Algebra

Anton Deitmar

Inhaltsverzeichnis

1 Gruppen

1.1 Permutationen

Für eine beliebige Menge M bezeichnen wir mit $\mathrm{Per}(M)$ die Gruppe der **Permutationen** von M, d.h., die Menge aller bijektiven Abbildungen $\sigma : M \to M$ mit der Hintereinanderausführung als Gruppenmultiplikation. Für eine natürliche Zahl n sei dann $\mathrm{Per}(n)$ die Gruppe $\mathrm{Per}(\{1, \ldots, n\})$. Wir nennen $\mathrm{Per}(n)$ auch die Gruppe der Permutationen in n Buchstaben.

Die Elemente der Permutationsgruppe $\mathrm{Per}(n)$ schreibt man zB in der Form $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$. Eine andere Schreibweise für dasselbe Element ist die **Zykelschreibweise**:

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

was soviel bedeutet wie 1 geht auf 2 geht auf 3 geht auf 1. Das Element, das 1 und 2 vertauscht, schreibt sich dann als $(1, 2)$. Nicht jedes Element von $\mathrm{Per}(n)$ ist als ein einziger Zykel schreibbar, so ist zum Beispiel in Per(4) das Element $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ in der Zykelschreibweise gleich

$$(1, 2)(3, 4).$$

Definition 1.1.1. Ein **Zykel** in $\mathrm{Per}(n)$ ist ein Tupel $(j_1, j_2, \ldots, j_r)$, $r \geq 2$ von verschiedenen natürlichen Zahlen $1 \leq j_1, j_2, \ldots, j_r \leq n$. Ein Zykel repräsentiert eine Permutation, die j_ν auf $j_{\nu+1}$ und j_r auf j_1 wirft und alle anderen Zahlen festhält. Der Zykel $(j_1, \ldots, j_r)$ repräsentiert dieselbe Permutation wie der Zykel $(j_2, j_3, \ldots, j_r, j_1)$, deshalb kann man den Zykel stets durch einen ersetzen, für den j_1 die kleinste der Zahlen $j_1, \ldots, j_k$ ist. Ein Zykel in dieser Form heisst **kanonisch**.

Zwei Zykel $(j_1, \ldots, j_k)$ und $(i_1, \ldots, i_s)$ heissen **disjunkt**, falls sie keine gemeinsamen Zahlen haben, also falls

$$\{j_1, \ldots, j_k\} \cap \{i_1, \ldots, i_s\} = \emptyset.$$

Beispiel 1.1.2. Wir schreiben die Permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 6 & 7 & 5 & 2 & 4 & 3 \end{pmatrix}$ als Produkt kanonischer Zykel:

$$(2, 6, 4, 5)(3, 7).$$

Satz 1.1.3.

(a) *Zwei kanonische Zykel stellen genau dann dieselbe Permutation dar, wenn sie gleich sind.*

(b) *Zwei disjunkte Zykel, aufgefasst als Elemente von* $\mathrm{Per}(n)$, *kommutieren miteinander.*

(c) *Jede Permutation* $\neq \mathrm{Id}$ *in* $\mathrm{Per}(n)$ *lässt sich als Produkt paarweise disjunkter kanonischer Zykel schreiben, diese sind eindeutig bestimmt bis auf die Reihenfolge.*

Beweis. (a) Seien $(j_1, j_2, \ldots, j_r)$ und $(i_1, i_2, \ldots, i_s)$ zwei kanonische Zykel, die dieselbe Permutation γ darstellen. Dann ist j_1 das kleinste Element von $\{1, \ldots, n\}$, das von γ überhaupt vertauscht wird und dasselbe gilt von i_1, also folgt $j_1 = i_1$. Ferner ist $j_2 = \gamma(j_1) = \gamma(i_1) = i_2$ und so weiter.

(b) Sei $\gamma = (j_1, \ldots, j_k)$ ein Zykel in $\mathrm{Per}(n)$ und sei $\tau \in \mathrm{Per}(n)$. Es gilt dann

$$\tau\gamma\tau^{-1} = (\tau(j_1), \ldots, \tau(j_k)).$$

Ist $\tau = (i_1, \ldots, i_s)$ auch ein Zykel, dann sind die $i_1, \ldots, i_s$ genau die Zahlen, die von τ überhaupt verändert werden. Ist also τ zu γ disjunkt, so folgt $\tau\gamma\tau^{-1} = \gamma$.

