eine Einheit } u,$$

oder äquivalent dazu,

$$(p_2')^{e_2} \cdot p_3^{e_3} \cdots p_n^{e_n} = q_1^{d_1 - e_1} \cdot q_2^{d_2} \cdots q_m^{d_m} \text{ mit } p_2' = u \cdot p_2.$$

Induktiv über n folgern wir, dass $n = m$, $d_1 = e_1$ und dass die irreduziblen Faktoren bis auf Permutation äquivalent sind. □

Aus der Bemerkung B.3 folgt, dass die Einheiten $\mathcal{U}(K[T])$ im Polynomring genau die Elemente aus $K \setminus \{0_K\}$ sind. Zusammen mit den Propositionen 2.30 und 2.34 folgern wir folgende Beschreibung der Polynome über einem Körper K.

Korollar 2.35. *Ein Polynom $P(T)$ aus dem Polynomring $K[T]$ mit Koeffizienten aus dem Körper K ist genau dann irreduzibel, wenn P sich nicht als ein Produkt zweier nicht-konstanter Polynome kleineren Grades schreiben lässt.*

Jedes Polynom aus $K[T]$ lässt sich als Produkt irreduzibler Polynome schreiben. Die Darstellung ist bis auf Permutation und Äquivalenz eindeutig, wobei zwei irreduzible Polynome äquivalent sind, wenn sie sich durch Multiplikation mit einem konstanten nicht-trivialen Polynom unterscheiden.

Für Polynome mit Koeffizienten aus den ganzen Zahlen $\mathbb{Z}$ haben wir ein wichtiges Kriterium, genannt das *Lemma von Gauß*.

Lemma 2.36. (*Das Lemma von Gauß*)
Sei $P(T)$ ein nicht-konstantes Polynom mit Koeffizienten aus $\mathbb{Z}$ derart, dass $P(T)$ primitiv *ist, das heißt, der größte gemeinsame Teiler seiner Koeffizienten ist* 1. *Das Polynom $P(T)$ ist genau dann irreduzibel in $\mathbb{Q}[T]$, wenn $P(T)$ sich nicht als Produkt $Q(T)R(T)$ zweier nicht-konstanter Polynome mit Koeffizienten aus $\mathbb{Z}$ schreiben lässt.*

Beweis. Eine Richtung ist trivial (und benutzt nicht, dass $P(T)$ primitiv ist): Wenn $P(T)$ irreduzibel ist (als Element von $\mathbb{Q}[T]$), aber $P(T) = Q(T)R(T)$ für zwei Polynome mit Koeffizienten aus $\mathbb{Z}$, dann muss $Q(T)$ oder $R(T)$ konstant sein.

Wir zeigen nun die Rückrichtung: Angenommen, dass $P(T) = Q(T)R(T)$ für zwei Polynome $Q(T)$ und $R(T)$ mit Koeffizienten aus $\mathbb{Q}$. Sei n das kleinste gemeinsame Vielfache der Zähler der Koeffizienten von Q und m das kleinste gemeinsame Vielfache der Zähler der Koeffizienten von R. Klarerweise ist

$$nmP(T) = nQ(T)mR(T) = Q'(T)R'(T) \text{ mit } \deg Q = \deg Q' \ \& \ \deg R = \deg R',$$

wobei die Koeffizienten von $Q'(T)$ und $R'(T)$ nun aus $\mathbb{Z}$ sind. Wir können den größten gemeinsamen Teiler von $Q'(T)$ und $R'(T)$ ausklammern, also

$$nmP(T) = DQ_1(T)R_1(T) \text{ mit } \deg Q_1 = \deg Q \ \& \ \deg R_1 = \deg R,$$

für eine ganze Zahl D, wobei die Polynome $Q_1(T)$ und $R_1(T)$ nun Koeffizienten aus $\mathbb{Z}$ haben und primitiv sind. Es genügt also zu zeigen, dass das Polynom $Q_1(T)R_1(T)$ wiederum primitiv ist: die ganze Zahlen D und nm müssen sich gegenseitig teilen, so

$$P(T) = \pm Q_1(T) \cdot R_1(T).$$

Aus unserer Annahme folgt, dass Q_1 oder R_1 konstant sein muss. Somit ist $Q(T)$ oder $R(T)$ konstant, wie gewünscht.

Wir zeigen also, dass das Produkt zweier primitiver Polynome $Q_1(T)$ und $R_1(T)$ mit Koeffizienten aus $\mathbb{Z}$ wiederum primitiv sind. Schreibe

$$Q_1(T) = \sum_{i=0}^{\deg Q_1} a_i T^i \text{ und } \sum_{j=0}^{\deg R_1} b_j T^j,$$

also

$$Q_1(T)R_1(T) = \sum_{k=0}^{\deg Q_1 + \deg R_1} c_k T^k \text{ mit } c_k = \sum_{i+j=k} a_i b_j.$$

Sei p eine beliebige Primzahl. Da $Q_1(T)$ primitiv ist, gibt es einen kleinsten Index i_0 derart, dass p den Koeffizienten a_{i_0} nicht teilt. Analog finden wir j_0 kleinstmöglich, dass p den Koeffizienten b_{j_0} nicht teilt. Nun kann p den Koeffizienten

$$c_{i_0+j_0} = a_{i_0}b_{j_0} + \sum_{\substack{i+j=k \\ i<i_0}} a_i b_j + \sum_{\substack{i+j=k \\ j<j_0}} a_i b_j$$

nicht teilen, weil p das Produkt $a_{i_0}b_{j_0}$ nicht teilt. □

Aufgabe. Sei p eine Primzahl und $P(T) = T^n + \sum_{i=0}^{n-1} a_i T^i$ ein normiertes Polynom mit Koeffizienten aus $\mathbb{Z}$ derart, dass die Reduktion modulo p

$$\overline{P}(T) = T^n + \sum_{i=0}^{n-1} \overline{a_i} T^i \text{ aus } \mathbb{Z}/p\mathbb{Z}[T]$$

irreduzibel ist. Schließe daraus, dass $P(T)$ irreduzibel in $\mathbb{Q}[T]$ ist.

Korollar 2.37. (*Eisensteinkriterium*)
Sei p eine Primzahl und $P(T) = \sum_{i=0}^{n} a_i T^n$ ein primitives Polynom mit Koeffizienten aus $\mathbb{Z}$ derart, dass p den Führungskoeffizienten a_n nicht teilt, jedoch p alle Koeffizienten a_i mit $0 \leq i < n$ teilt. Falls p^2 den konstanten Koeffizienten nicht teilt, so lässt sich $P(T)$ nicht als Produkt zweier nicht-konstanter Polynome mit Koeffizienten aus $\mathbb{Z}$ schreiben. Insbesondere, wenn $P(T)$ primitiv ist (z.B. wenn $P(T)$ normiert ist), so ist $P(T)$ irreduzibel im Polynomring $\mathbb{Q}[T]$, aus dem Lemma von Gauß 2.36.

Beweis. Wir nehmen an, dass wir $P(T) = Q(T)R(T)$ für zwei nicht-konstante Polynome

$$Q(T) = \sum_{i=0}^{d} b_i T^i \text{ und } R(T) = \sum_{j=0}^{m} c_j T^j$$

mit Koeffizienten aus $\mathbb{Z}$ schreiben können. Insbesondere sind d und m beide echt kleiner als n. Der konstante Koeffizient $a_0 = b_0 c_0$ ist durch p teilbar, also muss p die Zahl b_0 oder die Zahl c_0 teilen. Allerdings sind beide Fälle exklusiv, weil p^2 den Koeffizienten a_0 nicht teilt. Ohne Beschränkung der Allgemeinheit teilt p also b_0 aber nicht c_0. Da $a_n = b_d c_m$, teilt p den Koeffizienten b_d nicht. Wähle nun $0 \leq i_0$ maximal derart, dass p den Koeffizienten b_j für alle $j \leq i_0$ teilt. Beachte, dass $i_0 < d$. Also ist $i_0 + 1 \leq d < n$. Nun ist

$$a_{i_0+1} = b_{i_0+1} c_0 + \sum_{i=0}^{i_0} b_i c_{i_0+1-i}.$$

Da p den Koeffizienten a_{i_0+1} teilt, so teilt p die rechte Seite. Aus unserer Wahl von i_0 folgt, dass p das Produkt $b_{i_0+1} c_0$ und somit auch b_{i_0+1} teilt, was der Maximalität von i_0 widerspricht, wie gewünscht. □

2.4 Lokalisierungen und Quotientenkörper

In diesem Abschnitt sind alle Ringe kommutativ und nicht-trivial.

Definition 2.38. Eine Teilmenge S eines Ringes R ist *multiplikativ*, falls S die Eins 1_R enthält, jedoch 0_R nicht in S liegt, und unter Multiplikation abgeschlossen ist, d.h. für a und b aus S liegt $a \cdot b$ in S.

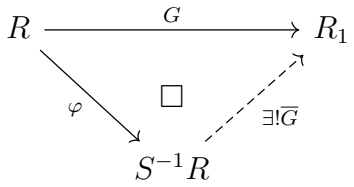
Beispiel 2.39. Gegeben ein Element a aus einem Ring R, so ist die Menge $a^{\mathbb{N}} = \{a^n\}_{n \in \mathbb{N}}$ multiplikativ.

Der Ring R ist genau dann ein Integritätsbereich, wenn $S = R \setminus \{0\}$ multiplikativ ist.

Proposition 2.40. *Sei S eine multiplikative Teilmenge eines kommutativen nicht-trivialen Ringes R. Es gibt einen nicht-trivialen kommutativen Ring $S^{-1}R$ zusammen mit einem Ringhomomorphismus $\varphi : R \to S^{-1}R$ derart, dass $\varphi(s)$ eine Einheit in $S^{-1}R$ für jedes s aus S ist. Ferner ist*

$$\mathrm{Ker}(\varphi) = \{a \in R \mid at = 0_R \text{ für ein } t \text{ aus } S\}.$$

Des Weiteren, gegeben einen Ringhomomorphismus $G : R \to R_1$ derart, dass für jedes s aus S das Bild $G(s)$ in $\mathcal{U}(R_1)$ liegt, so gibt es einen eindeutig bestimmten Homomorphismus $\overline{G} : S^{-1}R \to R_1$ mit



Es folgt aus dem kommutativen Diagram, dass die *Lokalisierung* $S^{-1}R$ von R nach S bis auf Isomorphie eindeutig ist.

Beweis. Definiere eine Äquivalenzrelation $\sim_S$ auf der Menge $R \times S$ durch:

$$(r, s) \sim_S (r_1, s_1) \iff \exists t \in S\ (trs_1 = tr_1s).$$

Wir bezeichnen mit $\frac{r}{s}$ die Äquivalenzklasse von (r, s) bezüglich $\sim_S$. Beachte, dass die Menge $S^{-1}R$ aller Äquivalenzklassen folgenderweise eine wohldefinierte Addition und Multiplikation bekommt:

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1s_2 + r_2s_1}{s_1s_2} \text{ und } \frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \frac{r_1r_2}{s_1s_2}.$$

Mit den obigen Operationen ist $S^{-1}R$ ein Ring mit $0_{S^{-1}R} = \frac{0_R}{1_R}$ und $1_{S^{-1}R} = \frac{1_R}{1_R}$. Beachte, dass $1_{S^{-1}R} \neq 0_{S^{-1}R}$, denn S das Element 0_R nicht enthält. Des Weiteren ist

$$\begin{array}{rccc} \varphi: & R & \to & S^{-1}R \\ & r & \mapsto & \frac{r}{1_R} \end{array}$$

ein Ringhomomorphismus derart, dass $\varphi(s) = \frac{s}{1_R}$ als multiplikatives Inverses das Element $\frac{1_R}{s}$ von $S^{-1}R$ besitzt.

Das Element a liegt genau dann in $\mathrm{Ker}(\varphi)$, wenn $\frac{a}{1_R} = \frac{0_R}{1_R}$, oder äquivalent dazu, wenn es ein t aus S so gibt, dass $at = 0_R$.

Wir nehmen nun an, dass es einen Ringhomomorphismus $G : R \to R_1$ derart gibt, dass für jedes s aus S das Element $G(s)$ eine Einheit in R_1 ist. Wenn eine Abbildung $\overline{G} : S^{-1}R \to R_1$ mit $\overline{G} \circ \varphi = G$ existieren soll, folgt es, dass

$$\overline{G}\big(\frac{r}{s}\big) = \overline{G}(\varphi(r)\varphi(s)^{-1}) = \overline{G}(\varphi(r))\overline{G}(\varphi(s))^{-1} = G(r)G(s)^{-1}.$$

Also ist $\overline{G}$ eindeutig bestimmt, wenn wir zeigen, dass die Vorschrift

$$\frac{r}{s} \mapsto G(r)G(s)^{-1}$$

einen wohldefinierten Homomorphismus definiert. Falls $\frac{r}{s} = \frac{r_1}{s_1}$, so gibt es ein t aus S mit $trs_1 = tr_1s$. Also

$$G(t)G(r)G(s_1) = G(t)G(r_1)G(s).$$

Weil S multiplikativ ist, ist tss_1 wiederum in S. Insbesondere ist $G(tss_1)^{-1} = G(t)^{-1}G(s)^{-1}G(s_1)^{-1}$ und somit

$$G(r)G(s)^{-1} = 1_{R_1}G(r)G(s)^{-1} = 1_{R_1}G(r_1)G(s_1)^{-1} = G(r_1)G(s_1)^{-1},$$

wie gewünscht.

Die Verträglichkeit von $\overline{F}$ mit den Ringoperationen auf $S^{-1}R$ lässt sich problemlos beweisen. □

Korollar 2.41. *Jeder Integritätsbereich R lässt sich als Unterring in einen Körper* $\mathrm{Quot}(R)$*, genannt* Quotientenkörper*, einbetten. Gegeben einen Ringmonomorphismus $F : R \hookrightarrow K$ mit K einem Körper, so gibt es eine eindeutige Fortsetzung* $\mathrm{Quot}(R) \hookrightarrow K$*.*

Beweis. Weil R ein Integritätsbereich ist, folgt aus dem Beispiel 2.39, dass die Menge $S = R \setminus \{0_R\}$ multiplikativ ist. Sei also $\mathrm{Quot}(R) = S^{-1}R$. Aus der Proposition 2.40 folgt, dass der entsprechende Homomorphismus $a \mapsto \frac{a}{1_R}$ injektiv ist.

Beachte weiterhin, dass $\mathrm{Quot}(R)$ ein Körper ist: Gegeben $\frac{a}{b} \neq 0_{\mathrm{Quot}(R)}$, so ist insbesondere $a \neq 0_R$ und somit $\frac{b}{a}$ aus $\mathrm{Quot}(R)$ das gesuchte multiplikative Inverse. □

Die Konstruktion der rationalen Zahlen aus $\mathbb{Z}$, welche wir in der Vorlesung Analysis gesehen haben, zeigt, dass $\mathrm{Quot}(\mathbb{Z}) = \mathbb{Q}$.

Kapitel 3

Galoistheorie

3.1 (Algebraische) Körpererweiterungen

Definition 3.1. Sei K ein Körper. Ein *Teilkörper* von K ist ein Teilring, welcher zusätzlich ein Körper ist.

Der *Primkörper* ist der kleinste Teilkörper von K, also gleich dem Durchschnitt

$$\bigcap_{k \underset{Teilkörper}{\subset} K} k.$$

Bemerkung 3.2. Wenn die Charakteristik des Körpers K Null ist, so ist der Primkörper isomorph zu $\mathbb{Q}$ wegen der Bemerkung 2.14 und des Korollars 2.41. Wir erlauben uns, die Notation $\mathbb{Q} \subset K$ zu verwenden.

Des Weiteren, wenn die Charakteristik des Körpers K die Primzahl $p > 0$ ist, so ist der Primkörper isomorph zu $\mathbb{Z}/p\mathbb{Z}$. Wir erlauben uns, die Notation $\mathbb{F}_p \subset K$ zu verwenden, wobei $\mathbb{F}_p$ den Körper $\mathbb{Z}/p\mathbb{Z}$ bezeichnet.

Definition 3.3. Sei $k \subset K$ eine *Körpererweiterung*, das heißt, der Körper k ist ein Teilkörper des Oberkörpers K. Gegeben eine Teilmenge $A \subset K$, so ist der *von A über k erzeugte Teilring*

$$k[A] = \bigcap_{k \cup A \subset R \underset{Teilring}{\subset} K} R = \{P(a_1, \ldots, a_n) \mid P(T_1, \ldots, T_n) \in k[T_1, \ldots, T_n] \ \&\ a_1, \ldots, a_n \in A\}_{n \in \mathbb{N}},$$

wobei $k[T_1, \ldots, T_n]$ den Polynomring in n Variablen bezeichnet.

Des Weiteren ist der *von A über k erzeugte Teilkörper*

$$k(A) = \bigcap_{k \cup A \subset L \underset{Teilkörper}{\subset} K} L = \mathrm{Quot}(k[A]) =$$

$$= \left\{ \frac{P(a_1, \ldots, a_n)}{Q(a_1, \ldots, a_n)} \mid P(a_1, \ldots, a_n) \ \&\ 0_K \neq Q(a_1, \ldots, a_n) \in k[A] \right\}.$$

Die Körpererweiterung ist *endlich erzeugt*, falls $K = k(A)$ für eine endliche Teilmenge $A = \{a_1, \ldots, a_n\}$ von K. In diesem Fall schreiben wir $K = k(a_1, \ldots, a_n)$. Eine endlich erzeugte Körpererweiterung $k \subset K$ ist *einfach*, falls $K = k(a)$ für ein Element a aus K, welches dann *primitiv* heißt.

Bemerkung 3.4. Seien $k \subset K$ eine Körpererweiterung und a ein Element aus K. Betrachte den Ringhomomorphismus

$$\begin{array}{rccc} \varphi: & k[T] & \to & K \\ & P(T) & \mapsto & P(a) \end{array}$$

mit Bild $k[a]$. Beachte, dass $\mathrm{Ker}(\varphi)$ ein Ideal ist wegen der Bemerkung 2.8.

Falls $\mathrm{Ker}(\varphi) = (0_{k[T]})$, so ist $k[a] \simeq_k k[T]$ (das heißt *isomorph über* k): Der Isomorphismus $k[T] \to k[a]$ ist die Identität auf k. Wir nennen a dann *transzendent über* k.

Ansonsten gibt es ein nicht-triviales Polynom $m_a(T)$ kleinsten Grades in $\mathrm{Ker}(\varphi)$. Da wir über einem Körper arbeiten, können wir annehmen, dass es normiert ist. Aus der Division mit Rest im Polynomring $k[T]$ folgt, dass jedes $P(T)$ aus $k[T]$ sich als

$$P(T) = m_a(T)Q(T) + r(T) \text{ für ein } r(T) \text{ mit } \deg(r) < \deg(m_a)$$

schreiben lässt. Nun ist genau dann $P(a) = 0$, wenn $m_a(T)$ das Polynom $P(T)$ teilt, also $\mathrm{Ker}(\varphi) = (m_a(T))$. In diesem Fall nennen wir das normierte Polynom $m_a(T)$ das *Minimalpolynom* des *algebraischen* Elementes a über k. Insbesondere ist $k[a]$ isomorph über k zum Quotientenring $k[T]/(m_a(T))$.

Bemerkung 3.5. Das Minimalpolynom eines algebraischen Elementes a über k ist irreduzibel, wegen der Minimalität des Grades. Wenn a Nullstelle eines normierten irreduziblen Polynoms $P(T)$ aus $k[T]$ ist, so ist $m_a(T) = P(T)$. Es folgt aus dem Beispiel 2.28 sowie aus der Bemerkung 2.33 und aus dem Korollar 2.23, dass der Ring $k[a]$ bereits ein Teilkörper ist, wenn a algebraisch über k ist. Also ist $k(a) = k[a]$.

Gegeben einen Isomorphismus $F : k \to k'$, ist insbesondere

$$F(m_a(T)) = F\Big(\sum_{i=0}^{\deg(m_a)} \lambda_i T^i\Big) = \sum_{i=0}^{\deg(m_a)} F(\lambda_i) T^i$$

wiederum irreduzibel in $k'[T]$. Gegeben eine Körpererweiterung $k' \subset K'$ und ein Element b aus K', das Nullstelle von $F(m_a(T))$ ist, so ist $m_b(T) = F(m_a(T))$ und wir finden eine Fortsetzung des Isomorphismus $F : k \to k'$ zu einem Isomorphismus $\widetilde{F} : k(a) \to k'(b)$. Die Körpererweiterungen $k \subset k(a)$ und $k' \subset k'(b)$ sind dann also *isomorph*.

