

Algebra

Anton Deitmar
Sommer 2026

Inhaltsverzeichnis

1	Gruppen	2
1.1	Gruppenordnung	2
1.2	Nebenklassen	5
1.3	Homomorphismen und Operationen	8
1.4	Zyklische Gruppen	16
1.5	Normalteiler	17
1.6	Homomorphiesätze	20
1.7	Freie Gruppen	24
1.8	Sylow-Gruppen	25
1.9	Kommutatoren	31
2	Ringe	34
2.1	Definition	34
2.2	Ideale	37
2.3	Der chinesische Restsatz	41
2.4	Teilbarkeit	43
2.5	Quotientenkörper	48
2.6	Polynomringe	50
3	Körper	53
3.1	Homomorphismen und Erweiterungen	53
3.2	Adjunktion von Nullstellen	56
3.3	Algebraische und endliche Körpererweiterungen	60
3.4	Algebraischer Abschluss	64
3.5	Zerfällungskörper und normale Erweiterungen	67
3.6	Separable Körpererweiterungen	70
3.7	Separabilitätsgrad	72
3.8	Primitive Elemente	77
3.9	Galois-Erweiterungen	81
3.10	Endliche Körper	87
3.11	Der Fundamentalsatz der Algebra	90
3.12	Kreisteilungskörper und das Galois-Umkehrproblem	92
3.13	Konstruktionen mit Zirkel und Lineal	97
3.14	Auflösbarkeit in Radikalen	103
3.15	Unendliche Erweiterungen	109

1 Gruppen

1.1 Gruppenordnung

Definition 1.1.1. Sei G eine Gruppe und $S \subset G$ eine Teilmenge. Wir schreiben

$$\langle S \rangle$$

für die von S **erzeugte Untergruppe**, also

$$\langle S \rangle = \bigcap_{\substack{H \supset S \\ H \text{ Untergruppe von } G}} H.$$

Lemma 1.1.2. Die Gruppe $\langle S \rangle$ besteht genau aus allen Gruppenelementen der Form $s_1 s_2 \cdots s_k$ wobei $k \in \mathbb{N}$ und für jedes j gilt

$$s_j \in S \quad \text{oder} \quad s_j^{-1} \in S.$$

Beweis. Sei $\widehat{S}$ die Menge all dieser Produkte in G . Dann gilt $\widehat{S} \subset \langle S \rangle$. Da aber $\widehat{S}$ selbst schon eine Gruppe ist, tritt $\widehat{S}$ in dem Schnitt auf und daher folgt Gleichheit. □

Definition 1.1.3. Ist G eine endliche Gruppe, so nennt man die Anzahl $|G|$ der Elemente die **Ordnung** der Gruppe G ,

$$\text{ord}(G) = |G|.$$

Wir schreiben auch 1 für das neutrale Element e einer Gruppe.

Ist $a \in G$, so bezeichnet $\langle a \rangle$ die von a **erzeugte Gruppe**, also die kleinste Untergruppe von G , die a enthält. Diese beschreibt man einmal als

$$\langle a \rangle = \bigcap_{\substack{H \text{ Untergruppe} \\ H \ni a}} H,$$

wobei man sich klarmachen muss, dass dies wieder eine Untergruppe ist. Andererseits kann man $\langle a \rangle$ konstruktiv beschreiben:

$$\langle a \rangle = \{a^k : k \in \mathbb{Z}\}.$$

Ist $\langle a \rangle$ eine endliche Gruppe, so nennt man die Ordnung von $\langle a \rangle$ auch die **Ordnung** des Elements a und man schreibt

$$\text{ord}(a) = \text{ord}(\langle a \rangle) = |\langle a \rangle|.$$

Ist $\langle a \rangle$ nicht endlich, so setzt man $\text{ord}(a) = \infty$.

Beispiele 1.1.4. (a) $\text{Per}(n)$ ist die Gruppe der **Permutationen** der Menge $\{1, \dots, n\}$. Sie hat die Ordnung

$$|\text{Per}(n)| = n! = n(n-1)(n-2) \cdots 1.$$

(b) $\text{Per}^+(n)$ ist die Untergruppe der **geraden Permutationen**, also

$$\begin{aligned} \text{Per}^+(n) &= \{\sigma \in \text{Per}(n) : \text{sign}(\sigma) = 1\} \\ &= \{\tau_1 \tau_2 \cdots \tau_{2k} : \tau_1, \dots, \tau_{2k} \text{ Transpositionen}\} \end{aligned}$$

(c) Seien $n \in \mathbb{N}$, p eine Primzahl und $\mathbb{F}_p = \mathbb{Z}/p$ der Körper mit p Elementen. Die Gruppe $\text{GL}_n(\mathbb{F}_p)$ aller invertierbaren $n \times n$ Matrizen hat die Ordnung

$$\begin{aligned} |\text{GL}_n(\mathbb{F}_p)| &= (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1}) \\ &= p^{1+2+\cdots+(n-1)} (p^n - 1)(p^{n-1} - 1) \cdots (p - 1) \\ &= p^{\frac{n(n-1)}{2}} (p^n - 1)(p^{n-1} - 1) \cdots (p - 1). \end{aligned}$$

Begründung: Die erste Spalte kann alle Elemente von $\mathbb{F}_p^n$ enthalten, außer ohne den Nullvektor, es gibt also $p^n - 1$ mögliche erste Spalten. Die zweite Spalte kann alle Vektoren enthalten, außer den Vielfachen der ersten Spalte, also $p^n - p$ Vektoren und so weiter.

(d) Die Gruppe B_n aller oberen Dreiecksmatrizen in $\text{GL}_n(\mathbb{F}_p)$ hat

$$|B_n| = (p-1)^n p^{\frac{n(n-1)}{2}}$$

Elemente.

(e) Sei $n \in \mathbb{N}$ dann ist

$$\begin{aligned} \mu_n &= \{e^{2\pi i k/n} : 0 \leq k \leq n-1\} \\ &= \{z \in \mathbb{C} : z^n = 1\} \end{aligned}$$

eine Untergruppe von $\mathbb{C}^\times$, die Gruppe der **n -ten Einheitswurzeln**. Sie hat die Ordnung n .

- (f) Sei $n \in \mathbb{N}$ die **Diedergruppe** D_n , $n \geq 3$ der Ordnung $2n$ ist eine Gruppe erzeugt von zwei Elementen σ, τ mit den Relationen

$$\sigma^n = 1 = \tau^2 \quad \text{und} \quad \tau\sigma\tau^{-1} = \sigma^{-1}.$$

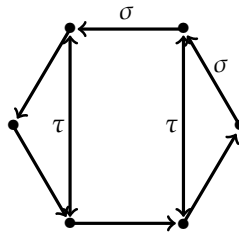
Insbesondere soll σ die Ordnung n haben und τ die Ordnung 2.

Das bedeutet, D_n besteht genau aus den Elementen

$$1, \sigma, \sigma^2, \dots, \sigma^{n-1}, \tau, \tau\sigma, \dots, \tau\sigma^{n-1}$$

und die Produkte dieser Elemente rechnet man mit den Relationen aus.

Man kann sie als Untergruppe von $\text{Per}(n)$ wie folgt darstellen. Stellen wir uns die Elemente von $\{1, 2, \dots, n\}$ auf einem Kreis in gleichen Abständen angeordnet vor. Dann ist σ die Rotation um den Winkel $2\pi/n$ und τ ist irgendeine Spiegelung an einer Geraden, die die Menge $\{1, \dots, n\}$ in sich abbildet.



Es gilt $D_2 \cong \mathbb{Z}/2$, sowie $D_4 \cong (\mathbb{Z}/2) \times (\mathbb{Z}/2)$ und schliesslich

$$D_6 \cong \text{Per}(3).$$

Lemma 1.1.5. Sei a ein Element der Gruppe G . Die von a erzeugte Gruppe $\langle a \rangle$ ist genau dann endlich, wenn es ein $n \in \mathbb{N}$ gibt mit $a^n = 1$. Es gilt

$$\text{ord}(a) = \min \{n \in \mathbb{N} : a^n = 1\}.$$

Ist k die Ordnung von a so gilt für jedes $n \in \mathbb{N}$

$$a^n = 1 \quad \Leftrightarrow \quad k \mid n.$$

Definition 1.1.6. Eine Gruppe, die von einem Element erzeugt wird, nennen wir eine **zyklische Gruppe**.

Sind G, H zwei Gruppen, so wird das Produkt $G \times H$ durch die Vorschrift

$$(g, h)(g', h') = (gg', hh')$$

eine Gruppe. Das neutrale Element ist $(1, 1)$. Das Inverse zu (g, h) ist (g^{-1}, h^{-1}) . Für die Ordnungen gilt

$$\text{ord}(G \times H) = \text{ord}(G) \text{ord}(H).$$

Beispiel 1.1.7. Wir bezeichnen mit $\mathbb{Z}/m\mathbb{Z}$ oder auch $\mathbb{Z}/m$ die **zyklische Gruppe** mit m Elementen, $m \in \mathbb{N}$, also die Gruppe $\{0, 1, 2, \dots, m-1\}$ mit Verknüpfung: $a \boxplus b = \text{Rest von } a + b \text{ modulo } m$.

1.2 Nebenklassen

Definition 1.2.1. Sei G eine Gruppe und sei $H \subset G$ eine Untergruppe. Ist $a \in G$, so ist die **Linksnebenklasse** von a nach H gleich der Menge

$$aH = \{ah : h \in H\}.$$

Da H eine Gruppe ist, gilt für $h \in H$ schon

$$hH = H.$$

Wir schreiben

$$G/H$$

für die Menge der H -Nebenklassen in G .

Beispiele 1.2.2. (a) Ist V ein Vektorraum und $U \subset V$ ein Unterraum, dann sind die Nebenklassen nach U genau die affinen Räume $v + U$, die U als linearen Teil haben.

(b) Sei $G = D_n$ die Diedergruppe und sei $H = \langle \tau \rangle$ die von τ erzeugte Untergruppe, dann ist $H = \{1, \tau\}$ und die H -Linksnebenklassen sind

$$\underbrace{\{1, \tau\}}_{=H}, \underbrace{\{\sigma, \sigma\tau\}}_{=\sigma H}, \dots, \underbrace{\{\sigma^{n-1}, \sigma^{n-1}\tau\}}_{=\sigma^{n-1}H}.$$

(c) Seien $G = \text{GL}_n(\mathbb{F}_p)$ und $H = B_n$, dann gibt es $p^{\frac{n(n-1)}{2}}$ Nebenklassen, also

$$|G/H| = p^{\frac{n(n-1)}{2}}$$

Begründung: Sei U die Untergruppe von $\text{GL}_n(\mathbb{F}_p)$ bestehend aus allen unteren Dreiecksmatrizen mit Einsen auf der Diagonalen. Wir behaupten

$$G/H = \bigsqcup_{u \in U} uH.$$

In LinA beweist man $G = UH = \{uh : u \in U, h \in H\}$, so dass jede Nebenklasse in der Form uH geschrieben werden kann. Es bleibt zu zeigen, dass zwei verschiedene $u, u' \in U$ zwei verschiedene Nebenklassen liefern. Es gelte also $uH = u'H$. Dann ist $u^{-1}u' \in H$ aber gleichzeitig ist $u^{-1}u' \in U$ und damit $u^{-1}u' = I$ also $u = u'$ wie gewünscht.

Lemma 1.2.3. *Sei G eine Gruppe und H eine Untergruppe. Die Anzahl der Nebenklassen $|G/H| \in \mathbb{N} \cup \{\infty\}$ wird der **Index** von H in G genannt. Zwei Linksnebenklassen sind entweder gleich oder disjunkt, daher kann man G disjunkt in seine Nebenklassen zerlegen, es gibt also eine Familie $(x_i)_{i \in I}$ in G so dass*

$$G = \bigsqcup_{i \in I} x_i H.$$

Beweis. Sei $xH \cap yH \neq \emptyset$. Wir zeigen $xH \subset yH$. Aus Symmetrie folgt dann die andere Richtung. Sei also $z \in xH \cap yH$, dann existieren $h_1, h_2 \in H$ so dass $z = xh_1 = yh_2$. Es folgt $x = yh_2h_1^{-1} \in yH$ und ist $u \in xH$, also $u = xh_3$, so folgt $u = xh_3 = y \underbrace{h_2h_1^{-1}h_3}_{\in H} \in yH$. □

Beispiele 1.2.4. (a) Sei $G = D_n$ die Diedergruppe und sei $H = \langle \tau \rangle$ die von τ erzeugte Untergruppe, dann ist $|G/H| = n$.

(b) Seien $G = \text{GL}_n(\mathbb{F}_p)$ und $H = B_n$, dann ist der Index $|G/H| = p^{\frac{n(n-1)}{2}}$.

Proposition 1.2.5. *Sei G eine endliche Gruppe. Ist H eine Untergruppe, dann ist die Ordnung $|H|$ ein Teiler der Ordnung $|G|$ von G . Genauer gilt*

$$|G| = |H||G/H|,$$

wobei G/H die Menge aller Nebenklassen aH ist.

Insbesondere gilt für jedes Element x

$$\text{ord}(x) \mid \text{ord}(G),$$

d.h., die Ordnung von x teilt die Gruppenordnung. Insbesondere folgt

$$x^{\text{ord}(G)} = 1.$$

Beweis. Wir haben $G = \bigsqcup_{i \in I} x_i H$, und da G endlich ist, muss I endlich sein, wir finden also $x_1, \dots, x_n \in G$ so dass $G = \bigsqcup_{j=1}^n x_j H$. Also folgt

$$\text{ord}(G) = \sum_{j=1}^n |x_j H|.$$

Die Untergruppe H bildet selbst eine Nebenklasse, wir können also $x_1 = e$ annehmen. Die Abbildung $h \mapsto x_j H$ ist eine Bijektion von H nach $x_j H$, also haben alle Nebenklassen gleich viele Elemente, nämlich $\text{ord}(H)$ viele, es ist also

$$\text{ord}(G) = \sum_{j=1}^n \text{ord}(H) = n \text{ord}(H).$$

Ist $a \in G$ ein beliebiges Element und ist $H = \langle a \rangle$ die von a erzeugte Untergruppe, dann ist $\text{ord}(a) = \text{ord}(H)$ ein Teiler von $\text{ord}(G)$. $\square$

Lemma 1.2.6. *Ist G eine abelsche Gruppe und $a, b \in G$ von endlichen Ordnungen m, n . Sind m und n teilerfremd, dann ist $\langle ab \rangle = \langle a, b \rangle$ und hat die Ordnung mn .*

Beweis. Wegen $(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m = 1$ hat ab endliche Ordnung k und diese ist ein Teiler von mn . Es gilt dann $1 = (ab)^k = a^k b^k$, also $a^k = b^{-k}$. Die Ordnung von a^k ist ein Teiler von m , die Ordnung von b^{-k} ist ein Teiler von n , daher müssen beide Ordnungen gleich 1 sein, also $a^k = 1 = b^k$. Damit ist k ein Vielfaches von m und von n , die Ordnung von ab ist also mn .

Es bleibt zu zeigen, dass $a, b \in \langle ab \rangle$. Da m und n teilerfremd sind, gibt es $x, y \in \mathbb{Z}$ mit $1 = mx + ny$. Daher ist $a = a^1 = a^{mx} a^{ny} = (a^m)^x (a^n)^y$. Damit folgt $(ab)^{ny} = a^{ny} b^{ny} = a^{ny} = a$ und daher liegt a in der von ab erzeugten Gruppe. Aus Symmetriegründen gilt dasselbe für b . $\square$

1.3 Homomorphismen und Operationen

Definition 1.3.1. Eine Abbildung $\phi : G \rightarrow H$ zwischen zwei Gruppen heisst **Gruppenhomomorphismus**, falls

$$\phi(ab) = \phi(a)\phi(b)$$

für alle $a, b \in G$ gilt.

Beispiele 1.3.2. (a) Die aus der LinA bekannt Signum-Abbildung $\text{sign} : \text{Per}(n) \rightarrow \{\pm 1\}$ ist ein Gruppenhomomorphismus.

(b) Ist G eine abelsche Gruppe und ist $n \in \mathbb{N}$, dann ist

$$x \mapsto x^n$$

ein Gruppenhomomorphismus $G \rightarrow G$, denn $(ab)^n = a^n b^n$.

(c) Die natürliche Abbildung $\phi : \text{Per}(n) \rightarrow \text{Per}(n+1)$ ist ein Gruppenhomomorphismus.

(d) Die Determinante $\det : \text{GL}_n(\mathbb{F}_p) \rightarrow \mathbb{F}_p^\times$ ist ein Gruppenhomomorphismus.

(e) Die Abbildung $\text{GL}_n(\mathbb{F}_p) \rightarrow \text{GL}_{n+1}(\mathbb{F}_p)$, $A \mapsto \begin{pmatrix} A & \\ & 1 \end{pmatrix}$ ist ein Gruppenhomomorphismus.

(f) Ist G eine Gruppe und ist $a \in G$, dann ist die Abbildung

$$\phi : x \mapsto axa^{-1}$$

Ein Homomorphismus von G nach G . Wir nenne diesen Homomorphismus die **Konjugation** mit a .

Beweis. Für $x, y \in G$ gilt $\phi(xy) = axya^{-1} = axa^{-1}aya^{-1} = \phi(x)\phi(y)$. □

(g) Sei G die Gruppe $\text{GL}_n(K)$ aller invertierbarer $n \times n$ Matrizen über dem Körper K . Dann ist die Abbildung $\psi : G \rightarrow G$,

$$\psi(A) = A^{-t} = (A^t)^{-1} = (A^{-1})^t$$

ein Gruppenhomomorphismus.

Definition 1.3.3. Ein Gruppenhomomorphismus $f : G \rightarrow H$ heisst **Isomorphismus**, wenn es einen Gruppenhomomorphismus $g : H \rightarrow G$ gibt so dass $f \circ g = \text{Id}_H$ und $g \circ f = \text{Id}_G$ ist.

Zwei Gruppen G, H heißen **isomorph**, falls es einen Isomorphismus zwischen Ihnen gibt. Wir schreiben in diesem Fall $G \cong H$.

Lemma 1.3.4. *Ein Gruppenhomomorphismus $f : G \rightarrow H$ ist genau dann ein Isomorphismus, wenn die Abbildung f bijektiv ist.*

Beweis. Die Abbildung f ist genau dann bijektiv, wenn es eine Umkehrabbildung gibt. Die Aussage des Lemmas ist also die, dass die Umkehrabbildung automatisch ein Gruppenhomomorphismus ist. Sei hierzu $g : H \rightarrow G$ die Umkehrabbildung. Für $x, y \in H$ gilt

$$f(g(xy)) = xy = f(g(x))f(g(y)) = f(g(x)g(y))$$

und da f injektiv ist, folgt $g(xy) = g(x)g(y)$, also ist g ein Gruppenhomomorphismus. □

Lemma 1.3.5. *Ist $\phi : G \rightarrow H$ ein Gruppenhomomorphismus, dann gilt $\phi(1) = 1$ und $\phi(a^{-1}) = \phi(a)^{-1}$.*

Beweis. Übungsaufgabe Blatt 1. □

Definition 1.3.6. Sei G eine Gruppe und M eine Menge. Eine **Operation** von G auf M ist eine Abbildung

$$\begin{aligned} G \times M &\rightarrow M \\ (g, m) &\mapsto g.m \end{aligned}$$

mit den Eigenschaften

- $1.m = m$ (das neutrale Element operiert neutral)
- $(ab).m = a.(b.m)$ (Operation und Multiplikation sind kompatibel)

Beispiele 1.3.7. (a) Sei G eine Gruppe. Dann definiert die Vorschrift

$$g.m = gm$$

eine Operation der Gruppe auf sich selbst, die **Linkstranslationsoperation**.

Beweis. Es gilt $1.m = 1m = m$ und $(ab).m = (ab)m = a(bm) = a.(b.m)$. □

(b) Sei G eine Gruppe, dann operiert G durch

$$g.m = mg^{-1}$$

auf sich selbst, dies ist die **Rechtstranslationsoperation**.

Beweis. Es gilt $1.m = m1^{-1} = m1 = m$ und $(ab).m = m(ab)^{-1} = (mb^{-1})a^{-1} = a.(b.m)$. $\square$

(c) Sei G eine Gruppe, dann operiert G auf sich selbst durch die Vorschrift

$$g.m = gm g^{-1}$$

dies ist die **Konjugationsoperation**.

Beweis. Es gilt $1.m = 1m1^{-1} = m$ und $(ab).m = abm(ab)^{-1} = abmb^{-1}a^{-1} = a.(b.m)$. $\square$

(d) (Abgeleitete Operationen.) Operiert die Gruppe G auf der Menge M und ist S eine weitere Menge, dann operiert G auf der Menge $A = \text{Abb}(M, S)$ aller Abbildungen von M nach S durch

$$g.\phi(m) = \phi(g^{-1}.m).$$

Beweis. Es ist $e.\phi(m) = \phi(e^{-1}.m) = \phi(m)$ und $(ab).\phi(m) = \phi((ab)^{-1}.m) = \phi(b^{-1}.a^{-1}.m) = b.\phi(a^{-1}.m) = a.(b.\phi(m))$. $\square$

(e) Die Gruppe $\text{GL}_n(\mathbb{F}_p)$ operiert durch Matrixmultiplikation auf $\mathbb{F}_p^n$. Dies folgt aus der Assoziativität der Matrixmultiplikation.

(f) Die Gruppe $\text{GL}_n(\mathbb{F}_p)$ operiert auf $M_n(\mathbb{F}_p)$ durch

$$x.a := xax^t,$$

wobei x^t die transponierte Matrix ist.

Lemma 1.3.8. Sei $M \neq \emptyset$ eine Menge. Operiert die Gruppe G auf der Menge M , dann ist die Abbildung $\phi : G \rightarrow \text{Per}(M)$, $g \mapsto (m \mapsto gm)$ ein Gruppenhomomorphismus. Ist umgekehrt $\phi : G \rightarrow \text{Per}(M)$ ein Gruppenhomomorphismus, dann definiert

$$gm = \phi(g)(m)$$

eine Operation. Diese Zuordnungen (Operation) $\mapsto$ (Gruppenhomomorphismus) und umgekehrt sind invers zueinander. Also ist eine Operation dasselbe wie ein Gruppenhomomorphismus nach $\text{Per}(M)$.

Beweis. Die Gruppe G operiere auf M . Für $g \in G$ sei $\phi(g) : M \rightarrow M$, $m \mapsto gm$. Zunächst müssen wir zeigen, dass $\phi(g)$ bijektiv ist, wir also wirklich in $\text{Per}(M)$

landen. Wir behaupten, dass $\phi(g^{-1})$ eine Umkehrabbildung zu $\phi(g)$ ist. Dies folgt aus

$$\phi(g)(\phi(g^{-1})(m)) = \phi(g)(g^{-1}m) = gg^{-1}m = 1m = m$$

und

$$\phi(g^{-1})(\phi(g)(m)) = \phi(g^{-1})(gm) = g^{-1}gm = 1m = m.$$

Wir haben also in der Tat eine Abbildung $\phi : G \rightarrow \text{Per}(M)$. Wir rechnen nun nach, dass dies ein Gruppenhomomorphismus ist. Für $g, h \in G$ gilt

$$\phi(gh)(m) = (gh)m = g(hm) = \phi(g)(hm) = \phi(g)(\phi(h)(m)) = \phi(g)\phi(h)(m).$$

Also ist ϕ ein Gruppenhomomorphismus. Die Umgekehrte Richtung ist leicht nachzurechnen und die Tatsache, dass diese Zuordnungen invers zueinander sind, auch. $\square$

Definition 1.3.9. Die Gruppe G operiere auf der Menge M . Für gegebenes $m \in M$ ist die Menge

$$Gm = \{gm : g \in G\}$$

die **Bahn** oder das **Orbit** von m . Ferner ist

$$G_m = \{g \in G : gm = m\}$$

der **Stabilisator** von m .

Beispiele 1.3.10. (a) Sei G eine Gruppe. Operiert die Gruppe durch Linkstranslation auf sich selbst, also $g.x = gx$, dann ist der Stabilisator immer gleich $\{1\}$.

(b) In der Operation von $\text{GL}_n(\mathbb{F}_p)$ auf $\mathbb{F}_p^n$ ist etwa der Stabilisator von $e_1 = (1, 0, \dots, 0)$ gleich der Menge aller Matrizen mit erster Spalte e_1 .

Satz 1.3.11. Die Gruppe G operiere auf der Menge M .

(a) Der Stabilisator eines Punktes $m \in M$ ist eine Untergruppe von G . Er wird auch die **Standgruppe** von m genannt.

(b) Sei $H = G_m$ die Standgruppe von m . Die Abbildung $gH \mapsto gm$ ist eine Bijektion von G/H zum Orbit von m .

(c) Die Orbits zweier Punkte sind entweder gleich oder disjunkt, man kann deshalb M disjunkt in seine Orbits zerlegen. Man schreibt $G \backslash M$ für die Menge aller Orbits.

(d) (Bahnengleichung) Sind G und M endliche Mengen, so gilt

$$|M| = \sum_{Gm \in G \backslash M} \frac{|G|}{|G_m|}.$$

Man kann Teil (c) auch so ausdrücken, dass man sagt: die Operation von G definiert eine Äquivalenzrelation auf M , wobei m und m' äquivalent heißen, falls sie in demselben Orbit liegen. Der Quotient nach dieser Äquivalenzrelation wird dann mit $G \backslash M$ bezeichnet.

Beweis. (a) Sei $H = G_m$, dann gilt offensichtlich $e \in H$. Sind $a, b \in H$, dann ist

$$(ab)m = a(bm) = am = m,$$

also liegt auch ab wieder in H . Ferner folgt aus $am = m$ durch Anwenden von a^{-1} schon $m = a^{-1}m$, so dass auch $a^{-1} \in H$ folgt. Also ist H eine Untergruppe.

(b) Sei $\psi : G/H \rightarrow Gm$ diese Abbildung. Zunächst ist festzustellen, dass sie überhaupt wohldefiniert ist, ist also $gH = g'H$, dann ist $g' = gh$ für ein $h \in H$ und damit ist $g'm = g(hm) = gm$, somit ist ψ wohldefiniert.

Injektivität. Sei $\psi(aH) = \psi(bH)$, dann ist $am = bm$ also $a^{-1}bm = m$, was soviel heisst wie $a^{-1}b \in H$ und somit $bH = aH$.

Surjektivität. Sei $z \in Gm$, also $z = gm$ für ein $g \in G$, dann folgt $z = \phi(gH)$.

(c) Sei $Gm \cap Gm' \neq \emptyset$, dann ist zu zeigen, dass $Gm = Gm'$ gilt. Sei $z \in Gm \cap Gm'$

dann existieren also $g, g' \in G$ so dass $gm = z = g'm'$. Es folgt $m' = (g')^{-1}gm$ so dass $m' \in Gm$ und damit $hm' \in Gm$ für jedes $h \in G$, was soviel heisst wie $Gm' \subset Gm$. Aus Symmetrie folgt die umgekehrte Inklusion.

(d) folgt aus (b) und (c). □

Definition 1.3.12. Sei G eine Gruppe. Das **Zentrum** $Z = Z(G)$ von G ist die Menge aller $x \in G$, die mit allen Elementen vertauschen, also

$$Z(G) = \{x \in G : xy = yx \ \forall y \in G\}.$$

Beispiele 1.3.13. (a) Ist G abelsch, so gilt $Z(G) = G$ und umgekehrt.

(b) Ist $G = GL_n(\mathbb{F}_p)$, dann besteht das Zentrum aus die Matrizen der Form λI , wobei $\lambda \in \mathbb{F}_p^\times$. Dies ist eine Übungsaufgabe der Linearen Algebra. (Man löse zuerst den Fall $n = 2$, dann sieht man auch den allgemeinen Beweis.)

(c) Ist $n \geq 3$, dann ist das Zentrum von $G = \text{Per}(n)$ die triviale Gruppe.

Beweis. Sei σ im Zentrum von $\text{Per}(n)$ und $n \geq 3$. Sei $1 \leq i \leq n$ und sei $1 \leq j \leq n$ von i und von $\sigma(i)$ verschieden. Dann vertauscht σ mit der Transposition $\tau = \tau_{i,j}$, die man als Zykel in der Form (i, j) schreibt. Es gilt also $\sigma(j) = \sigma(\tau(i)) = \tau(\sigma(i))$. Wäre nun $\sigma(i)$ von i und j verschieden, dann wäre $\sigma(j) = \tau(\sigma(i)) = \sigma(i)$, was der Injektivität von σ widerspricht! Damit muss $\sigma(i)$ gleich i oder j sein, der Fall j ist aber in der Annahme ausgeschlossen. Es folgt $\sigma(i) = i$ und also $\sigma = \text{Id}$. □

(d) Das Zentrum der Gruppe B_n der oberen Dreiecksmatrizen ist $\mathbb{F}_p^\times I$ falls $p \neq 2$ und im Fall $p = 2$ ist es die Menge aller Matrizen der Form

$$\begin{pmatrix} 1 & & * \\ & \ddots & \\ & & 1 \end{pmatrix}$$

also rechts oben in der Ecke kann ein beliebiger Eintrag sein, ansonsten ist es die Einheitsmatrix.

Begründung: Sei A im Zentrum. Für $i < j$ ist $I + E(i, j) \in B_n$ und da A mit I vertauscht, vertauscht es auch mit $E = E(i, j)$. Für $z < s$ folgt

$$\sum_{k=1}^n E_{z,k} A_{k,s} = (EA)_{z,s} = (AE)_{z,s} = \sum_{k=1}^n A_{z,k} E_{k,s}. \quad (*)$$

Ist $i \neq z$ und $j \neq s$, sind beide Seiten Null. Für $i = z < j \leq s$ folgt

$$A_{j,s} = \begin{cases} 0 & j \neq s, \\ A_{i,i} & j = s. \end{cases}$$

Der Fall $j = s$ ergibt $A_{j,j} = A_{i,i}$, so dass alle Diagonaleinträge gleich sind. Der Fall $j < s$ liefert $A_{j,s} = 0$ und da j alle Werte $> z \geq 1$ annehmen kann, folgt $A_{z,s} = 0$, falls $z > 1$, das heißt, wir haben die behauptete Gestalt unterhalb der ersten Zeile.

Werten wir (*) für $j = s$ und $z \neq i$ aus, so erhalten wir $0 = A_{z,i}$. Diese Gleichung enthält nur dann neue Informationen, wenn $z < i$. Uns fehlt aber nur der Fall $z = 1$ und in diesem Fall ist wegen $i < j$ die erste Zeile Null bis auf die letzte Position, damit haben wir A in der Gestalt

$$\begin{pmatrix} \lambda & & * \\ & \ddots & \\ & & \lambda \end{pmatrix}$$

mit einem $\lambda \in \mathbb{F}_p^\times$. Im Fall $p = 2$ muss $\lambda = 1$ sein und es muss nur noch gezeigt werden, dass jede Matrix dieser Form zentral ist, was man schnell nachrechnet. Im Fall $p \neq 2$ sei $\mu \in \mathbb{F}_p^\times$ und $M = \text{diag}(\mu, 1, \dots, 1)$ die Diagonalmatrix mit den Einträgen $\mu, 1, \dots, 1$. Dann gilt $AM = MA$ und wir folgern

$$A_{1,n} = (AM)_{1,n} = (MA)_{1,n} = \mu A_{1,n}.$$

da dies für jedes μ gilt und es wegen $p > 2$ ein $\mu \neq 1$ gibt, folgt $A_{1,n} = 0$.