(c) Wir geben ein Verfahren zum Finden der Zykel zu einem gegebenen $\gamma \in \mathrm{Per}(n)$. Sei j_1 die kleinste Zahl in $\{1, \ldots, n\}$, die von γ überhaupt verändert wird. Sei dann $j_2 = \gamma(j_1)$ und so weiter. Die Folge $j_1, j_2, \ldots$ kann nicht unendlich sein, also gibt es ein kleinstes $k \in \mathbb{N}$ und zu diesem ein kleinstes $s \in \mathbb{N}$ so dass $j_{k+s} = j_k$ gilt. Das heisst also $\gamma(j_{k+s-1}) = j_k$. Ist $k > 1$, so gilt aber auch $\gamma(j_{k-1}) = j_k$, woraus aber $j_{k+s-1} = j_{k-1}$ folgt, was der Minimalität von k widerspricht. Es ist also $k = 1$ und damit ist $\alpha = (j_1, \ldots, j_s)$ ein Zykel, der die Zahlen $(j_1, \ldots, j_s)$ genauso abbildet wie γ, so dass $\alpha^{-1}\gamma$ sie alle festhält. Dieser ist dann gleich e oder nicht, in welchem Fall wir das Verfahren wiederholen und einen zweiten Zykel β finden, der disjunkt zu α ist und so weiter. Das Verfahren bricht wegen Endlichkeit des Problems ab. □

Beispiel 1.1.4. Wir können die Elemente von Per(3) als Zykel hinschreiben:
$e, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)$.

1.2 Ordnung

Definition 1.2.1. Ist G eine endliche Gruppe, so nennt man die Anzahl $|G|$ der Elemente die **Ordnung** der Gruppe G,

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

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:

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

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

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

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

Beispiel 1.2.2. Ist $z \in \mathrm{Per}(n)$ ein Zykel $z = (j_1, \ldots, j_k)$, dann gilt

$$\mathrm{ord}(z) = k.$$

Wir nennen k dann wahlweise die Ordnung oder die **Länge** des Zykels z.

Lemma 1.2.3. *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*

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

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

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

Beweis. Sei $\langle a \rangle$ endlich. Da die Elemente $1, a, a^2, \ldots$ nicht alle verschieden sein können, gibt es ein $m, n \in \mathbb{N}$ so dann $a^m = a^{m+n}$, also $1 = a^n$ gilt. Die Umkehrung ist klar, da $\langle a \rangle$ genau aus den Potenzen von a besteht. Ist schliesslich $k \in \mathbb{N}$ die kleinste natürliche Zahl mit $a^k = 1$, dann besteht $\langle a \rangle$ genau aus den Elementen $1, a, a^2, \ldots, a^{k-1}$.

Zum Schluss sei $k = \mathrm{ord}(a)$ und $a^n = 1$. Dann folgt $n \geq k$, wir können also $n = rk + s$ schreiben mit $0 \leq s < k$. Es ist dann

$$1 = a^n = a^{rk+s} = (a^k)^r a^s = a^s,$$

so dass $s = 0$, also $k \mid n$ folgt. Die Umkehrung ist klar. □

Lemma 1.2.4. *Ist G eine abelsche Gruppe und $a, b \in G$ von endlichen Ordnungen m, n. Sind m und n teilerfremd, dann hat ab die Ordnung mn.*

Beweis. Ist $1 = (ab)^k = a^k b^k$, 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. □

Definition 1.2.5. 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

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

Beispiele 1.2.6.