Definition 3.6. Gegeben eine Körpererweiterung $k \subset K$, so ist der Körper K insbesondere ein k-Vektorraum. Wir bezeichnen die Dimension $\dim_k K$ von K als k-Vektorraum als *Grad* $[K : k]$ der Körpererweiterung.

Bemerkung 3.7. Sei a aus K algebraisch über k. Der Ring $k[a]$ ist isomorph über k zu $k[T]/(m_a(T))$, welcher als k-Vektorraum die Basis $\{1, T, \ldots, T^{\deg(m_a)-1}\}$ besitzt. Insbesondere ist $k(a) = k[a]$ ein k-Vektorraum mit Basis $\{1, a, \ldots, a^{\deg(m_a)-1}\}$. Somit ist der Grad der Körpererweiterung $k \subset k(a)$ endlich und gleich $\deg(m_a)$.

Beachte, dass der Grad der Körpererweiterung nicht gleich dem Index $(k(a) : k)$ der additiven Untergruppe k in $k(a)$ ist!

Wenn a transzendent über k ist, dann ist der Grad $[k(a) : k] = \infty$.

Korollar 3.8. *Der Grad ist* multiplikativ*:*

$$[K : k] = [K : L][L : k], \text{ falls } k \subset L \subset K.$$

Beweis. Falls $[K : L]$ unendlich ist, so besitzt K eine unendliche lineare unabhängige Familie über L (und somit auch über k), also ist $[K : k]$ auch unendlich. Des Weiteren ist jede linear unabhängige Familie in L über k auch eine Teilmenge von K und somit ist $[K : k]$ auch unendlich, falls $[L : k]$ unendlich ist.

Wir können also annehmen, dass K endlichdimensional über L und L endlichdimensional über k sind. Wähle eine k-Basis $(b_1, \ldots, b_n)$ von L sowie eine L-Basis $(c_1, \ldots, c_m)$ von K. Beachte, dass jedes Element a aus K sich als

$$a = \sum_{j=1}^{m} \lambda_j c_j \text{ mit } \lambda_j = \sum_{i=1}^{n} \mu(j)_i b_i \text{ aus } L$$

schreiben lässt, für $\mu(j)_i$'s aus k mit $1 \leq i \leq n$ und $1 \leq j \leq m$. Also

$$a = \sum_{i=0}^{n} \sum_{j=1}^{m} \mu(j)_i b_i c_j.$$

Es folgt somit, dass die Produkte $(b_i c_j)_{i,j}$ ein Erzeugendensystem von K über k bilden. Es lässt sich leicht zeigen, dass dieses System linear unabhängig ist, also

$$\dim_k L \cdot \dim_L K = \dim_k K,$$

wie gewünscht. □

Definition 3.9. Eine Körpererweiterung $k \subset K$ ist *algebraisch*, falls jedes Element aus K algebraisch über k ist.

Die algebraische Körpererweiterung $k \subset K$ ist *endlich*, falls K als Körper über k endlich erzeugt ist.

Lemma 3.10. *Eine algebraische Körpererweiterung $k \subset K$ ist genau dann endlich, wenn der Grad $[K : k]$ endlich ist.*

Insbesondere, wenn $k \subset L$ und $L \subset K$ beide algebraisch sind, so ist auch $k \subset K$ algebraisch.

Beweis. Wenn $K = k(a_1, \ldots, a_n)$, beachte, dass jedes a_i algebraisch über k ist und somit auch über $k(a_1, \ldots, a_{i-1})$. Wir haben also eine endliche Kette von Körpererweiterungen

$$k \subset k(a_1) \subset \ldots \subset k(a_1, \ldots, a_n) = K$$

derart, dass die Lineardimension von $L_{i+1} = k(a_1, \ldots, a_{i+1})$ über $L_i = k(a_1, \ldots, a_i)$ endlich ist für $0 \leq i < n$, wegen der Bemerkung 3.7. Aus dem Korollar 3.8 folgt, dass der Grad $[K : k]$ wiederum endlich ist.

Wir nehmen nun an, dass die Lineardimension von K als k-Vektorraum endlich ist. Sei also $\{a_1, \ldots, a_n\}$ eine k-Basis von K als k-Vektorraum, also $K = k[a_1, \ldots, a_n]$. Da $k \subset k(a_i) \subset K$, folgt aus dem Korollar 3.8, dass der Grad $[k(a_i) : k]$ für $0 \leq i \leq n$ auch endlich ist. Insbesondere ist a_i algebraisch über k und somit auch über $L_{i-1} = k(a_1, \ldots, a_{i-1})$. Es folgt also, dass $L_i = L_{i-1}[a_i]$ und induktiv folgern wir, dass $K = k(a_1, \ldots, a_n)$ und somit dass K auch als Körper endlich erzeugt ist über k, wie gewünscht.

Für die letzte Behauptung bemerke, dass $[L : k]$ und $[K : L]$ endlich sind, wenn $k \subset L$ und $L \subset K$ beide algebraisch sind. Damit ist

$$[K : k] = [K : L][L : k]$$

endlich und $k \subset K$ algebraisch. □

Proposition 3.11. *Seien $P_1(T), \ldots, P_n(T)$ nicht-konstante Polynome über einem Körper k. Dann gibt es einen* Zerfällungskörper $K_{\mathcal{F}} \supset k$ *für die Kollektion $\mathcal{F} = \{P_1(T), \ldots, P_n(T)\}$, das bedeutet, jedes Polynom $P_i(T)$ zerfällt über $K_{\mathcal{F}}$ in Linearfaktoren*

$$P_i(T) = \lambda_i(T - c(i)_1) \cdots (T - c(i)_{\deg(P_i)})$$

mit Elementen $c(i)_1, \ldots, c(i)_{\deg(P)}$ aus $K_{\mathcal{F}}$ (möglicherweise mit Wiederholungen) und dem Führungskoeffizient $\lambda_i \neq 0_k$ von $P_i(T)$. Ferner wird der Körper $K_{\mathcal{F}}$ von den Nullstellen über k erzeugt, also $K_{\mathcal{F}} = k[(c(i)_j)_{j \leq \deg(P_i), i \leq n}]$.

Insbesondere sind je zwei Zerfällungskörper für $\mathcal{F}$ über k isomorph. Des Weiteren: Gegeben eine Körpererweiterung $k \subset L$ derart, dass jedes $P_i(T)$ in Linearfaktoren über L zerfällt, lässt sich $K_{\mathcal{F}}$ in L über k einbetten.

Beweis. Weil die Menge der Nullstellen genau der Nullstellenmenge des Produktes $\prod_{i=1}^n P_i(T)$ entspricht, können wir ohne Beschränkung der Allgemeinheit annehmen, dass $\mathcal{F}$ aus einem einzigen Polynom $P(T)$ besteht. Mit Hilfe des Korollars 2.35 wähle einen irrreduziblen Faktor $P'(T)$ von $P(T)$ über k. Das Ideal $(P'(T))$ ist maximal in $k[T]$ wegen dem Beispiel 2.28 sowie der Proposition 2.30 und der Bemerkung 2.33. Der Quotientenring $k' = k[T]/(P'(T))$ ist eine endliche Körpererweiterung von k, derart, dass die Klasse $c = T + (P'(T))$ eine Nullstelle von $P'(T)$ (und somit von $P(T)$) ist. Mit Hilfe des Korollars B.7 schreibe

$$P(T) = (T - c)^{\mathrm{ord}_c(P)} H(T)$$

für ein Polynom H aus $k'[T]$ mit $\deg(H) < \deg(P)$. Falls H konstant ist, sind wir fertig. Ansonsten finden wir induktiv über den Grad des Polynoms einen Zerfällungskörper $K \supset k'$ für H. Da $k' = k[c]$, wird K von den Nullstellen von $P(T)$ über k erzeugt, das heißt K ist ein Zerfällungskörper über k.

Seien nun K_1 und K_2 Zerfällungskörper für dieselbe Familie $\mathcal{F}$ nicht-konstanter Polynomen über k. Wir konstruieren einen k-Isomorphismus zwischen K_1 und K_2 als Vereinigung einer Kette kompatibler Isomorphismen zwischen Teilkörpern von K_1 und von K_2. Ohne Beschränkung der Allgemeinheit schreibe

$$K_1 = k[c_1, \ldots, c_n] \text{ und } K_2 = k[d_1, \ldots, d_n].$$

Wir fangen damit an, $F_0 : k \to k$ gleich der Identität zu setzen. Das Element c_1 in K_1 ist Nullstelle eines Polynoms $P(T)$ aus $\mathcal{F}$, welches ohne Beschränkung der Allgemeinheit irreduzibel gewählt werden kann. Weil K_2 ein Zerfällungskörper für $\mathcal{F}$ ist, finde eine Nullstelle d_j aus K_2 für $P(T)$. Aus der Bemerkung 3.5 gibt es einen k-Isomorphismus $F_1 : k[c_1] \to k[d_j]$. Wenn d_1 bereits in $\mathrm{Im}(F_1)$ liegt, so machen wir weiter. Ansonsten ist d_1 Nullstelle eines Polynoms $Q(T) = \sum_{i=0}^{\deg(Q)} a_i T^i$ aus der Kollektion $\mathcal{F}$. Wir können annehmen, dass $Q(T)$ irreduzibel über $k[d_j]$ ist (sonst betrachte einen irreduziblen Faktor davon).

Nun ist das Polynom

$$F_1^{-1}(Q(T)) = \sum_{i=0}^{\deg(P)} F_1^{-1}(a_i) T^i$$

wiederum irreduzibel über $k[c_1] \subset K_1$. Weil K_1 ein Zerfällungskörper für $\mathcal{F}$ ist, finde eine Nullstelle c_i aus K_2 für $F_1^{-1}(Q(T))$. Die Bemerkung 3.5 liefert nun einen Isomorphismus

$$F_2 : k[d_j, d_1] \to k[c_1, c_i],$$

welcher den Isomorphismus F_1 fortsetzt (also ist F_2 auch ein k-Isomorphismus). Iteriere dieses Verfahren weiter bis alle c_i's bzw. d_j's ausgeschöpft sind.

Analog liefert das obige Verfahren eine k-Einbettung vom Zerfällungskörper $K_{\mathcal{F}}$ in jedem Oberkörper $k \subset L$ derart, dass jedes Polynom aus $\mathcal{F}$ in Linearfaktoren über L zerfällt. □

Weil ein Polynom vom Grad D höchstens D Nullstellen in einem Körper besitzt, folgt das nächste Korollar direkt aus dem Beweis der Proposition 3.11.

Korollar 3.12. *Sei $P(T)$ ein nicht-konstantes Polynom über k und K ein Zerfällungskörper von $P(T)$ über k. Dann ist $k \subset K$ endlich mit $[K : k] \leq (\deg P)!$*

Definition 3.13. Eine algebraische Körpererweiterung $k \subset K$ ist *normal*, falls K folgende Eigenschaft besitzt: Wenn ein irreduzibles Poynom $P(T)$ aus $k[T]$ eine Nullstelle in K besitzt, so zerfällt $P(T)$ über K in Linearfaktoren.

Lemma 3.14. *Eine endliche Körpererweiterung $k \subset K$ ist genau dann normal, wenn K ein Zerfällungskörper eines Polynoms mit Koeffizienten aus k ist.*

Beweis. Wir nehmen zuerst an, dass K normal ist. Die Erweiterung $k \subset K$ ist endlich, also $K = k(a_1, \ldots, a_n)$. Für jedes a_i ist das Minimalpolynom $m_{a_i}(T)$ irreduzibel und besitzt eine Nullstelle in K. Also zerfällt $m_{a_i}(T)$ in Linearfaktoren über K. Es folgt, dass

$$Q(T) = m_{a_1}(T) \cdots m_{a_n}(T)$$

in Linearfaktoren über K zerfällt. Des Weiteren wird K von den Nullstellen von $Q(T)$ erzeugt, das heißt $k \subset K$ ist ein Zerfällungskörper für $Q(T)$, wie gewünscht.

Sei nun K ein Zerfällungskörper für das Polynom $R(T)$ aus k. Wir wollen zeigen, dass K normal über k ist. Betrachte ein Element a aus K, das Nullstelle des irreduziblen Polynoms $P(T)$ aus $k[T]$ ist. Wenn wir $P(T)$ als Polynom über K betrachten, gibt es wegen der Proposition 3.11 einen Zerfällungskörper $M \supset K$. Wir müssen nur zeigen, dass $M = K$. Es genügt also zu zeigen, dass jede Nullstelle b von $P(T)$ aus M bereits in K liegt.

Nun sind die Körpererweiterung $k \subset k(a)$ und $k \subset k(b)$ isomorph über k wegen der Bemerkung 3.5. Klarerweise ist $k(a) \subset K(a) = K$ ein Zerfällungskörper für $R(T)$ (betrachtet als Polynom über $k(a)$). Insbesondere ist auch $k(b) \subset K(b)$ ein Zerfällungskörper für $R(T)$ (weil die Koeffizienten aus k kommen) und isomorph zu $k(a) \subset K(a) = K$. Aus dem Korollar 3.8 folgt, dass

$$[K(b) : k] = [K(b) : k(b)] \cdot [k(b) : k] = [K(a) : k(a)] \cdot [k(a) : k] = [K : k(a)] \cdot [k(a) : k] = [K : k].$$

Wir schließen also, dass $[K(b) : k] = [K(b) : K] \cdot [K : k] = [K : k]$ und somit $[K(b) : K] = 1$, oder äquivalent dazu, dass die Nullstelle b in K liegt, wie gewünscht. □

Mit Hilfe der obigen Charakterisierung gewinnen wir sofort folgendes Korollar.

Korollar 3.15. *Gegeben eine endliche Erweiterung $k \subset K$ gibt es einen Oberkörper $L \supset K$ mit $k \subset L$ endlich und normal, sodass $F = L$ für jeden Zwischenkörper $K \subset F \subset L$ mit $k \subset F$ normal.*

Die Erweiterung $k \subset L$ ist der normale Abschluss *der Erweiterung $k \subset K$. Je zwei normale Abschlüsse sind K-isomorph.*

Bemerkung 3.16. Sei $k \subset K$ eine normale (algebraische) Körpererweiterung. Es folgt, dass $k_1 \subset K$ wiederum normal ist, für jeden Zwischenkörper $k \subset k_1 \subset K$.

Beweis. Sei $P(T)$ ein irreduzibles Polynom aus $k_1[T]$, welches eine Nullstelle a in K besitzt. Das heißt $P(T)$ ist das Minimalpolynom von a über k_1. Das Element a aus K ist algebraisch mit Minimalpolynom $m_a(T)$ über k. Insbesondere teilt $P(T)$ das Polynom $m_a(T)$, welches in Linearfaktoren über K zerfällt, denn $k \subset K$ ist normal. Somit zerfällt auch $P(T)$ in Linearfaktoren über K, wie gewünscht. □

3.2 Separabilität

Definition 3.17. Sei K ein Körper der positiven Charakteristik $p > 0$. Der *Frobenius-Endomorphismus* ist der Endomorphismus

$$\begin{array}{rccc} \mathrm{Fr}: & K & \to & K \\ & a & \mapsto & a^p \end{array}.$$

Aus dem Korollar 2.26 folgt, dass jedes Element aus dem Primkörper $\mathbb{F}_p$ eine Nullstelle des Polynoms $T^p - T$ ist, welches höchstens p Nullstellen in einem Körper haben kann (siehe Korollar B.8). Insbesondere ist

$$\mathrm{Fix}(\mathrm{Fr}) = \{x \in K \mid \mathrm{Fr}(x) = x\} = \mathbb{F}_p.$$

Der Körper K ist *perfekt*, wenn der Frobenius-Endomorphismus ein Automorphismus ist, oder äquivalent dazu, wenn der Frobenius-Endomorphismus surjektiv ist.

Wenn der Körper K Charakteristik Null besitzt, so ist er immer *perfekt*.

Beachte, dass der Frobenius-Endomorphismus immer injektiv ist, weil Körper nullteilerfrei sind. Insbesondere gewinnen wir folgendes Lemma:

Lemma 3.18. *Endliche Körper sind perfekt.*

Bemerkung 3.19. Sei $k \subset K$ eine algebraische Erweiterung mit k perfekt. Der Körper K ist auch perfekt, denn für a aus K ist $\mathrm{Fr}(m_a)(T)$ das Minimalpolynom von $\mathrm{Fr}(a) = a^p$. Mit Hilfe des Korollars 3.8 folgt, dass $k(a) = k(a^p)$, also liegt a in $\mathrm{Im}(\mathrm{Fr})$, wie gewünscht.

Definition 3.20. Ein Polynom $P(T)$ über einem Körper k ist *separabel*, wenn $P(T)$ keine doppelte Nullstelle in einem (bzw. jedem) Zerfällungskörper $K \supset k$ besitzt.

Bemerkung 3.21. Wenn wir die formalen Ableitungen

$$\begin{array}{rccc} \frac{\partial}{\partial T}: & k[T] & \to & k[T] \\ & \sum_{i=0}^{D} a_i T^i & \mapsto & \sum_{i=1}^{D} i \cdot a_i T^{i-1} \end{array}$$

auf dem Polynomring betrachten, so folgt für $P(T) = (T-c)^2 Q(T)$, dass

$$\frac{\partial P}{\partial T}(T) = 2(T-c)Q(T) + (T-c)^2 \frac{\partial Q}{\partial T}(T) = (T-c)\Big(2Q(T) + (T-c)\frac{\partial Q}{\partial T}(T)\Big).$$

Das bedeutet, dass $P(T)$ genau dann eine doppelte Nullstelle besitzt, wenn der größte gemeinsame Teiler von $P(T)$ und seiner formalen Ableitung $\frac{\partial}{\partial T}(P)$ nicht konstant ist, aus dem Korollar 3.12. Wenn P irreduzibel ist, dann ist $P(T)$ nur inseparabel, wenn das Polynom $\frac{\partial P}{\partial T}(T)$ Null ist, denn es hat Grad echt kleiner als $\deg(P)$. In Charakteristik Null ist die formale Ableitung eines nicht-konstantes Polynoms nie Null, denn $\deg(P) \cdot a_{\deg(P)} \neq 0_K$.

In positiver Charakteristik p, beachte, dass

$$\frac{\partial P}{\partial T}(T) = \sum_{i=1}^{\deg(P)} i \cdot a_i T^{i-1} = 0_K + \sum_{\substack{i=1 \\ p \nmid i}}^{\deg(P)} i \cdot a_i T^{i-1},$$

also ist für ein irreduzibles Polynom $P(T)$ die formale Ableitung genau dann Null, wenn alle Koeffizienten der Form a_i mit i teilerfremd zu p gleich Null sind, oder äquivalent dazu, wenn $P(T) = Q(T^p)$ für ein Polynom $Q(T)$ über k. Beachte, dass $Q(T)$ irreduzibel sein muss, wenn $P(T)$ irreduzibel ist!

Wenn $Q(T)$ auch inseparabel ist, können wir das Verfahren iterieren. Jedes irreduzible Polynom $P(T)$ über k lässt sich also als $P(T) = R(T^{p^e})$ schreiben für ein e aus $\mathbb{N}$ sowie ein separables Polynom $R(T)$ aus $k[T]$.

In einem perfekten Körper k der positiven Charakteristik p ist $k = k^{p^e}$ für jedes e aus $\mathbb{N}$, was sofort das folgende Korollar liefert.

Korollar 3.22. *Wenn k perfekt ist, so ist jedes irreduzibles Polynom $P(T)$ über k separabel.*

Lemma 3.23. *Sei $k \subset K = k(a)$ eine einfache algebraische Körpererweiterung. Gegeben eine Körpererweiterung $k \subset L$ derart, dass das Minimalpolynom $m_a(T)$ in Linearfaktoren über L zerfällt (z. B. wenn L ein Zerfällungskörper für $m_a(T)$ ist), so ist die Menge der Nullstellen von $m_a(T)$ in L in Korrespondenz mit der Menge aller k-Einbettungen von K in L. Insbesondere gibt es höchstens $[k(a) : k]$ viele solche Einbettungen.*

Des Weiteren ist das Polynom $m_a(T)$ genau dann separabel, wenn die Anzahl aller k-Einbettungen von $k(a)$ in L gleich dem Grad $[k(a) : k]$ ist.

Beweis. Eine k-Einbettung $\varphi : k(a) \to L$ wird von dem Element $\varphi(a)$ eindeutig bestimmt, denn $k(a) = k[a]$ ist ein k-Vektorraum mit Basis $\{1, a, \ldots, a^{\deg(m_a)-1}\}$. Nun ist

$$0_L = \varphi(0_K) = \varphi(m_a(a)) = m_a(\varphi(a)),$$

weil φ ein k-Homomorphismus ist. Insbesondere ist $\varphi(a)$ eine Nullstelle von $m_a(T)$ aus L, wie gewünscht.