- (e) Das Zentrum der Diedergruppe D_n , $n \geq 3$ ist trivial, wenn n ungerade ist und es ist $\{1, \sigma^{n/2}\}$, wenn n gerade ist. *Begründung:* Sei zunächst n ungerade, wegen $\tau\sigma\tau^{-1} = \sigma^{-1}$ folgt $\tau\sigma^k\tau^{-1} = \sigma^{-k}$ für jedes $k \in \mathbb{Z}$. Eine Potenz σ^k wird also nur dann im Zentrum liegen, wenn $\sigma^k = \sigma^{-k}$, oder $\sigma^{2k} = 1$. Da die Ordnung von σ gleich n ist, passiert das genau dann, wenn n gerade ist und $k = n/2$. Das bedeutet, für gerades n ist $\sigma^{n/2}$ ist die einzige Potenz $\neq 1$ von σ , die im Zentrum liegt und für ungerades n liegt keine im Zentrum. Die verbleibenden Elemente sind von der Form $\tau\sigma^k$ und wenn so eines im Zentrum liegt, gilt

$$\tau\sigma^k = \tau(\tau\sigma^k)\tau^{-1} = \tau(\tau\sigma^k\tau^{-1}),$$

so dass dann σ^k im Zentrum liegen muss. Es gilt dann aber

$$\begin{aligned} \tau\sigma^k &= \sigma(\tau\sigma^k)\sigma^{-1} \\ &= \tau\sigma^{-1}\sigma^k\sigma^{-1} = \tau\sigma^{k-2}. \end{aligned}$$

Da aber $n \geq 3$ folgt $k - 2 \not\equiv k$ modulo n und daher liegt $\tau\sigma^k$ nicht im Zentrum. □

Definition 1.3.14. Wir lassen nun die endliche Gruppe G durch Konjugation auf sich selbst operieren und wenden die Bahnengleichung an. Die Orbits unter der Konjugation heißen auch **Konjugationsklassen**. Die Konjugationsklasse des Elementes $x \in G$ ist also die Menge

$$[x] = \{yxy^{-1} : y \in G\}.$$

Satz 1.3.15 (Klassengleichung). Sei G eine endliche Gruppe mit Zentrum Z und sei $x_1, \dots, x_n$ ein Vertretersystem der Konjugationsklassen von $G \setminus Z$. Dann gilt

$$\text{ord}(G) = \text{ord}(Z) + \sum_{j=1}^n \frac{|G|}{|G_{x_j}|},$$

wobei G_{x_j} der **Zentralisator** von x_j ist:

$$G_{x_j} = \{y \in G : yx_j = x_jy\}.$$

Beweis. Dies ist die Bahnengleichung auf die Konjugationsoperation angewendet. □

Beispiele 1.3.16. (a) Die Konjugationsklassen in $\text{Per}(n)$ sind gut zu beschreiben: Man schreibt ein gegebenes Element σ als Produkt disjunkter Zyklen $\sigma = Z_1 \cdots Z_k$. Da diese Zyklen disjunkt sind, vertauschen sie miteinander und man kann sie so anordnen, dass für die Längen gilt $\ell(Z_1) \geq \cdots \geq \ell(Z_k)$. Zwei Elemente σ und τ sind genau dann konjugiert, wenn für ihre so normalisierten Zykeldarstellungen $\sigma = Z_1 \cdots Z_k$ und $\tau = W_1 \cdots W_l$ gilt $k = l$ und $\ell(Z_j) = \ell(W_j)$ für alle $1 \leq j \leq k$. Das bedeutet, dass diese Zahlentupel genau die Konjugationsklassen liefern. Sei also $\mathcal{Z}$ die Menge aller Tupel $\langle m_1, \dots, m_k \rangle$ mit $m_1 \geq m_2 \geq \cdots \geq m_k \geq 2$ und $m_1 + \cdots + m_k \leq n$. Dann steht $\mathcal{Z}$ in Bijektion zur Menge aller nichttrivialen Konjugationsklassen in $\text{Per}(n)$. Die Klassen in $\text{Per}(3)$ sind dann gegeben durch

$$\langle 2 \rangle, \langle 3 \rangle,$$

es gibt also zwei Konjugationsklassen in $\text{Per}(3)$. Für $G = \text{Per}(4)$ gibt es

$$\langle 2 \rangle, \langle 2, 2 \rangle, \langle 3 \rangle, \langle 4 \rangle$$

also gibt es 4 Konjugationsklassen. Repräsentanten für diese Klassen sind (in Zykelschreibweise)

$$(1, 2) \quad (1, 2)(3, 4) \quad (1, 2, 3) \quad (1, 2, 3, 4)$$

Der Zentralisator von $(1, 2)$ ist die disjunkte Vereinigung zweier Nebenklassen $H, (1, 2)H$, wobei H die Gruppe aller Permutationen ist, die $\{1, 2\}$ punktweise festhalten. Daher permutiert H nur 3 und 4, so dass $|H| = 2$ und daher hat der Zentralisator $G_{(1,2)}$ zusammen 4 Elemente. Ebenso bestimmt man die Ordnungen der anderen Zentralisatoren

$$|G_{(1,2)(3,4)}| = 4, \quad |G_{(1,2,3)}| = 3, \quad |G_{(1,2,3,4)}| = 8.$$

die Klassengleichung liest sich dann

$$24 = 1 + \frac{24}{4} + \frac{24}{4} + \frac{24}{3} + \frac{24}{8} = 1 + 6 + 6 + 8 + 3$$

(b) Die Konjugationsklassen von $G = \text{GL}_n(\mathbb{F}_p)$ zu bestimmen, ist aufwändiger. Ersetzt man $\mathbb{F}_p$ durch einen algebraisch abgeschlossenen Körper, so liefert der Jordan-Normalform-Satz das Gewünschte.

1.4 Zyklische Gruppen

Eine Gruppe G heisst **zyklisch**, wenn G von einem Element erzeugt ist.

Beispiele 1.4.1.

- Die Gruppe $(\mathbb{Z}, +)$ ist zyklisch von unendlicher Ordnung.
- Für jedes $n \in \mathbb{N}$ gibt es eine zyklische Gruppe der Ordnung n , nämlich $\mathbb{Z}/n$.

Proposition 1.4.2. *Ist G zyklisch, dann ist G isomorph zu $\mathbb{Z}$ oder zu $\mathbb{Z}/n$, wobei $n = \text{ord}(G)$.*

Mit anderen Worten, alle unendlichen zyklischen Gruppen sind isomorph und eine endliche zyklische Gruppe ist durch ihre Ordnung festgelegt.

Beweis. Sei G zyklisch und sei τ ein Erzeuger.

1. *Fall.* τ hat endliche Ordnung $n \in \mathbb{N}$. Dann ist die Abbildung $\mathbb{Z}/n \rightarrow G, k \mapsto \tau^k$ ein Gruppenisomorphismus.
2. *Fall.* τ hat keine endliche Ordnung. Dann ist die Abbildung $\mathbb{Z} \rightarrow G, k \mapsto \tau^k$ ein Isomorphismus. □

Fangen wir an mit Gruppen der Ordnung 1. Diese sind alle isomorph zu $\{1\}$, damit ist dieser erste Schritt abgeschlossen. Bevor wir uns mit den Ordnungen 2 und 3 herumschlagen, beweisen wir lieber einen Satz.

Satz 1.4.3. *Sei p eine Primzahl. Jede Gruppe der Ordnung p ist zyklisch, also isomorph zu der Gruppe $\mathbb{Z}/p$.*

Beweis. Sei G eine Gruppe der Ordnung p . Sei $e \neq \tau \in G$. Dann muss $\text{ord}(\tau)$ ein Teiler von p sein. Da $\tau \neq e$, ist die Ordnung $\neq 1$, also ist $\text{ord}(\tau) = p$, damit hat die zyklische Untergruppe $\langle \tau \rangle$, die von τ erzeugt wird, die Ordnung p , ist also gleich G . $\square$

Satz 1.4.4. *Es gibt bis auf Isomorphie zwei Gruppen der Ordnung 4, die zyklische $\mathbb{Z}/4$ und die Kleinsche Vierergruppe $(\mathbb{Z}/2) \times (\mathbb{Z}/2)$.*

Beweis. Sei G eine Gruppe der Ordnung 4, die nicht zyklisch ist. Das bedeutet, dass jedes Element $\neq e$ die Ordnung 2 haben muss. Sei also a ein nichttriviales Element. Die Untergruppe $H = \langle a \rangle$ hat Index 2, ist also normal. Sei $b \in G$, so folgt $bHb^{-1} = H$, da H nur aus zwei Elementen, e und a besteht, folgt $bab^{-1} = a$, also ist G abelsch. Seien nun a, b zwei verschiedene Elemente von $G \setminus \{e\}$. Dann liefert die Abbildung $(\mathbb{Z}/2) \times (\mathbb{Z}/2) \rightarrow G, (i, j) \mapsto a^i b^j$ einen injektiven Gruppenhomomorphismus. Das Bild hat Ordnung 4, ist also G und G damit isomorph zur Vierergruppe. $\square$

1.5 Normalteiler

Definition 1.5.1. Sei $\phi : G \rightarrow H$ ein Gruppenhomomorphismus. Der **Kern** von ϕ ist die Menge

$$\ker(\phi) = \{g \in G : \phi(g) = 1\}.$$

Lemma 1.5.2. *Ein Gruppenhomomorphismus $\phi : G \rightarrow H$ ist genau dann injektiv, wenn der Kern trivial ist.*

Beweis. Ist ϕ injektiv und ist x im Kern, dann ist $\phi(x) = \phi(1)$, also $x = 1$, d.h., der Kern ist trivial. Ist umgekehrt der Kern trivial und ist $\phi(x) = \phi(y)$, dann ist $\phi(y^{-1}x) = \phi(y)^{-1}\phi(x) = \phi(x)^{-1}\phi(x) = 1$, also ist $y^{-1}x = 1$, d.h., $x = y$. $\square$

Lemma 1.5.3. Sei $\phi : G \rightarrow H$ ein Gruppenhomomorphismus. Dann ist der Kern N eine Untergruppe von G mit der Eigenschaft, dass

$$gNg^{-1} = N$$

für alle $g \in G$ gilt.

Definition 1.5.4. Eine Untergruppe $N \subset G$ mit der Eigenschaft aus dem Lemma heisst **Normalteiler** von G .

Beweis. [Beweis des Lemmas] Es reicht zu zeigen, dass $gNg^{-1} \subset N$ ist, denn dies gilt dann ja für jedes g , also auch für g^{-1} , also $g^{-1}Ng \subset N$. Daraus folgt durch Rechtsmultiplikation mit g , dass $Ng \subset gN$ und hieraus $N \subset gNg^{-1}$.

Sei also $n \in N$, d.h., $\phi(n) = 1$. Dann gilt für beliebiges $g \in G$:

$$\phi(gng^{-1}) = \phi(g)\phi(n)\phi(g)^{-1} = \phi(g)1\phi(g)^{-1} = \phi(g)\phi(g)^{-1} = 1,$$

also ist $gng^{-1} \in N$ wie verlangt. □

Beispiele 1.5.5. (a) Ist G abelsch, dann ist jede Untergruppe ein Normalteiler.

(b) Sei $G = \text{Per}(n)$. Dann ist $\text{Per}^+(n)$ ein Normalteiler und dies ist der Einzige. Dies kann man anhand der Klassifikation der Konjugationsklassen durch die Zykelstruktur beweisen.

(c) Ist H eine Untergruppe von $\mathbb{F}_p^\times$, dann ist $\det^{-1}(H)$ ein Normalteiler von $\text{GL}_n(\mathbb{F}_p)$.

(d) Die Abbildung $B_n \rightarrow (\mathbb{F}_p^\times)^n, \begin{pmatrix} \lambda_1 & & * \\ & \ddots & \\ & & \lambda_n \end{pmatrix} \mapsto (\lambda_1, \dots, \lambda_n)$ ist ein Gruppenhomomorphismus. Ist H eine Untergruppe von $(\mathbb{F}_p^\times)^n$, dann ist das Urbild von H ein Normalteiler.

(e) Ist $D_n = \langle \sigma, \tau \rangle$ die Diedergruppe, dann ist jede Untergruppe $N \subset \langle \sigma \rangle$ ein Normalteiler, denn ist $\sigma^k \in N$, dann folgt $\tau\sigma^k\tau^{-1} = \sigma^{-k} \in N$.

(f) Ist G irgendeine Gruppe, dann ist das Zentrum Z von G stets ein Normalteiler.

Beweis. Sei $z \in Z$ und $g \in G$. Dann ist

$$gzg^{-1} = zgg^{-1} = z \in Z,$$

also folgt $gZg^{-1} = Z$. □

(g) Ist G eine Gruppe und H eine Untergruppe vom Index 2, dann ist H ein Normalteiler.

Beweis. Es gibt genau zwei Linksnebenklassen $G = H \sqcup sH$ mit einem beliebigen $s \in G \setminus H$, also ist $sH = G \setminus H$ und ebenso fuer Rechtsnebenklassen: $G = H \sqcup Hs$, also $sH = G \setminus H = Hs$, oder $sHs^{-1} = H$. Dies gilt fuer jedes $s \notin H$ und fuer $s \in H$ gilt es sowieso. $\square$

Satz 1.5.6. *Ist $N \subset G$ ein Normalteiler, so lässt sich auf der Menge der Nebenklassen G/N genau eine Gruppenstruktur installieren, so dass die Projektion $G \rightarrow G/N$ ein Gruppenhomomorphismus ist.*

Ist umgekehrt $H \subset G$ eine Untergruppe mit einer Gruppenstruktur auf dem Nebenklassenraum G/H so dass die Projektion $G \rightarrow G/H$ ein Homomorphismus ist, dann ist H ein Normalteiler.

Insbesondere folgt, dass die Normalteiler genau die Kerne von Homomorphismen sind.

Beweis. Die zweite Aussage folgt sofort aus Lemma 1.5.3, beweisen wir also die erste. Sei N ein Normalteiler in G . Wir wollen eine Gruppenstruktur auf dem Nebenklassenraum G/N definieren durch

$$(aN)(bN) := abN.$$

Wir zeigen die Wohldefiniertheit: Sei $aN = a'N$ und $bN = b'N$, so ist zu zeigen, dass $abN = a'b'N$ gilt. Es gibt $n_1, n_2 \in N$ mit $a' = an_1$ und $b' = bn_2$. Da N ein Normalteiler ist, gilt

$$a'b' = an_1bn_2 = ab \underbrace{(b^{-1}n_1b)}_{\in N} n_2 \in abN,$$

also folgt $a'b'N \subset abN$ und aus Symmetriegründen folgt auch die umgekehrte Inklusion. Die so definierte Multiplikation definiert eine Gruppenstruktur auf G/N so dass die Projektion $G \rightarrow G/N$ ein Homomorphismus ist. Da dieser surjektiv ist, ist die Gruppenstruktur eindeutig bestimmt. $\square$

- Beispiele 1.5.7.** (a) Sei $G = \mathbb{Z}$ und $N = m\mathbb{Z}$ für ein gegebenes $m \in \mathbb{N}$. Da G abelsch ist, ist die Untergruppe N normal. Der Quotient $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/m$ ist eine endliche Gruppe der Ordnung m , die von einem Element, der 1, erzeugt wird.
- (b) Die Gruppe $\text{Per}(n)/\text{Per}^+(n)$ hat zwei Elemente, ist also Isomorph zu $\{\pm 1\} \cong \mathbb{Z}/2$.
- (c) Die Gruppe $\text{GL}_n(\mathbb{F}_p)/\text{SL}_n(\mathbb{F}_p)$ ist isomorph zu $\mathbb{F}_p^\times$. (Hierzu muss man nur zeigen, dass $\det : \text{GL}_n(\mathbb{F}_p) \rightarrow \mathbb{F}_p^\times$ surjektiv ist, was aber aus $\det \begin{pmatrix} x & \\ & 1 \end{pmatrix} = x$ folgt.)
- (d) Ist $G = D_n = \langle \sigma, \tau \rangle$ die Diedergruppe und ist $N = \langle \sigma \rangle$, dann ist G/N eine Gruppe der Ordnung 2, also isomorph zu $\mathbb{Z}/2$.

Proposition 1.5.8. *Sei G eine Gruppe mit Zentrum Z . Ist G/Z zyklisch, dann ist G abelsch, also $G = Z$ und G/Z ist trivial.*

Beweis. Sei $a \in G$, so dass G/Z von der Restklasse $[a]$ erzeugt wird. Sind dann $b, c \in G$ mit Restklassen $[b] = [a]^m$ und $[c] = [a]^n$, dann ist $b = a^m z$ und $c = a^n w$ mit $z, w \in Z$. Es folgt

$$bc = a^m z a^n w = a^n w a^m z = cb$$

und damit $[b][c] = [bc] = [cb] = [c][b]$ und G/Z ist abelsch. □

Korollar 1.5.9. *Sei G eine Gruppe und Z ihr Zentrum. Dann kann die Ordnung von G/Z keine Primzahl sein.*

Beweis. Wäre $\text{ord}(G/Z)$ eine Primzahl, dann wäre G/Z nach Satz 1.4.3 zyklisch und damit nach Proposition 1.5.8 $G/Z = \{e\}$, Widerspruch! □

1.6 Homomorphiesätze

Lemma 1.6.1. *Sei $N \subset G$ ein Normalteiler und sei $\alpha : G \rightarrow H$ ein Gruppenhomomorphismus mit $\alpha(N) = \{1\}$. Dann ist die Abbildung $\beta : G/N \rightarrow H$,*

$\beta(xN) = \alpha(x)$ ein wohldefinierter Gruppenhomomorphismus. Das Diagramm

$$\begin{array}{ccc} G & \xrightarrow{p} & G/N \\ & \searrow \alpha & \downarrow \beta \\ & & H \end{array}$$

kommutiert, d.h., $\alpha = \beta p$, wobei p die Projektion ist.

Beweis. Zur Wohldefiniertheit sei $xN = yN$, also $x = yn$ für ein $n \in N$, dann folgt $\alpha(x) = \alpha(yn) = \alpha(y)\alpha(n) = \alpha(y)$, also ist β wohldefiniert. Schliesslich ist wegen $\beta((xN)(yN)) = \beta(xyN) = \alpha(xy) = \alpha(x)\alpha(y) = \beta(xN)\beta(yN)$ die Abbildung β ein Gruppenhomomorphismus. $\square$

Satz 1.6.2. Sei $f : G \rightarrow H$ ein Gruppenhomomorphismus. Dann ist das Bild eine Untergruppe und f induziert einen Isomorphismus

$$\mu : G / \ker(f) \xrightarrow{\cong} \text{Bild}(f).$$

Beweis. Die Existenz von μ folgt aus Lemma 1.6.1. Die Surjektivität ist klar, da $\mu(x \ker(f)) = f(x)$ mit beliebigem x . Zur Injektivität sei $x(\ker(f))$ im Kern von ϕ . Das bedeutet $1 = \phi(x(\ker(f))) = f(x)$, also $x \in \ker(f)$, also $x \ker(f) = \ker(f)$. Das bedeutet, $x \ker(f)$ ist die triviale Klasse, also ist μ injektiv. $\square$

Satz 1.6.3. (a) Sind M, N Normalteiler in G so dass $M \subset N$, dann ist N/M ein Normalteiler in G/M und die Projektion induziert einen Isomorphismus

$$(G/M) / (N/M) \xrightarrow{\cong} G/N.$$

(b) Sind M, N Normalteiler in G , dann ist auch $N \cap M$ ein Normalteiler in G , ferner ist

$$MN = \{mn : m \in M, n \in N\}$$

eine Untergruppe von G und die Abbildung $m(M \cap N) \mapsto mN$ ist ein Isomorphismus

$$M/M \cap N \xrightarrow{\cong} MN/N.$$

Beweis. (a) Nach Lemma 1.6.1 ist

$$\begin{aligned} \phi : G/M &\rightarrow G/N, \\ xM &\mapsto xN. \end{aligned}$$

ein wohldefinierter Gruppenhomomorphismus. Wenn wir zeigen, dass der Kern gerade die Gruppe $N/M \subset G/M$ ist, folgt die Aussage (a) aus Satz 1.6.2. Es gilt

$$\begin{aligned} xM \in \ker(\phi) &\Leftrightarrow 1 = \phi(xM) = xN \\ &\Leftrightarrow x \in N \Leftrightarrow xM \in MN/M. \end{aligned}$$

(b) Sei $a \in N \cap M$ und sei $x \in G$. Dann ist xax^{-1} in N , da N normal ist und auch in M , da M normal ist, also liegt xax^{-1} in $N \cap M$. Damit ist $N \cap M$ normal.

Seien $a, a_1 \in MN$, also etwa $a = mn$, $a_1 = m_1n_1$. Dann gilt

$$a^{-1}a_1 = (mn)^{-1}m_1n_1 = n^{-1}m^{-1}m_1n_1 = \underbrace{(m^{-1}m_1)}_{\in M} \underbrace{(m^{-1}m_1)^{-1}n^{-1}m^{-1}m_1n_1}_{\substack{\in N \\ \in N}}$$

Daher ist $a^{-1}a_1 \in MN$, diese Menge also eine Untergruppe, da sie außerdem nicht leer ist.

Die Abbildung $\phi : M \rightarrow MN/N, m \mapsto mN$ ist ein surjektiver Gruppenhomomorphismus mit Kern $M \cap N$, so dass die Behauptung aus Satz 1.6.2 folgt. $\square$

Korollar 1.6.4. *Allgemeiner gilt: Sind M, N Untergruppen von G und wird N von M normalisiert, d.h. gilt*

$$mNm^{-1} = N$$

für alle $m \in M$, dann ist MN eine Untergruppe von G .

Beweis. Klar. $\square$

Man kann statt Linksnebenklassen natürlich auch **Rechtsnebenklassen** betrachten, sei also $H \subset G$ eine Untergruppe und $a \in G$ dann ist

$$Ha = \{ha : h \in H\}$$

die Rechtsnebenklasse von a . Genau wie bei den Linksnebenklassen zerfällt G in disjunkte Klassen.

Satz 1.6.5. (a) *Eine Untergruppe H von G ist genau dann ein Normalteiler, wenn die Rechts- und Linksnebenklassen übereinstimmen, wenn also für jedes $a \in G$ gilt*

$$aH = Ha.$$

(b) *Sei H eine Untergruppe von G vom Index 2, d.h. die Nebenklassenmenge G/H hat zwei Elemente. Dann ist H ein Normalteiler.*

Beweis. (a) Ist H ein Normalteiler, dann gilt $aHa^{-1} = H$, woraus durch Multiplikation von rechts mit a folgt $aH = Ha$. Die Umkehrung geht umgekehrt.

(b) Sei H eine Untergruppe vom Index 2. Die Gruppe G zerfällt in zwei Linksnebenklassen, H und der Rest, der dann $G \setminus H$ ist. Ebenso zerfällt G in zwei Rechtsnebenklasse H und $G \setminus H$. Also stimmen die Rechts- und Linksnebenklassen überein. $\square$

1.7 Freie Gruppen

Definition 1.7.1. Sei S eine Menge. Sei $T = S \times \{1, -1\}$. Wir schreiben $(s, \pm 1)$ als $s^{\pm 1}$, wobei wir den Exponenten 1 auch weglassen, also $s^1 = s$ schreiben. Ein **Wort** in T ist ein Element von T^n für ein $n \in \mathbb{N}_0$. Auf der Menge der Wörter $\mathcal{W}(T)$ gibt es eine Multiplikation durch "Hintereinanderschreiben", das Produkt von $(t_1, \dots, t_n)$ und $(t'_1, \dots, t'_k)$ ist $(t_1, \dots, t_n, t'_1, \dots, t'_k)$. Diese Multiplikation ist Assoziativ und das leere Wort ist neutral. Wir betrachten die Äquivalenzrelation erzeugt durch

$$(\dots, x, t, t^{-1}, z, \dots) \sim (\dots, x, z, \dots).$$

Dann ist $\mathcal{W}(T)/\sim$ eine Gruppe mit dem leeren Wort als neutralem Element, das wir auch als 1 schreiben. Dies ist die **freie Gruppe** $F(S)$ in der Erzeugermenge S . Wir schreiben $t_1 \cdots t_n$ statt $(t_1, \dots, t_n)$. Jedes Element $\neq 1$ von $F(S)$ lässt sich eindeutig in der Form

$$s_1^{k_1} s_2^{k_2} \cdots s_n^{k_n}$$

schreiben, wobei $n \in \mathbb{N}$ und $k_1, \dots, k_n \in \mathbb{Z} \setminus \{0\}$.

Wir fassen S als Teilmenge von $F(S)$ auf

Satz 1.7.2 (Universelle Eigenschaft). *Jede Abbildung $\phi : S \rightarrow G$ in eine Gruppe G lässt sich eindeutig zu einem Gruppenhomomorphismus $\tilde{\phi} : F(S) \rightarrow G$ fortsetzen. Die Zuordnung $\phi \mapsto \tilde{\phi}$ ist eine Bijektion*

$$\mathcal{Z} : \text{Abb}(S, G) \rightarrow \text{Hom}(F(S), G).$$

Beweis. Wir definieren die Fortsetzung durch

$$\tilde{\phi}(s_1^{k_1} \cdots s_n^{k_n}) := \phi(s_1)^{k_1} \cdots \phi(s_n)^{k_n},$$

wobei rechts das Produkt in G steht. Die Homomorphismeigenschaft ist klar und ist $\psi : F(S) \rightarrow G$ eine weitere Fortsetzung von ϕ , so gilt

$$\begin{aligned} \psi(s_1^{k_1} \cdots s_n^{k_n}) &= \psi(s_1)^{k_1} \cdots \psi(s_n)^{k_n} \\ &= \phi(s_1)^{k_1} \cdots \phi(s_n)^{k_n} \\ &= \tilde{\phi}(s_1^{k_1} \cdots s_n^{k_n}), \end{aligned}$$

also $\psi = \tilde{\phi}$. Da die Einschränkung von $\tilde{\phi}$ auf die Teilmenge S gleich ϕ ist, ist die Zuordnung Z injektiv. Ist $\alpha : F(S) \rightarrow G$ ein Gruppenhomomorphismus, dann ist α eine Fortsetzung von $\phi := \alpha|_S : S \rightarrow G$ und nach der Eindeutigkeit folgt $\alpha = \tilde{\phi} = Z(\phi)$ und Z ist demnach auch surjektiv. $\square$

Korollar 1.7.3. *Jede Gruppe ist Quotient einer freien Gruppe, also von der Form $F(S)/N$ für einen Normalteiler $N \subset F(S)$.*

Beweis. Sei G eine Gruppe und sei $S = G$ als Menge aufgefasst. Die Identität $G \rightarrow G$ setzt dann fort zu einem surjektiven Gruppenhomomorphismus $\alpha : F(S) \rightarrow G$, mit $N = \ker(\alpha)$ folgt dann also $G \cong F(S)/N$. $\square$

1.8 Sylow-Gruppen

Definition 1.8.1. Sei G eine endliche Gruppe und p eine Primzahl. G heisst **p -Gruppe**, wenn die Ordnung von G eine p -Potenz ist.

Eine Untergruppe H von G heisst **p -Sylow-Gruppe**, wenn $\text{ord}(H) = p^k$, $k \in \mathbb{N}$ und $\text{ord}(G) = p^k m$ wobei m teilerfremd zu p ist. Das heisst, die Ordnung von H

ist die maximale p -Potenz, die überhaupt in G auftreten kann.

Beispiel 1.8.2. Ist $G = \mathbb{Z}/n$ zyklisch und $n = p^k m$ mit $k \in \mathbb{N}$ und $p \nmid m$. Dann ist $m\mathbb{Z}/n \cong \mathbb{Z}/p^k$ die einzige p -Sylow-Gruppe von G .

Satz 1.8.3. Sei G eine Gruppe der Ordnung p^k mit einer Primzahl p und $k \in \mathbb{N}$. Dann ist das Zentrum von G nichttrivial.

Beweis. Betrachte die Klassengleichung

$$\text{ord}(G) = \text{ord}(Z) + \sum_{j=1}^n \frac{|G|}{|G_{x_j}|}.$$

Ist einer der Summanden $\frac{|G|}{|G_{x_j}|}$ gleich 1, dann ist für das betreffende x_j der Zentralisator $G_{x_j} = G$, was soviel bedeutet, dass x_j mit jedem $x \in G$ vertauscht, also ist x_j im Zentrum und das Zentrum ist damit nichttrivial. Wir können also annehmen, dass die Summanden $\frac{|G|}{|G_{x_j}|}$ ungleich 1. Da sie die Gruppenordnung teilen müssen, sind sie alle p -Potenzen, also folgt dass p die Summe $\sum_{j=1}^n \frac{|G|}{|G_{x_j}|}$ teilt. Daher muss p auch $\text{ord}(Z)$ teilen. $\square$

Beispiel 1.8.4. Sei $G = D_4$ die Diedergruppe mit 8 Elementen, also Erzeugern σ, τ und Relationen $\sigma^4 = 1 = \tau^2$ und $\tau\sigma\tau^{-1} = \sigma^{-1}$. Für $g = \sigma^2$ gilt dann $g^2 = 1$, sowie

$$g\sigma = \sigma g \quad \text{und} \quad \tau g \tau^{-1} = \tau \sigma^2 \tau^{-1} = \sigma^{-2} = g^{-1} = g.$$

Damit vertauscht g mit beiden Erzeugern σ und τ , ist also zentral.

Korollar 1.8.5. Sei p eine Primzahl und G eine Gruppe der Ordnung p^k für ein $k \in \mathbb{N}$. Dann gibt es eine Kette von normalen Untergruppen

$$\{1\} = G_0 \subset G_1 \subset \cdots \subset G_k = G,$$

so dass $\text{ord}(G_j) = p^j$ gilt. Also ist $G_j/G_{j-1} \cong \mathbb{Z}/p$ eine abelsche Gruppe.

Insbesondere hat G für jedes $1 \leq j \leq k$ eine Untergruppe H der Ordnung p^j und es gibt ein Element der Ordnung p in G .

Beweis. Induktion nach k . Der Fall $k = 1$ ist klar.

$k \rightarrow k + 1$: Wir wissen, dass G nicht-triviales Zentrum Z hat. Sei also $z_0 \in Z \setminus \{1\}$. Dann hat z_0 Ordnung p^l fuer ein $1 \leq l \leq k$ und damit hat $a := z_0^{p^{l-1}}$ die Ordnung p , also ist $G_1 := \langle a \rangle$ eine zentrale Untergruppe der Ordnung p . Nach Induktionsvoraussetzung hat G/G_1 eine solche Kette

$$1 = \overline{G}_1 \subset \overline{G}_2 \subset \cdots \subset \overline{G}_k = G/G_1$$

und wir definieren G_j als das Urbild von $\overline{G}_j$ unter der Projektion $G \mapsto G/G_1$.

Dann ist $G_j \subset G$ der Kern von $G \rightarrow G/G_1 = \overline{G}_k \rightarrow \overline{G}_k/\overline{G}_j$ also normal und es gilt $G_{j+1}/G_j \cong (G_{j+1}/G_1)/(G_j/G_1) = \overline{G}_{j+1}/\overline{G}_j \cong \mathbb{Z}/p$. $\square$

Satz 1.8.6. *Sei p eine Primzahl und G eine Gruppe der Ordnung p^2 . Dann ist G abelsch, genauer ist*

$$G \cong \mathbb{Z}/p^2 \quad \text{oder} \quad G \cong \mathbb{Z}/p \times \mathbb{Z}/p.$$

Beweis. Das Zentrum Z ist nichttrivial, also ist die Ordnung von G/Z gleich 1 oder p . Das zweite ist nach Korollar 1.5.9 (Die Ordnung von $G/Z(G)$ kann keine Primzahl sein) ausgeschlossen, also $G = Z$ und damit ist G abelsch.

Hat G ein Element der Ordnung p^2 , dann ist G zyklisch und wir sind fertig. Andernfalls haben alle Elemente $\neq 1$ die Ordnung p . Sei dann $x \neq 1$ irgendein Element und y ein Element von $G \setminus \langle x \rangle$. Wir behaupten, dass die Abbildung

$$\begin{aligned} f : \mathbb{Z}/p \times \mathbb{Z}/p &\rightarrow G, \\ (i, j) &\mapsto x^i y^j \end{aligned}$$

ein Isomorphismus ist. Es ist nun allerdings ein Homomorphismus und das Bild enthält x und y und damit ist die Ordnung des Bildes größer als $\text{ord}(\langle x \rangle) = p$. Da

die Ordnung des Bildes aber p^2 teilen muss, ist sie gleich p^2 und damit ist f surjektiv. Da die Gruppen G und $(\mathbb{Z}/p)^2$ die gleiche Ordnung haben, ist f auch injektiv. $\square$

Definition 1.8.7. Sei G eine Gruppe. Es gebe eine natürliche Zahl N so dass $x^N = 1$ für jedes $x \in G$ gilt. Dies ist zum Beispiel der Fall wenn G endlich ist. Die kleinste natürliche Zahl N , für die dies der Fall ist, heisst der **Exponent** von G .

Beispiel 1.8.8. Die Gruppe $G = \prod_{j=1}^{\infty} \mathbb{Z}/2$ ist eine unendliche Gruppe vom Exponenten 2.

Lemma 1.8.9. (a) *Sei G eine endliche abelsche Gruppe vom Exponenten N . Dann teilt die Gruppenordnung eine Potenz von N .*

(b) *Sei G eine endliche abelsche Gruppe und p eine Primzahl, die die Gruppenordnung teilt. Dann enthält G ein Element der Ordnung p .*

Beweis. (a) Induktion nach der Gruppenordnung. Für die triviale Gruppe ist die Behauptung erfüllt.

Sei $b \in G$ ein nichttriviales Element und sei H die zyklische Gruppe erzeugt von b . Wegen $b^N = 1$ ist die Ordnung k von b ein Teiler von N und N ist auch ein Exponent von G/H . Nach Induktion teilt die Ordnung von G/H eine Potenz von N und wegen $|G| = |H| |G/H|$ gilt das auch für die Ordnung von G .

(b) Wir folgern nun, dass die abelsche Gruppe G mit $|G| = mp^k$, $k \geq 1$ ein Element x haben muss mit Ordnung np^l für ein $l \geq 1$. Wäre dies nicht der Fall, wäre m ein Exponent von G , was Teil (a) widerspricht.

Habe also das Element x die Ordnung np^l mit $l \geq 1$. Dann hat $y = x^{np^{l-1}}$ die Ordnung p . $\square$

Satz 1.8.10 (Sylow). *Sei G eine endliche Gruppe und p eine Primzahl.*

(a) *G enthält eine p -Sylow-Gruppe. Genauer ist jede p -Untergruppe H von G in einer p -Sylowgruppe enthalten.*

(b) Alle p -Sylow-Gruppen von G sind zueinander konjugiert.

(c) Für die Anzahl s der p -Sylow-Gruppen gilt

$$s \mid \text{ord}(G), \quad s \equiv 1 \pmod{p}.$$

Beweis. (a): Wir zeigen die Existenz einer p -Sylowgruppe durch Induktion nach der Ordnung von G . Ist $p = |G|$ sind wir fertig. Sei also $|G| = p^k m$ mit $p \nmid m$. Ist H eine Untergruppe mit Index $|G/H|$ teilerfremd zu p , dann ist jede p -Sylow-Gruppe von H schon eine von G und wir sind fertig nach Induktion. Wir können also annehmen, dass jede echte Untergruppe einen Index hat, der von p geteilt wird. Die Klassengleichung sagt

$$p^k m = \text{ord}(Z) + \sum_{j=1}^n |G/G_{x_j}|,$$

wobei Z das Zentrum von G ist und die x_j Vertreter der nichttrivialen Konjugationsklassen. Die Summanden rechts werden nach Voraussetzung alle von p geteilt, damit auch $\text{ord}(Z)$. Nach Lemma 1.8.9 enthält Z ein Element z der Ordnung p . Sei dann S eine p -Sylow-Gruppe von $G/\langle z \rangle$ und sei $P : G \rightarrow G/\langle z \rangle$ die Projektion. Dann ist $P^{-1}(S)$ eine p -Sylow-Gruppe von G . Es gibt also eine p -Sylow-Gruppe.