- 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 $\{0, 1, 2, \ldots, m-1\}$ mit Verknüpfung: $a \boxplus b =$ Rest von $a + b$ modulo m.
- Sei $n \in \mathbb{N}$ die **Diedergruppe** D_{2n} der Ordnung $2n$ ist eine Gruppe erzeugt von zwei Elementen σ, τ mit den Relationen

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

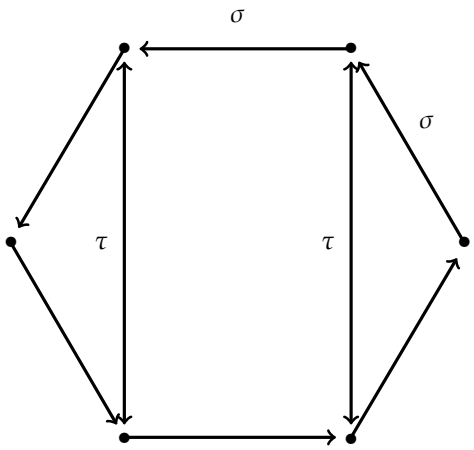
Insbesondere soll σ die Ordnung n haben und τ die Ordnung 2.

Das bedeutet, D_{2n} besteht genau aus den Elementen

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

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

Man kann sie als Untergruppe von Per(n) wie folgt darstellen. Stellen wir uns die Elemente von $\{1, 2, \ldots, n\}$ 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 $\{1, \ldots, n\}$ in sich abbildet.



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

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

Proposition 1.2.7. *Ist $g \in$ Per(n) eine Permutation, die wir gemäß Satz 1.1.3 als Produkt disjunkter Zykel schreiben:*

$$g = z_1 \cdots z_k$$

und sei $l_j = l(z_j)$ die jeweilige Länge des j-ten Zykels. Dann gilt

$$\text{ord}(g) = \text{kgV}(l_1, \ldots, l_k).$$

Beweis. Die z_j vertauschen miteinander. Da jedes z_j eine andere Teilmenge von $\{1, \ldots, n\}$ permutiert, folgt für $\nu \in \mathbb{N}$

$$g^\nu = 1 \quad \Leftrightarrow \quad z_j^\nu = 1 \text{ für jedes } j = 1, \ldots, k.$$

Dies ist genau dann der Fall, wenn ν ein Vielfaches von $\text{ord}(z_j) = l_j$ ist für jedes j, daher ist die Ordnung $\text{ord}(g) = \min\{\nu \in \mathbb{N} : g^\nu = 1\}$ das kleinste gemeinsame Vielfache der Einzelordnungen. □

1.3 Nebenklassen

Definition 1.3.1. 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

$$hH = H.$$

Beispiele 1.3.2.

- 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.
- Sei $G = D_{2n}$ die Diedergruppe und sei $H = \langle \tau \rangle$ die von τ erzeugte Untergruppe, dann ist $H = \{1, \tau\}$ und die H-Linksnebenklassen sind

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

Lemma 1.3.3. *Sei G eine Gruppe und H eine Untergruppe. 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 $u = xh_3 = y \underbrace{h_2h_1^{-1}h_3}_{\in H} \in yH$. □

Proposition 1.3.4. *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

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

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

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

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

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

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 $\mathrm{ord}(H)$ viele, es ist also

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

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

1.4 Homomorphismen und Operationen

Definition 1.4.1. Eine Abbildung $\phi : G \to H$ zwischen zwei Gruppen heisst **Gruppenhomomorphismus**, falls

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

für alle $a, b \in G$ gilt.

Lemma 1.4.2. *Ist $\phi : G \to H$ ein Gruppenhomomorphismus, dann gilt $\phi(1) = 1$ und $\phi(a^{-1}) = \phi(a)^{-1}$.*

Beweis. Übungsaufgabe Blatt 1. □

Beispiele 1.4.3.

- Ist G eine Gruppe und ist $a \in G$, dann ist die Abbildung

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

  Ein Homomorphismus von G nach G.

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

- Sind V, W Vektorräume über einem Körper K, so ist jede lineare Abbildung $T : V \to W$ ein Gruppenhomomorphismus $(V, +) \to (W, +)$.

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

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

  ein Gruppenhomomorphismus.

- Ist $G = \mathrm{Per}(n)$ die Gruppe der Permutationen in $\{1, \ldots, n\}$, dann ist die Vorzeichen- oder **Signumabbildung**

  $$\mathrm{sign} : \mathrm{Per}(n) \to \{\pm 1\}$$

  ein Gruppenhomomorphismus, wie in der Linearen Algebra gezeigt wird.