Das Polynom $m_a(T)$ ist genau dann separabel, wenn $m_a(T)$ genau $\deg(m_a)$ verschiedene Nullstellen in L besitzt, da wir annehmen, dass $m_a(T)$ in Linearfaktoren über L zerfällt. Insbesondere ist die Anzahl der k-Einbettungen gleich $\deg(m_a) = [k(a) : k]$. □

Korollar 3.24. *Normale Körpererweiterungen sind unter Automorphismen abgeschlossen: Gegeben $k \subset K \subset M$ mit $k \subset K$ normal, so ist $\varphi(K) \subset K$ (und somit ist $\varphi(K) = K$) für jeden k-Automorphismus φ von M, das heißt, die Abbildung $\varphi : M \to M$ ist ein Körperautomorphismus, welcher eingeschränkt auf k die Identität ist.*

Definition 3.25. Eine algebraische Erweiterung $k \subset K$ ist *separabel*, wenn jedes Element a aus K *separabel über* k ist, das heißt, dass es Nullstelle eines separablen Polynoms mit Koeffizienten aus k ist, oder äquivalent dazu, wenn das Minimalpolynom $m_a(T)$ aus $k[t]$ separabel ist.

Proposition 3.26. *Sei $k \subset k(a_1, \ldots, a_n)$ eine endliche Erweiterung derart, dass jedes Element a_i separabel über k ist. Gegeben eine Körpererweiterung $k \subset L$ derart, dass die Polynome $\{m_{a_i}(T)\}_{1 \leq i \leq n}$ in Linearfaktoren über L zerfallen, so gibt es genau $[k(a_1, \ldots, a_n) : k]$ viele k-Einbettungen $k(a_1, \ldots, a_n) \to L$.*

Insbesondere ist eine endliche Erweiterung $k \subset K$ genau dann separabel, wenn $K = k(b_1, \ldots, b_n)$ mit jedem b_i separabel über k.

Des Weiteren ist Separabilität transitiv*: gegeben einen Turm algebraischer (möglicherweise unendlicher) Körpererweiterungen $k \subset L \subset M$, so ist $k \subset M$ genau dann separabel, wenn $k \subset L$ und $L \subset M$ beide separabel sind.*

Beweis. Sei $k \subset k(a_1, \ldots, a_n)$ eine endliche Körpererweiterung mit jedem a_i separabel über k. Wähle eine Körpererweiterung $k \subset L$ derart, dass die Polynome $\{m_{a_i}(T)\}_{1 \leq i \leq n}$ in Linearfaktoren über L zerfallen.

Nun wird eine k-Einbettung $k(a_1, \ldots, a_n) \to L$ eindeutig bestimmt, wenn wir eine k-Einbettung $k(a_1) \to L$ finden, sowie eine entsprechende Fortsetzung $k(a_1, a_2) \to L$ usw, denn das Bild jedes Elementes aus $k(a_1, \ldots, a_n) = k[a_1, \ldots, a_n]$ wird durch die Bilder der Erzeugenden $a_1, \ldots, a_n$ eindeutig bestimmt. Wegen des Lemmas 3.23 gibt es genau $[k(a_1) : k)]$ viele k-Einbettungen $\psi_1 : k(a_1) \to L$. Das Element a_2 ist wiederum separabel über $k(a_1)$, weil sein Minimalpolynom über $k(a_1)$ das separable Polynom $m_a(T)$ teilt. Beachte, dass das Bild des Minimalpolynoms von a_2 über $k(a_1)$ für jede solche k-Einbettung ψ_1 in Linearfaktoren über L zerfällt, weil es so für $\psi_1(m_a)(T)$ gilt. Wegen des Lemmas 3.23 gibt es genau $[k(a_1, a_2) : k(a_1)]$ viele Fortsetzungen $\psi_2 : k(a_1, a_2) \to L$. Wir iterieren das Verfahren, da jedes a_i wiederum separabel über $k(a_1, \ldots, a_{i-1})$ ist, und schließen, dass es genau

$$[k(a_1) : k] \cdot [k(a_1, a_2) : k(a_1)] \cdots [k(a_1, \ldots, a_n) : k(a_1, \ldots, a_{n-1})] = [k(a_1, \ldots, a_n) : k]$$

viele k-Einbettungen von $k(a_1, \ldots, a_n) \to L$ gibt, wie gewünscht.

Wenn die endliche algebraische Erweiterung $k \subset K$ separabel ist, dann ist $K = k(b_1, \ldots, b_n)$ und jedes b_i ist separabel über k. Wir müssen also nur die Rückrichtung zeigen: Sei a aus $K = k(b_1, \ldots, b_n)$ beliebig. Mit Hilfe der Proposition 3.11 wähle eine Körpererweiterung $k \subset L$ derart, dass die Polynome $\{m_{b_i}(T)\}_{1 \leq i \leq n} \cup \{m_a(T)\}$ in Linearfaktoren über L zerfallen. Wegen des Lemmas 3.23 müssen wir nur zeigen, dass die Anzahl r der k-Einbettungen von $k(a)$ in L gleich dem Grad $[k(a) : k]$ ist.

Gegeben eine k-Einbettung $\varphi : k(a) \to L$, so ist jedes b_i wiederum separabel über dem Teilkörper $k(a, b_1, \ldots, b_{i-1})$, weil sein Minimalpolynom über $k(a, b_1, \ldots, b_{i-1})$ das Polynom $m_{b_i}(T)$ teilt. Es folgt aus dem Korollar 3.8, dass wir genau

$$r \cdot [k(a, b_1) : k(a)] \cdot [k(a, b_1, b_2) : k(a, b_1)] \cdots [k(a, b_1, \ldots, b_n) : k(a, b_1, \ldots, b_{n-1})] = r \cdot \frac{[K : k]}{[k(a) : k]}$$

verschiedene k-Einbettungen von $K = k(b_1, \ldots, b_n) = k(a, b_1, \ldots, b_n)$ in L finden. Aus der vorigen Diskussion gibt es genau $[K : k]$ viele k-Einbettungen von K in L und wir folgern, dass $r = [k(a) : k]$. Also ist das Element a separabel über k, wie gewünscht.

Sei nun $k \subset L \subset M$ eine Turm algebraischer Körpererweiterungen. Wenn $k \subset M$ separabel ist, so ist auch $k \subset L$ separabel. Ferner teilt das Minimalpolynom eines Elementes a aus M über L das Minimalpolynom $m_a(T)$ über k, welches separabel ist. Daher ist auch $L \subset M$ separabel.

Wir nehmen nun an, dass $k \subset L$ und $L \subset M$ beide separabel sind. Betrachte ein Element a aus M mit Minimalpolynom

$$P(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_0$$

mit Koeffizienten aus L. Die Erweiterung $K = k(a_0, \ldots, a_{n-1})$ ist separabel, weil $k \subset L$ separabel ist. Sei $k \subset \overline{L}$ eine Körpererweiterung derart, dass die Polynome $\{m_{a_i}(T)\}_{0 \leq i \leq n-1} \cup \{m_a(T)\}$ in Linearfaktoren über $\overline{L}$ zerfallen, wobei $m_a(T)$ das Minimalpolynom von a über k ist. Es gibt genau $[K : k]$ viele k-Einbettungen von K in $\overline{L}$. Das Bild von $P(T)$ unter jeder dieser k-Einbettungen zerfällt in verschiedene Linearfaktoren in $\overline{L}$ (weil es für $m_a(T)$ gilt!), also finden wir genau $[K(a) : K]$ viele Fortsetzungen $K(a) \to \overline{L}$. Weil jedes a_i separabel über $k(a, a_1, \ldots, a_{i-1})$ bleibt, schließen wir wie vorher, dass es genau $[k(a) : k]$ viele k-Einbettungen von $k(a) \to \overline{L}$ gibt. Somit ist das Element a separabel über k, wie gewünscht. □

Definition 3.27. Eine Körpererweiterung $k \subset K$ ist *rein inseparabel*, wenn die Charakteristik p von k (und somit auch von K) positiv ist und es für jedes Element a aus K eine natürliche Zahl n_a so gibt, dass $a^{p^{n_a}}$ in k liegt, oder äquivalent dazu, wenn das Minimalpolynom $m_a(T)$ eine einzige Nullstelle in jedem Zerfällungskörper besitzt.

In Charakteristik Null ist die einzige *rein inseparable Körpererweiterung* die triviale Erweiterung.

Wegen des Lemmas 3.23 gibt es eine einzige Einbettung einer rein separablen Erweiterung in einem passenden Zerfällungskörper.

Korollar 3.28. *Jede algebraische (möglicherweise unendliche) Körpererweiterung $k \subset K$ lässt sich zerlegen als $k \subset L \subset K$ mit $k \subset L$ separabel und $L \subset K$ rein inseparabel. Der Körper*

$$L = \{a \in K \mid a \text{ ist separabel über } k\}$$

ist eindeutig bestimmt und heißt der separable Abschluss *von k in K.*

Beweis. Beachte zuerst, dass die Menge

$$L = \{a \in K \mid a \text{ ist separabel über } k\}$$

ein Teilkörper von K ist, weil die Elemente $-a, a^{-1}, a + b$ und $a \cdot b$ im Körper $k(a, b)$ liegen, welcher wiederum separabel ist aus der Proposition 3.26.

Klarerweise ist $k \subset L$ separabel. Wenn die Charakteristik Null ist, so ist $L = K$, welches trivialerweise rein inseparabel ist. Wir müssen nur noch zeigen, dass die Körpererweiterung $L \subset K$ rein inseparabel ist, wenn die Charakteristik $p > 0$ ist. Sei also a aus K und betrachte sein Minimalpolynom $m_a(T)$ über k. Mit Hilfe der Bemerkung 3.21 schreibe $m_a(T) = Q(T^{p^e})$ für eine natürliche Zahl e sowie ein separables Polynom $Q(T)$ mit Koeffizienten aus k. Das bedeutet, dass a^{p^e} Nullstelle eines separables Polynom über k ist. Also ist die Erweiterung $k \subset k(a^{p^e})$ separabel und somit liegt a^{p^e} in L. Es folgt direkt aus der Definition, dass die Erweiterung $L \subset K$ rein inseparabel ist, wie gewünscht. □

Satz 3.29. (*Der Satz des primitiven Elements für unendliche Körper*) *Sei k ein unendlicher Körper. Jede endliche separable Körpererweiterung $k \subset K$ besitzt ein primitives Element: es gibt ein Element c aus K mit $K = k(c)$.*

Der Beweis zeigt sogar, dass die meisten (bis auf endlich viele Ausnahmen) der Elemente aus K primitiv sind. Hier benutzen wir stark, dass der Körper k unendlich ist.

Beweis. Ohne Beschränkung der Allgemeinheit können wir annehmen, dass K nur zwei Erzeugende über k braucht, also $K = k(a, b)$. Setze nun $c = a - \lambda b$ (wobei λ noch zu bestimmen ist). Wir werden zeigen, dass c für fast jede Wahl von λ (bis auf endlich viele) ein primitives Element der Körpererweiterung $k \subset K$ ist. Es genügt also zu zeigen, dass b in $k(c) \subset K$ liegt.

Mit Hilfe der Proposition 3.11 wähle eine Körpererweiterung $k \subset L$ derart, dass die Minimalpolynome $m_a(T)$ von a über k und $m_b(T)$ von b über k in (lauter verschiedene) Linearfaktoren über L zerfallen. Aus dem Lemma 3.23 können wir sogar annehmen, dass L ein Oberkörper von K ist. Betrachte nun das Polynom $P(T) = m_a(c + \lambda T)$ mit Koeffizienten aus $k(c)$. Klarerweise ist b eine Nullstelle von $P(T)$. Das Minimalpolynom $R(T)$ von b über $k(c)$ teilt $P(T)$ und auch $m_b(T)$. Wenn wir zeigen, dass der größte gemeinsame Teiler der Polynome $P(T)$ und $m_b(T)$ Grad 1 hat, folgt, dass $R(T) = (T - \mu)$ für ein μ aus $k(c)$ und somit liegt $b = \mu$ in $k(c)$, wie gewünscht.

Da $m_a(T)$ und $m_b(T)$ in lauter verschiedene Linearfaktoren in L zerfallen, hätte der größte gemeinsame Teiler der Polynome $P(T)$ und $m_b(T)$ Grad mindestens 2, wenn es eine Nullstelle $b' \neq b$ von $m_b(T)$ derart gäbe, dass $P(b') = 0_K$. Das bedeutet, dass $c + \lambda b' = a'$ eine Nullstelle von $m_a(T)$ ist. Da $c = a + \lambda b$, schließen wir, dass

$$\lambda = \frac{a - a'}{b - b'}.$$

Es gibt nur endlich viele Nullstellen von $m_a(T)$ und $m_b(T)$, also auch nur endlich viele λ's aus k, welche sich so schreiben lassen können. Für alle andere λ's aus k folgt, dass das Element c ein primitives Element der Körpererweiterung $k \subset K = k(a, b)$ ist. □

Bemerkung 3.30. Der obige Beweis lässt sich leicht adaptieren, um folgende Behauptung zu zeigen: Sei $k \subset K$ eine endliche Körpererweiterung mit k unendlich und derart, dass es nur endlich viele Zwischenkörper $k \subset L \subset K$ gibt. Dann ist $k \subset K$ einfach, also $K = k(c)$ für ein primitives Element c aus K.

In der Tat finden wir zwei verschiedene Werte $x \neq x'$ aus k mit $c = ax + b$, dass $k(c) = k(ax + b) = k(ax' + b)$. Somit liegt

$$a = \frac{(ax + b) - (ax' - b)}{x - x'}$$

in $k(c)$ und wir schließen, dass $k(a, b) = k(c)$, wie gewünscht.

3.3 Endliche Körper

Beachte, dass ein endlicher Körper $\mathbb{F}$ positiver Charakteristik sein muss, weil die Kollektion endlicher Summen $1_{\mathbb{F}} + \cdots + 1_{\mathbb{F}}$ endlich sein muss. Wenn p die Charakteristik von $\mathbb{F}$ ist, so enthält $\mathbb{F}$ den Primkörper $\mathbb{F}_p$. Klarerweise ist die Lineardimension des $\mathbb{F}_p$-Vektorraumes endlich, also $[\mathbb{F} : \mathbb{F}_p] = n$ für eine natürliche Zahl $n \geq 1$. Insbesondere ist $|\mathbb{F}| = p^n = q$.

Die multiplikative Gruppe $(\mathbb{F} \setminus \{0\}, \cdot)$ ist endlich, also $a^{q-1} = 1_{\mathbb{F}}$ für jedes $a \neq 0_{\mathbb{F}}$ aus $\mathbb{F}$. Dies bedeutet, dass jedes Element a aus $\mathbb{F}$ eine Nullstelle des Polynoms $P(T) = T^q - T$ mit

Koeffizienten aus $\mathbb{F}_p$ ist. Dieses Polynom ist klarerweise separabel, denn

$$\frac{\partial P}{\partial T}(T) = -1_{\mathbb{F}} \neq 0_{\mathbb{F}}.$$

Des Weiteren zerfällt $P(T)$ in lauter verschiedene Linearfaktoren über $\mathbb{F}$, also ist $\mathbb{F}$ ein Zerfällungskörper vom Polynom $P(T)$ und somit bis auf Isomorphie eindeutig bestimmt. Schreibe also $\mathbb{F}_q$ für den (bis auf Isomorphie eindeutig bestimmten) Körper mit genau $q = p^n$ Elementen.

Bemerkung 3.31. Sei $q = p^n$. Jeder Teilkörper $K \subset \mathbb{F}_q$ ist bis auf Isomorphie der Form $K = \mathbb{F}_{p^m}$.

Des Weiteren, wenn m die Zahl n teilt, so ist (bis auf Isomorphie) $\mathbb{F}_{p^m}$ ein Teilkörper von $\mathbb{F}_{p^n}$, nämlich

$$\mathbb{F}_{p^m} = \{x \in \mathbb{F}_{p^n} \mid \mathrm{Fr}^m(x) = \underbrace{\mathrm{Fr} \circ \cdots \circ \mathrm{Fr}}_{m}(x) = x\}.$$

Beweis. Sei $K \subset \mathbb{F}_q$. Nach dem Korollar 3.8 ist

$$n = [\mathbb{F}_q : \mathbb{F}_p] = [\mathbb{F}_q : K][K : \mathbb{F}_p],$$

also teilt $[K : \mathbb{F}_p] = m$ die Zahl n und $K = \mathbb{F}_{p^m}$.

Wir nehmen nun an, dass m die Zahl n teilt mit $n = mr$. Beachte, dass

$$p^n - 1 = (p^m - 1)(p^{(r-1)m} + p^{(r-2)m} \cdots + p^m + 1).$$

Insbesondere teilt $p^m - 1$ die Zahl $p^n - 1$ und das Polynom $T^{p^m-1} - 1$ teilt daher $T^{p^n-1} - 1$. Das bedeutet, dass jede Nullstelle von $T^{p^m} - T$ wiederum eine Nullstelle von $T^{p^n} - T$ ist. Da $\mathbb{F}_q$ ein Zerfällungskörper von $T^{p^n} - T$ ist, lässt sich $\mathbb{F}_{p^m}$ in $\mathbb{F}_q$ einbetten. Beachte, dass jedes Element aus $\mathbb{F}_{p^m}$ (als Teilmenge von $\mathbb{F}_q$) von dem Automorphismus Fr^m fixiert wird. Ein Element a aus $\mathbb{F}_q$ mit $\mathrm{Fr}^m(a) = a$ ist also eine Nullstelle von $T^{p^m} - T$ und liegt somit in $\mathbb{F}_{p^m}$. □

Proposition 3.32. *Sei K ein (endlicher oder unendlicher) Körper. Jede endliche Untergruppe G der multiplikativen Gruppe $(K \setminus \{0_K\}, \cdot)$ ist zyklisch.*

Insbesondere ist jede multiplikative Untergruppe eines endlichen Körpers zyklisch.

Beweis. Beachte, dass G eine endliche abelsche Gruppe ist, also schreibe (bis auf Isomorphie)

$$G = \bigoplus_{q,e} (\mathbb{Z}/q^e\mathbb{Z})^{n(q,e)}$$

mit Hilfe des Satzes 1.56. Wegen des Korollars 1.53 genügt es zu zeigen, dass kein Exponent $n(q, e) \geq 2$ oder dass für eine Primzahl q zwei verschiedene q-Untergruppen gleichzeitig vorkommen.

In beiden Fällen würde aus dem Lemma 1.57 folgen, dass es in G mehr als q Elemente a gibt, sodass $a^q = 1_K$. Aber das Polynom $T^q - 1_K$ kann wegen des Korollars B.8 höchstens q Nullstellen im Körper K besitzen, was den gewünschten Widerspruch liefert. □

Korollar 3.33. (*Der Satz des primitiven Elements für endliche Körper*) *Sei $\mathbb{F}$ ein endlicher Körper. Jede endliche (separable) Körpererweiterung $\mathbb{F} \subset K$ besitzt ein primitives Element: es gibt ein Element c aus K mit $K = \mathbb{F}(c)$.*

Der Beweis ist wesentlich einfacher als der Beweis des Satzes 3.29 für unendliche Körper. Wir benötigen die Separabilität der Körpererweiterung im Beweis nicht.

Beweis. Beachte, dass K ein $\mathbb{F}$-Vektorraum endlicher Dimension ist und somit auch K endlich ist. Die multiplikative Gruppe $K \setminus \{0_K\}$ ist zyklisch aus der Proposition 3.32. Wähle also ein erzeugendes Element c. Jedes Element aus K ist Null oder eine Potenz von c, also $K \subset \mathbb{F}(c) \subset K$. □

Korollar 3.34. *Sei $\mathbb{F}$ ein endlicher Körper. Für jede natürliche Zahl $n \geq 1$ gibt es ein irreduzibles (normiertes) Polynom über $\mathbb{F}$ vom Grad n.*

Beweis. Schreibe $\mathbb{F} = \mathbb{F}_q$ mit $q = p^e$ und betrachte $L = \mathbb{F}_{(p^e)^n}$. Dann ist L ein endlicher Körper mit $[L : \mathbb{F}] = n$. Aus dem Satz des primitiven Elementes 3.33 folgt die Existenz eines Elementes a aus L mit $L = \mathbb{F}(a)$. Das Minimalpolynom $m_a(T)$ von a über $\mathbb{F}$ hat Grad n und ist irreduzibel, wie gewünscht. □

Korollar 3.35. *Sei k ein (endlich oder unendlicher) Körper. Jede endliche separable Körpererweiterung $k \subset K$ besitzt nur endlich viele Teilkörper L mit $k \subset L \subset K$.*

Beweis. Aus dem Satz 3.29 und dem Korollar 3.33 folgt, dass K ein primitives Element a über k besitzt. Mit Hilfe der Proposition 3.11 wähle eine Körpererweiterung $k \subset M$ derart, dass das Minimalpolynom $m_a(T)$ von a über k in (lauter verschiedene) Linearfaktoren über M zerfällt. Wegen des Lemmas 3.23 können wir sogar annehmen, dass M ein Oberkörper von K ist.