(b): Sei nun $\mathcal{S}$ die Menge aller p -Sylow-Gruppen in G . Dann operiert G durch Konjugation auf $\mathcal{S}$. Sei $P \in \mathcal{S}$ und sei G_P der Stabilisator von P in G . Sei $\mathcal{S}_0 = G.P$ das Orbit von P und sei $H \subset G$ eine nichttriviale p -Gruppe. Dann operiert H auf dem Orbit $\mathcal{S}_0$ durch Konjugation und die Bahnengleichung sagt

$$\frac{|G|}{|G_P|} = |\mathcal{S}_0| = \sum_{v=1}^N \frac{|H|}{|H_{P_v}|},$$

wobei die P_ν durch ein Vertretersystem der H -Orbiten laufen. Da $P \subset G_p$, wird der Index $|G/G_p|$ nicht von p geteilt. Da $|H|$ eine p -Potenz ist, sind alle $\frac{|H|}{|H_{P_\nu}|}$ Potenzen von p , also muss für ein ν schon $H = H_{P_\nu}$ gelten. Also normalisiert H schon P_ν . Daher ist dann HP_ν eine Untergruppe von G mit P_ν als Normalteiler. Nach dem Homomorphiesatz folgt $HP_\nu/P_\nu \cong H/H \cap P_\nu$ so dass

$$|HP_\nu| = |P_\nu| |HP_\nu/P_\nu| = |P_\nu| |H/H \cap P_\nu|$$

eine p -Potenz ist. Da aber $|P_\nu|$ schon die maximal mögliche p -Potenz ist, folgt $HP_\nu = P_\nu$, also $H \subset P_\nu$. Damit ist (a) gezeigt. Wendet man dies auf $H = Q$ eine andere p -Sylow-Gruppe an, folgt wegen der Maximalität von Q , dass $Q = P_\nu$ sein muss, also sind alle p -Sylow-Gruppen in einem Orbit, sind also alle zueinander konjugiert und damit folgt (b).

(c): Die Anzahl s der p -Sylow-Gruppen ist dann gleich $|G/G_p|$ und damit ein Teiler von $\text{ord}(G)$.

Zum Schluss liefert die Bahnengleichung für $H = P$

$$s = |\mathcal{S}| = \frac{|P|}{|P|} + \sum_{P, P_\nu \neq P, P} \frac{|P|}{|P_{P_\nu}|}$$

Jedes P_{P_ν} rechts muss eine echte Untergruppe von P sein, denn sonst wäre $P \subset P_\nu$ nach obiger Argumentation. Also ist jeder Index $\frac{|P|}{|P_{P_\nu}|}$ durch p teilbar, somit also $s \equiv \frac{|P|}{|P|} = 1 \pmod{p}$. □

Definition 1.8.11. Eine Gruppe G heisst **einfach**, wenn sie keinen echten Normalteiler hat, also keinen Normalteiler ausser $\{1\}$ und G .

Beispiele 1.8.12. • $\mathbb{Z}/p$ ist einfach, wenn p eine Primzahl ist, denn diese Gruppe hat nicht einmal eine echte Untergruppe.

- Die Gruppe A_n der geraden Permutationen in $\text{Per}(n)$ ist einfach, falls $n \geq 5$.

Korollar 1.8.13. Sei G eine Gruppe der Ordnung pq für Primzahlen $p > q$. Dann ist die p -Sylow-Gruppe ein Normalteiler, die Gruppe G also nicht einfach.

Beweis. Die Anzahl der p -Sylow-Gruppen s teilt die Gruppenordnung, also ist $p = 1, q, p, pq$ und es gilt $s \equiv 1(p)$, so dass nur noch $s = 1$ in Frage kommt. Daher gibt es nur eine p -Sylow-Gruppe P . Da für $g \in G$ auch gPg^{-1} eine p -Sylow-Gruppe ist, folgt $gPg^{-1} = P$, also ist P ein Normalteiler. $\square$

Beispiele 1.8.14. (a) Die Gruppe $\text{Per}(3)$ hat Ordnung $6 = 2 \cdot 3$, daher gibt es 2 und 3 Sylow-Gruppen, beide sind zyklisch.

(b) $|\text{Per}(4)| = 24 = 2^3 \cdot 3$. Die 3-Sylow ist zyklisch und die 2-Sylow ist die Diedergruppe D_4 , die ja auch vier Punkte permutiert.

(c) Die Gruppe $\text{GL}_n(\mathbb{F}_p)$ hat die Ordnung $p^{\frac{n(n-1)}{2}} (p^n - 1)(p^{n-1} - 1) \cdots (p - 1)$. Daher hat jede p -Sylow die Ordnung $p^{\frac{n(n-1)}{2}}$. Ist $p \geq n$, dann ist die Gruppe S der oberen Dreiecksmatrizen mit Einsen auf der Diagonale

$$S = \begin{pmatrix} 1 & & * \\ & \ddots & \\ & & 1 \end{pmatrix}$$

eine p -Sylow-Gruppe. Dasselbe gilt für B_n .

(d) Die Diedergruppe $D_{2p} = \langle \sigma, \tau \rangle$ hat $\langle \sigma \rangle$ als p -Sylow und $\langle \tau \rangle$ als 2-Sylowgruppe.

1.9 Kommutatoren

Definition 1.9.1. Sind a, b Elemente einer Gruppe G , so sei

$$[a, b] = aba^{-1}b^{-1}$$

der **Kommutator** von a und b . Sei $[G, G]$ die Gruppe, die von allen Kommutatoren erzeugt wird, sie wird die **Kommutatorgruppe** genannt.

Die Kommutatorgruppe ist genau dann trivial, wenn die Gruppe G abelsch ist.

Proposition 1.9.2. Die Kommutatorgruppe $[G, G]$ ist ein Normalteiler von G . Der Quotient $G/[G, G]$ ist abelsch und $[G, G]$ ist der kleinste Normalteiler mit abelschem Quotienten. Andersherum ist $G/[G, G]$ der grösste abelsche Quotient von G und wird daher die **Abelisierung** der Gruppe G genannt und G^{ab} geschrieben.

Beweis. Sind $a, b \in G$ und ist $\phi : G \rightarrow H$ irgendein Gruppenhomomorphismus, so ist das Bild

$$\phi([a, b]) = \phi(aba^{-1}b^{-1}) = \phi(a)\phi(b)\phi(a)^{-1}\phi(b)^{-1} = [\phi(a), \phi(b)]$$

wieder ein Kommutator. Ist daher $\phi : G \rightarrow G, x \mapsto gxg^{-1}$, so folgt, dass $g[G, G]g^{-1} \subset [G, G]$ und damit ist $[G, G]$ normal. Ist N irgendein Normalteiler mit abelschem Quotienten G/N und sei $\phi : G \rightarrow G/N$ der entsprechende Gruppenhomomorphismus. Dann ist, da G/N abelsch ist, $\phi([a, b]) = [\phi(a), \phi(b)] = 1$, also liegt $[G, G]$ im Kern von ϕ , mit anderen Worten $[G, G] \subset N$, wie verlangt. $\square$

Definition 1.9.3. Sei G eine Gruppe. Für beliebige Teilmengen $A, B \subset G$ sei $[A, B]$ die Untergruppe erzeugt von allen Kommutatoren $[a, b]$ mit $a \in A$ und $b \in B$.

Lemma 1.9.4. Sei G eine Gruppe, $G_0 = G$ und $G_{j+1} = [G, G_j]$ für $j = 0, 1, \dots$. So folgt $G_0 \supset G_1 \supset \dots$ und jede Gruppe G_j ist ein Normalteiler in G . Die Gruppe G_j/G_{j+1} liegt im Zentrum von G/G_{j+1} .

Eine Gruppe G heisst **nilpotent**, falls $G_n = \{1\}$ für ein $n \in \mathbb{N}$ gilt.

Beweis. Es gilt $G_0 \supset G_1$ und induktiv folgt aus $G_{j-1} \supset G_j$ schon $G_j = [G, G_{j-1}] \supset [G, G_j] = G_{j+1}$. Ferner ist G_0 ein Normalteiler und ist G_j ein Normalteiler, so gilt für $g \in G$, dass

$$gG_{j+1}g^{-1} = g[G, G_j]g^{-1} = [G, gG_jg^{-1}] = [G, G_j] = G_{j+1},$$

also ist auch G_{j+1} ein Normalteiler und induktiv sind's dann alle. Wegen $[G, G_j] \subset G_{j+1}$ ist G_j zentral modulo G_{j+1} . $\square$

Lemma 1.9.5. Ist Z eine zentrale Untergruppe von G , dann gilt

$$G \text{ nilpotent} \quad \Leftrightarrow \quad G/Z \text{ nilpotent}.$$

Beweis. Homomorphe Bilder von nilpotenten Gruppen sind immer nilpotent, daher folgt " $\Rightarrow$ ". Sei also G/Z nilpotent. Da ϕ surjektiv ist, folgt $\phi(G_j) = (G/Z)_j$. Ist nun etwa $(G/Z)_n = \{1\}$, so folgt $\phi(G_n) = 1$, also $G_n \subset Z$ und da Z zentral ist $G_{n+1} = [G, G_n] \subset [G, Z] = 1$, so dass auch G nilpotent ist. $\square$

Beispiele 1.9.6.

Abelsche Gruppen sind nilpotent.

Sei K ein Körper, sei $n \in \mathbb{N}$ und sei G die Gruppe aller oberen Dreiecksmatrizen in $M_n(K)$ mit Einsen auf der Diagonale. Dann ist G nilpotent, denn G_j ist genau die Untergruppe aller Matrizen mit Nullen auf den ersten j Nebendiagonalen (Übungsaufgabe).

Proposition 1.9.7. *Sei p eine Primzahl. Dann ist jede endliche p -Gruppe nilpotent.*

Beweis. Induktion nach der Ordnung. Ist $|G| = 1$ dann ist G abelsch also nilpotent. Ist $|G| = p^{k+1}$, dann hat G ein nichttriviales Zentrum Z , also $|Z| = p^j$ fuer ein $j \in \mathbb{N}$. Damit ist G/Z eine Gruppe der Ordnung p^{k+1-j} und nach Induktionsvoraussetzung koennen wir G/Z als nilpotent voraussetzen, so dass nach Lemma 1.9.5 auch G nilpotent ist. $\square$

2 Ringe

2.1 Definition

Definition 2.1.1. Wenn wir in dieser Vorlesung **Ring** sagen, werden wir stets einen **kommutativen Ring mit Eins** meinen, also eine abelsche Gruppe $(R, +)$ mit einer weiteren Verknüpfung $(a, b) \mapsto ab$, so dass

Assoziativität: $(ab)c = a(bc)$ und

Kommutativität: $ab = ba$ sowie

Distributivität: $a(b + c) = ab + ac$ gelten und es ein Element $1 = 1_R$ gibt mit $a \cdot 1 = a$.

Definition 2.1.2. Ein **Ringhomomorphismus** $\phi : R \rightarrow S$ ist eine Abbildung zwischen Ringen, so dass

$$\phi(a + b) = \phi(a) + \phi(b), \quad \phi(ab) = \phi(a)\phi(b), \quad \phi(1) = 1$$

gelten.

Beispiele 2.1.3. (a) Jeder Körper ist ein Ring.

(b) $\mathbb{Z}$ ist ein Ring, der kein Körper ist.

(c) Der einfachste Ring ist der **Nullring** $N = \{0\}$. In diesem Ring gilt $0 = 1$. Ist R ein Ring, in dem $0 = 1$ gilt, dann ist R der Nullring, denn für $a \in R$ gilt

$$a = 1a = 0a = (1 - 1)a = a - a = 0.$$

(d) Sei $\alpha = \sqrt{2} \in \mathbb{R}$. Dann gilt $\alpha^2 = 2$. Wir definieren

$$\mathbb{Z}[\sqrt{2}] = \{k + l\alpha : k, l \in \mathbb{Z}\}.$$

Wegen $(k + l\alpha)(m + n\alpha) = km + 2ln + (kn + lm)\alpha$ ist $\mathbb{Z}[\sqrt{2}]$ ein Unterring von $\mathbb{R}$.

(e) Der **Gaußsche Zahlring** ist definiert als

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\} \subset \mathbb{C}.$$

(f) Ist R ein Ring, dann definiert man den Polynomring $R[x]$ genau wie im Körperfall. Elemente sind formale Ausdrücke der Form

$$a_0 + \cdots + a_n x^n$$

und die Multiplikation ist definiert durch

$$(a_0 + \cdots + a_n x^n)(b_0 + \cdots + b_m x^m) = c_0 + \cdots + c_{m+n} x^{m+n},$$

wobei $c_k = \sum_{i+j=k} a_i b_j$. Insbesondere kann man also den Übergang von einem Ring zum Polynomring wiederholen und erhält den **Polynomring in mehreren Variablen**,

$$R[X_1, \dots, X_r].$$

Die Elemente dieses Rings sind formale Ausdrücke der Form

$$\sum_{\alpha} c_{\alpha} X^{\alpha},$$

wobei α durch $\mathbb{N}_0^r$ läuft, $c_{\alpha} \in R$ ein Koeffizient ist, der nur für endlich viele α nicht Null ist und

$$X^{\alpha} = X_1^{\alpha_1} X_2^{\alpha_2} \cdots X_r^{\alpha_r}$$

ist.

- (g) Es gibt auch den **Polynomring in unendlich vielen Variablen**: Ist $(T_i)_{i \in I}$ eine Familie von Variablen, so definiert man

$$R[T_i, i \in I] := \bigcup_{\substack{E \subset I \\ E \text{ endlich}}} R[T_i : i \in E].$$

Die Elemente sind also endliche Linearkombinationen von endlichen Produkten der T_i .

- (h) Sei p eine Primzahl und sei $\mathbb{Z}_{(p)}$ die Menge aller rationalen Zahlen $\frac{a}{b} \in \mathbb{Q}$ für die der Nenner b zur Primzahl p teilerfremd ist, also von p nicht geteilt wird. Dies ist ein Unterring von $\mathbb{Q}$.
- (i) Für $m \in \mathbb{N}$ ist die Menge $\mathbb{Z}/m$ der Restklassen $\{0, 1, 2, \dots, m-1\}$ mit Addition und Multiplikation

$$a \boxplus b = \text{Rest von } a + b \text{ modulo } m,$$

$$a \cdot b = \text{Rest von } ab \text{ modulo } m$$

ein Ring, den wir ebenfalls mit $\mathbb{Z}/m$ bezeichnen.

Definition 2.1.4. Ein Element $0 \neq a \in R$ eines Rings heißt **invertierbar** oder **Einheit** des Rings, wenn es ein $b \in R$ gibt mit $ab = 1$. Die Menge $R^{\times}$ der invertierbaren Elemente ist eine abelsche Gruppe bzgl. der Multiplikation. Ein Ring R ist genau dann ein Körper, wenn $R^{\times} = R \setminus \{0\}$ gilt.

Beispiele 2.1.5. • Die Einheiten von $\mathbb{Z}$ sind ± 1 .

- Sei K ein Körper und sei $R = K[x]$ der Polynomring. Die Einheiten von R sind genau die konstanten Polynome $\neq 0$.
- Die Einheiten des Rings $R = \mathbb{Z}[\sqrt{-5}]$ sind genau die Zahlen 1 und -1 .

Beweis. Seien $a, b \in R$ mit $ab = 1$. Da $a, b \in \mathbb{C}$ ist, gilt diese Gleichung auch dort, also ist auch $1 = |ab|^2 = |a|^2 |b|^2$. Damit gilt $|a|^2 \leq 1$ oder $|b|^2 \leq 1$. Nehmen wir $|a|^2 \leq 1$ an. Sei $a = k + il\sqrt{5}$, dann ist $|a|^2 = k^2 + 5l^2$ und da $k, l \in \mathbb{Z}$, folgt $l = 0$ und $a = k = \pm 1$. Damit ist auch $b = \pm 1$ und die Behauptung ist gezeigt. $\square$

- Die Einheiten des Rings $\mathbb{Z}/m$ sind genau die Zahlen $1 \leq x \leq m-1$, die zu m teilerfremd sind. Dies zeigt man mit Hilfe der Division mit Rest (Übungsaufgabe!)

Definition 2.1.6. Ein Element $a \neq 0$ eines Rings R heißt **Nullteiler**, falls es ein $b \neq 0$ gibt mit $ab = 0$.

Ein Ring R mit $0 \neq 1$ heißt **nullteilerfrei**, oder **integer**, oder auch **Integritätsring**, falls gilt

$$ab = 0 \quad \Rightarrow \quad a = 0 \text{ oder } b = 0.$$

Beispiele 2.1.7. • Der Nullring ist kein Integritätsring.

- Körper sind Integritätsringe.
- Jeder Unterring eines Integritätsrings ist ein Integritätsring. So ist zum Beispiel $\mathbb{Z}[\sqrt{-5}]$ ein Integritätsring, da er ein Unterring des Körpers $\mathbb{C}$ ist.
- $\mathbb{Z}$ ist ein Integritätsring.
- $\mathbb{Z}/m$ ist genau dann ein Integritätsring, wenn m eine Primzahl ist.
- Sind R, S Ringe, dann ist auch das kartesische Produkt $R \times S$ ein Ring, indem man die Operationen Komponentenweise definiert. Das Nullelement ist $(0, 0)$ und die Eins ist $(1, 1)$. Dieser Ring ist kein Integritätsring, auch wenn R und S welche sind, denn es gilt

$$(0, 1) \cdot (1, 0) = (0, 0).$$

Satz 2.1.8. Ist R ein Integritätsring, dann auch der Polynomring $R[x]$.

Beweis. Seien $f, g \in R[x]$, beide $\neq 0$. Wir zeigen $fg \neq 0$. Sei dazu

$$f(x) = a_0 + \cdots + a_n x^n,$$

$$g(x) = b_0 + \cdots + b_m x^m$$

mit $a_n \neq 0 \neq b_m$. Dann gilt

$$f(x)g(x) = c_0 + \cdots + c_{m+n} x^{m+n},$$

wobei $c_k = \sum_{i+j=k} a_i b_j$. Insbesondere ist dann $c_{m+n} = a_n b_m \neq 0$, da R ein Integritätsring ist. □

Beispiele 2.1.9. • Die Inklusionen $\mathbb{Z} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C}$ sind Ringhomomorphismen.

- Sei $m \in \mathbb{N}$. Die Projektion $\mathbb{Z} \rightarrow \mathbb{Z}/m$, die $a \in \mathbb{Z}$ auf den Rest modulo m wirft, ist ein Ringhomomorphismus.
- Ist $R = K[x]$ ein Polynomring und ist $\alpha \in K$. Dann ist die **Auswertungsabbildung** $\delta_\alpha : K[x] \rightarrow K$, die $f(x)$ auf $f(\alpha)$ schickt, ein Ringhomomorphismus.

2.2 Ideale

Definition 2.2.1. Sei R ein Ring (kommutativ mit Eins). Ein **Ideal** in R ist eine additive Untergruppe $I \subset R$ so dass $RI \subset I$.

Proposition 2.2.2. (a) Ist $\phi : R \rightarrow S$ ein Ringhomomorphismus und ist $I \subset S$ ein Ideal, dann ist das Urbild $\phi^{-1}(I)$ ein Ideal. Insbesondere ist $\ker(\phi) = \{x \in R : \phi(x) = 0\}$ ein Ideal.

(b) Ist K ein Körper und ist R ein Ring, der nicht der Nullring ist, dann ist jeder Ringhomomorphismus $\phi : K \rightarrow R$ injektiv. Insbesondere ist jeder Homomorphismus zwischen Körpern injektiv.

Beweis. (a) Da ϕ ein additiver Gruppenhomomorphismus ist, ist das Urbild eine Untergruppe. Sei also $a \in \phi^{-1}(I)$ und $r \in R$. Dann folgt $\phi(ra) = \phi(r) \underbrace{\phi(a)}_{\in I} \in I$, also ist $ra \in \phi^{-1}(I)$.

(b) Da R nicht der Nullring ist, gilt $\phi(1) = 1 \neq 0$ und daher ist der Kern von ϕ nicht ganz K . Das einzige andere Ideal, das K hat, ist $\{0\}$. Damit ist ϕ injektiv. $\square$

Beispiele 2.2.3. • 0 und der ganze Ring R sind Ideale.

- Sei $I \subset R$ ein Ideal. Enthält I ein invertierbares Element, so ist $I = R$.
- Ist $r \in R$, so ist die Menge

$$rR = \{rx : x \in R\}$$

ein Ideal. Ein solches Ideal nennt man **Hauptideal**. Manche Autoren schreiben auch (a) für aR .

Definition 2.2.4. In der Regel ist nicht jedes Ideal ein Hauptideal. Ein **Hauptidealring** ist ein Ring R , der

- (a) integer ist und in dem
- (b) jedes Ideal ein Hauptideal ist.

Beispiele 2.2.5.

- Jeder Körper K ist ein Hauptidealring, denn er hat nur zwei Ideale, $\{0\} = 0K$ und $K = 1K$.
- $\mathbb{Z}$ ist ein Hauptidealring.

Beweis. Sei $I \subset \mathbb{Z}$ ein Ideal. Ist $I \cap \mathbb{N} = \emptyset$, dann ist auch $I \cap (-\mathbb{N}) = \emptyset$ und daher $I = \{0\} = 0\mathbb{Z}$. Ist $I \cap \mathbb{N} \neq \emptyset$, dann gibt es eine kleinste natürliche Zahl $m \in I$. Wir behaupten, dass $I = m\mathbb{Z}$. Klar ist $m\mathbb{Z} \subset I$. Sei also $k \in I$, dann existiert ein $p \in m\mathbb{Z}$ so dass $0 \leq k - p < m$. Da m minimal in $I \cap \mathbb{N}$ ist, folgt $k - p = 0$, also $k = p \in m\mathbb{Z}$. $\square$

- Ist K ein Körper, so ist der Polynomring $R = K[x]$ ein Hauptidealring.

Beweis. Sei $I \neq 0$ ein Ideal und sei $g \in I \setminus \{0\}$ ein Polynom von minimalem Grad. Sei $f \in I$ beliebig, dann ist $\text{grad}(f) \geq \text{grad}(g)$, also existieren nach der **Division mit Rest** Polynome q, r mit

$$f = qg + r$$

und $\text{grad}(r) < \text{grad}(g)$. Dann ist $r = f - qg \in I$ und da der Grad von g minimal war, ist $r = 0$, also $f = qg \in gR$. $\square$

- Sei K ein Körper. Der Polynomring $R = K[x, y]$ ist kein Hauptidealring.

Beweis. Betrachte das Ideal

$$I = xR + yR.$$

Erstens ist $I \neq R$, denn kein Polynom in I hat einen konstanten Term. Angenommen: I ist ein Hauptideal, also etwa $I = fR$, dann gibt es g mit $fg = x$, woraus $f \in K[x]$ folgt, da die Variable y nicht vorkommt. Ebenso gibt es h mit $fh = y$, also $f \in K[y]$, so dass $f \in K[x] \cap K[y] = K$, also muss f konstant sein. Da $I \neq 0$ ist $f \in K \setminus \{0\} = K^\times$, es gibt also ein f' mit $ff' = 1$, also ist $1 \in I$ und somit $I = R$, ein Widerspruch! $\square$

- Der Ring $R = \mathbb{Z}[\sqrt{-5}]$ ist kein Hauptidealring. Der Beweis hierzu wird auf später verschoben.

Definition 2.2.6. Sei R ein Hauptidealring und seien $a_1, \dots, a_n \in R$. Ein **größter gemeinsamer Teiler** $\text{ggT}(a_1, \dots, a_n)$ ist ein Erzeuger des Ideals $a_1R + \dots + a_nR$. Ein ggT ist bis auf Multiplikation mit einer Einheit eindeutig festgelegt.

Beispiel 2.2.7. In $R = \mathbb{Z}$ ist 5 ein ggT von 10 und 15.

Beweis. 5 teilt 10 und 15, also folgt $10\mathbb{Z} + 15\mathbb{Z} \subset 5\mathbb{Z}$. Andererseits ist $5 = 15 - 10$, liegt also in $10\mathbb{Z} + 15\mathbb{Z}$. $\square$

Definition 2.2.8. Sei R ein Ring und $I \subset R$ ein Ideal. Dann ist I eine Untergruppe von $(R, +)$ und wir können die Menge R/I der Nebenklassen betrachten.

Satz 2.2.9. *Auf der Menge R/I gibt es genau eine Ringstruktur, so dass die Projektion $\pi : R \rightarrow R/I$ ein Ringhomomorphismus ist. Für diesen Ringhomomorphismus gilt $I = \ker(\pi)$, also ist jedes Ideal der Kern eines Ringhomomorphismus.*

Beweis. Wir machen uns zunächst klar, dass für $a, b \in R$ die Bedingung $a + I = b + I$ gleichwertig ist zu $a - b \in I$.

Wir definieren Addition und Multiplikation durch $(a + I) + (b + I) = (a + b) + I$ und $(a + I)(b + I) = ab + I$. Hier ist Wohldefiniertheit zu prüfen. Seien $a + I = a' + I$ und $b + I = b' + I$, also $a - a', b - b' \in I$, dann folgt

$$(a + b) - (a' + b') = (a - a') + (b - b') \in I$$

also folgt $(a + b) + I = (a' + b') + I$ und damit die Wohldefiniertheit der Addition. Für die Multiplikation rechne

$$\begin{aligned} ab - a'b' &= ab - ab' + ab' - a'b' \\ &= a(b - b') + (a - a')b' \in I. \end{aligned}$$

Die Eindeutigkeit der Ringstruktur ist wegen der Surjektivität von π klar und der Kern der Projektion $R \rightarrow R/I$ ist die triviale Nebenklasse, also I . □

Beispiel 2.2.10. Der Ring $\mathbb{Z}/m$.

Ein Ideal $\mathfrak{m}$ eines Rings R heisst **maximales Ideal**, wenn $\mathfrak{m} \neq R$ und $\mathfrak{m}$ ist maximal in der Menge aller Ideale $I \neq R$, also mit anderen Worten:

(a) $1 \notin \mathfrak{m}$ und

(b) ist I ein Ideal mit $\mathfrak{m} \subset I$ und $I \neq R$, dann ist $\mathfrak{m} = I$.

Satz 2.2.11.

- (a) Jedes Ideal $I \neq R$ liegt in einem maximalen Ideal.
- (b) Jedes Element von $R \setminus R^\times$ liegt in einem maximalen Ideal.
- (c) Ein Ideal J ist genau dann maximal, wenn R/J ein Körper ist.

Beweis. (a) Sei $I \neq R$ ein Ideal und sei S die Menge aller Ideale J mit $1 \notin J$ und $J \supset I$. Dann ist S mit der Inklusion partiell geordnet und die Kettenbedingung ist erfüllt, denn sei $\emptyset \neq K \subset S$ eine Kette, also eine linear geordnete Teilmenge und sei $\mathfrak{a} = \bigcup_{J \in K} J$, dann ist $\mathfrak{a}$ wieder ein Ideal und es gilt $I \subset \mathfrak{a}$, sowie $1 \notin \mathfrak{a}$. Dieses $\mathfrak{a}$ ist dann eine obere Schranke zu K . Nach dem Lemma von Zorn gibt es ein maximales Element $\mathfrak{m}$ in S , also liegt I in einem maximalen Ideal.

(b) Sei $r \in R \setminus R^\times$ eine Nichteinheit und sei $I = (r) = rR$ das Hauptideal. Dann gilt $1 \notin I$, da r nicht invertierbar ist. Also gibt es nach Teil (a) ein maximales Ideal, das I und damit auch r enthält.

(c) Sei J ein maximales Ideal und sei $r \in R \setminus J$. Wegen der Maximalität von J muss das Ideal $\langle r, J \rangle = rR + J$ gleich dem ganzen Ring sein, also auch die Eins enthalten, es gibt also $r' \in R$ und ein $\alpha \in J$ mit $rr' + \alpha = 1$ oder $rr' \in 1 + J$, so dass in R/J gilt $(r + J)(r' + J) = rr' + J = 1 + J$, das heisst, dass r im Quotienten R/J invertierbar ist, also ist in R/J jedes Element $\neq 0$ invertierbar, d.h., R/J ist ein Körper.

Sei umgekehrt R/J ein Körper und sei $r \in R \setminus J$, dann ist r modulo J invertierbar, also existiert ein $r' \in R$ mit $rr' \in 1 + J$, so dass $1 \in rR + J$, also ist J maximal. $\square$

Definition 2.2.12. Ein Ideal $J \neq R$ eines Rings R heisst **Primideal**, wenn für $x, y \in R$ gilt

$$xy \in J \quad \Rightarrow \quad x \in J \text{ oder } y \in J.$$

Satz 2.2.13. *Ein Ideal $J \neq R$ ist genau dann ein Primideal, wenn R/J ein Integritätsring ist.*

Insbesondere ist jedes maximale Ideal ein Primideal.

Beweis. Sei J ein Primideal und seien $x, y \in R$ so dass für die Restklassen gilt $[x][y] = [0]$. Dann ist also $[xy] = [0]$, so dass $xy \in J$ folgt. Dann ist also $x \in J$ oder $y \in J$, was mit $[x] = [0]$ oder $[y] = [0]$ gleichbedeutend ist, das heisst, R/J ist ein Integritätsring. Für die Umkehrung liest man diesen Beweis rückwärts.

Der Zusatz folgt, da ein Ideal J genau dann maximal ist, wenn R/J ein Körper ist. □

2.3 Der chinesische Restsatz

Definition 2.3.1. Zwei Ideale I, J in einem Ring heißen **teilerfremd**, falls $I + J = R$ gilt.

Beispiel 2.3.2. In $R = \mathbb{Z}$ sind die Hauptideale $m\mathbb{Z}$ und $n\mathbb{Z}$ genau dann teilerfremd, wenn die Zahlen m und n keine echten gemeinsamen Teiler haben, wenn also m und n teilerfremd sind.

Beweis. Seien die Ideale teilerfremd, dann ist $1 \in m\mathbb{Z} + n\mathbb{Z}$, es gibt also $a, b \in \mathbb{Z}$ mit $am + bn = 1$. Würden nun m und n von einer Primzahl p geteilt, dann würde auch 1 von p geteilt, was ein Widerspruch ist.

Seien umgekehrt die Zahlen m und n teilerfremd. Das Ideal $m\mathbb{Z} + n\mathbb{Z}$ ist ein Hauptideal, also von der Form $g\mathbb{Z}$ für ein $g \in \mathbb{N}$. Dann ist $m \in g\mathbb{Z}$ also folgt $g \mid m$ und ebenso $g \mid n$ und daher ist $g = 1$, also sind die Ideale $m\mathbb{Z}$ und $n\mathbb{Z}$ teilerfremd. □

Definition 2.3.3. Sind I und J Ideale, so definieren wir das Ideal IJ als

$$IJ = \left\{ \sum_{j=1}^n a_j b_j : a_j \in I, b_j \in J \right\}.$$

Sind etwa beides Hauptideale, $I = aR$ und $J = bR$, dann ist auch IJ ein Hauptideal, nämlich $IJ = abR$.

Lemma 2.3.4. *Sind die Ideale I und J teilerfremd, dann gilt*

$$IJ = I \cap J.$$

Beweis. Die Inklusion " $\subset$ " gilt auch ohne die Teilerfremdheit, da $IJ \subset IR = I$ und ebenso für J .

Zum Beweis von " $\supset$ " seien also I und J teilerfremd, also gibt es Elemente $a \in I$ und $b \in J$ mit $1 = a + b$. Sei dann $x \in I \cap J$, dann ist $x = ax + bx$ und da ax und bx beide in IJ liegen, ist $x \in IJ$. □

Satz 2.3.5 (Chinesischer Restsatz). *Sei R ein Ring und $I_1, \dots, I_r$ seien paarweise teilerfremde Ideale. Sei $I = I_1 \cdots I_r = I_1 \cap \cdots \cap I_r$, dann liefern die kanonischen Projektionen einen Isomorphismus*

$$R/I \cong \prod_{v=1}^r R/I_v.$$

Beweis. Da $I_v \supset I$ für jedes v , gibt es kanonische Projektionen $\pi_v : R/I \rightarrow R/I_v$, also einen Ringhomomorphismus

$$\pi : R/I \rightarrow \prod_{v=1}^r R/I_v.$$

Injektivität: Sei $\pi(\bar{x}) = 0$, und $x \in R$ ein Urbild von $\bar{x}$. Dann ist $x \in I_v$ für jedes v . Nun sind die I_v paarweise teilerfremd, also gibt es beispielsweise $a \in I_1, b \in I_2$ mit $a + b = 1$. Dann ist $x = 1 \cdot x = (a + b)x = ax + bx$. Da $x \in I_2$ und $a \in I_1$, ist $ax \in I_1 I_2$ und ebenso für bx , also ist $x \in I_1 I_2$. Nun ist $I_1 I_2$ immer noch teilerfremd zu $I_3, \dots, I_r$, denn sind $a \in I_1$ und $b \in I_3$ mit $a + b = 1$ und $x \in I_2$ und $y \in I_3$ mit

$x + y = 1$, so gilt

$$1 = (a + b)(x + y) = \underbrace{ax}_{\in I_1 I_2} + \underbrace{ay + bx + by}_{\in I_3}.$$

Also kann man induktiv fortfahren und erhält schließlich $x \in I_1 \cdots I_r = I$, d.h., π ist injektiv.

Surjektivität. Für die Surjektivität reicht es, zu zeigen, dass es Elemente $x_j \in R$ gibt, mit $\pi_j(x_j) = 1$ und $\pi_k(x_j) = 0$ für $k \neq j$. Modulo Umnummerierung reicht es, x_1 nachzuweisen. Seien $a \in I_1$ und $b \in I_2 \cdots I_r$ mit $a + b = 1$. Dann ist $x_1 = b$ das gewünschte Element. $\square$

2.4 Teilbarkeit

Definition 2.4.1. Seien a, b Elemente eines Integritätsrings R .

(a) Man sagt a **teilt** b oder ist ein **Teiler** von b , falls es ein $c \in R$ gibt so dass $ac = b$.