Definition 1.4.4. Sei G eine Gruppe und M eine Menge. Eine **Operation** von G auf M ist eine Abbildung

$$G \times M \to M$$
$$(g, m) \mapsto g.m$$

mit den Eigenschaften

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

Beispiele 1.4.5.

- 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 $(ab).m = (ab)m = a(bm) = a.(b.m)$. □

- 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 $(ab).m = m(ab)^{-1} = (mb^{-1})a^{-1} = a.(b.m)$. □

- Sei G eine Gruppe, dann operiert G auf sich selbst durch die Vorschrift

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

dies ist die **Konjugationsoperation**.

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

- (Abgeleitete Operationen.) Operiert die Gruppe G auf der Menge M und ist S eine weitere Menge, dann operiert G auf der Menge $A = \mathrm{Abb}(M, S)$ 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
$(ab).\phi(m) = \phi((ab)^{-1}.m) = \phi(b^{-1}.a^{-1}.m) = b.\phi(a^{-1}.m) = a.(b.\phi)(m)$. □

Lemma 1.4.6. *Sei $M \neq \emptyset$ eine Menge. Operiert die Gruppe G auf der Menge M, dann ist die Abbildung $\phi : G \to \mathrm{Per}(M)$, $g \mapsto (m \mapsto gm)$ ein Gruppenhomomorphismus. Ist umgekehrt $\phi : G \to \mathrm{Per}(M)$ ein Gruppenhomomorphismus, dann definiert*

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

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

Beweis. Die Gruppe G operiere auf M. Für $g \in G$ sei $\phi(g) : M \to M$, $m \mapsto gm$. Zunächst müssen wir zeigen, dass $\phi(g)$ bijektiv ist, wir also wirklich in $\mathrm{Per}(M)$ 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 $\phi : G \to \mathrm{Per}(M)$. 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 Gruppenhomorphismus. Die Umgekehrte Richtung ist leicht nachzurechnen und die Tatsache, dass diese Zuordnungen invers zueinander sind, auch. □

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

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

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

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

der **Stabilisator** von m.

Satz 1.4.7. *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 Orbiten zweier Punkte sind entweder gleich oder disjunkt, man kann deshalb M disjunkt in seine Orbiten zerlegen. Man schreibt $G\backslash M$ für die Menge aller Orbiten.*

(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 $\psi : G/H \to Gm$ 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). □

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

$$Z(G) = \left\{x \in G : xy = yx \; \forall_{y \in G}\right\}.$$

Beispiele 1.4.8.

- Ist G abelsch, so gilt $Z(G) = G$ und umgekehrt.
- Ist $G = \mathrm{GL}_n(K)$ für einen Körper K, dann besteht das Zentrum aus die Matrizen der Form λI, wobei $\lambda \in K^\times$. Dies ist eine Übungsaufgabe der Linearen Algebra. (Man löse zuerst den Fall $n = 2$, dann sieht man auch den allgemeinen Beweis.)
- Ist $n \geq 3$, dann ist das Zentrum von $G = \mathrm{Per}(n)$ die triviale Gruppe.

  Beweis. Sei σ im Zentrum von $\mathrm{Per}(n)$ 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 $\sigma(j) = \sigma(\tau(i)) = \tau(\sigma(i))$. Waere nun $\sigma(i)$ von i und j verschieden, dann waere $\sigma(j) = \tau(\sigma(i)) = \sigma(i)$, was der Injektivitaet 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 $\sigma = \mathrm{Id}$. □

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

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

Satz 1.4.9 (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*

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

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

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

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

1.5 Zyklische Gruppen

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

Beispiele 1.5.1.

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

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 $\mathbb{Z}/n \to G$, $k \mapsto \tau^k$ ein Gruppenisomorphismus.
2. Fall. τ hat keine endliche Ordnung. Dann ist die Abbildung $\mathbb{Z} \to G$, $k \mapsto \tau^k$ 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 1.5.3. *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 $\operatorname{ord}(\tau)$ ein Teiler von p sein. Da $\tau \neq e$, ist die Ordnung $\neq 1$, also ist $\operatorname{ord}(\tau) = p$, damit hat die zyklische Untergruppe $\langle \tau \rangle$, die von τ erzeugt wird, die Ordnung p, ist also gleich G. □