Sei nun L ein Teilkörper von K mit $k \subset L \subset K$. Das Minimalpolynom $P(T)$ von a über L hat Koeffizienten $b_0, \ldots, b_{r-1}$. Setze $L' = k(b_0, \ldots, b_{r-1})$. Beachte, dass $L' \subset L$ und dass $P(T)$ auch das Minimalpolynom von a über L' ist. Wegen des Korollars 3.8 ist

$$\deg(P) = [K : L'] = [K : L] \cdot [L : L'] = \deg(P) \cdot [L : L'],$$

also $[L : L'] = 1$ und $L = L'$. Es folgt somit, dass jeder Teilkörper L von den Koeffizienten eines normierten Teilers $P(T)$ vom Minimalpolynom $m_a(T)$ erzeugt wird. Solche Teiler entstehen aus einer geeigneten Wahl der Zerlegung in Linearfaktoren von $m_a(T)$ über M (nicht jede Wahl liefert ein Polynom mit Koeffizienten in einem Teilkörper von K!). Es gibt also nur endlich viele Möglichkeiten und somit auch nur endlich viele solche Teilkörper L, wie gewünscht. □

Aufgabe. Beschreibe das Gitter der Teilkörper von $\mathbb{F}_{2^{30}}$ mit den entsprechenden Inklusionen.

3.4 Die Galoiskorrespondenz

Definition 3.36. Eine algebraische Körpererweiterung $k \subset K$ ist *galoissch* (benannt nach Évariste Galois), falls sie separabel und normal ist.

Bemerkung 3.37. Gegeben eine galoissche Körpererweiterung $k \subset K$, betrachte die *Galoisgruppe*

$$\mathrm{Gal}(K/k) = \{\varphi : K \to K \mid \varphi \text{ ist ein } k\text{-Automorphismus}\},$$

welche klarerweise eine Untergruppe von $\mathrm{Aut}(K)$ ist.

Wir nehmen nun an, dass die galoissche Körpererweiterung $k \subset K$ endlich ist. Aus dem Satz des primitiven Elements 3.29 & 3.33 folgt, dass die separable Körpererweiterung $k \subset K$

einfach ist, also $K = k(a)$ für ein a aus K. Das Minimalpolynom $m_a(T)$ hat Grad $n = [K : k]$ und zerfällt in Linearfaktoren über K, weil $k \subset K$ normal ist. Jeder k-Automorphismus φ aus $\mathrm{Gal}(K/k)$ wird von $\varphi(a)$ eindeutig bestimmt, denn

$$\begin{array}{rccc} \varphi: & K & \to & K \\ & \sum_{j=0}^{n-1} b_j a^j & \mapsto & \sum_{j=0}^{n-1} b_j \varphi(a)^j. \end{array} .$$

Das Element $\varphi(a)$ ist wiederum eine Nullstelle des Minimalpolynoms $m_a(T)$. Es folgt aus dem Lemma 3.23, dass die Gruppe $\mathrm{Gal}(K/k)$ endlich ist mit

$$|\mathrm{Gal}(K/k)| = [K : k].$$

Bemerkung 3.38. Gegeben eine galoissche Körpererweiterung $k \subset K$ sowie einen Zwischenkörper $k \subset F \subset K$, so ist $F \subset K$ wiederum galoissch, wegen der Bemerkung 3.16 und der Proposition 3.26. Insbesondere ist $\mathrm{Gal}(K/F)$ eine Untergruppe von $\mathrm{Gal}(K/k)$.

Für jede endliche separable Erweiterug $k \subset L$ gibt es eine Körpererweiterung $L \subset K$ mit $k \subset K$ galoissch und $[K : k] \leq [L : k]!$ wegen des Korollars 3.12: In der Tat, der Satz des primitiven Elementes 3.29 & 3.33 liefert, dass die Erweiterung $k \subset L$ einfach ist. Der Zerfällungskörper K eines separablen Polynoms liefert wiederum eine separable Körpererweiterung wegen der Proposition 3.26.

Satz 3.39. (*Der Hauptsatz der Galoistheorie*) *Sei $k \subset K$ eine endliche galoissche Körpererweiterung mit entsprechender* Galoisgruppe

$$\mathrm{Gal}(K/k) = \{\varphi : K \to K \mid \varphi \textit{ ist ein } k\textit{-Automorphismus}\}.$$

Betrachte die Kollektion $\mathcal{K}$ aller Zwischenkörper $k \subset F \subset K$ sowie die Kollektion $\mathcal{H}$ aller Untergruppen $H \leq \mathrm{Gal}(K/k)$. Die Abbildung

$$\begin{array}{rccc} \mathcal{F}: & \mathcal{K} & \to & \mathcal{H} \\ & F & \mapsto & \mathrm{Gal}(K/F) \end{array}$$

ist eine Bijektion mit inverser Abbildung

$$\begin{array}{rccc} \mathcal{F}^{-1}: & \mathcal{H} & \to & \mathcal{K} \\ & H & \mapsto & \mathrm{Fix}(H) = \{x \in K \mid \varphi(x) = x \textit{ für alle } \varphi \textit{ aus } H\} \end{array} .$$

Des Weiteren ist $\mathcal{F}$ kontravariant*:*

$$F_1 \subset F_2 \textit{ genau dann, wenn } \mathcal{F}(F_2) \leq \mathcal{F}(F_1).$$

Da $\mathrm{Gal}(K/k) = \mathcal{F}(k)$, gilt insbesondere dass $F = k$, wenn alle φ aus $\mathrm{Gal}(K/k)$ den Zwischenkörper F fixieren.

Beweis. Beachte, dass $\mathcal{F}$ und $\mathcal{F}^{-1}$ wohldefiniert sind. Die Menge $\mathrm{Fix}(H)$ ist ein Teilkörper von K und enthält k, aus der Definition von $\mathrm{Gal}(K/k)$.

Wir zeigen zuerst, dass $\mathcal{F}^{-1} \circ \mathcal{F}(F) = F$, was sofort die Injektivität von $\mathcal{F}$ liefert: Klarerweise ist $F \subset F_1 = \mathrm{Fix}(\mathrm{Gal}(K/F))$. Nun ist die Erweiterung $F \subset K$ wiederum galoissch mit

$|\operatorname{Gal}(K/F)| = [K : F]$ wegen der Bemerkung 3.37. Sei a aus F_1 mit Minimalpolynom $m_a(T)$ über F. Da $F \subset K$ normal ist, zerfällt $m_a(T)$ in Linearfaktoren. Die Automorphismen φ aus $\operatorname{Gal}(K/F)$ sind in Korrespondenz mit der Kollektion $\{\varphi(a)\}$ von Nullstellen von $m_a(T)$ (in K). Das Element a liegt in $\operatorname{Fix}(\operatorname{Gal}(K/F))$, also gibt es eine einzige Nullstelle für das Minimalpolynom. Da die Erweiterung $F \subset F_1$ wegen der Proposition 3.26 separabel ist, schließen wir, dass a in F liegt, also $F = F_1 = \operatorname{Fix}(\operatorname{Gal}(K/F))$, wie gewünscht.

Wir zeigen zuletzt, dass $\mathcal{F} \circ \mathcal{F}^{-1}(H) = H$. Sei $F = \operatorname{Fix}(H)$, also ist $\mathcal{F}(F) = \operatorname{Gal}(K/F)$ eine Untergruppe von $\operatorname{Gal}(K/k)$ mit $H \leq \operatorname{Gal}(K/F)$. Wir müssen nur zeigen, dass $|\operatorname{Gal}(K/F)| = [K : F] \leq |H|$. Aus dem Satz des primitiven Elements 3.29 & 3.33 folgt $K = k(a)$ für ein primitives Element a aus K. Betrachte das normierte Polynom

$$P(T) = \prod_{\varphi \in H} (T - \varphi(a)) = T^{|H|} + c_{|H|-1}T^{|H|-1} + \cdots + c_1 T + c_0,$$

wobei der Koeffizient

$$c_{|H|-j} = (-1)^j \sum_{\varphi_1,\ldots,\varphi_j \in H} \varphi_1(a) \cdots \varphi_j(a)$$

die j-te *elementare symmetrische Funktion* auf der Menge $\{\varphi(a)\}_{\varphi \in H}$ ist. Klarerweise liegt jeder Koeffizient $c_{|H|-j}$ in $F = \operatorname{Fix}(H)$. Es folgt, dass a Nullstelle eines (möglicherweise nicht irreduziblen) normierten Polynoms vom Grad $|H|$ mit Koeffizienten aus F ist, also $[K : F] \leq |H|$, wie gewünscht. □

Mit Hilfe der Bemerkungen 1.27 und 3.37 schließen wir folgendes Korollar.

Korollar 3.40. *Gegeben Zwischenkörper $k \subset F_1 \subset F_2 \subset K$ mit $k \subset K$ endlich galoissch, so gilt*

$$[F_2 : F_1] = \big(\operatorname{Gal}(K/F_1) : \operatorname{Gal}(K/F_2)\big).$$

Aufgabe. Sei k ein Teilkörper des Oberkörpers K sowie einen Zwischenkörper $k \subset L \subset K$ derart, dass $k \subset L$ galoissch ist. Gegeben α aus K algebraisch über k, zeige, dass die Erweiterung $k(\alpha) \subset L(\alpha)$ wiederum galoissch ist. Des Weiteren ist die Abbildung

$$\begin{array}{ccc} \operatorname{Gal}(L(\alpha)/k(\alpha)) & \to & \operatorname{Gal}(L/k) \\ \varphi & \mapsto & \varphi_{\restriction K} \end{array}$$

ein wohldefinierter Gruppenmonomorphismus (mit Hilfe des Korollars 3.24).

Sind die Galoisgruppen $\operatorname{Gal}(L(\alpha)/k(\alpha))$ und $\operatorname{Gal}(L/k)$ immer isomorph?

Proposition 3.41. *Gegeben eine endliche galoissche Körpererweiterung und einen Zwischenkörper $k \subset F \subset K$, so ist $k \subset F$ genau dann normal (und somit galoissch), wenn $\varphi(F) = F$ für jedes φ aus $\operatorname{Gal}(K/k)$ (vergleiche dies mit dem Korollar 3.24).*

Insbesondere ist $k \subset F$ genau dann normal, wenn die Untergruppe $\operatorname{Gal}(K/F)$ ein Normalteiler von $\operatorname{Gal}(K/k)$ ist. In diesem Fall ist $\operatorname{Gal}(F/k)$ isomorph zu der Quotientengruppe $\operatorname{Gal}(K/k)/\operatorname{Gal}(K/F)$ durch den Gruppenisomorphismus

$$\begin{array}{ccc} \operatorname{Gal}(K/k)/\operatorname{Gal}(K/F) & \to & \operatorname{Gal}(F/k)\ . \\ \varphi \cdot \operatorname{Gal}(K/F) & \mapsto & \varphi_{\restriction F} \end{array}$$

Beweis. Wir nehmen zuerst an, dass F unter k-Automorphismen von K abgeschlossen ist. Wir zeigen, dass $k \subset F$ normal ist mit Hilfe des Lemmas 3.14. Schreibe $F = k(b_1, \ldots, b_r)$ für gewisse Elemente $b_1, \ldots, b_r$. Beachte, dass das Mimimalpolynom $m_{b_i}(T)$ über k in Linearfaktoren über K zerfällt (weil $k \subset K$ normal ist). Die Nullstellen von $m_{b_i}(T)$ sind in Korrespondenz mit den Bildern $\{\varphi(b_i)\}_{\varphi \in \mathrm{Gal}(K/k)}$, welche in F liegen, weil $\varphi(F) = F$. Es folgt, dass F der Zerfällungskörper der Familie $\{m_{b_1}(T), \ldots, m_{b_r}(T)\}$ von Polynomen über k ist, und somit ist die Körpererweiterung $k \subset F$ normal.

Gegeben nun φ aus $\mathrm{Gal}(K/k)$, so ist $\mathrm{Gal}(K/\varphi(F)) = \mathcal{F}(\varphi(F)) = \mathrm{Gal}(K/F)^{\varphi^{-1}}$ wegen des Satzes 3.39, denn die Untergruppe $\mathrm{Gal}(K/F)^{\varphi^{-1}}$ fixiert genau den Zwischenkörper $\varphi(F)$. Es folgt aus der obigen Diskussion, dass $k \subset F$ genau dann normal ist, wenn die Untergruppe $\mathrm{Gal}(K/F)$ ein Normalteiler von $\mathrm{Gal}(K/k)$ ist.

Wenn die Erweiterung $k \subset F$ normal ist, dann ist die Abbildung

$$\begin{array}{rccc} \Phi: & \mathrm{Gal}(K/k) & \to & \mathrm{Gal}(F/k) \\ & \varphi & \mapsto & \varphi_{\restriction F} \end{array}$$

wohldefiniert wegen des Korollars 3.24. Beachte, dass die Abbildung Φ ein Gruppenhomomorphismus ist, dessen Kern gleich dem Normalteiler $\mathrm{Gal}(K/F)$ ist. Wir müssen nur zeigen, dass die Abbildung surjektiv ist: Sei also ψ ein Element aus $\mathrm{Gal}(F/k)$. Die Körpererweiterung $F \subset K$ ist wiederum galoissch, also $K = F(a)$ für ein primitives Element a von K über F. Definiere nun

$$\begin{array}{rccc} \widetilde{\psi}: & K & \to & K \\ & \sum_{j=0}^{s-1} b_j a^j & \mapsto & \sum_{j=0}^{s-1} \psi(b_j) a^j. \end{array} .$$

Die Abbildung $\widetilde{\psi}$ ist ein Element aus $\mathrm{Gal}(K/k)$, weil ψ ein k-Automorphismus ist. Des Weiteren setzt $\widetilde{\psi}$ den Automorphismus ψ fort, wie gewünscht. □

3.5 Der algebraische Abschluss eines Körpers

Definition 3.42. Der Körper K ist *algebraisch abgeschlossen*, wenn jedes nicht-konstante Polynom über K eine Nullstelle in K besitzt.

Bemerkung 3.43. Weder $\mathbb{R}$ noch $\mathbb{Q}$ sind algebraisch abgeschlossen, weil das Polynom $T^2 + 1$ mit ganzzahligen Koeffizienten keine Nullstelle in diesen Körpern besitzt. Der Körper $\mathbb{C}$ der komplexen Zahlen ist algebraisch abgeschlossen, wegen des Fundamentalsatzes der Algebra (siehe Appendix C).

Lemma 3.44. *Folgende Aussagen sind für einen Körper K äquivalent:*

(a) Der Körper ist algebraisch abgeschlossen.

(b) Jedes nicht-konstante Polynom $P(T)$ aus $K[T]$ zerfällt in Linearfaktoren über K.

(c) Die einzigen irreduziblen nicht-konstanten Polynome aus $K[T]$ sind linear.

Beweis. $(a) \Rightarrow (b)$: Mit Hilfe des Korollars B.8 schreibe

$$P = (T - c_1) \cdots (T - c_k) P_0$$

für eine natürliche Zahl $k \leq \deg(P)$ und ein Polynom P_0 ohne Nullstellen in K. Insbesondere muss P_0 konstant sein, weil K algebraisch abgeschlossen ist. Da P nicht-konstant ist, haben wir $P_0 = \lambda \neq 0_K$ und somit $k = \deg(P)$, wie gewünscht.

$(b) \Rightarrow (c)$: Diese Richtung ist trivial.

$(c) \Rightarrow (a)$: Sei $P(T)$ ein beliebiges nicht-konstantes Polynom über K. Mit Hilfe des Korollars 2.35 lässt sich $P(T)$ als ein Produkt irreduzibler Polynome über K schreiben. Da $P(T)$ nicht konstant ist, muss es einen Faktor $Q(T)$ geben, welcher nicht-konstant ist. Nun ist $Q(T)$ selbst linear aus unserer Annahme und besitzt insbesondere eine Nullstelle in K. Jede Nullstelle von $Q(T)$ ist auch eine Nullstelle von $P(T)$. Somit ist K algebraisch abgeschlossen. □

Bemerkung 3.45. Ein Körper K ist genau dann algebraisch abgeschlossen, wenn K keine echte algebraische Körpererweiterung besitzt.

Beweis. Beachte zuerst, dass ein Körper K genau dann keine echten algebraischen Körpererweiterungen besitzt, wenn K keine echten endlichen algebraischen Körpererweiterungen besitzt. Eine endliche algebraische Körpererweiterung von K ist isomorph über K zu der Körpererweiterung $K \subset K[T]/(P(T))$, wobei $P(T)$ ein nicht-konstantes irreduzibles Polynom ist, aus der Bemerkung 3.4. Diese Körpererweiterung ist genau dann trivial, wenn $P(T)$ linear ist. □

Definition 3.46. Ein *algebraischer Abschluss* des Körpers k ist eine algebraische Erweiterung $k \subset K$ derart, dass K algebraisch abgeschlossen ist.

Lemma 3.47. *Sei $\varphi : k \to k'$ ein Körperisomorphismus sowie K und K' algebraische Abschlüsse von k, beziehungsweise von k'. Es gibt eine Fortsetzung $\widetilde{\varphi} : K \to K'$ zu einem Körperisomorphismus.*

Insbesondere sind je zwei algebraische Abschlüsse des Körpers k isomorph über k.

Beweis. Der Beweis ist eine typische Anwendung des Zorn'schen Lemmas A.3. Betrachte die Kollektion von Tripeln

$$\mathcal{S} = \left\{ (F, F', \psi) \;\middle|\; \begin{array}{c} k \subset F \subset K \text{ und } k' \subset F' \subset K' \text{ sind Zwischenkörper} \\ \text{und} \\ \psi : F \to F' \text{ Isomorphismus, welcher } \varphi \text{ fortsetzt} \end{array} \right\}$$

mit der folgenden partiellen Ordnung

$$(F_1, F_1', \psi_1) \leq (F_2, F_2', \psi_2) \iff F_1 \subset F_2, F_1' \subset F_2' \text{ und } \psi_{2\restriction F_1} = \psi_1.$$

Wir wollen zeigen, dass $\mathcal{S}$ induktiv ist (siehe A.1). Sei Γ also eine linear geordnete Teilmenge von S. Falls $\Gamma = \emptyset$, dann ist das Tripel (k, k', φ) aus $\mathcal{S}$ bereits eine obere Schranke. Falls $\Gamma \neq \emptyset$, sind die Zwischenkörper

$$M = \bigcup_{(F,F',\psi)\in\Gamma} F = \{a \in K \mid \text{ es gibt ein } (F, F', \psi) \text{ aus } \Gamma \text{ mit } a \in F\}$$

und

$$M' = \bigcup_{(F,F',\psi)\in\Gamma} F' = \{b \in K' \mid \text{ es gibt ein } (F, F', \psi) \text{ aus } \Gamma \text{ mit } b \in F'\}$$

isomorph durch die Fortsetzung $\widetilde{\psi}$ von φ mit

$$\widetilde{\psi} = \bigcup_{(F,F',\psi)\in\Gamma} \psi = \{(a,b) \in K \times K' \mid \psi(a) = b, \text{ falls } a \in F, b \in F' \text{ und } (F,F',\psi) \in \Gamma\}.$$

Klarerweise liegt $(M, M', \widetilde{\psi})$ in $\mathcal{S}$ und ist eine obere Schranke für jedes Tripel (F, F', ψ) aus Γ.

Aus dem Zorn'schen Lemma A.3 folgt, dass ein maximales Element (F, F', ψ) in $\mathcal{S}$ existiert. Per Definition sind F und F' Zwischenkörper von K und K' und isomorph bezüglich der Fortsetzung ψ von φ. Wir müssen nur zeigen, dass $F = K$ und $F' = K'$. Sei a aus K beliebig. Da die Körpererweiterung $F \subset K$ algebraisch ist, betrachte das Minimalpolynom $m_a(T)$ über F. Wegen der Bemerkung 3.5 gibt es eine Fortsetzung $\psi_1 : F(a) \to F'(b)$, wobei a' aus K' eine Nullstelle des nicht-konstanten Polynoms $\psi(m_a(T))$ ist (Wir finden immer ein solches a', denn K' ist algebraisch abgeschlossen). Das Tripel $(F(a), F'(a'), \psi_1)$ liegt in $\mathcal{S}$, also folgt $F(a) = F$ aus der Maximalität des Tripels (F, F', ψ). Analog lässt sich zeigen, dass $K' = F'$, wie gewünscht. □

Aufgabe. Es folgt aus der Bemerkung 3.31, dass der Körper $\overline{\mathbb{F}_p} = \bigcup_{n\in\mathbb{N}} \mathbb{F}_{p^n}$ algebraisch abgeschlossen ist. Aus dem Korollar 3.34 folgt, dass $\overline{\mathbb{F}_p}$ sich in jeden algebraisch abgeschlossenen Körper der Charakteristik p einbetten lässt, so $\overline{\mathbb{F}_p}$ ist ein algebraischer Abschluss des endlichen Körper $\mathbb{F}_p$.