In diesem Fall schreibt man $a \mid b$. Ist a kein Teiler von b , so schreibt man $a \nmid b$.

(b) a und b heißen **assoziert**, wenn es eine Einheit $u \in R^\times$ gibt mit $a = bu$.

Beispiele 2.4.2. • Für zwei natürliche Zahlen m, n gilt m teilt n in $\mathbb{Z}$ genau dann, wenn m ein Teiler im üblichen Sinne ist.

- Zwei Elemente a, b in $\mathbb{Z}$ sind genau dann assoziiert, wenn $a = \pm b$ gilt.
- Jedes Element $a \in R$ teilt die Null, denn es gilt $a \cdot 0 = 0$. Die Null teilt nur sich selbst.

Lemma 2.4.3. Für zwei Elemente a, b eines Integritätsrings R sind äquivalent

- (i) $a \mid b$ und $b \mid a$,
- (ii) $aR = bR$,
- (iii) a und b sind assoziiert.

Beweis. (i) $\Rightarrow$ (iii): Es gelte $a = bc$ und $b = ad$. Wir nehmen an, dass $a \neq 0$, da sonst auch $b = 0$. Es ist $a = bc = acd$, also $a(1 - cd) = 0$ und da $a \neq 0$ und R integer ist, folgt $cd = 1$, also sind c, d Einheiten und a und b sind assoziiert.

(iii) $\Rightarrow$ (ii) Es sei $a = bu$ mit einer Einheit u . Wegen $uR = R$ folgt dann $aR = buR = bR$.

(ii) $\Rightarrow$ (i) Sei $aR = bR$, dann folgt $a \in bR$, also gibt es ein $c \in R$ mit $a = bc$, also $b \mid a$. Ebenso folgt $b \mid a$. $\square$

Definition 2.4.4. Sei R ein Integritätsring und p ein Element, das weder Null noch eine Einheit ist.

(a) Das Element p heißt **irreduzibel**, falls aus der Gleichung $p = ab$ in R stets folgt, dass a oder b eine Einheit ist.

(b) Das Element p heißt **Primelement**, falls aus $p \mid ab$ stets folgt $p \mid a$ oder $p \mid b$.

Lemma 2.4.5. Sei R ein Integritätsring. Ein Element $p \in R \setminus \{0\}$ ist genau dann ein Primelement, wenn pR ein Primideal ist.

Beweis. Für $x \in R$ gilt $x \in pR \Leftrightarrow p \mid x$, so dass die Eigenschaft p prim oder pR prim direkte Umformulierungen voneinander sind. $\square$

Beispiele 2.4.6. • In $R = \mathbb{Z}$ sind die Primelemente genau die Elemente der Form $\pm p$, wobei p eine Primzahl ist.

- In $R = \mathbb{C}[x]$ sind die Primelemente genau die Elemente $c(x - a)$ mit $c \in \mathbb{C}^\times$, $a \in \mathbb{C}$.
- In $R = \mathbb{R}[x]$ sind die Primelemente genau die Polynome der Form $c(x - \alpha)$ für ein $\alpha \in \mathbb{R}$ oder $c(x^2 + ax + b)$, falls dieses Polynom keine reelle Nullstelle hat.

Proposition 2.4.7. Sei R ein Integritätsring. Dann ist jedes Primelement von R auch irreduzibel.

Beweis. Seien p ein Primelement und sei $p = ab$. Dann teilt p das Produkt ab also teilt p einen der Faktoren, sagen wir a . Das heißt $a = pc = abc$, also $a(1 - bc) = 0$, also $bc = 1$, so dass b eine Einheit ist. $\square$

Satz 2.4.8. Sei R ein Hauptidealring und sei $p \in R$. Dann sind äquivalent

- (a) p irreduzibel,
- (b) p ist ein Primelement.

Beweis. Wir müssen nur $(a) \Rightarrow (b)$ zeigen: Sei p irreduzibel und p teile ab und $p \nmid a$. Wir müssen zeigen, dass p das Element b teilt. Sei I das von p und a erzeugte Ideal, also $I = aR + pR$. Dann ist dies ein Hauptideal, also etwa $I = (c)$. Dann folgt $c \mid a$ und $c \mid p$, also etwa $cd = p$. Da p irreduzibel ist, ist c oder d eine Einheit. Ist d eine Einheit, so ist $(p) = (c) = I = aR + pR$, also ist $a \in (p)$, d.h. p teilt a , was der Voraussetzung widerspricht. Also ist c eine Einheit, d.h., $I = R$ und es gibt $r, s \in R$ mit $ar + ps = 1$, also $b = abr + psb = p(r'r + sb)$ fuer ein r' , also $p \mid b$ wie verlangt. $\square$

Satz 2.4.9 (Primfaktorzerlegung). Sei R ein Hauptidealring und sei $a \in R \setminus \{0\}$ keine Einheit. Dann existieren Primelemente $p_1, \dots, p_n$, so dass $a = p_1 \cdots p_n$. Sind

$$a = p_1 \cdots p_n = q_1 \cdots q_m$$

zwei solche Darstellungen, dann folgt $n = m$ und es gibt Einheiten $u_1, \dots, u_n \in R^\times$ so dass nach Umnummerierung gilt

$$p_j = u_j q_j$$

fuer jedes $j = 1, \dots, n$.

Beweis. Da jedes irreduzible Element prim ist, genügt es, eine Zerlegung in irreduzible zu konstruieren. Sei $a \in R$ ungleich Null und keine Einheit.

Angenommen, a lässt sich nicht als Produkt von Irreduziblen schreiben. Dann ist a reduzibel und kann selbst als Produkt $a_1 a'_1$ von Nichteinheiten geschrieben werden. Da a kein Produkt von Irreduziblen ist, gilt dasselbe für mindestens einen der Faktoren, sagen wir a_1 , und a_1 kann als Produkt $a_2 a'_2$ zweier Nichteinheiten geschrieben werden. Iteration liefert eine Folge von Elementen

$$a = a_0, a_1, \dots \in R$$

so dass a_{j+1} ein Teiler von a_j , aber nicht assoziiert zu a_j ist. Also folgt für die Hauptideale

$$aR = a_0R \subsetneq a_1R \subsetneq a_2R \subsetneq \dots$$

Man prüft leicht nach, dass die Vereinigung einer aufsteigenden Folge von Idealen wieder ein Ideal ist, also ist

$$\bigcup_{j \in \mathbb{N}} a_j R$$

wieder ein Ideal in R , also ein Hauptideal bR . Dann ist $b \in a_j R$ für ein j und daher

$$bR \subset a_j R \subset a_{j+1} R \subset bR,$$

woraus Gleichheit folgt, ein *Widerspruch!* Daher ist die Annahme falsch, also ist jedes Element als Produkt von Irreduziblen darstellbar.

Die Eindeutigkeit liefert das folgende Lemma. □

Lemma 2.4.10. *Gilt in einem Integritätsring R die Gleichung*

$$p_1 \cdots p_r = q_1 \cdots q_s$$

für Primelemente p_j und irreduzible Elemente q_i , dann ist $r = s$ und nach Umnummerierung ist jedes p_j assoziiert zu q_j .

Beweis. Da $p_1 \mid q_1 \cdots q_s$, gibt es ein j mit $p_1 \mid q_j$. Nach Umnummerierung können

wir $p_1 \mid q_1$ annehmen. Es folgt $q_1 = \varepsilon_1 p_1$, wobei ε_1 auf Grund der Irreduzibilität von q_1 eine Einheit ist. Da wir uns in einem Integritätsring befinden, folgt

$$p_2 \cdots p_r = \varepsilon_1 q_2 \cdots q_s.$$

Wir iterieren diesen Vorgang und können die q_i so umnummerieren, dass p_j zu q_j assoziiert ist. Insbesondere folgt $r \leq s$. Ist $r < s$ erhalten wir

$$1 = \varepsilon q_{r+1} \cdots q_s,$$

woraus folgt, dass q_s eine Einheit ist, was ein Widerspruch ist, also ist $r = s$. $\square$

Korollar 2.4.11 (Berechnung des ggT). *Sei R ein HIR und $\mathcal{P}$ ein Vertretersystem der Primelemente modulo Assoziiertheit. Seien $a_1, \dots, a_n \in R$ Nichteinheiten und seien*

$$a_j = u_j \prod_{p \in \mathcal{P}} p^{v_p(j)}$$

ihre Primfaktorzerlegungen, also $u_j \in R^\times$ und $v_p(j) \in \mathbb{N}_0$, fast alle Null. Dann gilt

$$\text{ggT}(a_1, \dots, a_n) = \prod_{p \in \mathcal{P}} p^{w_p},$$

wobei $w_p = \min_{j=1}^n v_p(j)$.

Beweis. Sei r die rechte Seite. Dann teilt r jedes a_j , es gibt also $b_j \in R$ mit $a_j = r b_j$, also

$$a_1 R + \cdots + a_n R = r(b_1 R + \cdots + b_n R).$$

Wir ersetzen jedes a_j durch b_j , dass wir nur den Fall betrachten müssen, dass die a_j keinen gemeinsamen Primteiler haben. Wir sagen dann, die $a_1, \dots, a_n$ sind **teilerfremd**. Sei $gR = a_1 R + \cdots + a_n R$. Angenommen, g ist keine Einheit, dann gibt es einen Primteiler p von g . Da $a_j \in gR$, teilt p jedes a_j , was im Widerspruch zur Teilerfremdheit steht. Also ist g eine Einheit. $\square$

Korollar 2.4.12. Sei R ein Hauptidealring und $p \in R \setminus \{0\}$. Dann sind äquivalent:

- (a) p ist irreduzibel,
- (b) p ist ein Primelement,
- (c) R/pR ist ein Körper.

Beweis. Die Äquivalenz von (a) und (b) ist Satz 2.4.8. Sei p ein Primelement und sei $\bar{z} \in R/pR \setminus \{0\}$ die Äquivalenzklasse von $z \in R$. Dass $\bar{z} \neq 0$ ist bedeutet, dass $z \notin pR$ ist, was bedeutet, dass p in der Primfaktorzerlegung von z nicht vorkommt und damit ist $\text{ggT}(z, p) = 1$. Daher ist $zR + pR = R$, also gibt es $x, y \in R$ mit $zx + py = 1$, oder $\bar{z}\bar{x} = 1$ in $R/(p)$, so dass $\bar{z}$ invertierbar ist.

Für die Umkehrung sei R/pR ein Körper und p teile ein Produkt ab . Dann ist $\bar{a}\bar{b} = 0$ und daher $\bar{a} = 0$ oder $\bar{b} = 0$, also $p \mid a$ oder $p \mid b$. □

Beispiel 2.4.13. $\mathbb{Z}/m$ ist genau dann ein Körper, wenn $m = p$ eine Primzahl ist. In diesem Fall schreibt man $\mathbb{F}_p = \mathbb{Z}/p$.

2.5 Quotientenkörper

Proposition 2.5.1. Sei R ein Integritätsring und sei $S = R \setminus \{0\}$. Auf der Menge $R \times S$ führen wir eine Äquivalenzrelation ein:

$$(a, s) \sim (b, t) \iff at = bs.$$

Wir schreiben $\frac{a}{s}$ für die Äquivalenzklasse von (a, s) und wir schreiben $K = \text{Quot}(R)$ für die Menge der Äquivalenzklassen. Dann ist $\sim$ eine Äquivalenzrelation und K wird mit den Operationen

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

ein Körper. Das Einselement ist $\frac{1}{1}$. Die Abbildung $\phi : R \rightarrow K, a \mapsto \frac{a}{1}$ ist ein injektiver Ringhomomorphismus mit der Eigenschaft $\phi(S) \subset K^\times$.

Ist $\alpha : R \rightarrow L$ ein injektiver Ringhomomorphismus, wobei L ein Körper ist, dann lässt sich α in eindeutiger Weise zu einem Ringhomomorphismus $K \rightarrow L$ fortsetzen.

Beweis. Der einzige nichttriviale Punkt ist die Transitivität. Seien also $(a, s) \sim (b, t)$ und $(b, t) \sim (c, r)$ dann gilt

$$at = bs \quad \text{und} \quad br = ct.$$

Daraus folgt $art = brs = cts$, also $art = cst$ oder $(ar - cs)t = 0$. Da R integer ist und $t \neq 0$, folgt $ar = cs$, also $(a, s) \sim (c, r)$. Die Ringaxiome für K rechnet man direkt nach. Ebenso ist es leicht einzusehen, dass die Abbildung ϕ ein Ringhomomorphismus ist. Ist $\alpha \in K \setminus \{0\}$, also $\alpha = \frac{a}{s}$ mit $a \neq 0$, dann ist auch a in S , also liegt auch $\frac{s}{a}$ in K und es gilt $\frac{a}{s} \frac{s}{a} = \frac{1}{1} = 1$, also ist K ein Körper. Schliesslich zur Injektivität von ϕ . Ist $\phi(a) = 0$, also $\frac{a}{1} = 0 = \frac{0}{1}$, dann gilt in R , dass $a = a \cdot 1 = 0 \cdot 1 = 0$ und damit ist $a = 0$, also ϕ injektiv.

Die behauptete Fortsetzung von $\alpha : K \rightarrow L$ definiert man durch

$$\tilde{\alpha}\left(\frac{a}{b}\right) := \frac{\phi(a)}{\phi(b)}.$$

Wohldefiniertheit: ist $\frac{a}{b} = \frac{c}{d}$, also $ad = bc$, dann folgt $\alpha(a)\alpha(d) = \alpha(b)\alpha(c)$, also $\frac{\alpha(a)}{\alpha(b)} = \frac{\alpha(c)}{\alpha(d)}$. Dann ist $\tilde{\alpha}$ eine Fortsetzung von α und es ist ein

Ringhomomorphismus: Multiplikativität ist klar und Additivität folgt wegen

$$\tilde{\alpha}\left(\frac{a}{b} + \frac{c}{d}\right) = \tilde{\alpha}\left(\frac{ad + bc}{bd}\right) = \frac{\alpha(a)\alpha(d) + \alpha(b)\alpha(c)}{\alpha(b)\alpha(d)} = \frac{\alpha(a)}{\alpha(b)} + \frac{\alpha(c)}{\alpha(d)} = \tilde{\alpha}\left(\frac{a}{b}\right) + \tilde{\alpha}\left(\frac{c}{d}\right).$$

□

Beispiele 2.5.2. • Ist $R = \mathbb{Z}$, dann ist $K = \mathbb{Q}$.

- Ist $R = K[x]$ der Polynomring über einem Körper K , dann ist der Quotientenkörper der Körper $K(x) = \left\{ \frac{p(x)}{q(x)} \right\}$ der rationalen Funktionen über K .

Korollar 2.5.3. Ist R ein Hauptidealring mit Quotientenkörper K , dann hat jedes

Element $x \in K \setminus \{0\}$, eine Primfaktorzerlegung

$$x = u \prod_{j=1}^n p_j^{k_j}$$

mit $k_j \in \mathbb{Z}$ und $u \in R^\times$.

2.6 Polynomringe

Definition 2.6.1. Sei R ein Hauptidealring und $f(x) = a_0 + a_1x + \cdots + a_nx^n$ in $R[x]$. Schreibe dann $v(f)$ für den ggT der Koeffizienten $a_1, \dots, a_n$. Für $\alpha \in R \setminus \{0\}$ gilt dann

$$v(\alpha f) = \alpha v(f).$$

Ferner liegt $\frac{f}{v(f)}$ in $R[x]$ und hat teilerfremde Koeffizienten.

Ist nun $0 \neq f(x) \in K[x]$, also nicht notwendig in $R[x]$, dann existiert $0 \neq \lambda \in R$ so dass $\lambda f(x) \in R[x]$. Das Element

$$\frac{1}{\lambda} v(\lambda f)$$

hängt nicht von der Wahl von λ ab, denn ist $\mu \in R \setminus \{0\}$, so dass ebenfalls $\mu f \in R[x]$ gilt, so folgt $\lambda v(\mu f) = v(\lambda \mu f) = \mu v(\lambda f)$ und Division durch $\mu \lambda$ liefert $\frac{v(\mu f)}{\mu} = \frac{v(\lambda f)}{\lambda}$. Wir definieren also $v(f) := \frac{1}{\lambda} v(\lambda f)$.

Lemma 2.6.2. Sei $f \in K[x]$.

- (a) Es gilt $v(\alpha f) = \alpha v(f)$ für jedes $\alpha \in K^\times$.
- (b) Das Polynom $\frac{f}{v(f)}$ hat teilerfremde Koeffizienten in R .
- (c) Ist $v(f) \in R$, dann ist $f \in R[x]$.

Beweis. (a) Sei $\mu \in R$ so dass $\mu \alpha \in R$ und $\mu f \in R[x]$. Dann gilt

$$v(\alpha f) = \frac{1}{\mu^2} v(\mu^2 \alpha f) = \frac{1}{\mu^2} \alpha \mu v(\mu f) = \alpha \frac{1}{\mu} v(\mu f) = \alpha v(f).$$

(b) Für $f \in R[x]$ ist $v(f)$ der ggT der Koeffizienten, also ist in diesem Fall die Behauptung klar. Im allgemeinen Fall sei $\lambda \in R$ mit $\lambda f \in R[x]$ gegeben, dann gilt $\frac{f}{v(f)} = \frac{\lambda f}{v(\lambda f)}$ und damit die Behauptung.

(c) Nach (b) liegt $f = v(f) \frac{f}{v(f)}$ in $R[x]$. □

Lemma 2.6.3 (Gauß Lemma). *Sei R ein Hauptidealring und K sein Quotientenkörper. Seien $0 \neq f, g \in K[x]$. Dann gilt*

$$v(fg) = v(f)v(g).$$

Beweis. Wir multiplizieren beide Seiten der Behauptung mit $\frac{1}{v(f)v(g)}$. Die Behauptung wird dann äquivalent zu derselben Behauptung für $\frac{f}{v(f)}$ und $\frac{g}{v(g)}$, so dass wir annehmen können, dass f und g in $R[x]$ liegen und teilerfremde Koeffizienten haben. Wir müssen dann zeigen, dass $v(fg) = 1$. Seien

$$\begin{aligned} f(x) &= a_0 + a_1x + \cdots + a_nx^n, \\ g(x) &= b_0 + b_1x + \cdots + b_mx^m \end{aligned}$$

mit $a_n \neq 0 \neq b_m$. Dann ist fg wieder in $R[x]$ und es reicht zu zeigen, dass ein gegebenes Primelement p nicht alle Koeffizienten von fg teilt. Da nun aber p ein Primelement ist, ist pR ein Primideal, also ist R/pR ein Integritätsring und damit ist $(R/pR)[x] \cong R[x]/pR[x]$ ein Integritätsring. Die Voraussetzung, dass p nicht alle Koeffizienten von f und g teilt bedeutet gerade, dass die Restklasse von f und g ungleich Null sind, damit ist auch die Restklasse von fg ungleich Null nach Satz 2.1.8, so dass die Behauptung folgt. □

Korollar 2.6.4. *Sei R ein Hauptidealring und K sein Quotientenkörper. Seien f, g normierte Polynome in $K[x]$ so dass fg in $R[x]$ liegt. Dann liegen f und g beide in $R[x]$ und haben teilerfremde Koeffizienten.*

Beweis. Das Polynom $\frac{f}{v(f)}$ liegt in $R[x]$ und hat Leitkoeffizient $\frac{1}{v(f)}$, so dass $\frac{1}{v(f)}$ in R liegt. Dasselbe gilt für $\frac{1}{v(g)}$. Da andererseits $v(f)v(g) = v(fg)$ in R liegt, sind $v(f)$

und $v(g)$ Einheiten in R , also $v(f) = 1 = v(g)$ und $f = \frac{f}{v(f)}$ hat teilerfremde Koeffizienten in R . □

Satz 2.6.5 (Eisenstein Kriterium). *Seien R ein Hauptidealring und K sein Quotientenkörper. Sei $f(x) = a_0 + a_1x + \dots + a_nx^n$ ein Polynom vom Grad $n \geq 1$ in $R[x]$. Sei p ein Primelement von R und nimm an*

$$p \nmid a_n, \quad p \mid a_0, a_1, \dots, a_{n-1}, \quad p^2 \nmid a_0,$$

dann ist $f(x)$ irreduzibel in $K[x]$.

Beweis. Wir können $n \geq 2$ annehmen. Indem wir gemeinsame Primfaktoren herausziehen, können wir annehmen, dass $a_0, \dots, a_n$ keinen gemeinsamen Primfaktor haben, also $v(f) = 1$. **Angenommen**, es gibt eine Faktorisierung $f = gh$ in $K[x]$ so dass g und h beide nicht-konstant sind. Nach dem Gauss-Lemma folgt $f = \frac{f}{v(f)} = \frac{g}{v(g)} \frac{h}{v(h)}$ und dies ist eine Faktorisierung in $R[x]$. Ersetzen wir also g und h durch $g/v(g)$ und $h/v(h)$, so haben wir eine Faktorisierung $f = gh$ in $R[x]$, sagen wir $g(x) = b_0 + b_1x + \dots + b_kx^k$ und $h(x) = c_0 + \dots + c_mx^m$. Dann ist $a_0 = b_0c_0$ und da $p^2 \nmid a_0$ wird einer der beiden, sagen wir c_0 , nicht von p geteilt, aber $p \mid b_0$. Nun ist $p \mid a_1 = b_0c_1 + b_1c_0$ und daher $p \mid b_1$. Dieser Schluss iteriert sich, so dass wir $p \mid b_j$ für jedes j feststellen können, was aber in $p \mid f$ mündet. Dies ist ein **Widerspruch!** □

3 Körper

3.1 Homomorphismen und Erweiterungen

Definition 3.1.1. Ist L ein Körper und $K \subset L$ eine Teilmenge, die selbst ein Körper ist, so nennt man K einen **Unterkörper** zu L . Man nennt $L \supset K$ eine **Körpererweiterung**.

In diesem Fall ist L insbesondere ein K -Vektorraum. Wir definieren den **Grad der Körpererweiterung** als

$$[L : K] := \dim_K L$$

falls endlich und ∞ sonst. Wir sagen, die Körpererweiterung ist **endlich**, falls $[L : K] < \infty$ ist.

Schreibweise: Die übliche Schreibweise für eine Körpererweiterung ist L/K , die nicht mit der Quotientenbildung verwechselt werden darf, etwa bei Gruppen G/H . Da man aber bei Körpern keine Quotienten betrachtet, ist die Verwechslungsgefahr gering.

Lemma 3.1.2. Eine Teilmenge $M \subset K$ eines Körpers ist genau dann ein Unterkörper, wenn

- (a) M ist eine Untergruppe von $(K, +)$,
- (b) M enthält die Eins und ist abgeschlossen unter der Multiplikation, also $a, b \in M \Rightarrow ab \in M$ und
- (c) M ist abgeschlossen unter Inversenbildung, also $0 \neq a \in M \Rightarrow a^{-1} \in M$.

Beweis. Assoziativgesetze und das Distributivgesetz vererben sich, die Existenz der Eins und des Inversen wird gefordert. □

Beispiele 3.1.3. • $\mathbb{R}/\mathbb{Q}$ und $\mathbb{C}/\mathbb{R}$ sind Körpererweiterungen.

- $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ ist eine Körpererweiterung. Hierbei ist $\mathbb{Q}(\sqrt{2}) = \mathbb{Q} \oplus \mathbb{Q}\sqrt{2} = \text{Spann}_{\mathbb{Q}}(1, \sqrt{2})$ und dies ist ein Unterkörper von $\mathbb{R}$.

Beweis. Nach Definition ist $K = \mathbb{Q}(\sqrt{2})$ ein $\mathbb{Q}$ -Untervektorraum von $\mathbb{R}$. Er enthält die Eins und wegen

$$(a + b\sqrt{2})(c + d\sqrt{2}) = ac + 2bd + (ad + bc)\sqrt{2}$$

ist er abgeschlossen unter der Multiplikation. Für die Inversen sei $x = a + b\sqrt{2} \in K \setminus \{0\}$ gegeben. Ist $b = 0$, dann liegt das Inverse a^{-1} in K . Sei also $b \neq 0$. Es gilt

$$(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2.$$

Da $\sqrt{2} \notin \mathbb{Q}$, kann $a^2 - 2b^2 \in \mathbb{Q}$ nicht Null sein, also ist $\frac{a-b\sqrt{2}}{a^2-2b^2}$ invers zu x . □

Definition 3.1.4. Seien K, L Körper. Ein **Körperhomomorphismus** $\phi : K \rightarrow L$ ist dasselbe wie ein Ringhomomorphismus, nur eben zwischen Körpern. Da ein Körper keine echten Ideale hat, ist ein Körperhomomorphismus stets injektiv.

Beispiele 3.1.5. (a) Die komplexe Konjugation $\bar{\cdot} : \mathbb{C} \rightarrow \mathbb{C}$ ist ein Körperhomomorphismus.

(b) Ist L der Quotientenkörper von $K[x, y]$, dann ist $\phi : f(x, y) \mapsto f(y, x)$ ein Körperhom $L \rightarrow L$.

(c) Seien $K \subset L$ Körper und $K(x) = \text{Quot}(K[x])$. Für jedes $a \in L$ ist dann

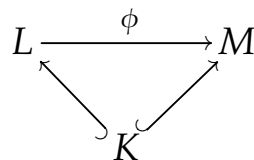
$$\begin{aligned} \varepsilon_a : K(x) &\rightarrow L, \\ f(x) &\mapsto f(a) \end{aligned}$$

ein Körperhom, der **Einsetzungshomomorphismus**.

Definition 3.1.6. Sind L/K und M/K Körpererweiterungen, so ist ein **Homomorphismus von Körpererweiterungen**, oder ein Homomorphismus von $L \rightarrow M$ über K ein Ringhomomorphismus

$$\phi : L \rightarrow M \quad \text{mit} \quad \phi|_K = \text{Id}.$$

Da L und M Körper sind, ist ϕ automatisch injektiv. Man verdeutlicht dies durch das kommutative Diagramm



Ist ϕ zusätzlich surjektiv, dann ist die Umkehrabbildung ebenfalls ein Ringhomomorphismus und ϕ heisst in diesem Falle ein **Isomorphismus von Körpererweiterungen**. Wir schreiben

$$\text{Hom}_K(L, M)$$

für die Menge aller Homomorphismen von Körpererweiterungen $L/K \rightarrow M/K$.

Beispiel 3.1.7. Sei $\phi : \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{R}$, $\phi(a, b) = a + b\sqrt{2}$, wobei $\sqrt{2}$ die eindeutig bestimmte reelle Zahl $\alpha > 0$ ist mit $\alpha^2 = 2$. Dann ist ϕ ein Homomorphismus von Körpererweiterungen $\mathbb{Q}(\sqrt{2})/\mathbb{Q} \rightarrow \mathbb{R}/\mathbb{Q}$.

Definition 3.1.8. Sei L/K eine Körpererweiterung und seien $\alpha_1, \dots, \alpha_n \in L$. Sei

$$K(\alpha_1, \dots, \alpha_n) = \bigcap_{\substack{K \subset L' \subset L \\ \alpha_1, \dots, \alpha_n \in L'}} L'$$

der Schnitt über alle Zwischenkörper, die $\alpha_1, \dots, \alpha_n$ enthalten. Dies ist wieder ein Körper, und zwar der kleinste Zwischenkörper

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

der alle $\alpha_1, \dots, \alpha_n$ enthält.

Lemma 3.1.9. In der Situation der Definition besteht der Körper $L = K(\alpha_1, \dots, \alpha_n)$ genau aus den Quotienten $\frac{p(\alpha_1, \dots, \alpha_n)}{q(\alpha_1, \dots, \alpha_n)}$, wobei $p, q \in K[x_1, \dots, x_n]$ Polynome in n Variablen sind, wobei $q(\alpha_1, \dots, \alpha_n) \neq 0$ vorausgesetzt wird.

Beweis. Die Menge M all dieser Elemente ist eine abelsche Untergruppe, enthält K , sowie die α_j und ist in der Tat ein Körper. Daher ist $L \subset M$. Andererseits enthält jeder Körper, der K und $\alpha_1, \dots, \alpha_n$ enthält, auch alle Elemente der Form $p(\alpha_1, \dots, \alpha_n)/q(\alpha_1, \dots, \alpha_n)$ falls $p, q \in K[x_1, \dots, x_n]$ und $q(\alpha_1, \dots, \alpha_n) \neq 0$. Daher folgt dann auch $M \subset L$. □

3.2 Adjunktion von Nullstellen

Sei K ein Körper und $f(x) \in K[x]$ ein nichtkonstantes Polynom, das keine Nullstelle in K hat. Wir werden zeigen, dass es eine endliche Körpererweiterung L/K gibt, so dass f eine Nullstelle in L hat. Der Ring $K[x]$ ist ein Hauptidealring, so dass f als ein Produkt von Primelementen $f = p_1 \cdots p_k$ geschrieben werden kann. Finden wir eine Erweiterung L/K in der, sagen wir, p_1 eine Nullstelle hat, haben wir eine Nullstelle von f gefunden. Wir können also annehmen, dass f selbst irreduzibel ist.

Satz 3.2.1. *Sei $f \in K[x]$ ein irreduzibles Polynom vom Grad n .*

(a) *$fK[x]$ ist ein Ideal und der Quotient*

$$K_f := K[x]/fK[x]$$

ein Körper, in dem f eine Nullstelle hat.

(b) *Ist M/K irgendeine Körpererweiterung, so dass f in M eine Nullstelle γ hat, dann gibt es genau einen Homomorphismus von Körpererweiterungen $\phi : K_f \rightarrow M$, mit $\phi(\alpha_0) = \gamma$. Das Bild von ϕ , geschrieben $K(\gamma)$, ist der kleinste Zwischenkörper $M \supset K(\gamma) \supset K$, der γ enthält.*

(c) *Die Körpererweiterung K_f/K hat Grad n und ist bis auf Isomorphie die einzige Erweiterung vom Grad $\leq n$, so dass f in K_f eine Nullstelle α_0 hat.*

Beweis. (a) Nach Korollar 2.4.12 ist der Ring $K_f = K[x]/fK[x]$ ein Körper, der K enthält. Sei $f(x) = a_0 + a_1x + \cdots + a_nx^n$ mit $a_n \neq 0$. Wir schreiben $\bar{x}$ für das Element $x + fK[x]$ in K_f . Dann folgt $f(\bar{x}) = f(x + fK[x]) = f(x) + fK[x] = fK[x]$ und dies ist die Null in K_f . Also hat f die Nullstelle $\bar{x}$ in K_f .

(b) Der Ringhomomorphismus $\phi : K[x] \rightarrow M$, $x \mapsto \gamma$ erfüllt $\phi(f) = 0$, faktorisiert also über $K_f = K[x]/fK[x]$. Der Körper $K(\gamma)$ besteht aus den Polynomen in γ ist also der kleinste Zwischenkörper, der γ enthält. Da K_f ein Körper ist, ist ϕ injektiv und damit $\dim M \geq \dim K_f$.

(c) Wir behaupten, dass $1, \bar{x}, \bar{x}^2, \dots, \bar{x}^{n-1}$ eine Basis von F_f über K ist.

Linear unabhängig: Sei $\lambda_0 + \lambda_1 \bar{x} + \dots + \lambda_{n-1} \bar{x}^{n-1} = 0$. Im Ring $K[x]$ bedeutet das

$$g(x) := \lambda_0 + \lambda_1 x + \dots + \lambda_{n-1} x^{n-1} \in fK[x].$$

Also ist $g = fh$ für ein Polynom h . Da $\deg g \leq n-1$ und $\deg f = n$, folgt, dass $h = 0$ sein muss, also ist auch $g = 0$, was soviel heißt wie $\lambda_0 = \dots = \lambda_{n-1} = 0$.

Erzeugend: Ist $g \in K[x]$, dann wollen wir zeigen, dass es Koeffizienten gibt, so dass $\bar{g}(x) = \lambda_0 + \lambda_1 \bar{x} + \dots, \lambda_{n-1} \bar{x}^{n-1}$ gilt. Im Polynomring bedeutet dies

$$g(x) = \lambda_0 + \lambda_1 x + \dots + \lambda_{n-1} x^{n-1} + fh$$

für ein $h \in K[x]$. Nach der **Division mit Rest** in $K[x]$ gibt es Polynome q, r mit $g = fq + r$ und $\deg(r) < \deg(f) = n$. Setzt man $h = q$ und

$\lambda_0 + \lambda_1 x + \dots + \lambda_{n-1} x^{n-1} := r(x)$, so folgt die Behauptung und damit $[K_f : K] = n$.

(c) Ist M/K eine weitere Körpererweiterung, in der f eine Nullstelle hat, dann ist nach obigem $\dim_K M \geq \dim_K K_f = n$ und damit folgt auch (c). $\square$

Der letzte Satz hat eine Verallgemeinerung auf beliebiger Mengen von Polynomen, die später nützlich werden wird.

Satz 3.2.2. Sei K ein Körper und sei $T \subset K[x]$ eine Menge von nichtkonstanten Polynomen. Dann existiert eine algebraische Körpererweiterung K_T/K so dass jedes Polynom $f \in T$ eine Nullstelle α_f in K_T hat.

Beweis. Sei $\mathcal{S}$ die Menge aller Paare (S, L) , wobei $S \subset T$ und L/K algebraisch, so dass jedes Polynom in T eine Nullstelle in L hat. Wir installieren eine Ordnung, in dem wir sagen

$$(S, L) \leq (S', L') \iff S \subset S' \text{ und } L \subset L'.$$

Das Lemma von Zorn gibt uns ein maximales Element (S, L) . Wir behaupten, dass schon jedes Polynom in T eine Nullstelle in L hat. Ist dies nicht der Fall für ein $f \in T$, dann $f \notin S$ und wir können eine Nullstelle α adjungieren, um einen Körper $L' = L(\alpha)$ zu erhalten, was der Maximalität von (S, L) widerspricht.