Satz 1.5.4. *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 $(\mathbb{Z}/2) \times (\mathbb{Z}/2) \to G$, $(i, j) \mapsto a^i b^j$ einen injektiven Gruppenhomomorphismus. Das Bild hat Ordnung 4, ist also G und G damit isomorph zur Vierergruppe. □

Satz 1.5.5. *Jede Untergruppe einer zyklischen Gruppe ist zyklisch.*

Proof. Sei $G = \langle \tau \rangle$ eine zyklische Gruppe und sei $\{1\} \neq H \subset G$ eine Untergruppe. Sei N die kleinste natuerliche Zahl mit $\gamma = \tau^N \in H$. Wir zeigen, dass H von γ erzeugt ist. Sei hierzu $h = \tau^n \in H$, dann ist $h\gamma^k = \tau^{n+kN} \in H$. Es gibt ein $k \in \mathbb{Z}$ mit $0 \leq n + kN < N$. Aus der Minimalitaet von N folgt $n + kN = 0$ und daher $h = \gamma^{-k}$. □

1.6 Normalteiler

Definition 1.6.1. Sei $\phi : G \to H$ ein Gruppenhomomorphismus. Der **Kern** von ϕ ist die Menge

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

Lemma 1.6.2. *Sei $\phi : G \to H$ 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 1.6.3. Eine Untergruppe $N \subset G$ mit der Eigenschaft aus dem Lemma heisst **Normalteiler** von G.

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 1.6.4.

- Ist G abelsch, dann ist jede Untergruppe ein Normalteiler.
- Sei $G = \mathrm{Per}(3)$ und H die Untergruppe erzeugt von $(1,2)$. Dann ist H kein Normalteiler, denn mit dem Element $\gamma = (1,3)$ gilt
$$\gamma(1,2)\gamma^{-1} = (2,3).$$
- 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 $gZg^{-1} = Z$. □
- Ist G eine Gruppe und H eine Untergruppe vom Index 2, dann ist H ein Normalteiler.

  Beweis. Es gibt genau zwei Linksnebenklassen $G = H \sqcup sH$, 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. □

Satz 1.6.5. *Ist $N \subset G$ ein Normalteiler, so lässt sich auf der Menge der Nebenklassen G/N genau eine Gruppenstruktur installieren, so dass die Projektion $G \to G/N$ ein Gruppenhomomorphismus ist.*

Ist umgekehrt $H \subset G$ eine Untergruppe mit einer Gruppenstruktur auf dem Nebenklassenraum G/H so dass die Projektion $G \to G/H$ 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 1.6.2, 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 $G \to G/N$ ein Homomorphismus ist. Da dieser surjektiv ist, ist die Gruppenstruktur eindeutig bestimmt. □

Beispiel 1.6.6. 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.

Proposition 1.6.7. *Sei G eine Gruppe mit Zentrum Z. Ist G/Z zyklisch, dann ist G abelsch.*

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

$$bc = a^m z a^n w = a^n w a^m z = cb. \qquad \square$$

Korollar 1.6.8. *Sei G eine Gruppe und Z ihr Zentrum. Dann kann die Ordnung von G/Z keine Primzahl sein.*

Beweis. Ist $\mathrm{ord}(G/Z)$ eine Primzahl, dann ist G/Z nach Satz 1.5.3 zyklisch, dann ist G aber abelsch nach Proposition 1.6.7, somit also $G = Z$ und damit $G/Z = \{e\}$. $\square$

1.7 Homomorphiesätze

Definition 1.7.1. Ein Gruppenhomomorphismus $f : G \to H$ heisst **Isomorphismus**, wenn es einen Gruppenhomomorphismus $g : H \to G$ gibt so dass $f \circ g = \mathrm{Id}_H$ und $g \circ f = \mathrm{Id}_G$ ist.