Bemerkung 3.48. Es lässt sich mit Hilfe des Zorn'schen Lemmas A.3 und mit dem Hauptsatz der Algebra C.1 leicht zeigen, dass der Körper $\mathbb{Q}$ einen algebraischen Abschluss besitzt, welchen wir nach dem Lemma 3.47 mit den Notationen $\overline{\mathbb{Q}}$ oder $\mathbb{Q}^{alg}$ bezeichnen werden (beide Schreibweisen kommen in der Literatur häufig vor).

In der Tat, betrachte die Kollektion

$$\mathcal{S} = \{F \subset \mathbb{C} \mid \mathbb{Q} \subset F \text{ ist eine algebraische Körpererweiterung}\}$$

mit der durch Inklusion gegebenen partiellen Ordnung. Es lässt sich leicht zeigen, dass $\mathcal{S}$ induktiv ist (siehe A.1). Wähle also mit Hilfe des Zorn'schen Lemmas ein maximales Element K aus $\mathcal{S}$. Wir müssen nur noch zeigen, dass jedes nicht-konstante Polynom $P(T)$ aus $K[T]$ eine Nullstelle in K besitzt. Nun, weil $\mathbb{C}$ algebraisch abgeschlossen ist (siehe Satz C.1), besitzt $P(T)$ eine Nullstelle a aus $\mathbb{C}$. Die algebraische Körpererweiterung $K \subset K(a)$ liefert einen Teilkörper $K(a)$ von $\mathbb{C}$, welcher über $\mathbb{Q}$ algebraisch ist, da $\mathbb{Q} \subset K$ algebraisch ist. Insbesondere liegt $K(a)$ in $\mathcal{S}$, also $K = K(a)$ aus der Maximalität von K. Das Polynom $P(T)$ besitzt eine Nullstelle in K, wie gewünscht. Leider können wir diesen Beweis nicht direkt für beliebige Körper verallgemeinern, sodass wir einen alternativen Beweis 3.50 liefern werden.

Weil eine algebraische Körpererweiterung eines abzählbaren Körpers k wiederum abzählbar ist (denn es gibt nur abzählbar viele Polynome über k), folgt, dass (je)der algebraische Abschluss $\mathbb{Q}^{alg}$ von $\mathbb{Q}$ abzählbar ist. Insbesondere ist $\mathbb{C}$ kein algebraischer Abschluss von $\mathbb{Q}$: Es muss Elemente aus $\mathbb{C}$ geben, welche transzendent über $\mathbb{Q}$ sind. Zum Beispiel folgt aus dem Satz von Hermite-Lindemann-Weierstraß, dass die komplexen Zahlen π und e transzendent sind (wir werden die Beweise in dieser Vorlesung nicht sehen, weil hierfür tiefe Kenntnisse der Analysis benötigt werden).

Die Konstruktion des algebraischen Abschlusses in der Bemerkung 3.48 war nicht explizit. Wir werden demnächst einen alternativen Beweis liefern, welcher die Stärke der Galoistheorie

verwendet. Der algebraische Abschluss entsteht als Quotientenring nachdem wir ein geeignetes maximales Ideal gewählt haben. Hierfür brauchen wir zuerst einen Hilfssatz, welcher uns ermöglicht, die Konstruktion nicht iterieren zu müssen.

Proposition 3.49. *Sei $k \subset K$ eine algebraische Körpererweiterung derart, dass jedes nicht-konstante Polynom mit Koeffizienten aus k eine Nullstelle in K besitzt. Der Körper K ist algebraisch abgeschlossen und somit ein algebraischer Abschluss von k.*

Beweis. Es genügt, folgendes zu zeigen:

$$\textit{Jedes nicht-konstante Polynom aus } k[T] \textit{ zerfällt in Linearfaktoren über } K \qquad (\divideontimes)$$

Mit Blick auf Korollar 3.45 betrachte eine algebraische Körpererweiterung $K \subset L$ und wähle ein Element a aus L. Da $k \subset K$ algebraisch ist, ist a algebraisch über k mit Minimalpolynom $m_a(T)$. Da $m_a(T)$ aus $k[T]$ irreduzibel ist, zerfällt $m_a(T)$ nach der Annahme $(\divideontimes)$ in Linearfaktoren über K. Insbesondere muss a Nullstelle einer dieser Linearfaktoren sein, also liegt a in K. Es folgt, dass $L = K$, wie gewünscht.

Behauptung. *Wir können annehmen, dass k perfekt ist.*

Beweis der Behauptung. Wenn die Charakteristik Null ist, gibt es nichts zu zeigen. Sonst ist die Charakteristik gleich der Primzahl $p > 0$. Setze nun

$$F = \{a \in K \mid \text{es gibt ein } n \text{ aus } \mathbb{N} \text{ mit } a^{p^n} \in k\}$$

die *perfekte Hülle* von k in K. Klarerweise ist $k \subset F \subset K$ ein Zwischenkörper. Wir zeigen zuerst, dass F perfekt ist: Gegeben a in F beliebig, gibt es ein n aus $\mathbb{N}$ mit $b = a^{p^n}$ in k. Nun hat das nicht-konstante Polynom $T^{p^{n+1}} - b$ Koeffizienten aus k, also finden wir eine Nullstelle c in K aus unserer Hypothese. Das bedeutet, dass

$$(c^p)^{p^n} = c^{p^{n+1}} = b = a^{p^n},$$

so $c^p = a$. Das Element c liegt in F, also ist F perfekt, wie gewünscht.

Wir müssen noch zeigen, dass jedes nicht-konstante Polynom aus $F[T]$ eine Nullstelle in K besitzt. Dann folgt $(\divideontimes)$ für die Körpererweiterung $F \subset K$, was sofort $(\divideontimes)$ für $k \subset K$ liefert. Sei also $P(T) = \sum_{i=0}^{n} a_i T^i$ ein nicht-konstantes Polynom über F. Wähle m aus $\mathbb{N}$ groß genug, dass $b_i = a_i^{p^m}$ in k liegt für jedes $0 \leq i \leq n$. Das Polynom

$$Q(T) = \sum_{i=0}^{n} b_i T^i$$

hat Koeffizienten aus k und somit besitzt es aus unserer Annahme eine Nullstelle c in K. Nun ist K wegen der Bemerkung 3.19 wiederum perfekt, also wähle d aus K mit $d^{p^m} = c$. Es ist

$$P(d)^{p^m} = \big(\sum_{i=0}^{n} a_i d^i\big)^{p^m} = \sum_{i=0}^{n} a_i^{p^m} (d^{p^m})^i = Q(c) = 0,$$

also besitzt $P(T)$ eine Nullstelle in K, wie gewünscht. $\square_{\text{Beh.}}$

Wir nehmen also an, dass k perfekt ist und zeigen die stärkere Bedingung ($\circledast$). Wegen des Korollars 2.35 genügt es, wenn wir ($\circledast$) für irreduzible (nicht-konstante) Polynome $P(T)$ aus $k[T]$ zeigen. Aus dem Korollar 3.22 folgt, dass $P(T)$ separabel ist. Wir finden mit Hilfe der Bemerkung 3.38 eine endliche galoissche Körpererweiterung $k \subset L$ derart, dass $P(T)$ in Linearfaktoren über L zerfällt. Wegen des Satzes des primitiven Elements 3.29 & 3.33 ist $L = k(a)$ für ein primitives Element a aus L. Sei nun $m_a(T)$ das Minimalpolynom von a über k. Das Polynom $m_a(T)$ besitzt eine Nullstelle b in K, also sind die Körper $L = k(a)$ und $k(b) \subset K$ isomorph über k wegen der Bemerkung 3.5. Es folgt, dass $P(T)$ in Linearfaktoren über K zerfällt, weil es über L so ist. Somit haben wir die gewünschte stärkere Annahme ($\circledast$) gezeigt und wir folgern, dass K algebraisch abgeschlossen ist. □

Satz 3.50. (*Der Satz von Steinitz*) *Jeder Körper k besitzt einen algebraischen Abschluss.*

Beweis. Wähle eine Aufzählung $(P_i(T))_{i\in I}$ aller nicht-konstanten irreduziblen Polynome mit Koeffizienten aus k. Betrachte nun den verallgemeinerten Polynomring $k[T_i]_{i\in I}$, wobei wir eine neue Variable T_i für jeden Index i aus I hinzufügen. Die Elemente aus $k[T_i]_{i\in I}$ sind endliche Summen von Ausdrücken der Form

$$\lambda \cdot T_{i_1}^{k_1} \cdots_{i_n}^{k_n},$$

mit λ aus k und $n, k_1, \ldots, k_n$ aus $\mathbb{N}$. Analog zu der Bemerkung B.3 lässt sich zeigen, dass $k[T_i]_{i\in I}$ ein Integritätsbereich ist, denn in einem konkreten Element aus $k[T_i]_{i\in I}$ kommen nur endlich viele Variablen vor. Betrachte nun das Ideal I von $k[T_i]_{i\in I}$, welches von der Familie $(P_i(T_i))_{i\in I}$ erzeugt wird.

Behauptung. *Das Ideal I ist echt.*

Beweis der Behauptung. Angenommen, dass 1_k in I liegt, lässt es sich schreiben als eine Linearkombination

$$1_k = g_1 P_{i_1}(T_{i_1}) + \cdots + g_m P_{i_m}(T_{i_m}),$$

wobei die Elemente $g_1, \ldots, g_m$ aus $k[T_i]_{i\in I}$ kommen. Ohne Beschränkung der Allgemeinheit können wir annehmen, dass in $g_1, \ldots, g_m$ nur die Variablen $\{T_{i_1}, \ldots, T_{i_m}\}$ vorkommen. Für die Familie $\mathcal{F} = \{P_{i_1}(T), \ldots, P_{i_m}(T)\}$ aus $k[T]$ wähle einen Zerfällungskörper $K_{\mathcal{F}} \supset k$. Insbesondere besitzt $K_{\mathcal{F}}$ für jedes $1 \leq j \leq m$ eine Nullstelle α_j von $P_{i_j}(T)$. Wenn wir die obige Linearkombination auf dem Tupel $(\alpha_1, \ldots, \alpha_m)$ auswerten, bekommen wir einen Widerspruch, denn $1_k = 1_{K_{\mathcal{F}}} \neq 0_{K_{\mathcal{F}}}$ im Körper $K_{\mathcal{F}}$. Es folgt, dass I ein echtes Ideal ist. $\square_{\text{Beh.}}$

Aus der Proposition 2.25 schließen wir, dass das Ideal I in einem maximalen Ideal M des Ringes $k[T_i]_{i\in I}$ enthalten ist. Klarerweise ist die Abbildung

$$\begin{array}{rccc} \varphi: & k & \to & k[T_i]_{i\in I}/M \\ & \lambda & \mapsto & \lambda + M \end{array}$$

ein nicht-trivialer Ringhomomorphismus, also ist φ injektiv aus dem Lemma 2.22. Wir identifizieren k mit $\varphi(k)$ als Teilkörper des Körpers $K = k[T_i]_{i\in I}/M$ (siehe Korollar 2.23). Beachte, dass die Körpererweiterung $k \subset K$ algebraisch ist wegen des Lemmas 3.10, denn in einem konkreten Element aus $k[T_i]_{i\in I}$ kommen nur endlich viele Variablen vor und die Klasse $X_i + M$ ist über k algebraisch aus der Wahl von I. Die algebraische Körpererweiterung $k \subset K$ erfüllt die Bedingungen der Proposition 3.49, also ist K ein algebraischer Abschluss von k, wie gewünscht. □

3.6 Lösbarkeit von Gleichungen und Konstruktibilität

Definition 3.51. Eine algebraische Körpererweiterung $k \subset K$ ist eine *Radikalerweiterung*, falls es einen Turm einfacher Körpererweiterungen

$$k \subset k(a_1) \subset \cdots \subset k(a_1, \ldots, a_m) = K$$

derart gibt, dass für $1 \leq i \leq m$ das Element $a_i^{n_i}$ in $k(a_1, \ldots, a_{i-1})$ liegt für eine natürliche Zahl $n_i \neq 0$, oder äquivalent dazu, wenn a_i Nullstelle eines Polynoms der Form $T^{n_i} - b_i$ mit b_i aus $k(a_1, \ldots, a_{i-1})$ ist. Wir sagen, dass a_i eine n_i*-te Wurzel* von b_i ist.

Bemerkung 3.52. Eine einfache Radikalerweiterung $k \subset k(a)$ mit $0_k \neq a^n$ in k ist genau dann separabel, wenn die Charakteristik von k die Zahl n nicht teilt. Insbesondere ist jede Radikalerweiterung in Charakteristik Null separabel.

Aufgabe. Seien Elemente a und b aus einem algebraischen Abschluss k^{alg} eines Körpers k derart, dass a und b jeweils in Radikalerweiterungen $k \subset K_a \subset k^{alg}$ und $k \subset K_b \subset k^{alg}$ liegen. Zeige, dass der Zwischenkörper $k(a, b)$ in einer Radikalerweiterung von k liegt.

Beispiel 3.53. Ein typisches Beispiel einer einfachen Radikalerweiterung wird durch *Einheitswurzeln* gegeben. Sei k ein Körper und wähle mit Hilfe des Satzes 3.50 einen algebraischen Abschluss k^{alg}. Ein Element ξ aus k^{alg} ist eine n*-te Einheitswurzel*, falls $\xi^n = 1_k$.

Beachte, dass die Menge aller n-ten Einheitswurzeln eine endliche multiplikative Untergruppe von $k^{alg} \setminus \{0_k\}$ bildet. Aus der Proposition 3.32 folgt, dass diese Gruppe zyklisch ist. Die n-te Einheitswurzel ξ ist eine primitive Einheitswurzel, falls die davon erzeugte multiplikative Untergruppe $\langle \xi \rangle$ alle n-ten Einheitswurzeln sind.

Wenn die Charakteristik $p > 0$ ist, gibt es nur eine p^r-te Einheitswurzel (nämlich die triviale Lösung $\xi = 1_k$). Wenn p die Zahl n nicht teilt, ist die Erweiterung $k \subset k(\xi)$, für ξ eine primitive n-te Einheitswurzel, separabel mit

$$T^n - 1_K = (T-1)(T-\xi)(T-\xi^2)\cdots(T-\xi^{n-1}).$$

Insbesondere ist $k \subset k(\xi)$ normal und somit galoissch (es wird nicht behauptet, dass $T^n - 1_k$ das Minimalpolynom von ξ ist!). Beachte, dass $\mathrm{Gal}(k(\xi)/k)$ eine abelsche Gruppe ist: In der Tat, ein k-Automorphismus σ von $k(\xi)$ wird eindeutig von $\sigma(\xi)$ bestimmt, welches wiederum eine (primitive) n-te Einheitswurzel ist, also $\sigma(\xi) = \xi^{r_\sigma}$ für ein $1 \leq r_\sigma \leq n-1$. Insbesondere gilt

$$\tau \circ \sigma(\xi) = \tau(\xi^{r_\sigma}) = \tau(\xi)^{r_\sigma} = \xi^{r_\tau \cdot r_\sigma} = \sigma \circ \tau(\xi).$$

Beachte nun, dass die Kongruenzklasse $\overline{r_\sigma}$ der Zahl r_σ eine Einheit im Ring $\mathbb{Z}/n\mathbb{Z}$ sein muss: In der Tat bildet σ die Menge $\{1_k, \xi, \xi^2, \ldots, \xi^{n-1}\}$ in sich surjektiv ab, also $\xi = \sigma(\xi^m) = (\xi^{r_\sigma})^m = \xi^{mr_\sigma}$ oder äquivalent dazu $\xi^{mr_\sigma - 1} = 1_k$. Schreibe $mr_\sigma - 1 = nk + t$ mit $0 \leq t \leq n-1$ und schließe daraus, dass

$$1_k = \xi^{mr_\sigma - 1} = \xi^t.$$

Weil ξ Ordnung n hat (denn es gibt genau n Einheitswurzeln in $\overline{k}$) folgt, dass $t = 0$, also

$$mr_\sigma - 1 \equiv 0 \mod n,$$

und somit ist r_σ in $\mathcal{U}(\mathbb{Z}/n\mathbb{Z})$, wie gewünscht.

Proposition 3.54. *Gegeben eine Primzahl p, sei ζ_{p^e} eine primitive p^e-te Einheitswurzel (wobei $1 \leq e$ aus $\mathbb{N}$ kommt) in einem algebraischen Abschluss $\mathbb{Q}^{alg}$ von $\mathbb{Q}$. Der* Kreisteilungskörper *$\mathbb{Q}(\zeta_{p^e})$ hat Grad $p^{e-1}(p-1)$ über $\mathbb{Q}$.*
Insbesondere ist der Grad der Körpererweiterung $\mathbb{Q} \subset \mathbb{Q}(\zeta_p)$ gleich $p-1$.

Beweis. Beachte, dass

$$T^{p^e} - 1 = (T^{p^{e-1}} - 1)(T^{p^{e-1}(p-1)} + T^{p^{e-1}(p-2)} + \cdots + T^{p^{e-1}} + 1).$$

Weil $\zeta \neq 1$ folgt, dass ζ eine Nullstelle des Polynoms

$$P(T) = T^{p^{e-1}(p-1)} + T^{p^{e-1}(p-2)} + \cdots + T^{p^{e-1}} + 1$$

ist. Es genügt zu zeigen, dass $P(T)$, oder äquivalent dazu, dass $Q(T) = P(T+1)$ irreduzibel über $\mathbb{Q}$ ist. Mit Hilfe der binomischen Formel schreibe

$$Q(T) = T^{p^{e-1}(p-1)} + \sum_{j=1}^{p^{e-1}(p-1)-1} a_j T j + p,$$

wobei jedes a_j aus $\mathbb{Z}$ kommt.

Aus dem Lemma von Gauß 2.36 müssen wir nur zeigen, dass $Q(T)$ sich nicht als ein Produkt zwei echten Faktoren mit Koeffizienten aus $\mathbb{Z}$ schreiben lässt. Sonst ist $Q(T) = R(T) \cdot S(T)$. Beachte nun, dass

$$Q(T) \bmod p = \frac{(T+1)^{p^e} - 1}{(T+1)^{p^{e-1}} - 1} \bmod p = \frac{T^{p^e}}{T^{p^{e-1}}} \bmod p = T^{p^{e-1}(p-1)} \bmod p.$$

Wir folgern, dass die konstanten Terme von R und von S durch p teilbar sind, was den gewünschten Widerspruch liefert, denn der konstanten Term von $P(T)$ nur p ist und nicht durch p^2 teilbar ist. □

Proposition 3.55. (*Kummertheorie Teil I*) *Sei n eine natürliche Zahl derart, dass die Charakteristik des Körpers k die Zahl n nicht teilt. Wir nehmen an, dass k alle n-ten Einheitswurzel (oder äquivalent dazu, eine primitive n-te Einheitswurzel ζ) enthält. Gegeben b aus k, welches keine n-te Wurzel in k besitzt, und a in einem algebraischen Abschluss k^{alg} von k mit $a^n = b$, so ist die Körpererweiterung $k \subset k(a)$ galoissch mit zyklischer Galoisgruppe.*

Der Grad $[k(a) : k]$ teilt n und ist genau dann gleich n, wenn $T^n - b$ irreduzibel in $k[T]$ ist.

Beweis. Da b keine n-te Wurzel in k besitzt, ist $b \neq 0_k$, also $a \neq 0_k$. Nun sind die Nullstellen von $T^n - b$ gleich $a, a\zeta, a\zeta^2, \ldots, a\zeta^{n-1}$, welche alle verschieden sind, da $a \neq 0_{k^{alg}}$. Insbesondere ist die Erweiterung $k \subset k(a)$ galoissch, weil das Polynom $T^n - b$ separabel ist und in Linearfaktoren über $k(a)$ zerfällt. Ein k-Automorphismus σ aus $\mathrm{Gal}(k(a)/k)$ wird von $\sigma(a)$ eindeutig bestimmt. Beache, dass $\sigma(a) = a\zeta^{r_\sigma}$ für ein r_σ aus $\mathbb{N}$. Nur die Kongruenzklasse von r_σ modulo n spielt eine Rolle, also ist die Abbildung

$$\begin{array}{rccc} \varphi: & \mathrm{Gal}(k(a)/k) & \to & \mathbb{Z}/n\mathbb{Z} \\ & \sigma & \mapsto & r_\sigma + n\mathbb{Z} \end{array}$$

ein Gruppenmonomorphismus. Aus der Bemerkung 1.30 und dem Satz 1.39 folgt, dass $\mathrm{Gal}(k(a)/k)$ isomorph zu einer zyklischen Gruppe und somit selbst zyklisch ist. Beachte, dass $|\mathrm{Gal}(k(a)/k)| = |\mathrm{Im}(\varphi)|$ die Zahl n teilt wegen der Bemerkung 1.28.