Mit diesem Beweis gibt es, wie häufig in solchen Fällen, ein mengentheoretisches Problem: Die Paare (S, L) bilden keine Menge. Das Problem löst sich aber auf, wenn wir eine überabzählbare Menge $\mathcal{M} \supset K$ wählen mit $|\mathcal{M}| > |K|$ und nur Körper $L \subset \mathcal{M}$ zulassen. $\square$

Primkörper

Definition 3.2.3. Sei K ein Körper. Für $n \in \mathbb{N}$ sei $n \cdot 1 = 1 + \cdots + 1$ die n -fache Summe der Eins. Wir definieren die **Charakteristik** von K als

$$\text{Char}(K) = \min \{n \in \mathbb{N} : n \cdot 1 = 0\},$$

falls die Menge nicht leer ist. Ist sie hingegen leer, definieren wir $\text{Char}(K) = 0$.

Satz 3.2.4. Die Charakteristik eines Körpers ist entweder Null oder eine Primzahl. Jeder gegebene Körper K enthält einen kleinsten Unterkörper $P = P(K) \subset K$. Dieser ist

$$P \cong \begin{cases} \mathbb{Q} & \text{Char}(K) = 0, \\ \mathbb{F}_p & \text{Char}(K) = p > 0. \end{cases}$$

Hierbei ist p eine Primzahl und $\mathbb{F}_p = \mathbb{Z}/p$ der Körper mit p Elementen. Der Körper P wird der **Primkörper** von K genannt.

Korollar 3.2.5. Ist $\text{Char}(K) = 0$, dann ist die Abbildung $\mathbb{Z} \rightarrow K, n \mapsto n \cdot 1$ injektiv.

Beweis. [Beweis des Satzes] Sei $\text{Char}(K) = n \neq 0$. Wir wollen zeigen, dass n eine Primzahl ist. **Angenommen**, dies ist nicht der Fall, dann gilt $n = pq$ für zwei natürliche Zahlen $p, q > 1$. Dann ist in K :

$$(p \cdot 1)(q \cdot 1) = (pq) \cdot 1 = n \cdot 1 = 0.$$

Da K ein Körper ist, muss einer der Faktoren $p \cdot 1$ oder $q \cdot 1$ gleich Null sein, sagen wir $p \cdot 1 = 0$. Damit folgt $p \geq \text{Char}(K) = n = pq$, also $1 \geq q$, **Widerspruch!**

Nun zur zweiten Aussage. Da der Schnitt über alle Unterkörper ein Unterkörper ist, gibt es einen kleinsten Unterkörper P . Dieser muss die Eins enthalten und damit auch $n \cdot 1 = 1 + \dots + 1$ für $n \in \mathbb{N}$ und auch $-n \cdot 1$, da P eine additive Gruppe ist. Insgesamt also $\mathbb{Z} \cdot 1 \subset P$. Ist nun $\text{Char}(K) = p$ eine Primzahl, dann faktorisiert der Ringhomomorphismus $\mathbb{Z} \rightarrow K$ über $\mathbb{Z} \rightarrow \mathbb{Z}/p$, wir erhalten also einen Ringhomomorphismus vom Körper $\mathbb{F}_p = \mathbb{Z}/p$ nach K . Da Homomorphismen von Körpern immer injektiv sind haben wir also einen Unterkörper $\cong \mathbb{F}_p$. Da $\mathbb{F}_p$ genau die Summen der Eins enthält, hat er selbst keinen echten Unterkörper, also folgt $P = \mathbb{F}_p$.

Ist schliesslich $\text{Char}(K) = 0$, dann ist der Ringhomomorphismus $\mathbb{Z} \rightarrow K$ injektiv. Zu jedem $q \in \mathbb{N}$ existiert dann das inverse $(q \cdot 1)^{-1}$ und die Abbildung

$\frac{m}{q} \mapsto (m \cdot 1)(q \cdot 1)^{-1}$ ist ein Ringhomomorphismus $\mathbb{Q} \rightarrow K$. Nun hat aber auch $\mathbb{Q}$ keine Unterkörper und damit ist $P \cong \mathbb{Q}$. $\square$

Proposition 3.2.6. *Ist K ein Körper, $P \subset K$ der entsprechende Primkörper und $\phi : K \rightarrow K$ ein Ringhomomorphismus, dann ist $\phi(P) = P$ und $\phi|_P = \text{Id}_P$.*

Beweis. Da ϕ ein additiver Gruppenhomomorphismus ist, folgt $\phi(kx) = k\phi(x)$ für $x \in K$ und $k \in \mathbb{Z}$. Mit $x = 1$ folgt $\phi(\bar{k}) = \bar{k}$ mit $k \in \mathbb{Z}$, wobei $\bar{k}$ das Bild von k in K ist, also die k -fache Summe der Eins. Ist $\text{Char}(K) > 0$, folgt bereits die Behauptung, da dann die additive Gruppe $(P, +)$ genau aus den Vielfachen der Eins, also aus allen $\bar{k}$, $k \in \mathbb{Z}$ besteht.

Ist $\text{Char}(K) = 0$, also $P = \mathbb{Q}$, dann rechnen wir für $\frac{p}{q} \in \mathbb{Q}$,

$$\phi\left(\frac{p}{q}\right) = \frac{q}{q}\phi\left(\frac{p}{q}\right) = \frac{1}{q}\phi(p) = \frac{p}{q},$$

also, wie verlangt, $\phi|_{\mathbb{Q}} = \text{Id}$. $\square$

3.3 Algebraische und endliche Körpererweiterungen

Definition 3.3.1. Ein Element $\alpha \in L$ eines Oberkörpers zu K heisst **algebraisch** über K , falls es ein nichtkonstantes Polynom $f(x) \in K[x]$ gibt so dass

$$f(\alpha) = 0$$

gilt. Eine Körpererweiterung L/K heisst **algebraisch**, wenn jedes Element von L algebraisch über K ist.

- Beispiele 3.3.2.**
- Das Element $\sqrt{2} \in \mathbb{R}$ ist algebraisch über $\mathbb{Q}$, die Elemente e und π aber nicht, was aber schwierig zu zeigen ist. Leichter zu zeigen ist, dass $\mathbb{R}/\mathbb{Q}$ nicht algebraisch ist, denn es gibt nur abzählbar viele Polynome in $\mathbb{Q}[x]$, jedes Polynom hat nur endlich viele Nullstellen, also kann $\mathbb{R}$ nur abzählbar viele über $\mathbb{Q}$ algebraische Zahlen enthalten. Die Menge $\mathbb{R}$ ist aber überabzählbar.
 - Die Körpererweiterung $\mathbb{C}/\mathbb{R}$ ist algebraisch. Hierzu sei $\alpha \in \mathbb{C}$, etwa $\alpha = a + bi$. Ist $b = 0$, so ist $\alpha \in \mathbb{R}$ und nichts ist zu zeigen. Sonst gilt $(\alpha - a)^2 = (bi)^2 = -b^2$, also erfüllt α die Gleichung $f(x) = 0$ mit dem reellen Polynom $f(x) = (x - a)^2 + b^2$.

- Für einen Körper K und $n \in \mathbb{N}$ sei

$$\mu_n(K) = \{\varepsilon \in K : \varepsilon^n = 1\}.$$

Dann ist $\mu_n(K)$ eine Untergruppe von $K^\times$, genannt die Gruppe der **n -ten Einheitswurzeln** in K . Die Gruppe $\mu_n(K)$ hat höchstens n Elemente, da das Polynom $x^n - 1$ höchstens n Nullstellen hat. Jede Einheitswurzel ist algebraisch über dem Primkörper.

Lemma 3.3.3. *Sei $\phi : L/K \rightarrow M/K$ ein Morphismus von Körpererweiterungen.*

- (a) *Ist $f \in K[x]$ und $\alpha \in L$ eine Nullstelle von f , dann ist $\phi(\alpha)$ ebenfalls eine Nullstelle von f .*
- (b) *Ist L_{alg} die Menge aller Elemente von L , die über K algebraisch sind. Dann gilt $\phi(L_{\text{alg}}) \subset M_{\text{alg}}$.*

Beweis. (a) Schreibe $f(x) = a_0 + a_1x + \cdots + a_nx^n$ mit $a_j \in K$. Dann gilt

$$f(\phi(\alpha)) = a_0 + a_1\phi(\alpha) + \cdots + a_n\phi(\alpha)^n = \phi(a_0 + a_1\alpha + \cdots + a_n\alpha^n) = \phi(f(\alpha)) = 0.$$

(b) folgt unmittelbar aus (a). □

Definition 3.3.4. Im Folgenden werden wir oft eine Körpererweiterung L/K und einen Zwischenkörper $L \supset M \supset K$ betrachten. Wir schreiben dann

$$L/M/K.$$

Wir sprechen dann von den zwei Körpererweiterungen $L/M/K$ und meinen damit die Erweiterungen L/M und M/K . Wenn wir zum Beispiel sagen, dass die Körpererweiterungen $L/M/K$ endlich sind, dann meinen wir damit, dass L/M und M/K beide endlich sind.

Satz 3.3.5.

- (a) Jede endliche Körpererweiterung ist algebraisch.
- (b) Die beiden Körpererweiterungen $L/M/K$ sind genau dann endlich, wenn L/K endlich ist und in diesem Fall gilt

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

- (c) Jedes algebraische Element $\alpha \in L$ ist Nullstelle eines **irreduziblen** Polynoms in $K[x]$.
- (d) Sei L/K eine Körpererweiterung und seien $\alpha_1, \dots, \alpha_n$ algebraisch über K . Dann ist $K(\alpha_1, \dots, \alpha_n)$ endlich über K .
- (e) Die beiden Erweiterungen $L/M/K$ sind genau dann algebraisch, wenn L/K algebraisch ist.

Beweis. (a) Sei L/K endlich, etwa $[L : K] = n$. Sei $\alpha \in L$. Da L ein n -dimensionaler K -Vektorraum ist, sind die $n + 1$ Vektoren

$$1, \alpha, \alpha^2, \dots, \alpha^n$$

über K linear abhängig. Es gibt also Koeffizienten $a_j \in K$, nicht alle Null, so dass

$$a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_n\alpha^n = 0.$$

Das heisst, α ist Nullstelle des Polynoms $f(x) = a_0 + a_1x + \dots + a_nx^n \in K[x]$.

(b) “ $\Rightarrow$ ” Die Körpererweiterungen $L/M/K$ seien beide endlich und sei $v_1, \dots, v_n$ eine Basis von M über K und sei $w_1, \dots, w_m$ eine Basis von L über M . Wir behaupten, dass $(v_iw_j)_{i,j}$ eine Basis von L über K ist. Zur Linearen

Unabhängigkeit: Sei

$$0 = \sum_{j=1}^m \sum_{i=1}^n \lambda_{i,j} v_i w_j = \sum_{j=1}^m \left(\sum_{i=1}^n \lambda_{i,j} v_i \right) w_j$$

mit $\lambda_{i,j} \in K$, dann folgt, da $\mu_j := \sum_{i=1}^n \lambda_{i,j} v_i \in M$, wegen der linearen Unabhängigkeit der w_j , dass $\mu_j = 0$ für jedes j und wegen der linearen Unabhängigkeit der v_i folgt dann $\lambda_{i,j} = 0$ für alle i, j . Schliesslich zeigen wir, dass $(v_i w_j)$ ein Erzeugendensystem ist. Sei dazu $\alpha \in L$, dann existieren $\mu_j \in M$ so dass $\alpha = \sum_{j=1}^m \mu_j w_j$. Schliesslich existieren $\lambda_{i,j} \in K$ so dass $\mu_j = \sum_{i=1}^n \lambda_{i,j} v_i$ und damit

$$\alpha = \sum_{j=1}^m \sum_{i=1}^n \lambda_{i,j} v_i w_j.$$

“ $\Leftarrow$ ” Für die Umkehrung schliesslich sei L/K endlich, dann ist M ein K -Unterraum von L und damit selbst endlich-dimensional. Ist schliesslich $v_1, \dots, v_n$ eine Basis von L über K , dann ist dies ebenfalls ein Erzeugendensystem von L als M -Vektorraum, so dass auch L/M endlich ist.

(c) Sei α Nullstelle des Polynoms f und sei $f = f_1 \cdots f_s$ eine Zerlegung in irreduzible (=Primelemente von $K[x]$). Dann ist $0 = f(\alpha) = f_1(\alpha) \cdots f_s(\alpha)$ und damit muss einer der Faktoren $f_j(\alpha)$ gleich Null sein.

(d) Sei $\alpha \in L$ Nullstelle des irreduziblen Polynoms f . Dann ist $K(\alpha)$ endlich über K , denn $K(\alpha)$ gleich dem Bild des kanonischen Homomorphismus $K_f \rightarrow L$, der x auf α wirft. Das ist der Fall $n = 1$. Ansonsten beachte, dass $K(\alpha_1, \dots, \alpha_n)$ durch sukzessive Adjunktion der α_j entsteht, also

$$K(\alpha_1, \dots, \alpha_n) = K(\alpha_1)(\alpha_2) \cdots (\alpha_n).$$

(e) “ $\Rightarrow$ ” Seien die beiden Erweiterungen $L/M/K$ algebraisch und sei $\alpha \in L$. Nach

(b) ist $M(\alpha)$ endlich über M . Sei $f(x) = a_0 + a_1x + \cdots + a_nx^n$, dann ist jedes $a_0, \dots, a_n$ algebraisch über K und nach Teil (d) ist $K(a_0, \dots, a_n)$ endlich über K . Das Element α schliesslich ist algebraisch über $K(a_0, \dots, a_n)$ und damit ist $K(a_0, a_1, \dots, a_n, \alpha) = K(a_0, \dots, a_n)(\alpha)$ endlich über K und enthält α . Also ist α algebraisch über K und L/K ist algebraisch.

“ $\Leftarrow$ ” Für die Umkehrung sei L/K algebraisch, dann ist M/K auch algebraisch. Ist dann $\alpha \in L$, dann ist α Nullstelle eines Polynoms aus $K[x] \subset M[x]$ und damit ist α algebraisch über M . $\square$

Definition 3.3.6. Sei L/K eine Körpererweiterung und $\alpha \in L$ algebraisch über K . Dann gibt es genau einen normierten Erzeuger m_α des Ideals $I_\alpha = \{f \in K[x] : f(\alpha) = 0\}$. Da $K(\alpha) = K[x]/m_\alpha K[x]$, ist m_α prim. Wir nennen m_α das **Minimalpolynom**. Als Erzeuger hat es den niedrigsten Grad im Ideal I_α .

Beispiele 3.3.7.

- Das Minimalpolynom von i über $\mathbb{R}$ oder $\mathbb{Q}$ ist $x^2 + 1$, denn als quadratisches Polynom ohne reelle Nullstelle ist $x^2 + 1$ irreduzibel.
- Das Minimalpolynom der primitiven 9-ten Einheitswurzel $\alpha = e^{2\pi i/9}$ über $\mathbb{Q}$ ist nicht etwa $x^9 - 1$ oder $\frac{x^9-1}{x-1} = x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$, sondern $x^6 + x^3 + 1$, was in einem späteren Abschnitt bewiesen wird.

3.4 Algebraischer Abschluss

Ein Körper K heisst **algebraisch abgeschlossen**, falls jedes nichtkonstante Polynom $f(x) \in K[x]$ in K eine Nullstelle hat.

Beispiele 3.4.1.

- $\mathbb{Q}$ ist nicht algebraisch abgeschlossen, denn das Polynom $x^2 - 2$ hat keine Nullstelle in $\mathbb{Q}$.
- $\mathbb{R}$ ist nicht algebraisch abgeschlossen, denn das Polynom $x^2 + 1$ hat keine Nullstelle in $\mathbb{R}$.
- $\mathbb{C}$ ist algebraisch abgeschlossen. Diese Aussage ist als der Fundamentalsatz der Algebra bekannt und wird in Abschnitt 3.11 bewiesen.
- Ist p eine Primzahl, so gibt es zu jedem $n \in \mathbb{N}$ genau einen endlichen Körper $\mathbb{F}_{p^n}$ mit genau p^n Elementen und falls $m \mid n$, so ist $\mathbb{F}_{p^m}$ ein Unterkörper von $\mathbb{F}_{p^n}$. Dies wird in einem späteren Abschnitt bewiesen. Dann ist $\mathbb{F}_{p^\infty} = \bigcup_{n \in \mathbb{N}} \mathbb{F}_{p^n}$ ein algebraisch abgeschlossener Körper.

Satz 3.4.2. Für jeden Körper K existiert bis auf Isomorphie genau eine algebraische Körpererweiterung $\bar{K}/K$, so dass $\bar{K}$ algebraisch abgeschlossen ist. Man nennt $\bar{K}$ den **algebraischen Abschluss** von K .

Beweis. Nach Satz 3.2.2 existiert zu jeder Teilmenge $T \subset K[x]$ von nichtkonstanten Polynomen eine algebraische Körpererweiterung K_T/K in der jedes $f \in T$ eine Nullstelle besitzt. Wir wenden dies auf die Menge T aller nichtkonstanten Polynome $f \in K[x]$ an und erhalten einen Körper K_1 in dem jedes nichtkonstante Polynom f aus $K[x]$ eine Nullstelle besitzt. Wir wiederholen den Schritt und erhalten einen Körper K_2/K_1 in dem jedes nichtkonstante Polynom aus K_1 eine Nullstelle besitzt und so weiter. Wir erhalten eine Kette von Körpern $K \subset K_1 \subset K_2 \subset \dots$, so dass jedes nichtkonstante Polynom aus $K_n[x]$ eine Nullstelle in K_{n+1} besitzt. Sei

$$\bar{K} = \bigcup_{n \in \mathbb{N}} K_n.$$

Dann ist $\bar{K}$ wieder ein Körper und er ist algebraisch abgeschlossen, denn jedes irreduzible $f \in \bar{K}[x]$ hat Koeffizienten in einem K_n , so dass f in $K_{n+1} \subset \bar{K}$ eine Nullstelle hat. Ferner ist $\bar{K}$ algebraisch über K , denn jedes K_n ist algebraisch über K .

Nun zur Eindeutigkeit. Ist L/K eine weitere algebraische Erweiterung, die algebraisch abgeschlossen ist, dann müssen wir zeigen, dass es einen Isomorphismus $\phi : \bar{K} \xrightarrow{\cong} L$ gibt, der auf K die Identität ist.

Wir betrachten die Menge R aller Körperhomomorphismen $\phi : M \rightarrow L$ mit $\phi|_K = \text{Id}$, wobei $\bar{K} \supset M \supset K$ ein Zwischenkörper ist. Auf dieser Menge etablieren wir eine partielle Ordnung durch

$$(\phi : M \rightarrow L) \leq (\psi : P \rightarrow L) \iff M \subset P \text{ und } \psi|_M = \phi.$$

Wir wollen das Lemma von Zorn anwenden. Es ist leicht zu sehen, dass die Vereinigung einer Kette eine obere Schranke liefert, also liefert das Lemma von Zorn die Existenz eines maximalen Elements $\phi : M \rightarrow L$. Wir müssen zeigen, dass $M = \bar{K}$ und $\text{Bild}(\phi) = L$ ist. Sei $\alpha \in \bar{K}$. Da $\bar{K}/M$ algebraisch ist, gibt es ein irreduzibles Polynom $f \in M[x]$ mit $f(\alpha) = 0$ und es ist $M(\alpha) \cong M_f = M[x]/fM[x]$. Da L algebraisch abgeschlossen ist, gibt es einen Körperhomomorphismus $M(\alpha) \cong M_f \rightarrow L$, der ϕ fortsetzt. Da ϕ maximal ist, folgt $M(\alpha) = M$, also $\alpha \in M$. Wir haben also $M = \bar{K}$. Es bleibt zu zeigen, dass das Bild B von ϕ gleich L ist. Nun ist $B \cong \bar{K}$ und damit ist B algebraisch abgeschlossen. Ferner ist L/B algebraisch, da L/K algebraisch ist. Ist $\alpha \in L$, so ist α Nullstelle eines irreduziblen Polynoms $f \in B[x]$, welches aber in $B[x]$ in Linearfaktoren zerfällt, d.h. alle Nullstellen von f liegen in B , also auch $\alpha \in B$. $\square$

Satz 3.4.3. *Sei L/K eine algebraische Erweiterung und sei $\sigma : K \rightarrow \Omega$ ein Homomorphismus in einen algebraisch abgeschlossenen Körper Ω . Dann kann man σ zu einer Einbettung $L \hookrightarrow \Omega$ fortsetzen.*

Beweis. Da σ injektiv ist, kann man K als einen Teilkörper von Ω auffassen. Sei $\bar{K}$ die Menge aller $\omega \in \Omega$, die algebraisch über K sind. Dann ist $\bar{K}$ ein algebraischer Abschluss von K . Sei $\bar{L}$ ein algebraischer Abschluss von L . Da L algebraisch über K ist, ist $\bar{L}$ ebenfalls ein algebraischer Abschluss von K , also gibt es einen Isomorphismus $\bar{L} \xrightarrow{\cong} \bar{K} \subset \Omega$, dessen Einschränkung nach L das Gewünschte leistet. $\square$

Beispiele 3.4.4. • Der Algebraische Abschluss von $\mathbb{R}$ ist $\mathbb{C}$. (Wir werden noch beweisen, dass $\mathbb{C}$ algebraisch abgeschlossen ist.)

- Man kann den algebraischen Abschluss $\bar{\mathbb{Q}}$ von $\mathbb{Q}$ in den Körper $\mathbb{C}$ einbetten. Die Einbettung ist nicht eindeutig, wohl aber ihr Bild, es besteht aus allen Elementen von $\mathbb{C}$, die algebraisch über $\mathbb{Q}$ sind. Wir fassen daher zuweilen den algebraischen Abschluss $\bar{\mathbb{Q}}$ gleich als Unterkörper von $\mathbb{C}$ auf.

3.5 Zerfällungskörper und normale Erweiterungen

Definition 3.5.1. Sei K ein Körper und $f(x) \in K[x]$ ein nichtkonstantes Polynom. Ein **Zerfällungskörper** von f ist eine Körpererweiterung L/K so dass

- f über L in Linearfaktoren zerfällt, d.h., es gilt

$$f(x) = c(x - \alpha_1) \cdots (x - \alpha_n)$$

mit $\alpha_1, \dots, \alpha_n \in L$ und $c \in K^\times$ und

- L von den Nullstellen erzeugt wird, also

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

Satz 3.5.2. Sei E/K ein Zerfällungskörper zum nichtkonstanten Polynom $f \in K[x]$. Ist L/K ein weiterer Zerfällungskörper, dann gibt es einen Isomorphismus $\phi : E \rightarrow L$ über K .

Ist weiter $L \subset \Omega$ für einen algebraisch abgeschlossenen Körper Ω , so hat jeder Körperhomomorphismus $\sigma : E \rightarrow \Omega$ über K das Bild L und induziert einen Isomorphismus $E \xrightarrow{\cong} L$.

Beweis. Der algebraische Abschluss $\bar{L}$ ist auch einer von K und ebenso für E . Also gibt es einen K -Isomorphismus $\phi : \bar{E} \rightarrow \bar{L} \cong \Omega_{\text{alg}}$. Nach Lemma 3.3.3 wirft ϕ die Nullstellen von f auf Nullstellen von f . Da E von den Nullstellen von f erzeugt wird, folgt $\phi(E) \subset L$. Da auch L von den Nullstellen von f erzeugt wird, folgt Gleichheit.

Ist $L \subset \Omega$ und $\sigma : K \rightarrow \Omega$ wie im Satz, dann wirft σ ebenfalls Nullstellen von f auf Nullstellen von f und daher wird auch $\sigma(K)$ von den Nullstellen von f erzeugt, ist also gleich L . □

Definition 3.5.3. Ist I eine Indexmenge und für jedes $i \in I$ ein nichtkonstantes Polynom $f_i \in K[x]$ gegeben. Ein **Zerfällungskörper** der Familie $(f_i)_{i \in I}$ von Polynomen ist eine Körpererweiterung L/K so dass jedes f_i in L in Linearfaktoren zerfällt und L über K von den Nullstellen der f_i erzeugt wird.

Korollar 3.5.4. Sei L/K ein Zerfällungskörper der Familie $(f_i)_{i \in I}$ von Polynomen. Sei E/K ein weiterer Zerfällungskörper, dann gibt es einen Isomorphismus $L \xrightarrow{\cong} E$ über K .

Jeder Ringhomomorphismus von L nach $\bar{E}$ über K hat das Bild E und ist ein Isomorphismus $L \xrightarrow{\cong} E$ über K .

Beweis. Wie der Satz. □

Satz 3.5.5. Sei L/K eine algebraische Erweiterung von K und sei $\bar{K}$ ein algebraischer Abschluss von K . Dann sind die folgenden Bedingungen äquivalent:

(N1) Alle Homomorphismen $L \rightarrow \bar{K}$ über K haben dasselbe Bild.

(N2) L ist der Zerfällungskörper einer Familie von Polynomen.

(N3) Jedes irreduzible Polynom $f \in K[x]$, das in L eine Nullstelle hat, zerfällt in L in Linearfaktoren.

Definition 3.5.6. Eine algebraische Körpererweiterung L/K heisst **normal**, wenn sie die äquivalenten Bedingungen des Satzes erfüllt.

Beweis. Nimm an, dass (N1) erfüllt ist. Sei f ein irreduzibles Polynom in $K[x]$, das in L eine Nullstelle α hat. Sei β eine Nullstelle von f in $\bar{K}$. Indem wir α auf β werfen, erhalten wir einen Homomorphismus $K(\alpha) \rightarrow \bar{K}$ über K . Dieser lässt sich nach L fortsetzen, es folgt also, dass β in dem gemeinsamen Bild $\tilde{L}$ aller Homomorphismen von L nach $\bar{K}$ liegt. Da f über $\bar{K}$ in Linearfaktoren zerfällt und alle Nullstellen in $\tilde{L}$ liegen und da ferner $L \cong \tilde{L}$ ist, zerfällt f auch in $L[x]$ in Linearfaktoren. Damit folgt (N3).

Aus (N3) folgt (N2) indem man die Familie aller Minimalpolynome von Elementen in L nimmt.

(N2) schliesslich liefert (N1) mit demselben Beweis wie Satz 3.5.2. $\square$

Proposition 3.5.7. *Zu jeder algebraischen Erweiterung L/K existiert bis auf L -Isomorphie genau eine Körpererweiterung N/L so dass N/K normal ist und dass N minimal ist mit dieser Eigenschaft, d.h., ist Σ/L eine Körpererweiterung so dass Σ/K normal ist, dann existiert eine Einbettung $N \hookrightarrow \Sigma$ über L .*

Definition 3.5.8. Die Körpererweiterung N/K aus der Proposition wird die **Normale Hülle** von L/K genannt.

Beweis. Man nimmt als N den Zerfällungskörper aller irreduziblen Polynome in $K[x]$, die in L eine Nullstelle haben. Die Eigenschaften sind dann klar. $\square$

Beispiel 3.5.9. Hier ein Beispiel einer nichtnormalen Erweiterung. Sei $K = \mathbb{Q}$ und $f(x) = x^3 - 2 \in K[x]$. Die Körpererweiterung $L = K_f/K$ ist dann nicht normal, denn in $\mathbb{C}$ gibt es drei dritte Nullstellen von $f(x)$, nämlich $\sqrt[3]{2}, \varepsilon \sqrt[3]{2}, \varepsilon^2 \sqrt[3]{2}$, wobei $\varepsilon = e^{2\pi i/3}$ ist. Indem man die Nullstelle $\alpha \in K_f$ von f auf jede dieser Zahlen wirft, erhält man drei verschiedene Einbettungen von K_f nach $\mathbb{C}$ über K . Allerdings haben die nicht alle dasselbe Bild, denn das Bild der Einbettung, die α auf $\sqrt[3]{2}$ wirft, liegt ganz in $\mathbb{R}$, die beiden anderen nicht.

Definition 3.5.10. Eine Körpererweiterung L/K heisst **multiquadratische Erweiterung**, falls es eine Kette von Zwischenkörpern

$$K = L_0 \subset L_1 \subset \cdots \subset L_n = L$$

gibt mit $[L_j : L_{j-1}] = 2$ fuer jedes $j = 1, \dots, n$.

Lemma 3.5.11. *Ist L/K multiquadratisch und ist $N/L/K$ die normale Huelle, dann sind auch N/K und N/L multiquadratisch. Insbesondere ist der Grad $[N : K]$ eine Potenz von 2.*

Beweis. Seien $\sigma_1, \dots, \sigma_k$ die verschiedenen K -Einbettungen von L in einen algebraischen Abschluss $\bar{K}$ von K . Dann ist der von den Bildern $\sigma_1(L), \dots, \sigma_k(L)$ erzeugte Unterkörper von $\bar{K}$ isomorph zu N . Da L aus K durch sukzessives

Adjungieren von Quadratwurzeln entsteht, gilt dasselbe fuer jedes $\sigma_j(L)$ und damit auch fuer N . □

3.6 Separable Körpererweiterungen

Definition 3.6.1. Ist $\alpha \in L$ eine Nullstelle eines Polynoms $f \in L[x]$, dann zeigt Polynomdivision, dass $x - \alpha$ das Polynom $f(x)$ teilt, dass also $f(x) = (x - \alpha)g(x)$ für ein Polynom $g(x)$ gilt. Gilt sogar $(x - \alpha)^2 \mid f(x)$, dann sagen wir: α ist eine **mehrfache Nullstelle** von f .

Definition 3.6.2. Ein Polynom $f(x) \in K[x]$ heisst **separables Polynom**, falls f keine mehrfachen Nullstellen in $\overline{K}$ hat.

Ein Element $\alpha \in L$ in einer Körpererweiterung L/K heisst **separables Element**, falls sein Minimalpolynom separabel ist. Eine algebraische Körpererweiterung L/K heisst **separabel**, falls jedes Element separabel ist.

Lemma 3.6.3. Sei K ein Körper und sei $f(x) = a_0 + a_1x + \cdots + a_nx^n$ ein Polynom. Wir definieren die **formale Ableitung** von f als

$$f'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1}.$$

Die Abbildung $f \mapsto f'$ ist linear und erfüllt die **Leibniz-Regel**:

$$(fg)' = f'g + g'f.$$

Ein Element $\alpha \in K$ ist genau dann eine mehrfache Nullstelle des nichtkonstanten Polynoms f , wenn $f(\alpha) = 0$ und $f'(\alpha) = 0$ gilt.

Beweis. Sei $f(x) = \sum_j a_j x^j$ und $g(x) = \sum_i b_i x^i$, dann ist

$$\begin{aligned}
 (fg)'(x) &= \left(\sum_{i,j} a_j b_i x^{i+j} \right)' = \sum_{i,j} a_j b_i (i+j) x^{i+j-1} \\
 &= \sum_{j,i} (a_j b_i j x^{i+j-1} + a_j b_i i x^{i+j-1}) \\
 &= \left(\sum_j a_j j x^{j-1} \right) \left(\sum_i b_i x^i \right) + \left(\sum_j a_j x^j \right) \left(\sum_i b_i i x^{i-1} \right) \\
 &= f'(x)g(x) + f(x)g'(x).
 \end{aligned}$$

Ist α mehrfache Nullstelle, dann folgt $f(x) = (x - \alpha)^2 g(x)$. Damit ist

$$f'(x) = 2(x - \alpha)g(x) + (x - \alpha)^2 g'(x),$$

so dass α auch Nullstelle von f' ist. Ist umgekehrt, α eine einfache Nullstelle, dann ist $f(x) = (x - \alpha)g(x)$ mit $g(\alpha) \neq 0$. Es gilt

$$f'(x) = g(x) + (x - \alpha)g'(x),$$

so dass $f'(\alpha) \neq 0$ folgt. □

Korollar 3.6.4. *Es ist sogar schärfer so, dass die Ableitung eines irreduziblen Polynoms, das eine mehrfache Nullstelle hat, komplett verschwindet: Ist $f \in K[x]$ irreduzibel und hat f in $\bar{K}$ eine mehrfache Nullstelle in einer Erweiterung L/K , dann ist $f' = 0$.*

Beweis. Sei $\alpha \in L$ eine mehrfache Nullstelle. Wir können f als normiert voraussetzen, dann ist f das MiPo von α . Wegen $f'(\alpha) = 0$ folgt schon, dass $f'(x)$ in $K[x]$ ein Vielfaches von $f(x)$ sein muss. Da der Grad von f' aber kleiner ist als der von f , folgt $f' = 0$. □

Beispiel 3.6.5. Sei $K = \mathbb{F}_2(T)$ der Funktionenkörper über dem Körper $\mathbb{F}_2$ mit zwei Elementen, also $\mathbb{F}_2(T)$ ist der Quotientenkörper des Integritätsrings $\mathbb{F}_2[T]$. Sei $f(x) \in K[x]$ das Polynom $f(x) = x^2 - T$. Dieses ist nach Eisenstein irreduzibel, also $L = K(\sqrt{T}) = K[x]/x^2 - T$ eine Körpererweiterung vom Grad 2. Wie in Satz 3.2.1 hat das irreduzible

Polynom $f(x) = x^2 - T$ nun in L die Nullstelle $\alpha = x + f(x)K[x]$ und es gilt mit der neuen Unbestimmten y :

$$(y - \alpha)^2 = y^2 - \underbrace{2\alpha y}_{=0} + \alpha^2 = y^2 - \alpha^2 = y^2 - T = f(y),$$

damit hat das Polynom $f(y)$ in L eine doppelte Nullstelle, die Körpererweiterung L/K ist also nicht separabel!

Satz 3.6.6. *Ist $\text{Char}(K) = 0$, dann ist jede algebraische Erweiterung L/K separabel.*

Wir werden später lernen, dass auch Erweiterungen zwischen endlichen Körpern separabel sind.