Lemma 1.7.2. *Ein Gruppenhomomorphismus $f : G \to H$ 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 $g : H \to G$ die Umkehrabbildung. Für $x, y \in H$ gilt

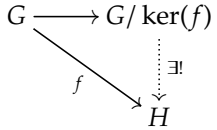
$$f(g(xy)) = xy = f(g(x))f(g(y)) = f(g(x)g(y))$$

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

Satz 1.7.3. *Sei $f : G \to H$ ein Gruppenhomomorphismus. Dann ist das Bild eine Untergruppe und f induziert einen Isomorphismus*

$$G/\ker(f) \xrightarrow{\cong} \mathrm{Bild}(f).$$

Beweis. Ist $x \in \mathrm{Bild}\, f$, sagen wir $x = f(a)$, dann ist $x^{-1} = f(a^{-1})$ ebenfalls im Bild von f. Sind ferner $x, y \in \mathrm{Bild}(f)$, sagen wir $x = f(a)$ und $y = f(b)$, dann ist $xy = f(ab)$ ebenfalls im Bild. Zusammen folgt, dass das Bild eine Untergruppe ist. Nun ist $\ker(f)$ ein Normalteiler, also existiert die Gruppe $G/\ker(f)$ und wegen $f(x) = f(xn)$ falls $n \in \ker(f)$, faktorisiert die Abbildung f über $G/\ker(f)$, d.h., es existiert genau eine Abbildung $G/\ker(f) \to H$, so dass das Diagramm



kommutiert. Diese Abbildung, nennen wir sie h, ist wegen
$h([x][y]) = h([xy]) = f(xy) = f(x)f(y) = h([x])h([y])$ ein Gruppenhomomorphismus. Sie ist injektiv, denn aus $h([x]) = h([y])$ folgt $e = h([x][y]^{-1}) = f(xy^{-1})$ und daher $xy^{-1} \in \ker(f)$, so dass
$[x] = x\ker(f) = y\ker(f) = [y]$. Da sie surjektiv auf Bild(f) ist, ist sie der Isomorphismus des Satzes. □

Lemma 1.7.4. *Sei G eine endliche abelsche Gruppe und für $n \in \mathbb{N}$ sei die n-***Torsion** *von G definiert durch*

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

Gilt $\left|G[n]\right| \leq n$ 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

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

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 1.2.4 das Element ab die Ordnung $mn = |G|$ hat, G also zyklisch ist. □

Satz 1.7.5. (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*

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

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

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

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

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

Beweis. (a) Um zu sehen, dass N/M ein Normalteiler ist, sei $xM \in G/M$, dann gilt $xNx^{-1} = N$, also auch $(xM)NM(xM)^{-1} = NM$. Sei $\phi : (G/M)\Big/(N/M) \to G/N$, $\phi(xM) = xN$. Dann ist ϕ ein

Gruppenhomomorphismus und wegen $xN = N \Leftrightarrow x \in N \Leftrightarrow xM \in N/M$ ist ϕ injektiv. Surjektiv ist es sowieso.

(b) Wegen $mnm_1n_1 = mm_1(m_1^{-1}nm_1)n_1$ ist MN abgeschlossen unter der Multiplikation und wegen $(mn)^{-1} = n^{-1}m^{-1} = (n^{-1}m^{-1}n)n^{-1} \in MN$ ist es eine Untergruppe. Die Bijektivität der genannten Abbildung sieht man analog zum obigen ein. □

Korollar 1.7.6. *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. □

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

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

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

Satz 1.7.7. (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. □

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 $\mathrm{ord}(H) = p^k$, $k \in \mathbb{N}$ und $\mathrm{ord}(G) = p^k m$ 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

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

Ist einer der Summanden $(G : G_{x_j})$ 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 koennen 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 $\operatorname{ord}(Z)$ teilen. □

Korollar 1.8.4. *Sei p eine Primzahl und G eine Gruppe der Ordnung p^k für ein $k \in \mathbb{N}$. Dann gibt es eine Kette von Untergruppen*

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

so dass $\operatorname{ord}(G_j) = p^j$ *gilt und G_{j-1} ein Normalteiler in G_j ist. 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. Zunächst machen wir uns klar, dass, wenn die Behauptung für einen Normalteiler N von G und für den Quotienten G/N gilt, dann gilt sie für G, denn ist $N_0 \subset \cdots \subset N_k$ die Kette von N und $(G/N)_0 \subset \cdots \subset (G/N)_s$ die Kette von G/N, sowie $P : G \to G/N$ die Projektion, dann erfüllt die Kette $G_0 = N_0, \ldots, G_k = N_k$ und $G_{k+j} = P^{-1}((G/N)_j)$ die Bedingung für G.