Wenn $T^n - b$ irreduzibel ist, dann ist es das Minimalpolynom $m_a(T)$ von a über k, also $n = [k(a) : k] \leq n$. Es folgt, dass $[k(a) : k] = n$, wie gewünscht. Des Weiteren, wenn $n = [k(a) : k]$, so muss $T^n - b$ gleich dem Minimalpolynom von a sein und ist somit irreduzibel. □

Satz 3.56. (*Kummertheorie Teil II*) *Mit den Hypothesen der Proposition 3.55 sei k ein Körper dessen Charakteristik die Zahl n nicht teilt. Wir nehmen ferner an, dass k eine primitive n-te Einheitswurzel ζ enthält. Jede endliche Körpererweiterung $k \subset K$ vom Grad n mit zyklischer Galoisgruppe* $\mathrm{Gal}(K/k)$ *ist der Zerfällungskörpers eines irreduziblen Polynoms der Form $T^n - b$ für ein b aus k. Insbesondere ist $K = k(a)$ mit $a^n = b$.*

Beweis. Sei σ ein Erzeuger der zyklischen Galoisgruppe $\mathrm{Gal}(K/k)$, das heißt $\mathbf{Id}_K, \sigma, \ldots, \sigma^{n-1}$ sind die verschiedenen k-Automorphismen aus der Galoisgruppe $\mathrm{Gal}(K/k)$. Wir beweisen zuerst eine schwache Version des Lemmas von Dedekind, welches als eine konkrete Version von Artins Satz über die Unabhängigkeit von Charakteren in einer Gruppe betrachtet werden kann.

Behauptung. *Die Potenzen von σ sind K-*linear unabhängig*: Gegeben $\lambda_0, \ldots, \lambda_{n-1}$ aus K derart, dass der Endomorphismus*

$$\begin{array}{rccl} \lambda_0\mathbf{Id}_K + \cdots + \lambda_{n-1}\sigma^{n-1} : & K & \to & K \\ & x & \mapsto & \lambda_0 x + \lambda_1\sigma(x) + \cdots + \lambda_{n-1}\sigma^{n-1}(x) \end{array}$$

der Null-Endomorphismus ist, so sind $\lambda_0 = \cdots = \lambda_{n-1} = 0_K$.

Beweis der Behauptung. Angenommen es gäbe eine solche nicht-triviale K-Linearkombination, dann ist $n \geq 2$, weil $\lambda_0\mathbf{Id}_K$ nur die Nullabbildung ist, wenn $\lambda_0 = 0_K$. Wir wählen n kleinstmöglich mit der Eigenschaft, dass es eine nicht-triviale K-Linearkombination wie oben gibt. Da σ^{n-1} injektiv ist, gibt es insbesondere einen Index $0 \leq i_0 \leq n-2$ mit $\lambda_{i_0} \neq 0_K$ gibt. Beachte, dass die k-Endomorphismen σ^{i_0} und σ^{n-1} verschieden sind, so finde y aus K mit $\sigma^{i_0}(y) \neq \sigma^{n-1}(y)$.

Weil alle Potenzen von σ Ringhomomorphismen sind, folgt

$$\big(\lambda_0\mathbf{Id}_K + \cdots + \lambda_{n-1}\sigma^{n-1}\big)(x \cdot y) = \lambda_0 x \cdot y + \cdots + \lambda_{n-1}\sigma^{n-1}(x)\sigma^{n-1}(y) = 0_K \text{ für alle } x \text{ aus } K.$$

Weil $\lambda_0 x + \cdots + \lambda_{n-1}\sigma^{n-1}(x) = 0_K$, ist auch

$$\lambda_0 x \cdot \sigma^{n-1}(y) + + \cdots + \lambda_{n-1}\sigma^{n-1}(x) \cdot \sigma^{n-1}(y) = 0_K \text{ für alle } x \text{ aus } K.$$

Wenn wir beide Gleichungen substrahieren, schließen wir, dass

$$\sum_{0 \leq j \leq n-2} \lambda_j(\sigma^j(y) - \sigma^{n-1}(y))\sigma^j(x) = 0_K \text{ für alle } x \text{ aus } K.$$

Aus der Minimalität von n folgt, dass

$$\lambda_j(\sigma^j(y) - \sigma^{n-1}(y)) = 0_K \text{ für alle } 0 \leq j \leq n-2.$$

Insbesondere ist $\lambda_{i_0}(\sigma^{i_0}(y) - \sigma^{n-1}(y)) = 0_K$, was unserer Wahl von λ_{i_0} und y widerspricht. $\square_{\text{Beh.}}$

Mit Hilfe der obigen Behauptung finde also ein Element c aus K mit

$$a = 1_k c + \zeta\sigma(c) + \cdots + \zeta^{n-1}\sigma^{n-1}(c) \neq 0_K.$$

Beachte, dass ζ in k liegt, also

$$\sigma(a) = \sigma(c) + \zeta\sigma^2(c) + \cdots + \zeta^{n-1}\sigma^n(c) = \zeta^{-1}a.$$

Insbesondere liegt $b = a^n$ wegen des Satzes 3.39 in k, denn es gilt

$$\sigma(b) = \sigma(a^n) = (\sigma(a))^n = (\zeta^{-1})^n a^n = b$$

und somit wird b von jedem Element aus $\mathrm{Gal}(K/k)$ fixiert. Es folgt, dass a eine Nullstelle des Polynoms $T^n - b$ ist, welches in Linearfaktoren über $k(a)$ zerfällt, denn

$$T^n - b = (T - a)(T - a\zeta)\cdots(T - a\zeta^{n-1}).$$

Die Körpererweiterung $k \subset k(a)$ ist also galoissch. Des Weiteren liefert $\tau = \sigma_{\restriction k}(a)$ ein Element aus $\mathrm{Gal}(k(a)/k)$ derart, dass die Potenzen $\{\mathbf{Id}_{k(a)}, \tau, \ldots, \tau^{n-1}\}$ alle verschieden sind, denn

$$\tau^j(a) = \zeta^{-j}a.$$

Insbesondere ist $n \leq \mathrm{Gal}(k(a)/k) = [k(a) : k]$, so $K = k(a)$ und das Polynom $T^n - b$ ist irreduzibel. □

Definition 3.57. Sei k ein Körper. Eine polynomiale Gleichung $P(T) = 0$ mit Koeffizienten aus k ist *auflösbar*, falls ein Zerfällungskörper von $P(T)$ Teilkörper einer Radikalerweiterung von k ist, oder äquivalent dazu (siehe die Aufgabe nach der Bemerkung 3.52), wenn jede Nullstelle von $P(T)$ in einer Radikalerweiterung von k liegt.

Mit Hilfe der Lösungsformel ist es leicht zu zeigen, dass jede polynomiale Gleichung vom Grad 2 über einem Körper der Charakteristik ungleich Null auflösbar ist. Mit Hilfe einer elementaren Transformation können wir die Cardanische Formel für eine geeignete kubische Gleichung anwenden, solange die Charakteristik weder 2 noch 3 ist. Es gibt eine ähnliche (jedoch etwas kompliziertere) Formel für eine Gleichung vierten Grades, solange die Charakteristik weder 2 noch 3 ist.

Satz 3.58. *Sei $P(T)$ ein Polynom mit Koeffizienten aus dem Körper k der Charakteristik Null. Die polynomiale Gleichung $P(T) = 0$ ist genau dann auflösbar, wenn die Galoisgruppe $\mathrm{Gal}(K/k)$ des Zerfällungskörpers K von $P(T)$ über k als Gruppe auflösbar ist (im Sinne der Definition 1.64).*

Beachte, dass isomorphe Zerfällungskörper einen Isomorphismus der entsprechenden Galoisgruppe induzieren. Aus diesem Grund hängt die Auflösbarkeit der Galoisgruppe nicht von der Wahl des Zerfällungskörpers ab.

Beweis. Ohne Beschränkung der Allgemeinheit können wir annehmen, dass K Teilkörper eines festen algebraischen Abschlusses $\overline{k}$ von k ist.

($\Rightarrow$) : Sei also $K \subset L \subset \overline{k}$ eine endliche algebraische Körpererweiterung derart, dass $k \subset L$ radikal ist. Aus dem Satz des primitiven Elementes 3.29 (weil der Körper k unmittelbar perfekt ist, da die Charakteristik Null ist 3.17) schreibe also $L = k(b)$ für ein primitives Element b aus L. Jede Nullstelle b' aus $\overline{k}$ des Minimalpolynoms $m_b(T)$ liefert einen k-Automorphismus $L \to L' = k(b')$, somit ist die Körpererweiterung $k \subset L'$ wiederum radikal. Insbesondere gibt es mit Hilfe der Aufgabe nach der Bemerkung 3.52 einen Zwischenkörper $L \subset M \subset \overline{k}$ derart,

dass $k \subset M$ eine galoissche Radikalerweiterung ist. Ohne Beschränkung der Allgemeinheit ist $M = L$. Wir zerlegen die Körpererweiterung $k \subset L$ als einen Turm einfacher Körpererweiterungen

$$k \subset k(a_1) \subset \cdots \subset k(a_1, \ldots, a_m) = L$$

so, dass für $1 \leq i \leq m$ das Element $a_i^{n_i}$ in $k(a_1, \ldots, a_{i-1})$ liegt für eine natürliche Zahl $n_i \neq 0$. Wähle nun ein gemeinsames Vielfaches N von $n_1, \ldots, n_m$ und sei ζ eine primitive N-te Einheitswurzel aus $\overline{k}$. Aus dem Beispiel 3.53 und dem Satz 3.56 folgt, dass der Turm einfacher Körpererweiterungen

$$k \subset k(\zeta) \subset k(\zeta, a_1) \subset \cdots \subset k(\zeta, a_1, \ldots, a_m) = L(\zeta)$$

aus galosisschen Körpererweiterungen mit abelschen Galoisgruppen besteht. Somit ist die Galoisgruppe $\mathrm{Gal}(L(\zeta)/k)$ auflösbar. Aus dem Lemma 1.65 folgt, dass

$$\mathrm{Gal}(K/k) \overset{3.41}{\simeq} \mathrm{Gal}(L(\zeta)/k)/\,\mathrm{Gal}(L(\zeta)/K)$$

auch auflösbar ist, wie gewünscht.

($\Leftarrow$) : Wir nehmen nun an, dass die Galoisgruppe $\mathrm{Gal}(K/k)$ des Zerfällungskörpers K von $P(T)$ über k auflösbar ist. Die entsprechende Normalreihe von Untergruppen liefert einen Turm endlicher galoisscher Körpererweiterungen

$$k \subset k_1 \subset \ldots \subset k_m = K$$

derart, dass die Galoisgruppe jeder Erweiterung $k_i \subset k_{i+1}$ mit $0 \leq i \leq m-1$ abelsch ist. Aus dem Satz 1.56 und der Galoiskorrespondenz 3.39 & 3.41 sowie aus dem Lemma von Cauchy 1.57 können wir die Turm so verfeinern, dass jede Galoisgruppe $\mathrm{Gal}(k_{i+1}/k_i)$ eine zyklische Gruppe der Ordnung p_i für eine Primzahl p_i ist. Sei n ein gemeinsames Vielfaches von $p_1, \ldots, p_m$ und wähle eine primitive n-te Einheitswurzel ζ aus $\overline{k}$. Klarerweise ist die Erweiterung $k \subset k(\zeta)$ radikal aus dem Beispiel 3.53. Es genügt also zu zeigen, dass $k(\zeta) \subset K(\zeta)$ eine Radikalerweiterung ist. Nun ist für $0 \leq i \leq m-1$ die Erweiterung $k_i(\zeta) \subset k_{i+1}(\zeta)$ galoissch und die Galoisgruppe $\mathrm{Gal}(k_{i+1}(\zeta)/k_i(\zeta))$ ist isomorph zu einer Untergruppe von $\mathbb{Z}/p_i\mathbb{Z}$, aus der Aufgabe nach dem Korollar 3.40. Mit Hilfe des Satzes 3.56 der Kummertheorie schließen wir, dass jede Körpererweiterung $k_i(\zeta) \subset k_{i+1}(\zeta)$, und somit auch $k \subset K$, radikal ist, wie gewünscht. □

Aufgabe. Sei $P(T) = T^5 - aT + b$ mit $a > 0$ und b reelle Zahlen. Zeige, dass $P(T)$ mindestens eine, aber höchstens drei reelle Nullstellen besitzt.

Schließe mit elementaren analytischen Methoden, dass das Polynom $P(T) = T^5 - 4T + 1$ genau drei reelle Nullstellen besitzt. Begründe, dass dieses Polynom irreduzibel in $\mathbb{Q}[T]$ ist.

Satz 3.59. *Es gibt Gleichungen fünften Grades über $\mathbb{Q}$, welche nicht auflösbar sind. Insbesondere gibt es keine allgemeine algebraische Formel mit Radikalen für die Nullstellen einer Gleichung fünften Grades über $\mathbb{Q}$.*

Beweis. Betrachte das irreduzible Polynom $P(T) = T^5 - 4T + 1$. Aus der Proposition 1.66 und dem Satz 3.58 reicht es, zu zeigen, dass die Galoisgruppe seines Zerfällungskörpers genau S_5 ist. Wähle also einen algebraischen Abschluss $\overline{Q}$ von $\mathbb{Q}$ als Teilkörper von $\mathbb{C}$ (aus dem Hauptsatz der Algebra C.1) und sei $K \subset \overline{\mathbb{Q}}$ das Zerfallkörpers von $P(T)$. Da $\mathbb{C}$ algebraisch abgeschlossen ist, zerfällt das Polynom in Linearfaktoren über $\mathbb{C}$. Aus der obigen Aufgabe besitzt $P(T)$ genau drei

reelle Nullstellen sowie zwei Nullstellen aus $\mathbb{C} \setminus \mathbb{R}$, welche dann zueinander komplex konjugiert sein müssen, denn

$$\overline{P(z)} = P(\overline{z}).$$

Hierfür benutzen wir, dass die komplexe Konjugation ein $\mathbb{R}$-Automorphismus von $\mathbb{C}$ ist.

Insbesondere ist $K = \mathbb{Q}(z_1, z_2, z_3, z_4, z_5)$ mit $z_2 = \overline{z_1} \neq z_1$ aus $\mathbb{C}$ und z_3, z_4 sowie z_5 aus $\mathbb{R}$. Die Wirkung jedes Elements φ aus $\mathrm{Gal}(K/\mathbb{Q})$ wird von der induzierten Wirkung auf der Menge $\{1, \ldots, 5\}$ der Indices eindeutig bestimmt. Insbesondere lässt sich somit $\mathrm{Gal}(K/\mathbb{Q})$ in S_5 einbetten, sodass wir $\mathrm{Gal}(K/\mathbb{Q})$ mit seinem Bildbereich als Untergruppe von S_5 identifizieren werden. Nun ist

$$|\operatorname{Gal}(K/\mathbb{Q})| \overset{3.37}{=} [K : \mathbb{Q}] \overset{3.8}{=} [K : \mathbb{Q}(z_1)] \cdot [K(z_1) : \mathbb{Q}] = 5[K : \mathbb{Q}(z_1)],$$

weil das Polynom $P(T)$ irreduzibel ist. Aus dem Lemma von Cauchy 1.57 besitzt also $\mathrm{Gal}(K/\mathbb{Q})$ einen 5-Zyklus σ. Des Weiteren induziert die komplexe Konjugation einen $\mathbb{Q}$-Automorphismus von K, welcher z_1 und z_2 miteinander permutiert, aber z_3, z_4 und z_5 fixiert. Es folgt, dass (das Bild von) $\mathrm{Gal}(K/\mathbb{Q})$ die Permutation (1 2) besitzt.

Wir müssen also nur noch zeigen, dass jede Untergruppe H von S_5, welche einen 5-Zyklus σ sowie die Transposition (1 2) enthält, gleich S_5 sein muss. Ohne Beschränkung der Allgemeinheit ist σ der Form

$$\sigma = (1\ 2\ i\ j\ k),$$

denn sonst ersetzen wir σ mit einer geeigneten Potenz. Sei nun τ die Permutation, welche 1 und 2 fixiert, aber $\{i, j, k\}$ nach $\{3, 4, 5\}$ abbildet. Aus der Aufgabe nach dem Beispiel 1.7 folgt, dass die konjugierte Untergruppe $H^{\tau^{-1}}$ die Transposition (1 2) sowie den Zyklus $(1\ \cdots\ 5)$ enthält. Wir schließen aus der Aufgabe nach der Bemerkung 1.9, dass $H^{\tau^{-1}}$, und somit auch H, gleich S_5 ist, wie gewünscht. □

Wir können uns als letztes dem Problem der Konstruktibilität mit Zirkel und Linear widmen, siehe ✪ im Kapitel 0. Wir fangen zuerst mit einer Umformulierung des Korollars ✪.7 in der Terminologie der Galoistheorie.

Proposition 3.60. *Folgende Aussagen sind für eine komplexe Zahl z äquivalent:*

(a) Die Zahl z ist konstruktibel.

(b) Die komplexe Zahl z liegt in einer galoisschen Erweiterung K von $\mathbb{Q}$ mit $[K : \mathbb{Q}] = 2^n$ für ein n aus $\mathbb{N}$.

Insbesondere muss der Grad der Körpererweiterung $\mathbb{Q} \subset \mathbb{Q}(z)$ eine Potenz von 2 sein, wenn z konstruktibel ist.

Beweis. $(a) \Rightarrow (b)$: Wenn z konstruktibel ist, gibt es aus dem Korollar ✪.7 eine Turm von Körpererweiterungen

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

mit z in K_r und $[K_{i+1} : K_i] \leq 2$ (es kann sein, dass einige der Polynome reduzibel sind). Aus dem Korollar 3.8 folgt, dass $[K_r : \mathbb{Q}]$. Weil der Grad multiplikativ ist, so ist $[\mathbb{Q}(z) : \mathbb{Q}]$ eine Potenz von 2.

Wenn $\mathbb{Q}(z)$ bereits alle Nullstellen des Minimalpolynoms $m_z(T)$ enthält, so ist $\mathbb{Q} \subset \mathbb{Q}(z)$ normal und somit galoissch. Ansonsten sei $z' \neq z$ eine andere Nullstelle von $m_z(T)$. Es gibt

einen $\mathbb{Q}$-Isomorphismus, welche $\mathbb{Q}(z)$ auf $\mathbb{Q}(z')$ abbildet. Dieser Körperisomorphismus induziert eine Turm von Körpererweiterungen

$$K_0 = \mathbb{Q} \subset K_1' \subset \cdots \subset K_r'$$

mit z' in K_r' und $[K_{i+1}' : K_i'] \leq 2$. Wir transportieren die Turm auf $\mathbb{Q}(z)$ und bekommen eine Turm von Körpererweiterungen

$$\mathbb{Q}(z) \subset K_1'(z) \subset \cdots \subset K_r'(z)$$

mit $[K_{i+1}'(z) : K_i'(z)] \leq 2$. Da $\mathbb{Q}(z, z') \subset K_r'(z)$ ein Teilkörper ist, so ist

$$[\mathbb{Q}(z, z') : \mathbb{Q}] = [\mathbb{Q}(z, z') : \mathbb{Q}(z)] \cdot [\mathbb{Q}(z) : \mathbb{Q}]$$

wieder eine Potenz von 2, aus dem Korollar 3.8. Wir iterieren dieses Verfahren und schließen, dass der Grad des Zerfällungskörpers K von $m_z(T)$ über $\mathbb{Q}$ eine Potenz von 2 ist, wie gewünscht.