Beweis. Sei L/K eine nichtseparable algebraische Körpererweiterung. Wir zeigen, dass die Charakteristik nicht Null sein kann. Sei $\alpha \in L$ mit Minimalpolynom $m(x) \in K[x]$ und so dass α eine mehrfache Nullstelle von $m(x)$ ist, also $m'(\alpha) = 0$. Da der Grad von m' echt kleiner ist als der von m und m das Minimalpolynom war, muss das Polynom m' gleich Null sein. Ist der Grad von $m(x)$ gleich $n \geq 2$, dann ist der Leitterm von $m'(x)$ gleich nx^{n-1} , also muss $n \cdot 1 = 0$ in K gelten, damit ist die Charakteristik positiv. □

3.7 Separabilitätsgrad

Definition 3.7.1. Sei L/K eine endliche Erweiterung und sei $\sigma : K \hookrightarrow \Omega$ eine Einbettung in einen algebraisch abgeschlossenen Körper Ω . Sei S_σ die Menge aller Fortsetzungen von σ zu einer Einbettung $\sigma^* : L \hookrightarrow \Omega$.

Lemma 3.7.2. S_σ ist endlich und die Kardinalität $|S_\sigma|$ hängt nicht von Ω oder σ ab. Wir nennen diese Kardinalität den **Separabilitätsgrad** von L/K und schreiben

$$[L : K]_s = |S_\sigma|.$$

Beweis. Wir zeigen zunäcst, dass S_σ endlich ist. Ist $a \in L$ und f das Minimalpolynom, dann muss jede Fortsetzung σ^* von σ das Element a auf eine Nullstelle von f werfen. Derer gibt es nur endlich viele, also nur endlich viele Wahlmoeglichkeiten fuer $\sigma^*(a)$. Ist $v_1, \dots, v_n$ eine Basis von L als K -Vektorraum, so gibt es auch nur endlich viele Moeglichkeiten fuer $\sigma^*(v_1), \dots, \sigma^*(v_n)$ und daher ist S_σ endlich.

Nun zur Unabhaengigkeit der Maechtigkeit. Da L/K algebraisch ist, ist für jede Fortsetzung σ^* der Körper $\sigma^*(L)$ algebraisch über $\sigma(K)$. Wir können also Ω durch die Menge aller über $\sigma(K)$ algebraischen Elemente ersetzen, dies ist ein Unterkörper von Ω und ein algebraischer Abschluss von K . Ist $\tau : K \hookrightarrow \Sigma$ eine andere Einbettung in einen algebraisch abgeschlossenen Körper, kann man auch Σ durch einen algebraischen Abschluss von K ersetzen. Es gibt dann einen Isomorphismus $\Omega \rightarrow \Sigma$ so dass das Diagramm

$$\begin{array}{ccc} K & \xrightarrow{\sigma} & \Omega \\ & \searrow \tau & \downarrow \psi \\ & & \Sigma \end{array}$$

kommutiert. Ist dann $\sigma^* : L \rightarrow \Omega$ eine Fortsetzung von σ , so ist $\psi \circ \sigma^*$ eine von τ und man erhält eine Bijektion $S_\sigma \xrightarrow{\cong} S_\tau$. $\square$

Beispiele 3.7.3. (a) Sei $K = \mathbb{Q}$ und $L = \mathbb{Q}(\sqrt{2})$. In $\Omega = \mathbb{C}$ gibt es genau zwei Zahlen α , die die Gleichung $\alpha^2 - 2 = 0$ erfuellen, die positive $\sqrt{2} > 0$ und die negative $-\sqrt{2}$. Es gibt dann zwei Fortsetzungen der Einbettung $\mathbb{Q} \hookrightarrow \mathbb{C}$ nach L , gegeben durch $\sigma_1(T) = \sqrt{2}$ und $\sigma_2(T) = -\sqrt{2}$. Damit ist der Separabilitätsgrad $[L : K]_s$ gleich 2.

(b) Seien $K = \mathbb{Q}$ und $L = \mathbb{Q}(\sqrt[3]{2})$. In $\Omega = \mathbb{C}$ gibt es drei verschiedene dritte Wurzeln aus 2, nämlich die eindeutig bestimmte reelle Zahl $\alpha \in \mathbb{R}$ mit $\alpha^3 = 2$, sowie $\alpha e^{2\pi i/3}$ und $\alpha e^{4\pi i/3}$. Indem man T auf jeweils eine der drei wirft, erhält man drei verschiedene Einbettungen von L über $\mathbb{Q}$ nach $\mathbb{C}$. Es folgt also, dass der Separabilitätsgrad von L über K gleich 3 ist.

(c) Sei $L/K = \mathbb{F}_2(\sqrt{T})/\mathbb{F}_2(T)$, mit einer Variablen T und sei $\sigma : K \rightarrow \Omega$ in einen algebraisch abgeschlossenen Körper Ω . Dann hat Ω ebenfalls Charakteristik 2 und daher hat das Polynom $x^2 - T$ nur eine Nullstelle. Damit wirft jede Erweiterung $\sigma^* : L \rightarrow \Omega$ von σ das Element $\sqrt{T}$ auf diese eine Nullstelle und ist damit eindeutig bestimmt. Es gilt also $[L : K]_s = 1$.

Satz 3.7.4. *Der Separabilitätsgrad ist multiplikativ in Körpertürmen, sind also $L/E/K$ endliche Körpererweiterungen, so gilt*

$$[L : K]_s = [L : E]_s [E : K]_s.$$

Ferner gilt $[L : K]_s \leq [L : K]$.

Beweis. Sei $\sigma : K \rightarrow \Omega$. Für jede Fortsetzung $\tau : E \rightarrow \Omega$ ist jede Fortsetzung von τ nach L eine Fortsetzung von σ nach L . Also erhalten wir eine Bijektion $S_\sigma(L) = \bigsqcup_{\tau \in S_\sigma(E)} S_\tau(L)$. Ferner haben alle S_τ dieselbe Kardinalität und damit folgt die erste Behauptung.

Für die zweite Behauptung schreibe $L = K(\alpha_1, \dots, \alpha_n)$ und beachte, dass man nach der ersten Behauptung die zweite nur für die Zwischenerweiterungen $K(\alpha_1, \dots, \alpha_{j+1})/K(\alpha_1, \dots, \alpha_j)$ zeigen muss. Sei also $L = K(\alpha)$. Dann ist $n = [L : K]$ der Grad des Minimalpolynoms $m(x)$ von α . In einem algebraisch abgeschlossenen Körper Ω , in den K einbettet, hat $m(x)$ höchstens n Nullstellen $\alpha_1, \dots, \alpha_n$. Jede Fortsetzung von σ nach L wirft α auf eine der α_j und die Wahl eines α_j legt die Fortsetzung fest. Daher gibt es höchstens n verschiedene Fortsetzungen. □

Satz 3.7.5. *Eine endliche Körpererweiterung L/K ist genau dann separabel, wenn $[L : K]_s = [L : K]$.*

Beweis. Sei L/K separabel. Da beide Grade multiplikativ in Türmen sind, können wir annehmen, dass $L = K(\alpha)$ für ein α . Sei $\tau : K \rightarrow \Omega$ ein Homomorphismus in einen algebraisch abgeschlossenen Körper Ω . Sei $m(x)$ das Minimalpolynom von α und n dessen Grad. Dann ist $[L : K] = n$. Ist ω eine Nullstelle von $m(x)$ in Ω ,

dann liefert die Abbildung $\alpha \mapsto \omega$ einen Homomorphismus $L \rightarrow \Omega$ über K . Umgekehrt wirft jeder Homomorphismus $L \rightarrow \Omega$ über K die Nullstelle α auf eine Nullstelle von $m(x)$. Das heisst, es gibt genau so viele Nullstellen von $m(x)$ in Ω wie es Homomorphismen $L \rightarrow \Omega$ über K gibt. Sei $k = [L : K]_s$ diese Anzahl. Mit Vielfachheit gezählt, hat $m(x)$ in Ω genau n Nullstellen. Es folgt also $k = n$, falls wir zeigen können, dass $m(x)$ keine mehrfache Nullstelle in Ω hat. Sei hierzu $\omega \in \Omega$ eine Nullstelle, dann ist $\alpha \mapsto \omega$ ein Isomorphismus $L = K(\alpha) \xrightarrow{\cong} K(\omega)$. Da α keine mehrfache Nullstelle ist, ist demzufolge ω auch keine und es folgt $[L : K] = n = k = [L : K]_s$. Diesen Beweis kann man auch rückwärts lesen und feststellen, dass aus $[L : K] = [L : K]_s$ folgt, dass in Ω keine mehrfachen Nullstellen liegen, also auch nicht in L . $\square$

Korollar 3.7.6. (a) Sei L/K eine Körpererweiterung und sei $\alpha \in L$ separabel. Dann ist $K(\alpha)/K$ eine separable Körpererweiterung.

(b) Ist Z der Zerfällungskörper einer Familie $(f_i)_{i \in I}$ von separablen Polynomen, dann ist Z/K separabel.

Beweis. (a) Das Minimalpolynom $m(x)$ von α habe die verschiedenen Nullstellen $\alpha_1, \dots, \alpha_n \in \bar{K}$. Dann gilt $n = \deg(m) = [K(\alpha) : K]$. Die Vorschrift $\sigma_j(\alpha) = \alpha_j$ liefert eine eindeutig bestimmte Einbettung $K(\alpha) \rightarrow \bar{K}$ und daher gibt es n verschiedene solcher Einbettungen, also gilt $[K(\alpha) : K]_s = n = [K(\alpha) : K]$.

(b) Sei $\alpha \in Z$. Da Z durch Adjunktion von Nullstellen der f_i entsteht, gibt es endlich viele solcher Nullstellen $\alpha_1, \dots, \alpha_n$, so dass $\alpha \in K(\alpha_1, \dots, \alpha_n)$. Nach Teil (a) ist $K(\alpha_1, \dots, \alpha_{j+1})/K(\alpha_1, \dots, \alpha_j)$ separabel, also ist $K(\alpha_1, \dots, \alpha_n)/K$ separabel und α separabel. $\square$

Satz 3.7.7. Für endliche Erweiterungen $L/F/K$ gilt

$$L/K \text{ separabel} \Leftrightarrow \left\{ \begin{array}{l} L/F \text{ separabel und} \\ F/K \text{ separabel.} \end{array} \right\}$$

Beweis. Wir haben

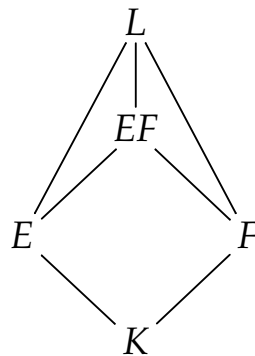
$$[L : K] = [L : F][F : K]$$

$$\vee \quad \vee \quad \vee$$

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

Gilt nun auf der einen Seite Gleichheit, dann gilt sie auch auf der anderen. $\square$

Definition 3.7.8. Sei L/K eine Körpererweiterung und seien E, F Zwischenkörper. Der kleinste Körper, der E und F enthält, heisst das **Kompositum** von E und F .



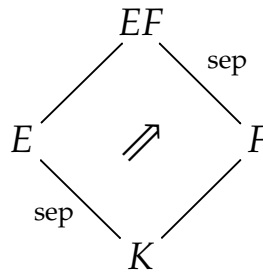
Beispiele 3.7.9. (a) Ist $E = K(\alpha_1, \dots, \alpha_n)$ und $F = K(\beta_1, \dots, \beta_m)$, dann folgt

$$EF = K(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m).$$

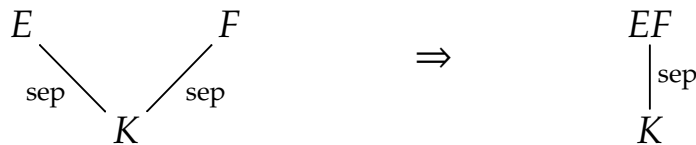
(b) Der Körper $\mathbb{Q}(\sqrt{2}, i)$ ist das Kompositum aus $\mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(i)$.

Satz 3.7.10. Sei L/K eine endliche Körpererweiterung und E, F Zwischenkörper.

(a) Ist E/K separabel, dann ist EF/F separabel.



(b) Sind E/K und F/K separabel, dann ist EF/K separabel.



Beweis. (a) Zunaechst nehmen wir an, dass $E = K(\beta)$ fuer ein Element β . Es folgt, dass $EF = F(\beta)$. Bette EF in einen algebraisch abgeschlossenen Koerper Ω ein. Dort hat das Minimalpolynom $m_K(x) \in K[x]$ von β keine mehrfache Nullstelle, also hat auch das Minimalpolynom M_F von β in $F[x]$, welches m_K teilt, keine mehrfache Nullstelle in EF . Allgemein ist $E = K(\alpha_1, \dots, \alpha_n)$. Wir erhalten die Aussage fuer jede Erweiterung $K(\alpha_1, \dots, \alpha_{j+1})/K(\alpha_1, \dots, \alpha_j)$ und koennen dann Satz 3.7.5 benutzen, um die Aussage allgemein zi folgern.

(b) Mit Teil (a) folgt, daass EF/F und EF/E separabel sind und mit Satz 3.7.7, dass EF/K separabel ist. $\square$

3.8 Primitive Elemente

Lemma 3.8.1. Sei G eine endliche abelsche Gruppe und fuer $n \in \mathbb{N}$ sei die n -Torsion von G definiert durch

$$G[n] := \{x \in G : x^n = 1\}.$$

Gilt $|G[n]| \leq n$ für jeden Teiler n der Gruppenordnung $|G|$, dann ist G zyklisch.

Beweis. Sei $N = |G|$ die Gruppenordnung. Wir machen eine Induktion nach der Anzahl der Primteiler von N . Für $N = 1$ ist nicht zu zeigen. Ist $N = p^k$ für eine Primzahl p und $k \in \mathbb{N}$, dann ist die Ordnung jedes Elementes von der Form p^l für ein $l \leq k$. Es muss nun ein Element der Ordnung p^k geben, denn sonst wäre $p^k = |G| = |G[p^{k-1}]| \leq p^{k-1}!$ Damit ist G zyklisch.

Ist N keine Primzahlpotenz, dann ist $N = mn$ mit teilerfremden Faktoren $m, n > 1$, die beide weniger Primfaktoren haben. Es ist klar, dass $G[m] \cap G[n] = \{1\}$, daher ist die Abbildung

$$\begin{aligned} G[m] \times G[n] &\rightarrow G \\ (x, y) &\mapsto xy \end{aligned}$$

ein injektiver Gruppenhomomorphismus. Da die Ordnungen gleich sind, ist es ein Isomorphismus. Nach Induktionsvoraussetzung sind die Untergruppen $G[m]$ und $G[n]$ zyklisch, es gibt also Elemente $a, b \in G$ der Ordnungen m und n , so dass nach Lemma 1.2.6 das Element ab die Ordnung $mn = |G|$ hat, G also zyklisch ist. □

Satz 3.8.2. Ist K ein Körper und ist $G \subset K^\times$ eine endliche Untergruppe. Dann ist G zyklisch.

Beweis. Sei $n \in \mathbb{N}$ und sei $G[n] = \{x \in G : x^n = 1\}$ die n -Torsion. Dann ist jedes $x \in G[n]$ Nullstelle des Polynoms $x^n - 1$, welches höchstens n Nullstellen haben kann, so dass

$$|G[n]| \leq n.$$

Nach Lemma 3.8.1 ist G zyklisch. □

Korollar 3.8.3. *Ist K ein Körper und $n \in \mathbb{N}$, dann gibt es maximal eine Untergruppe von $K^\times$ der Ordnung n .*

Beweis. Sei eine solche Untergruppe, dann liegt G in der Menge

$\mu_n = \{\alpha \in K : \alpha^n - 1 = 0\}$ also der Menge der Nullstellen des Polynoms $p(x) = x^n - 1$. Diese hat Grad n , also $\leq n$ Nullstellen. Ist $|G| = n$, dann folgt also $G = \mu_n$. □

Beispiele 3.8.4. (a) Ist K ein endlicher Körper, dann ist die ganze Einheitengruppe $K^\times$ zyklisch.

(b) Zu jedem $n \in \mathbb{N}$ ist die endliche Untergruppe der Kardinalität n erzeugt von $\langle e^{2\pi i/n} \rangle$.

Satz 3.8.5 (Satz vom primitiven Element). *Sei L/K endlich. Dann sind äquivalent*

(a) *Es gibt ein $\alpha \in L$ so dass $L = K(\alpha)$.*

(b) *Es gibt nur endlich viele Zwischenkörper $L \supset F \supset K$.*

*Ein solches α wird ein **primitives Element** der Erweiterung L/K genannt.*

Beweis. Ist K endlich, so ist auch L endlich und die multiplikative Gruppe von L ist nach Satz 3.8.2 zyklisch. Ein Erzeuger dieser Gruppe wird dann auch L als Körper erzeugen, also sind (a) und (b) beide erfüllt.

Sei nun also K unendlich und damit auch L .

(b) $\Rightarrow$ (a): Es gebe nur endlich viele Zwischenkörper. Seien $\alpha, \beta \in L$. Es gibt dann nur endlich viele Körper der Form $K(\alpha + c\beta)$ mit $c \in K$. Also gibt es $c_1 \neq c_2$ in K mit $K(\alpha + c_1\beta) = K(\alpha + c_2\beta)$. In diesem Körper liegt dann auch die Differenz $(c_1 - c_2)\beta$, also auch β , also auch α . Also kann $K(\alpha, \beta)$ von einem Element erzeugt werden. Man schreibt $L = K(\alpha_1, \dots, \alpha_n)$ und zeigt induktiv, dass L von einem Element erzeugt wird.

(a) $\Rightarrow$ (b): Umgekehrt sei $L = K(\alpha)$ und sei $m(x) \in K[x]$ das Minimalpolynom. Sei F ein Zwischenkörper, dann teilt das Minimalpolynom $m_F(x) \in F[x]$ von α über F das Minimalpolynom $m(x)$, welches nur endlich viele Teiler hat, also geht die Abbildung $F \mapsto m_F$ in eine endliche Menge. Sei F_0 der Unterkörper von F , der von den Koeffizienten von m_F erzeugt wird. Dann hat α über F_0 das Minimalpolynom m_F , also ist der Körpergrad $[L : F] = [L : F_0]$, also ist $F = F_0$ und damit gibt es nur endlich viele Zwischenkörper. $\square$

Korollar 3.8.6. *Ist L/K endlich und separabel, dann sind die äquivalenten Bedingungen des Satzes erfüllt, das heisst also*

Jede endliche separable Erweiterung hat ein primitives Element.

Beweis. Sei L/K separabel, $L \neq K$. Induktiv reicht es zu zeigen, dass $L = K(\alpha, \beta)$ ein primitives Element hat, falls $K(\alpha) \neq K$ und $K(\beta) \neq K$ separabel über K sind. Dann gibt es ≥ 2 Einbettungen von L in $\bar{K}$, da dies für $K(\alpha)$ gilt. Seien $\sigma_1, \dots, \sigma_n$ die verschiedenen Einbettungen von L in $\bar{K}$ über K . Das heisst $n = [L : K]_s = [L : K]$. Sei

$$P(x) = \prod_{i \neq j} (\sigma_i(\alpha + \beta x) - \sigma_j(\alpha + \beta x)).$$

Dann ist $P(x)$ nicht das Nullpolynom, also existiert ein $c \in K$ mit $P(c) \neq 0$. Die Elemente $\sigma_i(\alpha + \beta c)$ sind dann alle verschieden, also $[K(\alpha + \beta c) : K]_s = n$ und daher

$$[L : K] \geq [K(\alpha + \beta c) : K] \geq [K(\alpha + \beta c) : K]_s = n = [L : K]$$

also $L = K(\alpha + \beta c)$. $\square$

Beispiel 3.8.7. Die Körpererweiterung $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}$ hat $a = \sqrt{2} + i$ als primitives Element.

Beweis. Die Erweiterung ist Biquadratisch mit Zwischenkörper $\mathbb{Q}(\sqrt{2})$. Wäre a nicht primitiv, würde es also einen Zwischenkörper vom Grad 2 über $\mathbb{Q}$ erzeugen, es müsste also eine quadratische Gleichung der Form

$$a^2 + ra + s = 0, \quad r, s \in \mathbb{Q},$$

oder $a^2 + ra \in \mathbb{Q}$ erfüllen. Es gilt $a^2 = 2 + 2\sqrt{2}i - 1 = 1 + 2\sqrt{2}i$. Damit ist für $r \in \mathbb{Q}$

$$a^2 + ra = 1 + 2\sqrt{2}i + r\sqrt{2} + ri = (1 + \sqrt{2})r + (2\sqrt{2} + r)i$$

Damit diese Zahl in $\mathbb{Q}$ liegt, muss $1 + \sqrt{2} + r = 0$ sein, was nicht geht, da $\sqrt{2}$ nicht rational ist. $\square$

3.9 Galois-Erweiterungen

Sei L/K eine Körpererweiterung. Ein **Galois-Homomorphismus** von L über K ist ein Isomorphismus von Körpererweiterungen $L/K \rightarrow L/K$, also ein Isomorphismus $\sigma : L \rightarrow L$, der auf K die Identität ist.

Die **Galois-Gruppe** $\text{Gal}(L/K)$ der Erweiterung L/K ist die Gruppe aller Galois-Homomorphismen von L über K .

Lemma 3.9.1. (a) *Jeder Galois-Homomorphismus $\sigma \in \text{Gal}(L/K)$ ist insbesondere eine K -lineare Abbildung.*

(b) *Ist L/K endlich, dann ist $\text{Gal}(L/K)$ endlich und*

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

Beweis. (a) σ ist ein additiver Gruppenhomomorphismus. Für $a \in L$ und $\lambda \in K$ gilt

$$\sigma(\lambda a) = \sigma(\lambda)\sigma(a) = \lambda\sigma(a),$$

da σ auf K die Identität ist.

(b) Jeder K -Homomorphismus $\tau : L \rightarrow L$ kann zu einem K -Homomorphismus $L \rightarrow \bar{L} = \bar{K}$ fortgesetzt werden. Davon gibt es $[L : K]_s$ viele. $\square$

Beispiele 3.9.2. • Die komplexe Konjugation $z \mapsto \bar{z}$ ist ein Element der Galois-Gruppe $\text{Gal}(\mathbb{C}/\mathbb{R})$.

- Die Abbildung $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ ist ein Galois-Homomorphismus von $\mathbb{Q}(\sqrt{2}) = \mathbb{Q} \oplus \mathbb{Q}\sqrt{2}$ über $\mathbb{Q}$.
- Jeder endliche Körper K der Charakteristik $p > 0$ hat einen besonderen Automorphismus, den Frobenius-Automorphismus, der im nächsten Abschnitt vorgestellt wird.

Lemma 3.9.3. Sei L/K eine Körpererweiterung und sei $\Gamma \subset \text{Gal}(L/K)$ eine Untergruppe. Dann ist die Menge der Fixpunkte

$$L^\Gamma = \{x \in L : \gamma(x) = x \ \forall \gamma \in \Gamma\}.$$

ein Zwischenkörper $L \supset L^\Gamma \supset K$.

Beweis. Zunächst sind $0, 1 \in L^\Gamma$, da jeder Ringhomomorphismus diese bewahrt. Ferner gilt $x, y \in L^\Gamma \Rightarrow x + y \in L^\Gamma, xy \in L^\Gamma$, denn für jedes $\gamma \in \Gamma$ gilt

$$\gamma(x + y) = \gamma(x) + \gamma(y) = x + y, \quad \text{und} \quad \gamma(xy) = \gamma(x)\gamma(y) = xy.$$

Ebenso gilt $x \in L^\Gamma \Rightarrow -x \in L^\Gamma$ und für $x \neq 0$ ist auch $x^{-1} \in L^\Gamma$, also ist L^Γ ein Unterkörper von L . Da jedes γ auf K die Identität ist, ist $K \subset L^\Gamma$. $\square$

Definition 3.9.4. Eine Körpererweiterung L/K heisst **Galois-Erweiterung**, falls der Fixkörper von $\Gamma = \text{Gal}(L/K)$ gleich K ist, falls also $L^{\text{Gal}(L/K)} = K$ gilt.

Beispiele 3.9.5. (a) $\mathbb{C}/\mathbb{R}$ ist eine Galois-Erweiterung, da die komplexe Konjugation $\mathbb{R}$ als Fixkörper hat.

(b) $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ ist galoissch, da der Fixkörper von $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ gleich $\mathbb{Q}$ ist.

(c) Ist $\text{Char}(K) \neq 2$, dann ist jede quadratische Körpererweiterung galoissch.

Beweis. Nach der Mitternachtsformel entsteht L aus K durch Wurzelziehen, es gibt also ein $\alpha \in K$, so dass $L = K(\sqrt{\alpha})$. Da $\text{Char}(K) \neq 2$, ist $\tau : a + b\sqrt{\alpha} \mapsto a - b\sqrt{\alpha}$ ein nichttrivialer Körperautomorphismus mit Fixkörper K . $\square$

(d) $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ ist eine Körpererweiterung vom Grad 3, die nicht galoissch ist.

Beweis. Nach Eisenstein ist $x^3 - 2$ irreduzibel, also ist $L = \mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q}[x]/(x^3 - 2)\mathbb{Q}[x]$ eine Körpererweiterung von $\mathbb{Q}$ vom Grad 3.

Sei $\tau : L \rightarrow L$ ein Galois-Homomorphismus. Das Element $\alpha = \sqrt[3]{2}$ ist eine Nullstelle des Polynoms $f(x) = x^3 - 2$. Ist $\tau(\alpha) = \alpha$, so ist $\tau = \text{Id}$, da α die Körpererweiterung erzeugt. Wir zeigen, dass dies immer der Fall ist. Nun ist $\alpha = \sqrt[3]{2}$ die einzige reelle Zahl, die die Gleichung $\alpha^3 = 2$ erfüllt und damit ist α auch das einzige Element von L mit dieser Eigenschaft. Also ist $\tau(\alpha) = \alpha$ und damit $\tau = \text{Id}$, also ist die Galois-Gruppe trivial und folglich $L^{\text{Gal}(L/K)} = L$. $\square$

Lemma 3.9.6. Sei L/K eine algebraische separable Erweiterung. Sei $n \in \mathbb{N}$ und nimm an, dass jedes Element von L Nullstelle eines Polynoms in $K[x]$ vom Grad $\leq n$ ist. Dann ist L/K endlich vom Grad $\leq n$.

Beweis. Sei $\alpha \in L$ so dass der Grad $[K(\alpha) : K]$ maximal ist, sagen wir $m \leq n$. Wir behaupten, dass $L = K(\alpha)$. Ist dies nicht der Fall, so gibt es ein $\beta \in L$ mit $\beta \notin K(\alpha)$. Nach dem Satz vom primitiven Element gibt es ein $\gamma \in L$ so dass $K(\alpha, \beta) = K(\gamma)$. Wegen $K(\gamma) = K(\alpha, \beta) \supsetneq K(\alpha)$ folgt, dass der Grad $[K(\gamma) : K] > m$ sein muss, ein Widerspruch! $\square$

Satz 3.9.7 (Artin). Sei L ein Körper und sei Γ eine endliche Untergruppe von $\text{Aut}(L)$ der Ordnung n . Sei K der Fixkörper

$$K = L^\Gamma = \{x \in L : \gamma(x) = x \ \forall \gamma \in \Gamma\}.$$

Dann ist L/K eine endliche Erweiterung vom Grad

$$[L : K] = n = |\Gamma|.$$

Die Erweiterung L/K ist normal und separabel.

Beweis. Sei $\alpha \in L$ und sei $\{\gamma_1, \dots, \gamma_r\}$ eine maximale Teilmenge von Γ so dass die Elemente $\gamma_1\alpha, \dots, \gamma_r\alpha$ paarweise verschieden sind. Dann ist α eine Nullstelle des Polynoms

$$f(x) = \prod_{j=1}^r (x - \gamma_j\alpha).$$

Ist $\tau \in \Gamma$, dann unterscheidet sich $(\tau\gamma_1\alpha, \dots, \tau\gamma_r\alpha)$ von $(\gamma_1\alpha, \dots, \gamma_r\alpha)$ nur in der Reihenfolge. Daher gilt $f^\tau = f$, also $f \in K[x]$. Das bedeutet, dass jedes $\alpha \in L$ Nullstelle eines separablen Polynoms in $K[x]$ vom Grad $r \leq n$ ist, welches über L in Linearfaktoren zerfällt. Daher ist L/K normal und separabel. Nach Lemma 3.9.6 folgt ausserdem, dass $[L : K] \leq n$. Andererseits setzt jedes $\gamma : L \rightarrow L$ in Γ zu einer K -Einbettung $L \rightarrow \bar{L} = \bar{K}$ fort, so dass $n \leq [L : K]_s \leq [L : K]$ und damit folgt Gleichheit. $\square$

Satz 3.9.8 (Hauptsatz der Galois-Theorie I). *Fuer eine endliche Erweiterung L/K sind aequivalent:*

- (a) L/K ist galoisch.
- (b) L/K ist normal und separabel.

Beweis. (a) $\Rightarrow$ (b): Nach Lemma 3.9.1 ist $\Gamma = \text{Gal}(L/K)$ endlich und damit folgt (a) $\Rightarrow$ (b) aus dem Satz von Artin 3.9.7.

(b) $\Rightarrow$ (a): Sei umgekehrt L/K normal und separabel und sei $\alpha \in L^\Gamma$. Sei $\sigma : K(\alpha) \rightarrow \bar{L}$ eine Einbettung über K in einen algebraischen Abschluss von L . Wir dehnen σ zu einer Einbettung $L \hookrightarrow \bar{L}$ aus. Dann ist σ ein Automorphismus von L über K , also ein Element von Γ . Deshalb lässt σ das Element α fest, also folgt $|\text{Hom}_K(K(\alpha), \bar{L})| = 1$. Da α separabel über K ist, folgt $1 = [K(\alpha) : K]_s = [K(\alpha) : K]$, also $\alpha \in K$ und (b) $\Rightarrow$ (a) ist bewiesen. $\square$

Korollar 3.9.9. *Fuer eine endliche Erweiterung L/K sind aequivalent:*

- (a) L/K ist galoisch.
- (b) L ist der Zerfaellungskoeper eines separablen Polynoms.

Beweis. (a) $\Rightarrow$ (b): Waehlt man im Beweis von Satz 3.9.7 (Artin) α als primitives Element, so folgt, dass L/K Zerfaellungskoeper des im Beweis angegebenen Polynoms ist.

(b) $\Rightarrow$ (a): Ist L Zerfaellungskoeper eines separablen Polynoms, dann ist L/K normal und separabel, also nach dem Hauptsatz 3.9.8 galoisch. $\square$

Satz 3.9.10 (Hauptsatz der Galois-Theorie II). *Sei L/K eine endliche Körpererweiterung und sei $\Gamma = \text{Gal}(L/K)$ ihre Galois-Gruppe.*

- (a) *Sei L/K galoissch. Ist $L \supset F \supset K$ ein Zwischenkörper, dann ist L/F galoissch. Die Erweiterung F/K ist genau dann galoissch, wenn die Galois-Gruppe $\Sigma = \text{Gal}(L/F)$ ein Normalteiler in Γ ist. In diesem Fall gilt*

$$\text{Gal}(F/K) \cong \Gamma/\Sigma.$$

- (b) *Ist L/K galoissch, so ist die Abbildung $F \mapsto \text{Gal}(L/F)$ eine Bijektion*

$$\phi : \{\text{Zwischenkörper } L \supset F \supset K\} \xrightarrow{\cong} \{\text{Untergruppen von } \Gamma\}.$$

Ihre Umkehrabbildung ist $\psi : \Sigma \mapsto L^\Sigma = \{x \in L : \sigma(x) = x \ \forall \sigma \in \Sigma\}$. Hierbei gehen die normalen Erweiterungen F/K genau auf die normalen Untergruppen von Γ .

Beweis. Da wir in beiden Fällen Separabilität von L/K verlangen und diese sich auf alle Zwischerweiterungen vererbt, ist nur die Normalität jeweils ein Thema.

(a) L/F ist normal nach Satz 3.5.5 (N1) und ist separabel nach Satz 3.7.10, also galoissch. Sei nun F/K ebenfalls galoissch und seien $\sigma \in \text{Gal}(L/F)$ und $\tau \in \text{Gal}(L/K)$. Da F/K normal ist folgt nach Satz 3.5.5, N1, dass $\tau(F) = F$. Also folgt für $x \in F$, dass $\tau^{-1}\sigma\tau(x) = \tau^{-1}(\sigma(\tau(x))) = \tau^{-1}(\tau(x)) = x$, also $\tau^{-1}\sigma\tau \in \text{Gal}(L/F)$, diese Gruppe ist also ein Normalteiler. Da jedes $\tau \in \Gamma$ den Körper F fixiert, operiert Γ auf F , man erhält also einen Homomorphismus $\Gamma \rightarrow \text{Gal}(F/K)$ mit Kern Σ . Andererseits lässt sich jedes $\eta \in \text{Gal}(F/K)$ zu einer Abbildung $L \rightarrow \bar{F} = \bar{L}$ fortsetzen, deren Bild L ist, da L/K normal ist. Damit ist die Abbildung $\Gamma \rightarrow \text{Gal}(F/K)$ auch surjektiv und (b) ist bewiesen, bis auf die Rückrichtung.

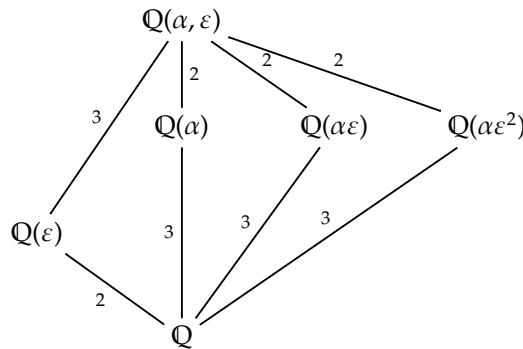
Sei also nun Σ ein Normalteiler, so ist zu zeigen, dass F/K normal ist. Sei dazu $\tau : F \rightarrow \bar{K} = \bar{F}$ eine Einbettung, dann kann man τ nach L ausdehnen $\tau : L \rightarrow \bar{K} = \bar{L}$, das Bild ist dann L , τ also in Γ . Da Σ ein Normalteiler ist, folgt nach obiger Rechnung, dass $\tau(F)$ ebenfalls von σ punktweise festgehalten wird. Da L/F galoissch ist, folgt, dass $\tau(F) = F$ ist und damit ist F/K normal nach Satz 3.5.5.