Wir beweisen nun die Behauptung durch Induktion nach k. Für $k = 0, 1$ ist nicht zu zeigen. Sei also die Behauptung für alle Ordnungen $\leq p^k$ gezeigt und sei $\operatorname{ord}(G) = p^{k+1}$. Da das Zentrum Z von G nichttrivial ist, gibt es ein Element $x \neq 1$ in Z. Sei p^j die Ordnung von x, dann hat $y = x^{p^{j-1}}$ die Ordnung p. Wir verwenden nun den obigen Schluss für $N = \langle y \rangle$. □

Satz 1.8.5. *Sei p eine Primzahl und G eine Gruppe der Ordnung p^2. Dann ist G abelsch, genauer ist*

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

Beweis. Das Zentrum Z ist nichttrivial, also ist die Ordnung von G/Z gleich 1 oder p. Das zweite ist nach Korollar 1.6.8 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

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

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 $\operatorname{ord}(\langle x \rangle) = p$. 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. □

Definition 1.8.6. 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 natuerliche Zahl N, fuer die dies der Fall ist, heisst der **Exponent** von G.

Beispiel 1.8.7. Die Gruppe $G = \prod_{j=1}^{\infty} \mathbb{Z}/2$ ist eine unendliche Gruppe vom Exponenten 2.

Lemma 1.8.8. *Sei G eine endliche abelsche Gruppe und p eine Primzahl, die die Gruppenordnung teilt. Dann enthält G ein Element der Ordnung p.*

Beweis. Sei G eine endliche abelsche Gruppe vom Exponenten N. Wir zeigen, dass dann die Gruppenordnung eine Potenz von N teilt. 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.

Wir folgern nun, dass die abelsche Gruppe G mit $p \mid \operatorname{ord}(G)$ ein Element x haben muss mit Ordnung $p^k m$ für ein $k \in \mathbb{N}$. Wäre dies nicht der Fall, hätten alle Elemente Ordnungen teilerfremd zu p und deren Produkt wäre ein Exponent teilerfremd zu p, was aber der Tatsache, dass die Gruppenordnung eine Potenz des Exponenten teilt, widerspricht.

Habe also das Element x die Ordnung $p^k m$ mit $p \nmid m$. Dann hat $y = x^{mp^{k-1}}$ die Ordnung p. □

Satz 1.8.9 (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*

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

Beweis. Wir zeigen die Existenz einer p-Sylowgruppe durch Induktion nach der Ordnung von G. Ist $p = \mathrm{ord}(G)$ sind wir fertig. Sei also $\mathrm{ord}(G) = p^k m$ 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

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

wobei Z das Zentrum von G ist und die x_j Vertreter der nichttrivialen Konjgationsklassen. Die Summanden rechts werden nach Voraussetzung alle von p geteilt, damit auch $\mathrm{ord}(Z)$. Nach Lemma 1.8.8 enthält Z ein Element z der Ordnung p. Sei dann S eine p-Sylow-Gruppe von $G/\langle z\rangle$ und sei $P : G \to G/\langle z\rangle$ die Projektion. Dann ist $P^{-1}(S)$ eine p-Sylow-Gruppe von G. Es gibt also eine p-Sylow-Gruppe.

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

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

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. Gleichzeitig ist aber gezeigt, dass jede p-Gruppe H in einer P_ν enthalten ist. 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.

Die Anzahl s der p-Sylow-Gruppen ist dann gleich $(G : G_P)$ und damit ein Teiler von $\mathrm{ord}(G)$.

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 $s \equiv \frac{|P|}{|P|} = 1 \mod p$. □

Definition 1.8.10. Eine Gruppe G heisst **einfach**, wenn sie keinen echten Normalteiler hat, also keinenNormalteiler ausser $\{1\}$ und G.

Beispiele 1.8.11.