$(b) \Rightarrow (a)$: Wir nehmen an, dass z in einer galoisschen Körpererweiterung $\mathbb{Q} \subset K$ mit $[K : \mathbb{Q}]$ eine Potenz von 2 liegt. Aus der Proposition 3.11 und dem Satz C.1 können wir annehmen, dass K ein Teilkörper von $\mathbb{C}$. Insbesondere ist die Galoisgruppe $\mathrm{Gal}(K/\mathbb{Q})$ eine 2-Gruppe. Mit Hilfe des Korollars 1.58 sowie der Galoiskorrespondenz 3.39 & 3.41 konstruieren wir eine Turm von Körpererweiterungen

$$K_0 = \mathbb{Q} \subset K_1 \subset \cdots \subset K_m = K$$

derart, dass $[K_{i+1} : K_i] = 2$. Insbesondere ist z konstruktibel, nach dem Korollar ✪.7. □

Aufgabe. Ein Winkel θ ist konstruktibel, wenn $\cos(\theta)$ (oder äquivalent dazu $\sin(\theta)$) konstruktibel ist.

Lässt sich jeder konstruktible Winkel dreiteilen?

Bemerkung 3.61. Sei $n \geq 3$ eine natürliche Zahl. Das regelmäßige n-Eck ist genau dann konstruktibel (siehe Definition ✪.4), wenn eine (oder äquivalent dazu, jede) primitive n-Einheitswurzel (als Element von $\overline{Q} \subset \mathbb{C}$) konstruktibel ist.

Korollar 3.62. (*Der Satz von Gauß*) *Das regelmäßige n-Eck ist genau dann konstruktibel, wenn n der Form*

$$n = 2^m \cdot p_1 \cdots p_r,$$

mit m aus $\mathbb{N}$ und paarweise verschiedene Primzahlen $p_1, \ldots, p_r$, wobei $p_i = 2^{k_i} + 1$ für ein k_i aus $\mathbb{N}$.

Primzahlen der Form $2^s + 1$ heißen *Fermat'sche Primzahlen*. Es lässt sich leicht zeigen, dass der Exponent s einer Fermat'schen Primzahl eine Potenz von 2 sein muss. Obwohl die größte bekannte Fermat'sche Primzahl $2^{2^4} + 1$ ist, wird dennoch vermutet, dass es unendlich viele Fermat'sche Primzahlen gibt.

Beweis. Aus der Bemerkung 3.61 müssen wir nur entscheiden, wann eine primitive n-te Einheitswurzel ζ_n aus $\mathbb{C}$ konstruktibel ist. Schreibe $n = n_1 \cdot n_2$ für zwei teilerfremden natürlichen Zahlen n_1 und n_2. Klarerweise, gegeben ζ_n, so ist $\zeta_n^{n_1}$ eine primitive n_2-te Einheitswurzel. Andererseits,

gegeben eine primitive n_1-te Einheitswurzel ζ_{n_1} und eine primitive n_2-te Einheitswurzel ζ_{n_2}, so ist ist die komplexe Zahl

$$\zeta_{n_1} \cdot \zeta_{n_2}$$

eine primitive n-te Einheitswurzel aus dem (ersten Teil im Beweis vom) Satz 1.56. Weil die konstruktiblen komplexen Zahlen unter Multiplikation abgeschlossen sind, so folgt, dass ζ_n genau dann konstruktibel ist, wenn jede p^e-te primitive Einheitswurzel ζ_{p^e} konstruktibel ist für jeden nicht-trivialen Faktor p^e in der Zerlegung von n als Potenzen von Primzahlen. Dies ist äquivalent mit Hilfe der Proposition 3.60 zu der Frage, wann die galoissche Körpererweiterung $\mathbb{Q} \subset \mathbb{Q}(\zeta_{p^e})$ Grad eine Potenz von 2 besitzt.

Aus der Proposition 3.54 ist $[\mathbb{Q}(\zeta_{p^e}) : \mathbb{Q}] = p^{e-1}(p-1)$. Diese Zahl ist genau dann eine Potenz von 2, wenn p die Primzahl 2 (mit e beliebig) ist oder wenn p ungerade mit $e = 1$ so ist, dass $p - 1$ eine Potenz von 2 ist, das heißt, dass p eine Fermatsche Primzahl ist, wie gewünscht. □

Korollar 3.63. *Die regelmässige Fünfeck, Sechseck sowie* 17*-Eck sind konstruktibel mit Zirkel und Lineal. Das regelmässige* 11*-Eck und* 13*-Eck sind nicht mit Zirkel und Lineal konstruktierbar.*

Appendix

A Das Zorn'sche Lemma

Definition A.1. Eine Menge $\mathcal{S}$ ist *partiell angeordnet*, falls sie eine binäre Relation $\leq$ mit den folgenden Eigenschaften besitzt:

Reflexivität $x \leq x$ für alle x aus $\mathcal{S}$;

Antisymmetrie Für alle x und y aus $\mathcal{S}$ gelten $x \leq y$ und $y \leq x$ gleichzeitig genau dann, wenn $x = y$;

Transitivität Für alle x, y und z aus $\mathcal{S}$ gilt die Implikation

$$x \leq y \text{ und } y \leq z \Longrightarrow x \leq z.$$

Wir schreiben $x < y$, falls $x \leq y$ aber $x \neq y$.
Eine partielle Ordnung $\leq$ auf $\mathcal{S}$ ist *total*, oder *linear*, falls $x < y$ oder $y < x$ für alle $x \neq y$ aus $\mathcal{S}$.
Sei $\leq$ eine partielle Ordnung auf $\mathcal{S}$.

- Ein Element x ist eine *obere Schranke* für die Teilmenge Γ von $\mathcal{S}$, falls $\gamma \leq x$ für alle γ aus Γ.
- Ein Element x ist eine *untere Schranke* für die Teilmenge Γ von $\mathcal{S}$, falls $x \leq \gamma$ für alle γ aus Γ.
- Das Element x aus $\mathcal{S}$ ist *maximal*, falls die einzige obere Schranke der Teilmenge $\{x\}$ von $\mathcal{S}$ das Element x selbst ist. Oder äquivalent dazu, dass kein y aus $\mathcal{S}$ mit $x < y$ existiert. Das Element x ist das größte Element der Teilmenge Γ, falls x in Γ liegt und $y \leq x$ für alle y aus Γ.
- Das Element x aus $\mathcal{S}$ ist *minimal*, falls die einzige untere Schranke der Teilmenge $\{x\}$ von $\mathcal{S}$ das Element x selbst ist. Oder äquivalent dazu, dass kein y aus $\mathcal{S}$ mit $y < x$ existiert. Das Element x ist das kleinste Element der Teilmenge Γ, falls x in Γ liegt und $x \leq y$ für alle y aus Γ.
- Das Element a ist das *Supremum* (oder das *Oberste*) der Teilmenge Γ von $\mathcal{S}$, falls a die kleinste obere Schranke von Γ ist. Das Element a ist das *Maximum* von Γ, wenn a das Supremum von Γ ist und a in Γ liegt.
- Ein Element a ist das *Infimum* der Teilmenge Γ von $\mathcal{S}$, falls a die größte untere Schranke von Γ ist. Das Element a ist das *Minimum* von Γ, wenn a das Infimum von Γ ist und a in Γ liegt.
- Die Menge $\mathcal{S}$ ist *induktiv*, falls jede linear geordnete Teilmenge eine obere Schranke in $\mathcal{S}$ besitzt.

Bemerkung A.2. Beachte, dass jede induktive partiell geordnete Menge $\mathcal{S}$ nicht-leer ist, da die leere Menge $\emptyset$ linear geordnet ist und somit eine obere Schranke in $\mathcal{S}$ besitzen muss. Jedes Element aus $\mathcal{S}$ ist eine obere Schranke für $\emptyset$.

Trotz des folgenden Namens ist das Zorn'sche Lemma eine Aussage der Mengenlehre, welche unabhängig vom Zermelo-Fraenkel-System und äquivalent zum *Auswahlaxiom* ist.

Lemma A.3 (Zorn'sches Lemma)**.** *Jede induktive partiell geordnete Menge* $(\mathcal{S}, \leq)$ *besitzt ein maximales Element.*

B Polynomringe

Sei K ein Körper (siehe Definition 2.20)

Definition B.1. Der *Polynomring über K in der Variablen T* ist die Kollektion $K[T]$ von Ausdrücken der Form

$$P = a_0 + a_1 T + \cdots + a_n T^n,$$

wobei n eine (beliebige) natürliche Zahlen ist und jeder Koeffizient a_i in K liegt. Das *Nullpolynom (oder das triviale Polynom)* 0 ist das Polynom, dessen Koeffizienten alle Null sind. Jedes nicht-triviale Polynom lässt sich eindeutig als

$$P = a_0 + a_1 T + \cdots + a_n T^n$$

schreiben, mit $a_n \neq 0$ für eine natürliche Zahl $n = \deg(P)$, genannt den *Grad* von P. Als Konvention setzen wir $\deg(0) = -\infty$.

Wenn P Grad n hat, ist der Koeffizient a_n in der Darstellung von P der *Führungskoeffizient* von P. Das Polynom P ist *normiert*, falls der Führungskoeffizient 1_K ist.

Bemerkung B.2. Jedes Element λ von K lässt sich als *konstantes Polynom* vom Grad 0 auffassen.

Auf dem Polynomring können wir folgenderweise eine Summe definieren: Gegeben Polynome

$$P = \sum_{i=1}^{n} a_i T^i \text{ und } Q = \sum_{j=1}^{m} b_j T^j,$$

können wir annehmen, dass $n = m$ ist (für $d = \max(n, m)$ setze für $n < i \leq d$ und $m < j \leq d$ die neuen Koeffizienten $a_i = b_j = 0$). Dann ist

$$P + Q = \sum_{i=1}^{n} (a_i + b_i) T^i.$$

Analog definieren wir folgendermaßen eine Multiplikation auf $K[T]$:

$$P \cdot Q = \sum_{k=1}^{n+m} c_k T^k \text{ mit } c_k = \sum_{i+j=k} a_i b_j.$$

Es lässt sich leicht zeigen, dass $K[T]$ mit diesen beiden Verknüpfungen ein kommutativer Ring mit Eins ist und eine kompatible Struktur als K-Vektorraum derart besitzt, dass für alle λ aus K sowie Polynome P und Q aus $K[T]$ gilt:

$$\lambda(P \cdot Q) = (\lambda P) \cdot Q = P(\lambda Q).$$

Solche Ringe heißen *kommutative K-Algebren*.

Bemerkung B.3. Der Polynomring $K[T]$ ist ein Integritätsbereich (siehe Definition 2.12): Wenn P und Q beide nicht trivial sind, so ist $PQ \neq 0$, da

$$c_{\deg(P)+\deg(Q)} = a_{\deg(P)} b_{\deg(Q)} \neq 0_K.$$

Hierfür benutzen wir, dass der Körper K ein Integritätsbereich ist.

Insbesondere ist $\deg(PQ) = \deg(P) + \deg(Q)$.

Bemerkung B.4. Der Polynomring über K in einer Variablen kann leicht in folgender Weise konstruiert werden. Betrachte die Menge $\mathcal{I}$ aller abzählbaren Folgen $(a_n)_{n\in\mathbb{N}}$ aus K derart, dass alle bis auf endlich viele a_n Null sind.

Die Folge $(a_n)_{n\in\mathbb{N}}$ aus $\mathcal{I}$ ist eindeutig in Korrespondenz mit dem Polynom

$$P(T) = a_0 + a_1 T + \cdots$$

Beachte, dass wegen der Definition von $\mathcal{I}$ der obige Ausdruck in der Tat ein Polynom ist. Die Summe von Polynomen ist in Korrespondenz mit der koordinatenweisen Summe von Folgen. Allerdings entspricht das Produkt von Polynomen nicht dem koordinatenweisen Produkt von Folgen. Die Nullfolge $(0)_{n\in\mathbb{N}}$ stellt das triviale Polynom dar.

Der Polynomring ist bis auf K-Algebra-Isomorphismus eindeutig bestimmt. Daher reden wir von dem Polynomring anstatt von einem Polynomring.

Satz B.5. (*Division mit Rest*) *Gegeben Polynome P und Q mit* $\deg(Q) > 0$*, existieren eindeutig bestimmte Polynome H und R mit*

$$P = HQ + R \text{ und } \deg(R) < \deg(Q).$$

Das Polynom H ist der *Quotient* und das Polynom R der *Rest* der Division mit Rest von P durch Q. Wenn $R = 0$ ist, dann *teilt* Q das Polynom P. Das Polynom Q ist ein *echter Teiler (oder Faktor)* von P, falls Q das Polynom P teilt und $0 < \deg(Q) < \deg(P)$.

Beweis. **Existenz:** Wenn $\deg(P)$ in der Menge $\{-\infty, 0, 1, \ldots, \deg(Q) - 2\}$ liegt, setze $H = 0$ und $R = P$. Ohne Beschränkung der Allgemeinheit können wir annehmen, dass $\deg(P) = \deg(Q) - 1 + k$ für eine natürliche Zahl k. Wir beweisen die Existenz des Quotienten und des Restes induktiv über k. Für $k = 0$ setze $H = 0$ und $R = P$. Für $k > 0$ schreibe

$$P = \sum_{i=1}^{\deg(P)} a_i T^i \text{ und } Q = \sum_{j=1}^{\deg(Q)} b_j T^j,$$

mit $a_{\deg(P)} \neq 0_K$ und $b_{\deg(Q)} \neq 0_K$. Setze nun

$$P' = P - a_{\deg(P)} b_{\deg(Q)}^{-1} T^{k-1} Q = c_0 + c_1 T + \cdots + c_{\deg(P)-1} T^{\deg(P)-1}$$

für gewisse Elemente c_i aus K (es wird nicht behauptet, dass $c_{\deg(P)-1} \neq 0_K$). Beachte, dass $\deg(P') \leq \deg(P) - 1 = \deg(Q) - 1 + k - 1$. Wegen der Induktionsannahme gibt es H' und R' mit $\deg(R') < \deg(Q)$ und

$$P - a_{\deg(P)} b_{\deg(Q)}^{-1} T^k Q = H'Q + R',$$

also

$$P = \left(a_{\deg(P)} b_{\deg(Q)}^{-1} T^k + H'\right) Q + R',$$

wie gewünscht.

Eindeutigkeit: Wir nehmen an, dass $P = QH_1 + R_1 = QH_2 + R_2$ mit $\deg(R_1), \deg(R_2) < \deg(Q)$. Dann gilt

$$R_1 - R_2 = Q(H_2 - H_1).$$

Weil der Grad von $R_1 - R_2$ echt kleiner als $\deg(Q)$ ist, muss das Polynom $H_2 - H_1$ trivial sein. Das heißt, dass $H_1 = H_2$ und somit $R_1 = R_2$, wie gewünscht. □

Bemerkung B.6. Jedes Polynom $P = \sum_{i=0}^{n} a_i T^i$ definiert in folgender Weise eine Abbildung auf K:

$$\begin{array}{rccc} P: & K & \to & K \\ & c & \mapsto & \sum_{i=0}^{n} a_i c^i \end{array}$$

Das Element c aus K ist eine *Nullstelle* von P, falls $P(c) = 0$. Zum Beispiel besitzt das Polynom $T^2 - 3$ zwei Nullstellen in $\mathbb{R}$, aber das Polynom $T^2 + 1$ hat keine Nullstellen in $\mathbb{R}$.

Für das triviale Polynom ist jedes Element aus K eine Nullstelle, aber ein konstantes nicht-triviales Polynom besitzt keine Nullstelle.

Korollar B.7. *Gegeben ein Element c aus K, lässt sich jedes nicht-konstante Polynom P eindeutig als*

$$P = (T - c)^k H + P(c)$$

schreiben, für ein Polynom H mit $H(c) \neq 0_K$ und eine natürliche Zahl k. Insbesondere ist $k \geq 1$ und

$$P = (T - c)^k H,$$

wenn c eine Nullstelle von P ist.

Die Zahl $k = \mathrm{ord}_c(P)$ heißt die *Vielfachheit* der Nullstelle c.

Beweis. Wir zeigen zuerst, dass eine solche Darstellung eindeutig ist: Angenommen, dass

$$P = (T - c)^k H + P(c) = (T - c)^\ell H' + P(c),$$

mit $k \neq \ell$, können wir ohne Beschränkung der Allgemeinheit annehmen, dass $k < \ell$, also

$$(T - c)^k H = (T - c)^{k+(\ell-k)} H' = (T - c)^k (T - c)^{\ell-k} H'.$$

Weil der Polynomring ein Integritätsbereich ist, folgt sofort, dass

$$H = (T - c)^{\ell-k} H'.$$

Weil $H(c) \neq 0_K$, jedoch $\ell - k \geq 1$, liefert dies den gewünschten Widerspruch.

Die Existenz wird induktiv über $\deg(P)$ bewiesen. Weil P nicht konstant ist, ist $\deg(P)$ eine positive natürliche Zahl. Wir wenden nun Division mit Rest B.5 für $Q = T - c$ (welches nicht-trivial ist) an. Also

$$P = (T - c)P_1 + R,$$

wobei $\deg(R) < \deg(T - c) = 1$. Dies bedeutet, dass $R = b$ ein konstantes Polynom ist (möglicherweise ist der Rest R das triviale Polynom). Wenn wir in die obige Gleichung c einsetzen, erhalten wir $P(c) = R(c) = b$.

Wir machen nun eine Fallunterscheidung: Falls $P_1(c) \neq 0_K$, setze $H = P_1$ und $k = 1$. Wenn $P_1(c) = 0_K$, beachte, dass P_1 nicht konstant sein kann, denn sonst wäre $P_1 = 0_{K[T]}$ und somit wäre $P = P(c)$ konstant. Weil

$$\deg(P) = \deg\big((T - c)P_1 + R\big) = \max(\deg((T - c)P_1), 0) = \deg\big((T - c)P_1\big) = 1 + \deg(P_1),$$

schreibe nun induktiv P_1 als

$$P_1 = (T - c)^\ell H + P_1(c) = (T - c)^\ell H,$$

mit $H(c) \neq 0_K$. Insbesondere ist

$$P = (T-c)P_1 + P(c) = (T-c)\big((T-c)^\ell H\big) + P(c) = (T-c)^{\ell+1}H + P(c),$$

also setze $k = \ell + 1$. □

Korollar B.8. *Jedes nicht-triviale Polynom P über K lässt sich (bis auf Permutation) eindeutig schreiben als*

$$P = (T-c_1)\cdots(T-c_k)P_0,$$

für eine natürliche Zahl $0 \leq k \leq \deg(P)$ sowie Elemente $c_1, \ldots, c_k$ aus K (möglicherweise mit Wiederholungen) und ein Polynom P_0, das keine Nullstelle in K besitzt.

Insbesondere besitzt ein nicht-triviales Polynom höchstens $\deg(P)$ viele Nullstellen im Körper K.

Beweis. Da jede Nullstelle von P eines der Elemente c_i sein muss, folgt die zweite Behauptung sofort aus der obigen Darstellung. Wir beweisen die Existenz einer solchen Darstellung wie oben induktiv über $\deg(P)$. Wenn $\deg(P) = 0$, ist das Polynom P konstant und besitzt keine Nullstelle in K. Setze also $k = 0$ und $P_0 = P$. Wir nehmen nun an, dass $\deg(P) \geq 1$. Wenn P keine Nullstelle in K besitzt, sind wir fertig: setze $k = 0$ und $P_0 = P$. Sei also c_1 eine Nullstelle von P. Mit Hilfe des Korollars B.7 schreiben wir $P = (T-c_1)^{\mathrm{ord}_c(P)}H$ für ein Polynom H mit $H(c_1) \neq 0_K$. Weil $\mathrm{ord}_c(P) \geq 1$, ist

$$\deg\Big((T-c_1)^{\mathrm{ord}_c(P)-1}H\Big) < \deg(P)$$

und so können wir induktiv schreiben

$$(T-c_1)^{\mathrm{ord}_c(P)-1}H = (T-c_2)\cdots(T-c_k)P_0,$$

für eine natürliche Zahl k mit $k-1 \leq \deg\Big((T-c_1)^{\mathrm{ord}_c(P)-1}H\Big)$, wobei das Polynom P_0 keine Nullstelle in K besitzt. Insbesondere ist $k \leq \deg(P)$ und

$$P = (T-c_1)^{\mathrm{ord}_c(P)}H = (T-c_1)\big((T-c_1)^{\mathrm{ord}_c(P)-1}H\big) = (T-c_1)\cdots(T-c_k)P_0,$$

wie gewünscht. Die Eindeutigkeit der Darstellung folgt leicht aus der Kommutativität des Polynomringes, zusammen mit der Bemerkung B.3. □

Aufgabe. Kann die Menge $\{P(c)\}_{c\in K}$ endlich sein, wenn P ein nicht-konstantes Polynom ist?

C Der Hauptsatz der Algebra

Wir werden in diesem Abschnitt einen *einfachen* Beweis des Hauptsatzes der Algebra sehen, welcher nur den Zwischenwertsatz für Polynome ungeraden Grades über $\mathbb{R}$ benutzt.