(b) Sei F ein Zwischenkörper, so folgt $F \subset \psi(\phi(F))$. Da aber L/F galoissch ist, ist $[L : F] = |\phi(F)| = [L : \psi(\phi(F))]$ und damit folgt $\psi \circ \phi = \text{Id}$. Sei umgekehrt Σ eine Untergruppe von Γ , dann ist $\Sigma \subset \phi(\psi(\Sigma))$ und es gilt $|\Sigma| = [L : \psi(\Sigma)] = |\phi(\psi(\Sigma))|$, woraus die Behauptung folgt. Die letzte Bemerkung folgt aus (b). $\square$

Beispiel 3.9.11. Sei $L = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$. Dann ist L der Zerfällungskörper des Polynoms $f(x) = x^3 - 2$, also ist L/K normal und separabel, also galoissch. Da die Galois-Gruppe die drei Nullstellen von f permutiert, ist sie eine Untergruppe von $\text{Per}(3)$. Der Zwischenkörper $\mathbb{Q}(\sqrt[3]{2})$ hat die Grade

$$[L : \mathbb{Q}(\sqrt[3]{2})] = 2, \quad [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3,$$

da im ersten Fall eine Nullstelle von $x^2 + x + 1$ adjungiert wird, im zweiten eine von $x^3 - 2$. Damit ist $[L : K] = 6$ und daher muss die Galois-Gruppe gleich der ganzen $\text{Per}(3)$ sein. Diese hat 3 Untergruppen der Ordnung 2 und eine der Ordnung 3. Wir schreiben $\alpha = \sqrt[3]{2}$ und $\varepsilon = e^{2\pi i/3}$ und erhalten folgende vollständige Liste aller Zwischenkörper, wobei wir an die Erweiterungen ihre jeweiligen Grade geschrieben haben.



Hierbei benutzen wir folgende Überlegungen: Die Nullstellen von $f(x)$ sind $\alpha, \alpha\varepsilon, \alpha\varepsilon^2$. Die Untergruppe, die $\alpha\varepsilon$ und $\alpha\varepsilon^2$ vertauscht, lässt α invariant, hat also $\mathbb{Q}(\alpha)$ als Fixkörper.

Korollar 3.9.12. Ist L/K galoissch und ist M ein Zwischenkörper. Schreibe $\Gamma = \text{Aut}(L/K)$ und $\Lambda = \text{Aut}(L/M) \subset \Gamma$. Dann sind äquivalent:

- (a) M/K ist galoissch,
- (b) M/K ist normal,

(c) Λ ist ein Normalteiler von Γ .

3.10 Endliche Körper

Sei F ein endlicher Körper. Dann muss der Primkörper von der Form $\mathbb{F}_p = \mathbb{Z}/p$ sein. Insbesondere hat dann der Körper F die Charakteristik p .

Lemma 3.10.1. *Sei F ein Körper der Charakteristik p , für eine Primzahl p . Dann ist die Abbildung $F \rightarrow F$,*

$$x \mapsto x^p$$

*ein Ringhomomorphismus. Man nennt ihn den **Frobenius-Homomorphismus** Fr_p . Insbesondere ist dann auch die k -fache Hintereinanderschaltung $\text{Fr}_p^k = \text{Fr}_{p^k}$ ein Ringhomomorphismus.*

Beweis. Die Abbildung Fr ist multiplikativ und schickt die Eins auf die Eins. Es bleibt zu zeigen, dass $\text{Fr}(x + y) = \text{Fr}(x) + \text{Fr}(y)$ gilt. Nach den binomischen Formeln ist

$$\text{Fr}(x + y) = (x + y)^p = \sum_{j=0}^p \binom{p}{j} x^j y^{p-j}$$

und die Behauptung folgt, wenn wir zeigen, dass die nichttrivialen Binomialkoeffizienten in Charakteristik p verschwinden, also dass der Binomialkoeffizient $\binom{p}{j} \in \mathbb{N}$ für jedes $1 \leq j \leq p-1$ von der Primzahl p geteilt wird. Nun ist $\binom{p}{j} = \frac{p!}{j!(p-j)!} = p \frac{(p-1)!}{j!(p-j)!}$. Da der Binomialkoeffizient ganzzahlig ist, folgt

$$j!(p-j)! \mid p! = p(p-1)!$$

Jeder Primteiler von $j!(p-j)!$ ist $< p$ und daher folgt schon

$$j!(p-j)! \mid (p-1)!$$

Also ist $\frac{(p-1)!}{j!(p-j)!}$ ganz und p teilt $\binom{p}{j}$. □

In Charakteristik p gilt also

$$(x + y)^p = x^p + y^p.$$

Lemma 3.10.2. *Sei $\text{Char}(K) = p$ eine Primzahl und sei $n \in \mathbb{N}$ teilerfremd zu p . Dann hat das Polynom $x^n - 1$ keine mehrfachen Nullstellen in K .*

Beweis. Angenommen, es hat eine, nämlich α . Dann ist α auch Nullstelle der formalen Ableitung, also gilt $n\alpha^{n-1} = 0$ in K . Da n teilerfremd zu p ist, ist $n \neq 0$ in K und damit ist $\alpha^{n-1} = 0$, also $\alpha = 0$, was im Widerspruch zu $\alpha^n = 1$ steht. □

Satz 3.10.3. (a) *Für jede Primzahlpotenz $q = p^k$ gibt es bis auf Isomorphie genau einen Körper $\mathbb{F}_q$ der Kardinalität q .*

(b) *$\mathbb{F}_q$ ist genau dann ein Unterkörper von $\mathbb{F}_r$, wenn r eine Potenz von q ist, dies ist genau dann der Fall, wenn $q = p^k$ und $r = p^n$ mit $k \mid n$ gilt. In diesem Fall ist die Körpererweiterung $\mathbb{F}_{p^n}/\mathbb{F}_{p^k}$ ein Galois-Erweiterung. Die Galois-Gruppe ist zyklisch von Ordnung n/k und wird von dem*

Frobenius-Homomorphismus

$$\text{Fr}_q : x \mapsto x^q$$

erzeugt

Insbesondere sind Erweiterungen endlicher Körper stets normal und separabel.

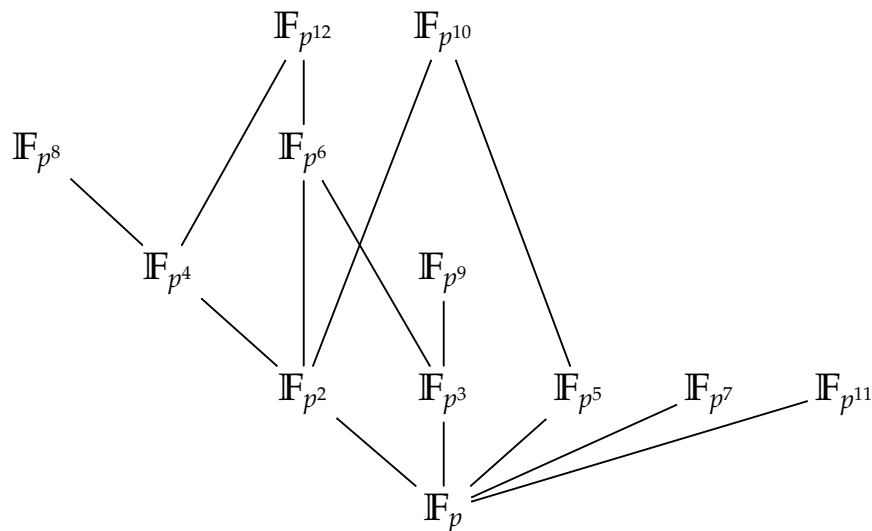
Beweis. Ist F ein endlicher Körper der Kardinalität $q = p^k$, dann ist jedes Element von $F^\times$ Nullstelle des Polynoms $f(x) = x^{q-1} - 1$ welches nach nach Lemma 3.10.2 separabel ist, also $q - 1$ Nullstellen hat, also besteht $F^\times$ genau aus den Nullstellen

des Polynoms $f(x)$, so dass F der Zerfällungskörper des separablen Polynoms f über $\mathbb{F}_p$ ist. Diese Beschreibung zeigt, dass F durch seine Kardinalität bis auf Isomorphie eindeutig festgelegt ist.

Ist nun $q = p^k$ eine Primpotenz, dann definiere $\mathbb{F}_q$ als den Zerfällungskörper von $f(x) = x^{q-1} - 1$ über $\mathbb{F}_p = \mathbb{Z}/p$, was die Existenz sichert. Ist $\mathbb{F}_r/\mathbb{F}_q$ eine Körpererweiterung, dann ist $\mathbb{F}_r$ ein $\mathbb{F}_q$ -Vektorraum, r muss also eine Potenz von q sein. Ist r eine Potenz von $q = p^k$, dann ist $\mathbb{F}_r$ auch der Zerfällungskörper von $x^{r-1} - 1$ über $\mathbb{F}_q$ und damit sind alle Erweiterungen galoissch.

Um schliesslich zu zeigen, dass die Galois-Gruppe $\Gamma = \text{Gal}(\mathbb{F}_r/\mathbb{F}_q)$ von Fr_q erzeugt wird, reicht es, einzusehen, dass $\mathbb{F}_q$ genau aus den Fixpunkten von Fr_q besteht. Dies ist aber klar, denn $\text{Fr}(x) = x$ ist äquivalent mit $x^q = x$ oder $x(x^{q-1} - 1) = 0$. □

Im Bild sieht man den Anfang des Inklusionsdiagramms der endlichen Körper über $\mathbb{F}_p$.



Proposition 3.10.4 (Einheitswurzeln in $\mathbb{F}_{p^k}$). *Alle Elemente $\neq 0$ von $\mathbb{F}_{p^k}$ sind Einheitswurzeln, genauer gilt*

$$\mathbb{F}_{p^k}^\times = \mu_{p^k-1}.$$

Ist $n \in \mathbb{N}$ teilerfremd zu p , so sind n verschiedene n -te Einheitswurzeln in dem

algebraischen Abschluss $\overline{\mathbb{F}_p}$ enthalten.

Es gibt keine p -ten Einheitswurzeln, denn wegen

$$x^p - 1 = (x - 1)^p$$

ist $x - 1$ der einzige irreduzible Faktor von $x^p - 1$.

Beweis. Die Gruppe $\mathbb{F}_{p^k}^\times$ besteht genau aus den Nullstellen des separablen Polynoms $x^{p^k-1} - 1$.

Sei nun n teilerfremd zu p . Das Polynom $x^n - 1$ hat Ableitung $nx^{n-1} \neq 0$, hat also n -verschiedene Nullstellen in $\overline{\mathbb{F}_p}$. Der Rest ist klar. $\square$

Korollar 3.10.5. (a) Der algebraische Abschluss $\mathbb{F}_{p^\infty} := \overline{\mathbb{F}_{p^k}} = \overline{\mathbb{F}_p}$ eines endlichen Körpers $\mathbb{F}_{p^k}$ ist die Vereinigung aller endlichen Erweiterungen $\mathbb{F}_{p^{kl}}$, $l \in \mathbb{N}$.

(b) Jedes irreduzible Polynom ueber einem endlichen Koerper $\mathbb{F}_q$ ist ein Faktor eines Polynoms der Form $x^n - 1$, wobei $n = q^l - 1$ fuer ein $l \in \mathbb{N}$.

Beweis. (a) Sei F diese Vereinigung. Dies ist selbst ein Koerper, da es fuer $a \in \mathbb{F}_q$ und $b \in \mathbb{F}_r$ ein s gibt, so dass $\mathbb{F}_q, \mathbb{F}_r \subset \mathbb{F}_s$ und daher existieren $ab, a + b$ in $\mathbb{F}_s$. Ist nun $f \in F[x]$ ein nichtkonstantes Polynom, dann ist $f \in \mathbb{F}_q[x]$ fuer ein q . Sei dann $\mathbb{F}_r/\mathbb{F}_q$ der Zerfaellungskoeper von f , dann hat f in $\mathbb{F}_r \subset F$ eine Nullstelle.

(b) Ist f ein solches Polynom und ist $\mathbb{F}_r$ sein Zerfaellungskoeper. Dann ist jede Nullstelle von f schon eine Nullstelle von $x^{r-1} - 1$. $\square$

3.11 Der Fundamentalsatz der Algebra

Satz 3.11.1 (Fundamentalsatz der Algebra).

Der Körper $\mathbb{C}$ ist algebraisch abgeschlossen.

Beweis. 1. Schritt: Der Körper $\mathbb{C}$ hat keine Erweiterung vom Grad 2.

Denn: Ist $[E : \mathbb{C}] = 2$, dann hat das Minimalpolynom von jedem $a \in E \setminus \mathbb{C}$ den Grad 2, aber jedes Polynom in $\mathbb{C}[x]$ vom Grad 2 hat nach der Mitternachtsformel eine Nullstelle in $\mathbb{C}$, also muss a in $\mathbb{C}$ liegen.

2. Schritt: $\mathbb{C}$ hat keine Galois-Erweiterung vom Grad 2^k , $k \in \mathbb{N}$.

Ist $L/\mathbb{C}$ galoisch vom Grad 2^k , dann hat die Galois-Gruppe $G = \text{Gal}(L/\mathbb{C})$ die Ordnung 2^k , also hat sie eine Untergruppe G' vom Index 2. Dann hat $F = \text{Fix}(G')$ den Grad 2 ueber $\mathbb{C}$, was nach dem ersten Schritt nicht sein kann.

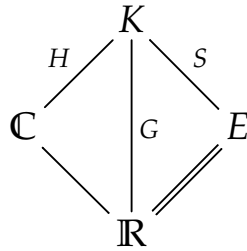
3. Schritt: Der Körper $\mathbb{R}$ hat keine Erweiterung ungeraden Grades.

Ist $E/\mathbb{R}$ eine Erweiterung ungeraden Grades und ist $a \in E$, dann muss das Minimalpolynom m_a ebenfalls ungeraden Grad haben, da $\text{grad}(m_a) = [\mathbb{R}(a) : \mathbb{R}]$ ein Teiler von $[E : \mathbb{R}]$ ist. Aus dem Zwischenwertsatz der Analysis folgt, dass m_a eine reelle Nullstelle hat, da es irreduzibel ist, ist m_a linear, also $a \in \mathbb{R}$ und damit $E = \mathbb{R}$.

4. Schritt: Finale.

Sei K eine endliche Erweiterung von $\mathbb{C}$. Wir wollen zeigen, dass $K = \mathbb{C}$ gilt. Die Erweiterung $K/\mathbb{R}$ ist separabel, da wir in Charakteristik Null sind. Wir koennen K durch seine normale Huelle ueber $\mathbb{R}$ ersetzen und also $K/\mathbb{R}$ als galoisch annehmen.

Sei $G = \text{Gal}(K : \mathbb{R})$ und sei S eine 2-Sylow-Gruppe in G . Der Körper $E = \text{Fix}(S)$ hat den Grad $[E : \mathbb{R}] = \frac{[K:\mathbb{R}]}{[K:E]} = \frac{|G|}{|S|}$ und dieser ist ungerade. Nach dem zweiten Schritt folgt $E = \mathbb{R}$ und das bedeutet, dass $G = S$ eine 2-Sylowgruppe ist. Damit ist auch die Untergruppe $H = \text{Gal}(K : \mathbb{C})$ eine 2-Sylowgruppe. Nach dem zweiten Schritt muss $H = \{1\}$ sein, also $K = \mathbb{C}$. □



3.12 Kreisteilungskörper und das Galois-Umkehrproblem

Für $n \in \mathbb{N}$ sei

$$C_n(x) = \prod_{\substack{0 \leq j \leq n-1 \\ \text{ggT}(j,n)=1}} (x - e^{2\pi i j/n})$$

das n -te **Kreisteilungspolynom** in $\mathbb{C}[x]$.

Der Grad des n -ten Kreisteilungspolynoms C_n ist gleich

$$\phi(n) = |(\mathbb{Z}/n)^\times|$$

die **Eulersche ϕ -Funktion**. Man beachte $\phi(1) = \phi(2) = 1$.

Lemma 3.12.1. *Die Eulersche ϕ -Funktion ist schwach multiplikativ, d.h., sind m und n in $\mathbb{N}$ teilerfremd, dann ist $\phi(mn) = \phi(m)\phi(n)$. Ist p eine Primzahl und $k \in \mathbb{N}$, dann gilt*

$$\phi(p^k) = p^k - p^{k-1}.$$

Ist also $n = \prod_{j=1}^n p_j^{k_j}$ die Primfaktorzerlegung, dann ist

$$\phi(n) = \prod_{j=1}^n (p_j^{k_j} - p_j^{k_j-1}).$$

Beweis. Mit dem chinesischen Restsatz folgt für teilerfremde m, n , dass $\mathbb{Z}/mn \cong \mathbb{Z}/m \times \mathbb{Z}/n$ und also folgt auch

$$(\mathbb{Z}/mn)^\times \cong (\mathbb{Z}/m)^\times \times (\mathbb{Z}/n)^\times$$

und damit die Multiplikativität. Die Elemente von $\mathbb{Z}/p^k$, die nicht teilerfremd zu p^k sind, sind genau die Vielfachen von p und damit das Bild der injektiven Abbildung $\mathbb{Z}/p^{k-1} \hookrightarrow \mathbb{Z}/p^k, (n + p^{k-1}\mathbb{Z}) \mapsto (np + p^k\mathbb{Z})$. $\square$

Sei μ_n die Gruppe der n -ten Einheitswurzeln in $\mathbb{C}$. Diese Gruppe ist zyklisch und wird von $\zeta_n = e^{2\pi i/n}$ erzeugt. Eine Einheitswurzel $\zeta \in \mu_n$ heisst **primitive n -te Einheitswurzel**, wenn ζ die Gruppe μ_n erzeugt. Dies ist genau dann der Fall, wenn $\zeta = e^{2\pi i j/n}$ ist für ein j , das teilerfremd zu n ist. Daher sind die Nullstellen von C_n genau die primitiven n -ten Einheitswurzeln, also

$$C_n(x) = \prod_{\zeta \in \mu_n^{\text{prim}}} (x - \zeta),$$

wobei μ_n^{prim} die Menge der primitiven n -ten Einheitswurzeln bezeichnet.

Proposition 3.12.2. *Es gilt*

$$x^n - 1 = \prod_{d|n} C_d(x),$$

wobei das Produkt über alle $d \in \mathbb{N}$ läuft, die n teilen.

Beweis. Das Polynom auf der linken Seite hat genau alle Elemente von μ_n als Nullstellen, jede ist eine einfache Nullstelle. Ist $\zeta \in \mu_n$ von Ordnung d , dann ist d ein Teiler von n und ζ ist einfache Nullstelle des Kreisteilungspolynoms C_d und keines anderen. Damit haben beide Seiten der behaupteten Gleichung dieselben Nullstellen, alle sind einfach, also sind die beiden Polynome gleich. $\square$

Hier eine Liste der ersten Kreisteilungspolynome:

$$C_1(x) = x - 1$$

$$C_2(x) = x + 1$$

$$C_3(x) = x^2 + x + 1$$

$$C_4(x) = x^2 + 1$$

$$C_5(x) = x^4 + x^3 + x^2 + x + 1$$

$$C_6(x) = x^2 - x + 1$$

$$C_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

$$C_8(x) = x^4 + 1$$

$$C_9(x) = x^6 + x^3 + 1$$

$$C_{10}(x) = x^4 - x^3 + x^2 - x + 1$$

Lemma 3.12.3. *Ist die primitive n -te Einheitswurzel ζ Nullstelle des irreduziblen normierten Polynoms $f \in \mathbb{Q}[x]$ und ist $p \nmid n$ eine Primzahl, dann ist auch ζ^p eine Nullstelle von f .*

Beweis. Sowohl ζ als auch ζ^p sind Nullstellen von $x^n - 1 = f(x)g(x)$ für ein normiertes Polynom $g(x)$. Nach Korollar 2.6.4 sind f und g beide in $\mathbb{Z}[x]$.

Angenommen, $f(\zeta^p) \neq 0$, dann folgt $g(\zeta^p) = 0$, also ist ζ Nullstelle von $g(x^p)$. Da f das Minimalpolynom von ζ ist, gibt es ein Polynom $h \in \mathbb{Q}[x]$ so dass $g(x^p) = h(x)f(x)$. Wieder gilt $h \in \mathbb{Z}[x]$. Seien $\bar{f}, \bar{g}, \bar{h}$ die Bilder in $\mathbb{Z}/p\mathbb{Z}[x]$. Es ist dann $\bar{f}(x)\bar{h}(x) = \bar{g}(x^p) = \bar{g}(x)^p$. Daher folgt über dem endlichen Körper $\mathbb{F}_p$, dass $x^n - 1 = \bar{f}\bar{g}$. Jeder irreduzible Faktor von $\bar{f}$ ist wegen $\bar{g}^p = \bar{f}\bar{h}$ auch ein Faktor von $\bar{g}$ und damit hat $x^n - 1$ mehrfache Nullstellen. Das kann aber nicht sein, denn die Ableitung von $x^n - 1$ ist nx^{n-1} und die hat nur die Null als Nullstelle,

Widerspruch!

□

Satz 3.12.4 (Kreisteilungskörper). *Das Kreisteilungspolynom C_n liegt in $\mathbb{Z}[x]$ und ist irreduzibel. Sei ζ eine primitive n -te Einheitswurzel in $\mathbb{C}$. Die Erweiterung $\mathbb{Q}(\zeta)/\mathbb{Q}$ ist galoissch mit Galois-Gruppe isomorph zu $(\mathbb{Z}/n)^\times$.*

*Man nennt $\mathbb{Q}(\zeta)$ den n -ten **Kreisteilungskörper**. Er hängt nicht von der Auswahl von ζ ab.*

Beweis. Der Körper $K = \mathbb{Q}(\zeta)$ enthält alle n -ten Einheitswurzeln und ist daher der Zerfällungskörper des separablen Polynoms $x^n - 1$ und damit galoisch über $\mathbb{Q}$. Ist $P \subset \mu_n$ die Teilmenge der primitiven n -ten Einheitswurzeln und ist $\tau \in \text{Gal}(K/\mathbb{Q})$ dann bildet τ die Gruppe μ_n isomorph auf sich selbst ab und damit folgt $\tau(P) = P$, da P gerade die Menge der Erzeuger der Gruppe μ_n ist. Da $C_n(x) = \prod_{z \in P} (x - z)$ folgt $\tau(C_n) = C_n$ und da dies für jedes τ gilt, ist $C_n \in \mathbb{Q}[x]$. Da C_n normiert ist und $C_n(x) \mid (x^n - 1)$, folgt nach Korollar 2.6.4, dass $C_n \in \mathbb{Z}[x]$ ist. Für die Irreduzibilität sei ζ eine primitive n -te Einheitswurzel und f ihr Minimalpolynom. Wir müssen zeigen, dass $f = C_n$. Wir sind fertig, wenn wir zeigen können, dass jede andere primitive n -te Einheitswurzel ebenfalls Nullstelle von f ist. Sei dazu ε eine weitere Primitive n -te Einheitswurzel, dann ist $\varepsilon = \zeta^d$ mit $\text{ggT}(d, n) = 1$. Es folgt $d = p_1 \cdots p_k$ mit zu n teilerfremden Primzahlen. Nach dem Lemma ist ζ^{p_1} eine Nullstelle von f und dann $\zeta^{p_1 p_2}$ und so fort bis zu $\zeta^d = \varepsilon$. Daher ist C_n irreduzibel.

Wir bestimmen nun die Galois-Gruppe $G = \text{Gal}(K/\mathbb{Q})$. Sei ζ eine primitive n -te Einheitswurzel in K . Ist $k \in \mathbb{Z}$, so hängt die Potenz ζ^k nur von der Restklasse von k in $\mathbb{Z}/n$ ab. Ferner ist ζ^k genau dann primitiv in μ_n , wenn k teilerfremd zu n ist, wenn k also ein Element in $(\mathbb{Z}/n)^\times$ induziert.

Ist $\tau \in \text{Gal}(K/\mathbb{Q})$, dann ist $\tau(\zeta)$ wieder eine primitive Einheitswurzel, also ist $\tau(\zeta) = \zeta^k$ für ein eindeutig bestimmtes $k \in (\mathbb{Z}/n)^\times$. Da τ durch das Bild $\tau(\zeta)$

eindeutig festgelegt ist, erhalten wir eine injektive Abbildung

$$\theta : \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \hookrightarrow (\mathbb{Z}/n)^\times,$$

gegeben durch $\tau \mapsto k = k(\tau)$. Ist $\gamma \in \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ ein weiteres Element, dann gilt

$$\gamma\tau(\zeta) = \gamma(\tau(\zeta)) = \gamma(\zeta^{k(\tau)}) = \gamma(\zeta)^{k(\tau)} = (\zeta^{k(\gamma)})^{k(\tau)} = \zeta^{k(\gamma)k(\tau)}.$$

Daher ist θ ein Gruppenhomomorphismus. Wir haben

$$|\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})| = [\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg(C_n) = |(\mathbb{Z}/n)^\times|.$$

Daher folgt, dass der injektive Gruppenhomomorphismus θ ein Isomorphismus ist. □

Satz 3.12.5 (Dirichletscher Primzahlsatz). *Seien $a, n \in \mathbb{N}$ teilerfremd, dann gibt es unendlich viele Primzahlen p mit $p \equiv a \pmod{n}$. Insbesondere gibt es unendlich viele Primzahlen p mit $p \equiv 1 \pmod{n}$.*

Beweis. Hier machen wir eine Anleihe in der analytischen Zahlentheorie. □

Satz 3.12.6. *Jede abelsche endliche Gruppe tritt als Galois-Gruppe über $\mathbb{Q}$ auf. Das heisst, zu jeder abelschen endlichen Gruppe G gibt es eine Galois-Erweiterung $K/\mathbb{Q}$ mit $\text{Gal}(K : \mathbb{Q}) \cong G$.*

Beweis. Sei A eine endliche abelsche Gruppe. Nachdem Hauptsatz über endlich-erzeugte abelsche Gruppen ist A ein Produkt von zyklischen Gruppen

$$A \cong Z_{n_1} \times \cdots \times Z_{n_k},$$

wobei Z_n die zyklische Gruppe der Ordnung n bezeichnet. Für jedes j wählen wir eine Primzahl p_j mit $n_j \mid p_j - 1$ und zwar so, dass alle p_j paarweise verschieden sind, was nach dem Dirichletschen Primzahlsatz möglich ist. Sei $N = p_1 \cdots p_k$ und $L = \mathbb{Q}(\zeta_N)$. Dann ist nach dem chinesischen Restsatz

$$\begin{aligned} G = \text{Gal}(L/\mathbb{Q}) &\cong (\mathbb{Z}/N)^\times \cong (\mathbb{Z}/p_1)^\times \times \cdots \times (\mathbb{Z}/p_k)^\times \\ &\cong Z_{p_1-1} \times \cdots \times Z_{p_k-1}. \end{aligned}$$

Sei H die Untergruppe, die isomorph ist zu $Z_{(p_1-1)/n_1} \times \cdots \times Z_{(p_k-1)/n_k}$. Dann ist $G/H \cong A$, also hat $K = L^H$ die Galois-Gruppe A über $\mathbb{Q}$. $\square$

3.13 Konstruktionen mit Zirkel und Lineal

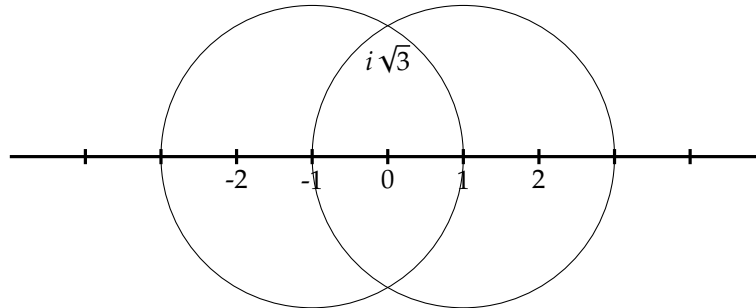
Definition 3.13.1. Wir definieren die Menge $\mathcal{C} \subset \mathbb{C}$ der **konstruierbaren Zahlen** induktiv wie folgt:

1. $0, 1 \in \mathcal{C}$,
2. (Schnittpunkt zweier Geraden) Sind $z_1 \neq z_2$ und $z_3 \neq z_4$ in $\mathcal{C}$ und schneiden sich die Geraden durch (z_1, z_2) und durch (z_3, z_4) in genau einem Punkt z , dann liegt z in $\mathcal{C}$.
3. (Schnittpunkte von Gerade und Kreis) Sind $z_1, \dots, z_5 \in \mathcal{C}$ mit $z_1 \neq z_2$ und ist z ein Schnittpunkt der Geraden (z_1, z_2) mit dem Kreis mit Radius $|z_3 - z_4|$ um den Punkt z_5 , dann ist $z \in \mathcal{C}$. Hierbei ist es erlaubt, dass die Gerade tangential zum Kreis liegt, es also nur einen Schnittpunkt gibt.
4. (Schnittpunkte zweier Kreise) Sind $z_1, \dots, z_6$ in $\mathcal{C}$ und ist z ein Schnittpunkt des Kreises mit Radius $|z_1 - z_2|$ um den Punkt z_3 mit dem Kreis mit Radius $|z_4 - z_5|$ um den Punkt z_6 , dann ist $z \in \mathcal{C}$. Hierbei wird vorausgesetzt, dass die beiden Kreise verschieden sind.

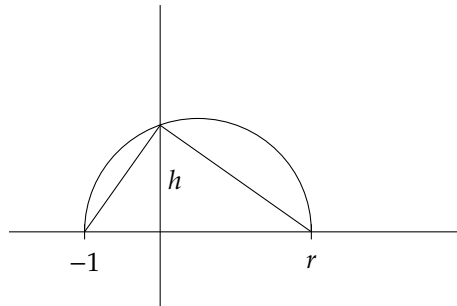
Die Menge $\mathcal{C}$ ist dann die Menge aller komplexen Zahlen, die jeweils durch endlich viele Schritte der Form 2-4 aus 0 und 1 gewonnen werden koennen.

Beispiele 3.13.2. (a) Indem man den Kreis um 1 vom Radius 1 mit der Geraden $(0,1)$ schneidet, erhaelt man den Punkt 2 dann 3 und 4 usw. Auf der negativen Seite ebenso, so dass $\mathbb{Z} \subset \mathcal{C}$.

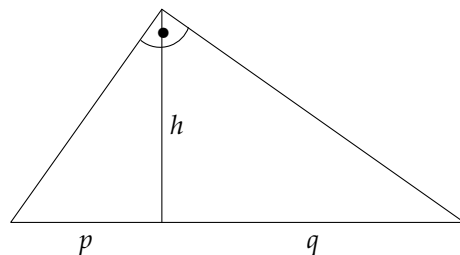
Schneidet man andererseits den Kreis vom Radius 2 um 1 mit dem Kreis vom Radius 2 um -1, erhaelt man einen Punkt auf der imaginären Achse, den nach Pythagoras gleich $i\sqrt{3}$ ist.



(b) Man kann Wurzeln ziehen in $\mathcal{C}$. Genauer gilt: Ist $z \in \mathcal{C}$ und ist $a \in \mathbb{C}$ mit $a^2 = z$, dann ist $a \in \mathcal{C}$. Sei $z = re^{i\theta}$ mit $r > 0$ und $\theta \in (-\pi, \pi]$. Dann ist $a = \pm \sqrt{r}e^{i\theta/2}$. Ferner ist $r \in \mathcal{C}$, da man den Kreis um Null mit Radius $r = |z|$ nur mit der x -Achse schneiden muss. Da man Winkel durch Konstruktion halbieren kann, reicht es zu zeigen, dass $\sqrt{r}$ in $\mathcal{C}$ liegt.



Man bestimmt den Mittelpunkt zwischen -1 und r und schlägt darüber den Halbkreis mit Radius $\frac{r+1}{2}$, den Thaleskreis. Dieser schneidet die imaginäre Achse in ih und nach dem Höhensatz gilt $h^2 = 1 \cdot r = r$, also $\sqrt{r} = h \in \mathcal{C}$.



Höhensatz:

$$h^2 = pq$$

Satz 3.13.3. Die Menge $\mathcal{C}$ der konstruierbaren Zahlen ist ein Unterkörper von $\mathbb{C}$.
Für eine komplexe Zahl z sind äquivalent:

- (a) $z \in \mathcal{C}$.
- (b) Es existiert eine Körperkette $\mathbb{Q} = L_0 \subset L_1 \subset \cdots \subset L_n$ so dass $z \in L_n$ und $[L_{j+1} : L_j] = 2$ für jedes $j = 0, \dots, n-1$.
Mit anderen Worten, z liegt in einer **multiquadratischen Erweiterung** von $\mathbb{Q}$.
- (c) z liegt in einer Galoiserweiterung $L/\mathbb{Q}$, deren Grad eine Potenz von 2 ist:
 $[L : \mathbb{Q}] = 2^m$.

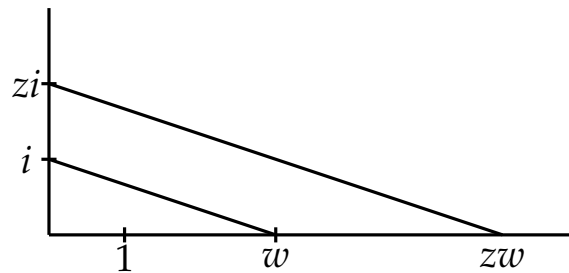
Bemerkung: Damit eine komplexe Zahl z konstruierbar ist, reicht es *nicht* aus, dass sie in einem Körper $K/\mathbb{Q}$ vom Grad 2^k über $\mathbb{Q}$ liegt, denn es gibt Körper $K/\mathbb{Q}$ vom Grad 4, die nicht galoisch über $\mathbb{Q}$ sind und deren normale Hülle $L/K/\mathbb{Q}$ einen Grad haben, der keine 2-Potenz ist. Beispiel hierzu: Man kann zeigen, dass es zu jeder endlichen Permutationsgruppe $\text{Per}(n)$ eine Galois-Erweiterung $L/\mathbb{Q}$ gibt mit Gruppe $\text{Gal}(L/\mathbb{Q}) \cong \text{Per}(n)$. Die Gruppe $G = \text{Per}(4)$ hat 24 Elemente und hat $H = \text{Per}(3)$ als nicht-normale Untergruppe vom Index 4. Sei also $K = L^H$, dann ist $K/\mathbb{Q}$ vom Grad 4 und ist nicht galoisch.

Beweis des Satzes. Indem wir die Schnittpunkte der beiden Kreise in obiger Zeichnung, also $\pm i\sqrt{3}$ verbinden, erhalten wir die imaginäre Achse. Diese schneiden wir mit dem Einheitskreis und erhalten $\pm i \in \mathcal{C}$. Ferner gilt: $z \in \mathcal{C} \Rightarrow \bar{z} \in \mathcal{C}$, was man auf verschiedene Weise einsehen kann. Eine ist die, einen Kreis um z mit grossem Radius mit der x -Achse zu schneiden, um die beiden Schnittpunkte Kreise gleichen Radius' zu schlagen. Der zweite Schnittpunkt dieser beiden Kreise ist $\bar{z}$.

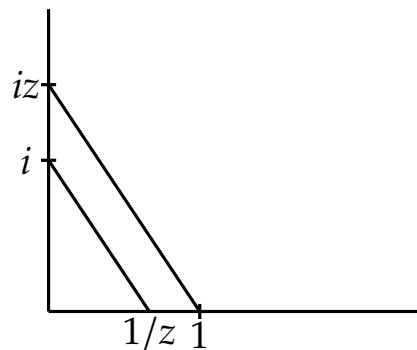
Wir zeigen: $z, w \in \mathcal{C} \Rightarrow z \pm w \in \mathcal{C}$: Wir können die Parallele zu einer gegebenen

Geraden durch einen gegebenen Punkt konstruieren. Wir können daher die Parallele zur Geraden $(0, w)$ durch den Punkt z mit dem Kreis vom Radius $|w|$ um z schneiden. Die beiden Schnittpunkte sind $z \pm w$.

Wir zeigen: $z, w \in \mathcal{C} \Rightarrow zw \in \mathcal{C}$. Wir können konstruktiv Winkel addieren. Es reicht also, anzunehmen, dass $z, w > 0$ gilt. Dann geht die Konstruktion wie folgt. Konstruiere iz . Dann bilde die Parallele zur Geraden (i, w) durch den Punkt iz und schneide sie mit der x -Achse. Das Ergebnis ist nach dem Strahlensatz zw , siehe Bild.



Wir zeigen: $z \in \mathcal{C}, z \neq 0 \Rightarrow \frac{1}{z} \in \mathcal{C}$. Wieder reicht es, $z > 0$ anzunehmen. Wir schneiden die Parallele zu $(1, iz)$ durch i mit der x -Achse und erhalten $1/z$.



Hieraus folgt, dass $\mathcal{C}$ ein Körper ist, insbesondere liegt $\mathbb{Q}$ in $\mathcal{C}$. Um $(a) \Rightarrow (b)$ zu zeigen, reicht es, nachzuweisen, dass jeder der Konstruktionsschritte 2., 3., 4. einer höchstens quadratischen Körpererweiterung entspricht. Genauer heisst das in jedem der Schritte: Sind die z_j in einem Körper K , der invariant unter der komplexen Konjugation ist, dann liegt z in K oder in einer quadratischen Erweiterung von K .

Schnitt zweier Geraden: Wir zeigen hier folgendes: liegen $z_1, \dots, z_4$ in einem Körper $K \subset \mathbb{C}$ und ist z der einzige Schnittpunkt der Geraden (z_1, z_2) und (z_3, z_4) , dann liegt auch z in K . In diesem Fall ist also keine Körpererweiterung nötig.

Ein Punkt der Geraden (z_1, z_2) ist von der Form $z(t) = z_1 + t(z_1 - z_2)$ für ein $t \in \mathbb{R}$ und er liegt genau dann auf der Geraden (z_3, z_4) , wenn $z(t) - z_3$ kollinear ist zu $z_3 - z_4$, oder, was dasselbe bedeutet, wenn $z(t) - z_3$ senkrecht auf $i(z_3 - z_4)$ steht, wenn also

$$\operatorname{Re} \left((z(t) - z_3) \overline{i(z_4 - z_3)} \right) = 0.$$

Dies ist äquivalent zu

$$0 = -i(z_1 - z_3 + t(z_1 - z_2)) \overline{(z_4 - z_3)} + i \overline{(z_1 - z_3 + t(z_1 - z_2))} (z_4 - z_3).$$

Dies ist eine Gleichung der Form $at - b = 0$ mit $a, b \in K$. Da z der Schnittpunkt zweier nichtparalleler Geraden ist, ist das t , das diese Gleichung löst, eindeutig bestimmt und daher ist $a \neq 0$, damit ist $t \in K$ und also auch $z(t) \in K$.

Schnitt von Kreis und Gerade: Ein Punkt auf der Geraden (z_1, z_2) , also ein Punkt der Form $z(t) = z_1 + t(z_1 - z_2)$ liegt genau dann auf dem Kreis um z_5 vom Radius $|z_3 - z_4|$, wenn gilt

$$|z_1 + t(z_1 - z_2) - z_5|^2 = |z_3 - z_4|^2.$$

Indem wir $|z|^2 = z\bar{z}$ schreiben, wird daraus eine Gleichung der Form

$$(a + bt)(\bar{a} + \bar{b}t) = c$$

wobei a, b, c in dem Körper K liegen. Das gesuchte t ist eine Lösung der quadratischen Gleichung

$$|a|^2 - c + t(a\bar{b} + \bar{a}b) + |b|^2 t^2 = 0,$$

deren Koeffizienten in K liegen, also liegt t entweder in K oder einer quadratischen Erweiterung. Dasselbe gilt dann für $z(t)$.

Schnitt zweier Kreise: Hier muss z die folgenden zwei Gleichungen erfüllen:

$$|z - z_3|^2 = |z_1 - z_2|^2$$

$$|z - z_6|^2 = |z_4 - z_5|^2,$$

was zu Gleichungen der Form

$$(z - a)(\bar{z} - \bar{a}) = b$$

$$(z - c)(\bar{z} - \bar{c}) = d$$

mit $a, b, c, d \in K$ führt. Hier können wir $b \neq 0$ und damit $z - a \neq 0$ annehmen, da sonst $z = a$ schon in K liegt. Dann führt die erste Gleichung zu

$$\bar{z} = \frac{b}{z - a} + \bar{a}.$$

Setzen wir dies in die zweite Gleichung ein, erhalten wir

$$(z - c)\left(\frac{b}{z - a} + \bar{a} - \bar{c}\right) = d,$$

was zu einer quadratischen Gleichung über K führt, so dass die Behauptung bewiesen ist.

Damit ist (a) $\Rightarrow$ (b) gezeigt. Für die Umkehrung erfülle $z \in \mathbb{C}$ eine quadratische Gleichung über K . Dann ist $z = a + b\sqrt{\alpha}$ mit $a, b, \alpha \in K$. Man kann aber aus α auch dessen Wurzel konstruieren, wie wir in Beispiel 3.13.2 gesehen haben, so dass man auch z konstruieren kann.

(b) $\Rightarrow$ (c) Dies folgt aus Lemma 3.5.11, da es besagt, dass mit L auch die normale Hülle von L ueber $\mathbb{Q}$ multiquadratisch ist.

(c) $\Rightarrow$ (b): Sei $z \in L$ mit $L/\mathbb{Q}$ galoisch von 2-Potenzgrad. Nach Korollar 1.8.5 gibt es in $G = \text{Gal}(L/\mathbb{Q})$ eine Kette von Untergruppen $1 = G_0 \subset \cdots \subset G_k = G$ so dass $[G_{j+1} : G_j] = 2$. Die entsprechenden Fixkoerper erfuellen nach dem Hauptsatz

der Galoistheorie die Bedingung von (b). □

Beispiele 3.13.4. • **Die Quadratur des Kreises.** ...ist nicht möglich. Genauer, zu einem gegebenen Kreis lässt sich kein Quadrat gleichen Flächeninhalts konstruieren. Sagen wir, der Kreis hätte Radius 1, dann ist der Flächeninhalt π . Es geht also darum, die Zahl $\sqrt{\pi}$ zu konstruieren. Diese aber ist nicht einmal algebraisch, wie von Lindemann 1882 bewiesen wurde.

- **Die Verdopplung des Würfels.** Es ist nicht möglich, zu einem gegebenen Würfel einen des doppelten Volumens zu konstruieren. Habe der Ursprungswürfel Kantenlänge 1 und der zu konstruierende Kantenlänge a , so muss $a^3 = 2$ gelten, also $a = \sqrt[3]{2}$. Die Körpererweiterung $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ hat aber Grad 3!
- **Die Dreiteilung des Winkels.** Man kann nicht einen beliebigen Winkel in drei gleiche Teile teilen. Würde dies zB mit dem Winkel $2\pi/3$ gehen, könnte man also die neunte Einheitswurzel $\varepsilon = e^{2\pi i/9}$ konstruieren. Der Körper $\mathbb{Q}(\varepsilon)$ hat aber Grad $\phi(9) = 6$!
- **Das regelmaessige 17-Eck** ist konstruierbar. Genauer sei p eine Primzahl der Gestalt $p = 2^k + 1$, dann ist die primitive p -te Einheitswurzel

$$\zeta_p = e^{2\pi i/p}$$

konstruierbar. Beachte hierzu, dass $K = \mathbb{Q}(\zeta_p)$ eine Galoiserweiterung von $\mathbb{Q}$ vom Grad $\phi(p) = p - 1 = 2^k$ ist.

3.14 Aufloesbarkeit in Radikalen

Satz 3.14.1 (Lineare Unabhaengigkeit von Charakteren). *Seien K ein Koerper, G eine Gruppe und $\chi_1, \dots, \chi_n : G \rightarrow K^\times$ verschiedene Gruppenhomomorphismen. Dann sind die χ_j linear unabhaengig im Vektorraum $\text{Abb}(G, K)$.*

Beweis. Induktion nach n . Ist $n = 1$, haben wir nur einen Morphismus, der hat Werte in $K^\times$, ist also nicht Null.

$n \rightarrow n + 1$. Seien $\lambda_1, \dots, \lambda_{n+1} \in K$ mit $F := \lambda_1 \chi_1 + \dots + \lambda_{n+1} \chi_{n+1} = 0$. Seien $g, x \in G$. Dann gilt einmal

$$\begin{aligned} 0 &= F(gx) = \lambda_1 \chi_1(gx) + \dots + \lambda_n \chi_n(gx) \\ &= \lambda_1 \chi_1(g) \chi_1(x) + \dots + \lambda_n \chi_n(g) \chi_n(x). \end{aligned}$$

und zum anderen:

$$0 = \chi_{n+1}(g)F(x) = \lambda_1 \chi_{n+1}(g) \chi_1(x) + \cdots + \lambda_n \chi_{n+1}(g) \chi_n(x)$$

Ziehen die zweite Null von der ersten ab, dann heben sich die letzten Summanden auf und es folgt

$$0 = \lambda_1(\chi_1(g) - \chi_{n+1}(g))\chi_1(x) + \cdots + \lambda_n(\chi_n(g) - \chi_{n+1}(g))\chi_n(x).$$

Wir halten g fest und lassen x laufen. Da diese Abbildung in x gleich Null ist, folgt aus der Induktionshypothese, dass

$$0 = \lambda_1(\chi_1(g) - \chi_{n+1}(g)) = \cdots = \lambda_n(\chi_n(g) - \chi_{n+1}(g))$$

Sei $1 \leq j \leq n$. Da $\chi_{n+1} \neq \chi_j$, gibt es ein $g \in G$ mit $\chi_j(g) \neq \chi_{n+1}(g)$, also ist $\lambda_j = 0$. Damit folgt schliesslich $0 = \lambda_{n+1}\chi_{n+1}(gx)$, so dass auch $\lambda_{n+1} = 0$ folgt. $\square$

Definition 3.14.2. Eine Gruppe G heisst **aufloesbar**, wenn eine Reihe von Untergruppen

$$G = U_0 \supset U_1 \supset \cdots \supset U_n = 1$$

gibt so dass U_{j+1} normal in U_j ist und U_j/U_{j+1} abelsch.

Beispiel 3.14.3. Die Gruppe der oberen Dreiecksmatrizen in $\text{GL}_n(K)$ ist aufloesbar.

Satz 3.14.4. Sei $[a, b] = aba^{-1}b^{-1}$ die Kommutatorklammer und fuer jede Untergruppe H sei $[H, H]$ die von allen Kommutatoren $[x, y]$, $x, y \in H$ erzeugte Untergruppe.

(a) Sei $G^{(0)} = G$ und induktiv $G^{(j+1)} = [G^{(j)}, G^{(j)}]$. die Gruppe G ist genau dann aufloesbar, wenn $G^{(n)} = 1$ fuer ein $n \in \mathbb{N}$ gilt.

(b) Bilder und Untergruppen aufloesbarer Gruppen sind aufloesbar.

(c) Sei N ein Normalteiler in G . Die Gruppe G ist genau dann auflösbar, wenn N und G/N auflösbar sind.

Beweis. (a) Sei G auflösbar und $G = U_0 \supset U_1 \supset \cdots \supset U_n = 1$ eine Reihe von Untergruppen so dass U_j/U_{j+1} abelsch ist. Das bedeutet, dass jeweils $[U_j, U_j] \subset U_{j+1}$ gilt. Wir zeigen induktiv, dass dann $G^{(j)} \subset U_j$ gilt. Für $j = 0$ ist dies klar. Sei es für j bewiesen, dann folgt $G^{(j+1)} = [G^{(j)}, G^{(j)}] \subset [U_j, U_j] \subset U_{j+1}$.

Gilt umgekehrt $G^{(n)} = \{1\}$, dann ist $G = G^{(0)} \supset \cdots \supset G^{(n)}$ eine Kette mit abelschen Quotienten, also ist G auflösbar.

(b) Sei $U \subset G$ eine Untergruppe einer auflösbaren Gruppe G . Wir zeigen induktiv $U^{(j)} \subset G^{(j)}$. Für $j = 0$ ist dies klar und aus $U^{(j)} \subset G^{(j)}$ folgt $U^{(j+1)} = [U^{(j)}, U^{(j)}] \subset [G^{(j)}, G^{(j)}] = G^{(j+1)}$. Damit ist auch U auflösbar. Ist $\phi : G \rightarrow H$ surjektiv, so folgt ebenso induktiv, dass $\phi(G^{(j)}) = H^{(j)}$ und damit ist H auflösbar.

(c) Ist G auflösbar, dann sind N und G/N auflösbar nach Teil (b). Seien umgekehrt N und G/N auflösbar. Da G/N auflösbar, gibt es ein n so dass $G^{(n)} \subset N$ gilt. Damit folgt dann induktiv $G^{(n+k)} \subset N^{(k)}$ und da N auflösbar ist, muss auch G auflösbar sein. □

Proposition 3.14.5. Seien $n \in \mathbb{N}$ und der Körper K enthalte eine primitive n -te Einheitswurzel $\varepsilon = \varepsilon_n$.

(a) Sei α in einer Körpererweiterung mit $\alpha^n \in K$ und n ist minimal mit dieser Eigenschaft. Dann ist $K(\alpha)/K$ galoisch mit Galoisgruppe $\cong \mathbb{Z}/n$.

(b) Umgekehrt, ist L/K zyklisch vom Grad n , dann ist $L = K(\alpha)$ für ein α mit $\alpha^n \in K$.

Beweis. (a) Sei $\alpha^n = c \in K$. Der Körper $K(\alpha)$ enthält α und alle anderen Nullstellen $\varepsilon\alpha, \dots, \varepsilon^{n-1}\alpha$ des Polynoms $p(x) = x^n - c$, also ist er der Zerfällungskörper und damit ist L/K galoisch. Wir zeigen, dass

$p(x) = (x - \alpha)(x - \varepsilon\alpha) \cdots (x - \varepsilon^{n-1}\alpha) \in K[x]$ irreduzibel ist. Sei dazu $m(x)$ ein nichtkonstanter irreduzibler normierter Faktor. Dann ist
 $m(x) = (x - \varepsilon^{k_1}\alpha) \cdots (x - \varepsilon^{k_s}\alpha)$ fuer geeignete verschiedene $k_j \bmod n$ und $s \leq n$.
 Da dieses Polynom Koeffizienten in K hat, liegt auch der nullte in K , also

$$\varepsilon^{k_1 + \cdots + k_s} \alpha^s \in K,$$

also $\alpha^s \in K$. Da n minimal ist und $s \leq n$, folgt $s = n$ und damit $m(x) = p(x)$, welches damit irreduzibel ist. Daher ist

$$K(\alpha) \cong K[x]/p(x) \cong K(\varepsilon^j \alpha)$$

und da $K(\alpha) = K(\varepsilon^k \alpha)$, induziert $\alpha \mapsto \varepsilon^k \alpha$ einen Galoishomomorphismus $\sigma_k \in \text{Gal}(L/K)$. Wir erhalten einen Gruppenhomomorphismus $\mathbb{Z}/n \rightarrow \text{Gal}(L/K)$, $k \mapsto \sigma_k$. Dieser ist injektiv, denn jedes $\eta \in G$ ist durch $\eta(\alpha)$ eindeutig festgelegt und er ist surjektiv, da er injektiv zwischen zwei gleichmaechtgen Menge laeuft.

(b) Fuer die Umkehrung sei σ ein Erzeuger von $G = G_f$. Es reicht, ein Element $\alpha \in L^\times$ zu finden, so dass $\sigma(\alpha) = \varepsilon^{-1}\alpha$, denn dann folgt $\sigma(\alpha^k) = \varepsilon^{-k}\alpha$ und α^n ist damit die kleinste Potenz von α , die σ -invariant ist, also in K liegt. Nach Teil (a) ist $K(\alpha)/K$ zyklisch vom Grad $n = [L : K]$, also ist dann $L = K(\alpha)$.

Wir finden jetzt also so ein α . Da $1, \sigma, \dots, \sigma^{n-1}$ verschiedene Gruppenhomomorphismen $F^\times \rightarrow F^\times$ sind, folgt nach der Linearen Unabhaengigkeit von Charakteren, Satz 3.14.1, dass $\sum_{j=0}^{n-1} \varepsilon^j \sigma^j$ ungleich Null ist, also gibt es ein $\gamma \in L^\times$ mit $\alpha := \sum_j \varepsilon^j \sigma^j(\gamma) \neq 0$. Es folgt

$$\sigma(\alpha) = \sum_{j \bmod n} \varepsilon^j \sigma^{j+1}(\gamma) = \sum_{i \bmod n} \varepsilon^{i-1} \sigma^i(\gamma) = \varepsilon^{-1} \alpha. \quad \square$$

Definition 3.14.6. Eine **Radikalerweiterung** ist eine Koerpererweiterung L/K so dass $L = K(\alpha)$, so dass es ein $n \in \mathbb{N}$ gibt mit $\alpha^n \in K$.

(L entsteht durch “Wurzelziehen”, lateinisch “radizieren” aus K . Ein Radikal

einer Zahl ist eine Wurzel.)

Definition 3.14.7. Ein irreduzibles Polynom $f(x) \in K[x]$ heisst **aufloesbar in Radikalen**, falls es Koerpererweiterungen

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_n = L$$

gibt, so dass jede K_j/K_{j-1} eine Radikalerweiterung ist und L alle Nullstellen von f enthaelt.

Definition 3.14.8. Die **Galoisgruppe** G_f **eines Polynoms** $f(x) \in K[x]$ ist die Galoisgruppe $\text{Gal}(Z/K)$ des Zerfaellungskoeppers von f .

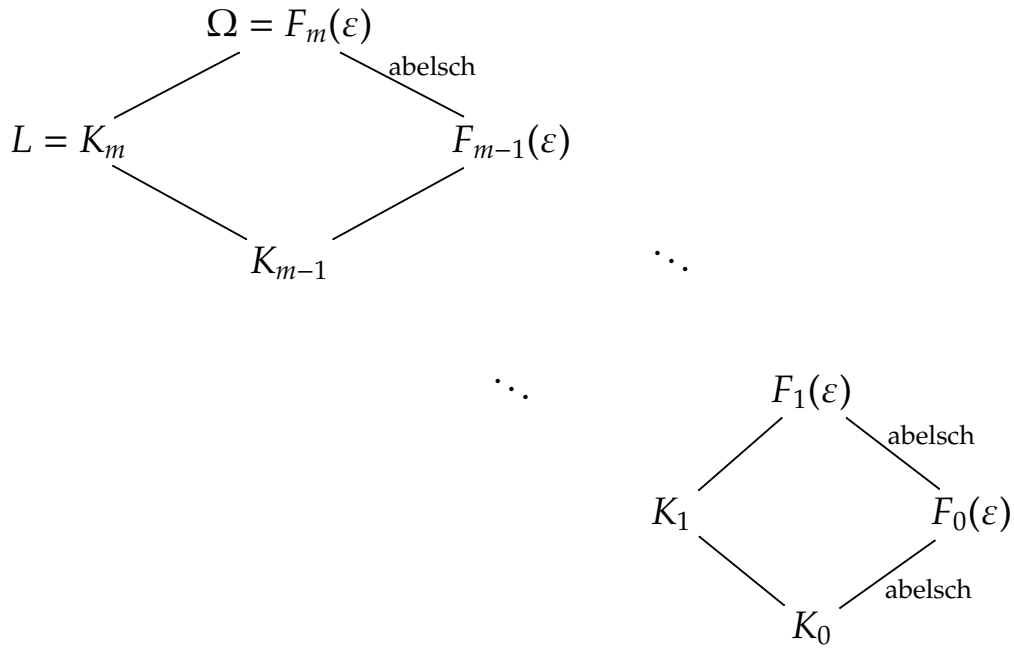
Satz 3.14.9 (Galois). Sei $\text{Char}(K) = 0$. Fuer irreduzibles Polynom $f(x) \in K[x]$ sind aequivalent:

- (a) $f(x)$ ist durch Radikale aufloesbar,
- (b) die Galoisgruppe G_f ist aufloesbar.

Beweis. (a) $\Rightarrow$ (b): Nach Satz 3.14.4 reicht es, zu zeigen, dass G_f Quotient einer aufloesbaren Gruppe ist. Wir haben Koerpererweiterungen $K = K_0 \subset \cdots \subset K_m$ mit $K_j = K_{j-1}(\alpha_j)$ und $\alpha_j^{r_j} \in K_{j-1}$. Sei jeweils F_j die normale Huelle von K_j/K .

Sei $n = r_1 \cdots r_m$ und sei $\Omega = F_m(\varepsilon_n)$. Dann ist Ω/K galoisch. Sei $E = K(\varepsilon_n)$, dann

haben wir die Koerperweiterungen



Sei $N_j = \text{Gal}(\Omega/F_j(\varepsilon))$. Dann ist N_{j-1} normal in N_j , da die Erweiterung $F_j(\varepsilon)/F_{j-1}(\varepsilon)$ galoisch ist. Die Quotienten $N_j/N_{j-1} = \text{Gal}(F_j/F_{j-1})$ sind abelsch nach Proposition 3.14.5. Der Zerfaellungskoeper Z liegt in Ω , die aufloesbare Galoisgruppe $\text{Gal}(\Omega/K)$ bildet surjektiv auf $\text{Gal}(Z/K) = G_f$ ab.

(b) $\Rightarrow$ (a): Das Polynom $f \in K[x]$ habe aufloesbare Galois-Gruppe G_f . Sei $K' = K(\varepsilon)$ mit $\varepsilon = \varepsilon_n$ fuer $n = (\deg(f)!)^!$. Sei G'_f die Galois-Gruppe von f als Element von $K'[x]$. Dann ist G'_f eine Untergruppe von G_f , also auch aufloesbar. Es gibt also Untergruppen

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{1\},$$

so dass G_{j-1}/G_j zyklisch ist. Sei L der Zerfaellungskoeper von $f(x)$ ueber K' und sei $F_j = L^{G_j}$. Dann

$$K \subset K(\varepsilon) = K' = K_0 \subset \cdots \subset K_m = L,$$

wobei K_j/K_{j-1} zyklisch ist. Nach Proposition 3.14.5 ist $K_j = K_{j-1}(\alpha_j)$ mit $\alpha_j^{[K_j:K_{j-1}]} \in K_{j-1}$, also ist f in Radikalen aufloesbar. □

3.15 Unendliche Erweiterungen

Definition 3.15.1. Sei L/K eine Körpererweiterung. Eine Teilmenge $S \subset L$ heisst **algebraisch unabhängig** über K , falls aus einer Gleichung der Art

$$P(s_1, \dots, s_n) = 0, \quad s_1, \dots, s_n \in S$$

für ein Polynom $P \in K[x_1, \dots, x_n]$ schon folgt, dass P das Nullpolynom ist, also $P = 0$ gilt.

Mit dem Lemma von Zorn macht man sich klar, dass es zu jeder Körpererweiterung L/K eine maximale algebraisch unabhängige Menge $S \subset L$ gibt. Man nennt eine solche Menge eine **Transzendenzbasis** von L über K .

Beispiel 3.15.2. Ist $L/K = \mathbb{C}(X, Y)/\mathbb{C}$ mit Variablen X, Y , dann ist X, Y eine Transzendenzbasis.

Satz 3.15.3. Sei L/K eine Körpererweiterung.

- (a) Ist $S \subset L$ eine Transzendenzbasis, so ist $L/K(S)$ algebraisch.
- (b) Je zwei Transzendenzbasen haben dieselbe Mächtigkeit. Diese wird der **Transzendenzgrad** von L über K genannt.
- (c) Ist $\Gamma \subset L$ irgendeine Erzeugermenge, d.h., es gilt $L = K(\Gamma)$ und ist $\Sigma \subset \Gamma$ eine algebraisch unabhängige Teilmenge, dann existiert eine Transzendenzbasis S mit $\Sigma \subset S \subset \Gamma$.

Beweis. (a) ist klar.

(b) Seien S und T Transzendenzbasen. Es reicht zu zeigen $|S| \leq |T|$. Wir nehmen zunäcchst an, dass T endlich ist und benutzen Induktion nach $n = |T|$. Ist $n = 0$, dann ist L algebraisch ueber K und jede Transzendenzbasis ist leer. Nimm also $n \geq 1$ an und sei $s \in S$. Nach Zorns Lemma gibt es eine maximale Teilmenge

$T_s \subset T$ so dass $s \notin T_s$ und $\{s\} \cup T_s$ algebraisch unabhangig ist. Dann muss $|T_s| < n$ sein. Sei $K_1 = K(s)$ und $S' = S \setminus \{s\}$. Dann sind T_s und S' jeweils algebraisch unabhangig ueber dem Korper K_1 , nach Induktionsvoraussetzung ist also $|T_s| \geq |S'|$ und damit $|T| \geq |S|$.

Sei nun T unendlich. Jedes $x \in T$ ist algebraisch ueber S , es gibt also eine endliche Teilmenge $S(x) \subset S$ so dass x algebraisch ueber $K(S(x))$ ist. Sei $S' = \bigcup_{x \in T} S(x) \subset S$ und da T unendlich ist, ist $|S'| \leq |T|$. Da jedes Element von T algebraisch ueber $K(S')$ und jedes Element von L algebraisch ueber $K(T)$, ist jedes Element von L auch algebraisch ueber $K(S')$ und daher ist S' eine Transzendenzbasis, also $S' = S$.

(c) ist mit Zorns Lemma klar. □

Bei nicht-algebraischen Erweiterungen geht die Galois-Theorie schief. Das zeigt der folgende Satz.

Satz 3.15.4. *Sei K ein algebraisch abgeschlossener Korper und sei $L = K(t) = \text{Quot}(K[t])$ der rationale Funktionenkorper.*

- (a) *Es ist $G = \text{Gal}(L/K) \cong \text{PGL}_2(K) := \text{GL}_2(K)/K^\times I$.*
- (b) *Sei H die Untergruppe von G isomorph zu $\left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in K \right\}$. Dann ist $L^H = K$. Insbesondere ist bei transzendenten Erweiterungen der Hauptsatz der Galois-Theorie verletzt, denn $\text{Gal}(L/L^H) \neq H$.*

Beweis. (a) Jedes Element von L kann in der Form $\alpha = \frac{a(t)}{b(t)}$ geschrieben werden wobei $a, b \in K[t]$, das Polynom b ist normiert und a und b haben keine gemeinsamen Nullstellen. Wir wollen α als Funktion von $\hat{K} = K \cup \{\infty\}$ in sich auffassen, indem wir sagen $\alpha(c) = \infty$, wenn $c \in K$ eine Nullstelle von b ist. Ferner

soll

$$\alpha(\infty) = \begin{cases} 0 & \text{grad}(a) < \text{grad}(b), \\ \infty & \text{grad}(a) > \text{grad}(b), \\ \frac{\text{Leitkoeffizient von } a}{\text{Leitkoeffizient von } b} & \text{grad}(a) = \text{grad}(b) \end{cases}$$

sein. Jedes $\alpha \in K$ liefert dann die konstante Abbildung. Wir behaupten, dass jedes $\alpha \in L \setminus K$ eine surjektive Abbildung $\hat{K} \rightarrow \hat{K}$ liefert. Sei hierzu $c \in K$. Dann ist $\alpha(x) = c$ äquivalent zu $a(x) = cb(x)$ und diese polynomiale Gleichung hat in dem algebraisch abgeschlossenen Körper K eine Lösung, es sei denn $c = 0$ und a ist konstant. In diesem Fall ist aber $\alpha(\infty) = c$, also hat $c \in K$ in jedem Fall ein Urbild. Ist $c = \infty$, so beachte, dass $\alpha(y) = \infty$, wenn y eine Nullstelle von b ist. Hat b keine Nullstellen, dann gilt $\alpha(\infty) = \infty$, also hat auch ∞ ein Urbild.

Sei nun $\sigma \in G$, dann ist $\sigma(t) = \frac{p(t)}{q(t)}$, $\sigma^{-1}(t) = \frac{f(t)}{g(t)}$, also folgt

$$t = \frac{f(p(t)/q(t))}{g(p(t)/q(t))}.$$

Als nichttriviale rationale Funktion nimmt p/q als Abbildung von $K \cup \{\infty\}$ in sich jeden Wert an, insbesondere die Polstellen von f/g . Da t nur einen Pol hat, kann f/g auch nur einen Pol besitzen, also $\text{grad}(g) \leq 1$. Dasselbe gilt für Nullstellen, so dass $\text{grad}(f) \leq 1$.

(b) Sei $f/g \in K(t)$ f, g teilerfremd zueinander mit $f/g \in L^H$. Dann sind die Nullstellen von f invariant unter Translation, also ist f konstant. Ebenso ist g konstant. □

Definition 3.15.5. Sei K ein Körper der Charakteristik Null (damit es keine inseparablen Erweiterungen gibt). Die **absolute Galois-Gruppe** zu K ist

$$\Gamma_K = \text{Gal}(\bar{K}/K).$$

Lemma 3.15.6. (a) Ist L/K endlich galoisch, dann ist die Abbildung

$$\Gamma_K/\Gamma_L \rightarrow \text{Gal}(L/K) \text{ ein Isomorphismus.}$$

(b) Der Körper K ist der Fixkörper von Γ_K , also

$$(\overline{K})^{\Gamma_K} = K.$$

Proof. (a) Kennen wir schon fuer endliche Galois-Erweiterungen, der Beweis benutzt aber die Endlichkeit gar nicht.

(b) Ist $x \in \overline{K}$, dann liegt x in einer endlichen Galois-Erweiterung L/K . Nach (a) ist x Fixpunkt von $\text{Gal}(L/K)$ und damit $x \in K$. $\square$

Satz 3.15.7. Die Abbildung

$$\Gamma_K \rightarrow \prod_{L/K \text{ endlich galoisch}} \text{Gal}(L/K)$$

ist injektiv. Das Bild ist die Menge aller $(\sigma_L)_L$ mit der Kompatibilitaetseigenschaft

$$\sigma_L|_F = \sigma_F,$$

falls $L/F/K$ und F/K galoisch.

Beweis. Sei σ im Kern dieser Abbildung und sei $x \in \overline{K}$. Dann liegt x in einer endlichen Galois-Erweiterung L/K . Sei σ_L das Bild von σ in $\text{Gal}(L/K)$, dann gilt

$$\sigma(x) = \sigma_L(x) = \text{Id}(x) = x.$$

Da x beliebig ist, folgt $\sigma = 1$.

Ist eine Familie $(\sigma_L)_L$ das Bild eines $\sigma \in \Gamma_K$, dann ist die Kompatibilitaetseigenschaft klar. Sei umgekehrt eine kompatible Familie $(\gamma_L)_L$ gegeben. Wir konstruieren ein $\sigma \in \Gamma_K$, so dass $\sigma_L = \gamma_L$ gilt. Sei also $x \in \overline{K}$. Dann liegt x in einer endlichen Galois-Erweiterung L/K und wir definieren $\sigma(x) := \gamma_L(x)$. Wir muessen Wohldefiniertheit checken: Ist L'/K eine weitere

endliche Galois-Erweiterung mit $x \in L'$, dann betrachten wir das Kompositum $F = LL'$ und wir haben wegen der Kompatibilit  t:

$$\gamma_L(x) = \gamma_F(x) = \gamma_{L'}(x).$$

Damit ist σ wohldefiniert und erf  ll $\sigma_L = \gamma_L$.

□