Satz C.1. (*Der Hauptsatz der Algebra*) *Der Körper $\mathbb{C}$ der komplexen Zahlen ist algebraisch abgeschlossen.*

Beweis. Beachte, dass die Körpererweiterung $\mathbb{R} \subset \mathbb{C}$ algebraisch vom Grad 2 ist. Wegen der Bemerkung 3.43 müssen wir nur zeigen, dass $\mathbb{C}$ keine echte endliche algebraische Körpererweiterung $L \supset \mathbb{C}$ besitzt. Weil die Körpererweiterung $\mathbb{R} \subset L$ endlich algebraisch ist, können wir mit Hilfe der Bemerkung 3.38 annehmen, dass $\mathbb{R} \subset L$ galoissch ist mit Galoisgruppe $G = \mathrm{Gal}(L/\mathbb{R})$. Aus der Bemerkung 3.37 und dem Korollar 3.8 folgt, dass

$$|G| = [L : \mathbb{R}] = [L : \mathbb{C}] \cdot [\mathbb{C} : \mathbb{R}] = 2[L : \mathbb{C}],$$

also schreibe $|G| = 2^e m$ mit $e \geq 1$ und m ungerade. Wähle eine 2-Sylowgruppe S von G mit Hilfe des Lemmas 1.60. Aus der Galoiskorrespondenz 3.39 bekommen wir den folgenden Turm von Körpererweiterungen

$$\begin{array}{c} L \\ | \, 2^e \\ F = \mathrm{Fix}(S) \\ | \, m \\ \mathbb{R} \end{array}$$

Beachte, dass die Körpererweiterung $\mathbb{R} \subset F$ separabel ist, weil wir in Charakteristik Null sind. Aus dem Satz des primitiven Elementes 3.29 folgt also $F = \mathbb{R}(a)$ für ein primitives Element a aus F mit Minimalpolynom $m_a(T)$ von ungeradem Grad m. Nun besitzt jedes nicht-konstante Polynom ungeraden Grades über $\mathbb{R}$ eine Nullstelle in $\mathbb{R}$, also muss $m_a(T)$ linear sein, weil es irreduzibel ist. Es folgt, dass $\mathbb{R} = F = \mathrm{Fix}(S)$. Also ist $S = G$ eine 2-Gruppe der Ordnung 2^e. Wir müssen daher nur zeigen, dass $e = 1$ und somit $L = \mathbb{C}$, wie gewünscht.

Wir nehmen sonst an, dass $e \geq 2$ und betrachten die Untergruppe $H = \mathrm{Gal}(L/\mathbb{C})$ mit $|H| = 2^{e-1} \geq 2$ (weil $[\mathbb{C} : \mathbb{R}] = 2$). Wegen des Korollars 1.58 besitzt H einen Normalteiler N von Index 2. Mit Hilfe der Proposition 3.41 gewinnen wir den folgenden Turm von Körpererweiterungen

$$\left.\begin{array}{c} L \\ | \, 2^{e-2} \\ F_1 = \mathrm{Fix}(N) \\ | \, 2 \\ \mathbb{C} \end{array}\right\} 2^{e-1}$$

Die quadratische Körpererweiterung $\mathbb{C} \subset F_1$ ist also der Form $\mathbb{C}(\sqrt{z})$ für eine komplexe Zahl z, welche kein Quadrat in $\mathbb{C}$ besitzt. Wir müssen somit nur noch zeigen, dass jede komplexe Zahl z bereits eine quadratische Wurzel in $\mathbb{C}$ besitzt.

Sei also $0 \neq z = a + ib$ eine beliebige komplexe Zahl. Der Standardabsolutbetrag $|z| = \sqrt{a^2 + b^2} \geq |a|$. Da

$$b^2 = |z|^2 - a^2 = (|z| - a)(|z| + a),$$

müssen die beiden reellen Zahlen $|z| + a$ und $|z| - a$ positiv sein. Schreibe also

$$x^2 = \frac{|z| + a}{2} \text{ und } y^2 = \frac{|z| - a}{2}$$

für reelle Zahlen x und y. Es lässt sich sofort zeigen, dass

$$a + ib = z = x^2 - y^2 + 2ixy = (x + iy)^2,$$

wie gewünscht. □

D Quadratische Reziprozität

Definition D.2. Wir sagen, dass eine Kongruenzklasse $\bar{a}$ *ein Quadrat in* $\mathbb{F}_p$ ist, wenn es eine natürliche Zahl x gibt, sodass $x^2 \equiv a$ modulo $\mathbb{F}_p$. Gegeben eine ungerade Primzahl p definiere das *Legendre-Symbol* folgendermaßen:

$$\begin{array}{rcl} \mathbb{Z} & \to & \{0,1,-1\} \\ a & \mapsto & \left(\frac{a}{p}\right) = \begin{cases} 0, \text{ falls } p \text{ die Zahl } a \text{ teilt} \\ 1, \text{ falls die Kongruenzklasse } \bar{a} = a + p\mathbb{Z} \neq 0_{\mathbb{F}_p} \text{ ein Quadrat in } \mathbb{F}_p \text{ ist} \\ -1, \text{falls die Kongruenzklasse } \bar{a} = a + p\mathbb{Z} \neq 0_{\mathbb{F}_p} \text{ kein Quadrat in } \mathbb{F}_p \text{ ist} \end{cases} \end{array}$$

Bemerkung D.3. Klarerweise ist $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$, falls a und b kongruent modulo p sind. Insbesondere induziert das Legendre-Symbol eine Abbildung

$$\begin{array}{rcl} \mathbb{F}_p^* = \mathbb{F}_p \setminus \{0_{\mathbb{F}_p}\} & \to & \{1,-1\} \\ \bar{a} & \mapsto & \left(\frac{a}{p}\right) \end{array} .$$

Beachte, dass $\left(\frac{a^2}{p}\right) = 1$ ist.

Lemma D.4. (*Eulers Kriterium*) *Gegeben eine ungerade Primzahl p und ein ganze Zahl a mit Kongruenzklasse $\bar{a} \neq 0_{\mathbb{F}_p}$, so gilt*

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

Insbesondere ist die induzierte Abbildung

$$\begin{array}{rcl} \mathbb{F}_p^* & \to & \{1,-1\} \\ \bar{a} & \mapsto & \left(\frac{a}{p}\right) \end{array}$$

ein Gruppenhomomorphismus.

Beweis. Beachte zuerst, dass 1 und -1 nicht kongruent modulo p sind, da p ungerade ist. Des Weiteren zerfällt das Polynom

$$(T^2 - 1) = (T - 1) \cdot (T + 1)$$

in zwei verschiedenen Linearfaktoren modulo $\mathbb{F}_p$. Aus dem kleinen Satz von Fermat 2.26 folgt, dass

$$\bar{a}^{p-1} = (\bar{a}^{\frac{p-1}{2}})^2 = 1_{\mathbb{F}_p}$$

für $\bar{a} \neq 0_{\mathbb{F}_p}$. Insbesondere kann $\bar{a}^{\frac{p-1}{2}}$ nur die Werte 1 und -1 (modulo p) annehmen. Wir müssen also nur zeigen, dass $\bar{a}$ ein Quadrat in $\mathbb{F}_p^*$ genau dann ist, wenn $\bar{a}^{\frac{p-1}{2}} = 1$ (Wir identifizeren die Zahl 1 mit der Kongruenzklasse $1_{\mathbb{F}_p}$).

Klarerweise, wenn $\bar{a} = \bar{b}^2$, so ist $\bar{b} \neq 0_{\mathbb{F}_p}$. Nun ist

$$\bar{a}^{\frac{p-1}{2}} = (\bar{b}^2)^{\frac{p-1}{2}} = \bar{b}^{p-1} = 1$$

aus dem kleinen Satz von Fermat.

Wir nehmen also nun an, dass $\bar{a}^{\frac{p-1}{2}} = 1$ und folgern, dass $\bar{a}$ ein Quadrat in $\mathbb{F}_p^*$ ist. Aus der Proposition 3.32 folgt, dass die multiplikative Gruppe $\mathbb{F}_p^*$ zyklisch der Mächtigkeit $p-1$ ist, so wähle ζ ein erzeugendes Element. Schreibe $\bar{a} = \zeta^k$ für eine Zahl $1 \leq k \leq p-1$. Nun ist

$$1 = \bar{a}^{\frac{p-1}{2}} = \zeta^{k\frac{p-1}{2}},$$

also teilt $p-1$ die Zahl $k\frac{p-1}{2}$ nach Korollar 1.32. Es folgt somit, dass k gerade sein muss, so $k = 2k'$. Nun ist

$$\bar{a} = \zeta^k = (\zeta^{k'})^2$$

ein Quadrat in $\mathbb{F}_p^*$, wie gewünscht.

Für die letzte Behauptung, beachte, dass

$$\left(\frac{a \cdot b}{p}\right) = (\bar{a} \cdot \bar{b})^{\frac{p-1}{2}} = \bar{a}^{\frac{p-1}{2}} \cdot \bar{b}^{\frac{p-1}{2}} = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right),$$

also ist das Legendre-Symbol multiplikativ, wie gewünscht. □

Korollar D.5. (*Erster Ergänzungssatz*) *Gegeben eine ungerade Primzahl p, so gilt*

$$(-1_{\mathbb{F}_p}) \text{ ein Quadrat in } \mathbb{F}_p \iff p \equiv 1 \mod 4.$$

Um das quadratische Reziprozitätsgesetz zu zeigen, benötigen wir zuerst zwei Hilfslemmata.

Lemma D.6. (*Der Satz von Wilson*) *Für jede Primzahl p (möglicherweise auch $p = 2$) gilt:*

$$(p-1)! = 1 \cdots (p-1) \equiv (-1) \mod p.$$

Beweis. Der Satz ist trivial für $p = 2$ und $p = 3$, wir nehmen also ohne Beschränkung der Allgemeinheit an, dass $p \geq 5$ eine ungerade Primzahl ist.

Gegeben eine nicht-triviale Kongruenzklasse $\bar{a}$ aus $\mathbb{F}_p^*$, ist $\bar{a}$ gleich $\bar{a}^{-1}$ genau dann, wenn $\bar{a}^2 = 1_{\mathbb{F}_p}$ oder äquivalent dazu, wenn $\bar{a}$ entweder $1_{\mathbb{F}_p}$ oder $-1_{\mathbb{F}_p} = \overline{p-1}$. Dies bedeutet, dass im obigen Produkt

$$1 \cdot 2 \cdots (p-2) \cdot (p-1)$$

das Inverse $\bar{a}^{-1}$ von der Restklasse $\bar{a}$ aus $\{2, \ldots, p-2\}$ wiederum in dieser Menge liegt. Somit folgt sofort, dass

$$1 \cdot 2 \cdots (p-2) \cdot (p-1) \equiv 1^{\frac{p-1}{2}+1} \cdot (-1) \mod p,$$

wie gewünscht. □

Lemma D.7. *Gegeben eine ungerade Primzahl p, so gilt*

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (p-1)! \cdot (-1)^{\frac{p-1}{2}} \mod p.$$

Beweis. Für $1 \leq k \leq \frac{p-1}{2}$, so liegt $p-k$ in der Menge $\{\frac{p-1}{2}+1, \ldots, p-1\}$. Des Weiteren sind $p-k$ und $-k$ kongruent modulo p. Daraus folgt, dass

$$(p-1)! = 1 \cdots \left(\frac{p-1}{2}\right) \cdot \left(\frac{p-1}{2}+1\right) \cdots (p-1) \equiv \left(\left(\frac{p-1}{2}\right)!\right)^2 \cdot (-1)^{\frac{p-1}{2}} \mod p,$$

wie gewünscht. □

Satz D.8. (*Das quadratische Reziprozitätsgesetz*) *Gegeben zwei verschiedene ungerade Primzahlen p und q, so gilt*

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Dieses Gesetz ermöglicht es, schnell zu bestimmen, ob eine ungerade Primzahl ein Quadrat modulo einer anderen ungeraden Primzahl ist. Um zum Beispiel die Frage beantworten zu können, ob 7 ein Quadrat modulo 17 ist, müssen wir nur noch entscheiden, ob 17 ein Quadrat modulo 7 ist (oder äquivalent dazu aus der Bemerkung D.3, ob 3 ein Quadrat modulo 7), denn

$$\left(\frac{7}{17}\right) = (-1)^{8\cdot 3} \cdot \left(\frac{17}{7}\right) = \left(\frac{3}{7}\right).$$

Nun, hierfür können wir wieder das quadratische Reziprozitätsgesetz anwenden, denn $7 \equiv 1$ ist ein Quadrat modulo 3, so

$$\left(\frac{3}{7}\right) = (-1)^{1\cdot 3} \cdot \left(\frac{7}{3}\right) = -1.$$

Dies bedeutet, dass 7 kein Quadrat modulo 17 ist (obwohl wir nicht berechnet haben, welche Restklassen modulo 17 ein Quadrat sind).

Es gibt zahlreiche Beweise des quadratischen Reziprozitätsgesetzes. Wir haben uns dafür entschieden, einen gruppentheoretischen Beweis zu geben, der lediglich das eulersche Kriterium sowie den chinesischen Restsatz anwendet. Der angegebene Beweis ist im Wesentlichen aus dem Beweis von Rousseau [3] abgeschrieben.

Beweis. Sei G die multiplikative Gruppe $\mathcal{U}(\mathbb{Z}/pq\mathbb{Z})$, welche aus dem chinesischen Restsatz 2.18 zum kartesischen Produkt $\mathcal{U}(\mathbb{Z}/p\mathbb{Z}) \times \mathcal{U}(\mathbb{Z}/qZ)$ isomorph ist. In G betrachte die Untergruppe $H = \{1_G, -1_{\mathbb{Z}/pq\mathbb{Z}}\}$ (beachte, dass $-1_{\mathbb{Z}/pq\mathbb{Z}}$ die Kongruenzklasse der Zahl $pq-1$ darstellt).

Durch den obigen Isomorphismus können wir Elemente aus G als Paare (a, b) in $\mathbb{F}_p \times \mathbb{F}_q$ darstellen. Somit entspricht H die Untergruppe $H' = \{(1_{\mathbb{F}_p}, 1_{\mathbb{F}_q},), (-1_{\mathbb{F}_p}, -1_{\mathbb{F}_q})\}$, denn $pq-1$ ist genau kongruent zu -1 modulo p und modulo q. Wir betrachten nun das Produkt

$$\theta = \prod_{g \in G/H} gH$$

der verschiedenen Klassen von Elementen aus G modulo H sind. Dieses Produkt werden wir erstmal intrinsisch in G/H berechnen und dann auch als Paare in $\mathbb{F}_p \times \mathbb{F}_q$ modulo H'.

Beachte, dass die Klasse gH gleich der Menge $\{g, -g\}$ ist. Daraus folgt, dass wir wie im Beweis vom Lemma D.7 im Produkt θ nur die Einheiten in $\{1, \cdots, \frac{pq-1}{2}\}$ multiplizieren müssen. Dies ist gerade die Teilmenge der Elemente, die weder durch p noch durch q teilbar sind. Sei A die Menge der Elemente aus $\{1, \cdots, \frac{pq-1}{2}\}$, welche nicht durch p teilbar sind, sowie B die Teilmenge aus A der Elemente, welche sich von q teilen lassen. Folglich

$$B = \{q, 2q, \ldots, \frac{p-1}{2}q\}$$

und

$$\begin{aligned} A = \{&1, 2, \ldots, p-1, \\ &p+1, p+2, \ldots, 2p-1, \\ &2p+1, 2p+2, \ldots, 3p-1, \\ &\qquad \ddots \\ &\frac{q-1}{2}p+1, \frac{q-1}{2}p+2, \ldots, \frac{pq-1}{2}\}. \end{aligned}$$

Die erste Koordinate von θ (bezüglich dem Isomorphismus, welcher G als Paare in $\mathbb{F}_p \times \mathbb{F}_q$ darstellt) ist also $\prod_{k\in A\setminus B} \bar{k}$ (modulo H'), oder äquivalent dazu,

$$\frac{\prod_{k\in A} \bar{k}}{\prod_{k\in B} \bar{k}} \overset{\text{mod } \mathbb{F}_p}{=} \frac{(p-1)!^{\frac{q-1}{2}} \left(\frac{p-1}{2}\right)!}{q \cdot 2q \cdots \frac{p-1}{2}q} \overset{\text{Wilson}D.6}{=} \frac{(-1_{\mathbb{F}_p})^{\frac{q-1}{2}} \left(\frac{p-1}{2}\right)!}{\left(\frac{p-1}{2}\right)! \, q^{\frac{p-1}{2}}} \overset{\text{Euler}D.4}{=} \frac{(-1_{\mathbb{F}_p})^{\frac{q-1}{2}}}{\left(\frac{q}{p}\right)} = (-1_{\mathbb{F}_p})^{\frac{q-1}{2}} \cdot \left(\frac{q}{p}\right).$$

Analog ist die zweite Koordinate von θ gleich dem Produkt $(-1_{\mathbb{F}_q})^{\frac{p-1}{2}} \cdot \left(\frac{p}{q}\right)$.

Nun, wie im Beweis vom Lemma D.7, wenn b aus $\{1, \ldots, \frac{q-1}{2}\}$ so liegt ein Repräsentant der Restklasse von $-b$ in der Menge $\{\frac{q+1}{2}, \cdots, q-1\}$. Es folgt, dass das Produkt θ sich also (modulo H') darstellen lässt durch

$$\prod_{\substack{1\le a\le p-1 \\ 1\le b\le \frac{q-1}{2}}} (a, b).$$

In dieser Darstellung kommt also jede zweite Koordinate $p-1$-mal vor, daher ist die zweite Koordinate von θ gerade

$$\left((\frac{q-1}{2})!\right)^{p-1} = \left(\left((\frac{q-1}{2})!\right)^2\right)^{\frac{p-1}{2}} \overset{D.7}{=} \left((-1_{\mathbb{F}_q})^{\frac{q-1}{2}} \cdot (q-1)!\right)^{\frac{p-1}{2}} \overset{\text{Wilson}D.6}{=} (-1_{\mathbb{F}_q})^{\frac{p-1}{2}} \cdot (-1_{\mathbb{F}_q})^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Nun kommt der Wert a in der ersten Koordinate des obigen Produktes $q-1$-mal vor, die erste Koordinate von θ ist daher gleich

$$\left(\prod_{1\le a\le p-1} a\right)^{\frac{q-1}{2}} = ((p-1)!)^{\frac{q-1}{2}} \overset{\text{Wilson}D.6}{=} (-1_{\mathbb{F}_p})^{\frac{q-1}{2}}.$$

Wenn wir beide Darstellungen vergleichen, sehen wir, dass

$$\left((-1_{\mathbb{F}_p})^{\frac{q-1}{2}}, (-1_{\mathbb{F}_q})^{\frac{p-1}{2}} \cdot (-1_{\mathbb{F}_q})^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\right) = \pm\left((-1_{\mathbb{F}_p})^{\frac{q-1}{2}} \cdot \left(\frac{q}{p}\right), (-1_{\mathbb{F}_q})^{\frac{p-1}{2}} \cdot \left(\frac{p}{q}\right)\right),$$

oder äquivalent dazu,

$$\left(1, (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\right) = \pm\left(\left(\frac{q}{p}\right), \left(\frac{p}{q}\right)\right).$$

Falls $\left(\frac{q}{p}\right) = 1$, so ist $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$ und

$$\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}},$$

wie gewünscht. Falls nun $\left(\frac{q}{p}\right) = -1$, so ist $-\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$. Wir schließen, dass

$$\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

□

Aufgabe. Zeige, dass eine ungerade Zahl $p \neq 5$ genau dann kongruent zu 1 oder 4 modulo 5 ist, wenn 5 ein Quadrat in $\mathbb{F}_p$ besitzt.

Schließe daraus, dass es unendliche viele Primzahlen gibt, welche kongruent zu 4 modulo 5 sind. Hierfür betrachte $n = (2p_1 \cdots pk)^2 - 5$, wobei $p_1, \ldots, p_k$ ungerade Primzahlen verschieden von 5 sind, welche bereits kongruent zu 4 modulo 5 sind.

Literaturverzeichnis

[1] A. Huber-Klawitter, *Algebra und Zahlentheorie*, Skript, (2021), `http://home.mathematik.uni-freiburg.de/arithgeom/lehre/ws21/azt/algebra21.pdf`

[2] S. Kebekus, *Algebra und Zahlentheorie*, Skript, (2021).

[3] G. Rousseau, *On the quadratic reciprocity law*, Journal of the Australian Mathematical Society **51** (1991), 423–425.

[4] M. Ziegler, *Einführung in die Algebra*, Skript, (2014), `https://home.mathematik.uni-freiburg.de/ziegler/skripte/algebra.pdf`