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

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

Korollar 1.8.12. *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. □

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 $G/[G, G]$ is abelsch und $[G, G]$ ist der kleinste Normalteiler mit abelschem Quotienten. Andersherum ist $G/[G, G]$ der groesste 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 $\phi : G \to H$ 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 $\phi : G \to G$, $x \mapsto gxg^{-1}$, 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 uns sei $\phi : G \to G/N$ der entsprechende Gruppenhomomorphismus. Dann ist, da G/N abelsch ist, $\phi([a, b]0 = [\phi(a), \phi(b)] = 1$, also liegt $[G, G]$ im Kern von ϕ, mit anderen Worten $[G, G] \subset N$, wie verlangt. □

Definition 1.9.3. Sei G eine Gruppe. Fuer 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 $G_{j+1} = [G, G_j]$ fuer $j = 0, 1, \ldots$. So folgt $G_0 \supset G_1 \supset \ldots$ 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 $G_n = \{1\}$ fuer 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 fuer $g \in G$, 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}. □

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

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

Proof. Homomorphe Bilder von nilpotenten Gruppen sind immer nilpotent, daher folgt "⇒". 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. □

Beispiele 1.9.6.

Abelsche Gruppen sind nilpotent.

Sei K ein Koerper, sei $n \in \mathbb{N}$ und sei G die Gruppe aller oberen Dreieckmatrizen in $\mathrm{M}_n(K)$ 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 (Uebungsaufgabe).

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. □

Lemma 1.9.8. *Sei G eine Gruppe und seien $M, N \subset G$ Normalteiler mit*

$$G = MN, \qquad M \cap N = 1.$$

Dann ist die Abbildung $M \times N \to G$, $(m, n) \mapsto mn$ ein Isomorphismus.

Iterativ stellt man fest: Sind $N_1, \ldots, N_k$ Normalteiler mit

$$N_j \cap \left(N_{j+1} \cdots N_k\right) = 1$$

fuer $1 \leq j < k$ und $G = N_1 \cdots N_k$, dann ist das Produkt ebenfalls direkt, also $G \cong N_1 \times \cdots \times N_k$.

Beweis. Es ist zu zeigen, dass die Elemente von M und N miteinander kommutieren. Seien also $m \in M$ und $n \in N$. Es ist $mnm^{-1} \in N$ und $nm^{-1}n^{-1} \in M$. Multiplizieren wir den ersten von rechts mit n^{-1}, so folgt $[m, n] = mnm^{-1}n^{-1} \in N$. Multiplizieren wir den zweiten von lin=ks mit m, folgt $[m, n] = mnm^{-1}n^{-1} \in M$, also liegt der Kommutator $[m, n]$ in $M \cap N = 1$, also $[m, n] = 1$ oder $mn = nm$. □

Definition 1.9.9. Sei G eine Gruppe und U eine Untergruppe. Die Menge $N(U)$ aller $g \in G$ mit

$$gUg^{-1} = U$$

wird der **Normalisator** von U genannt.

Der Normalisator ist genau dann gleich ganz G, wenn U ein Normalteiler ist. Der Normalisator ist stets eine Untergruppe zwischen U und G und U ist normal in $N(U)$.

Satz 1.9.10. (a) *Ist G eine nilpotente Gruppe, U eine echte Untegruppe und $N(U)$ ihr Normalisator. Dann ist $N(U)$ echt groesser als U.*

(b) *Endliche nilpotente Gruppen sind direkte Produkte von p-Gruppen.*

Beweis. (a) Sei $G = G_0 \supset G_1 \supset \cdots \supset G_n = 1$ die Kommutatorreihe. Dann gibt es einen Index mit $G_j \not\subset U$ und $G_{j+1} \subset U$. Da G_j zentral modulo G_{j+1} ist, folgt $[g, u] \in G_{j+1} \subset U$ fuer alle $g \in G_j$, $u \in U$, was impliziert $G_{j+1} \subset N(U)$.

(b) Sei G eine endliche Gruppe und sei P eine p-Sylow-Gruppe. Sei $P \subset N(P) \subset G$ der Normalisator von P. Dann ist P die einzige p-Sylowgruppe von $N(P)$ und daher muss P unter allen Automorphismen von $N(P)$ bewahrt bleiben. Ist damit g ein Element des Normalisators von $N(P)$, also $g \in N(N(P))$, dann folgt $gPg^{-1} = P$ und damit schon $g \in N(P)$, das heisst der Normalisator der Gruppe $N(P)$ ist $N(P)$ selbst. Ist nun G nilpotent, so folgt nach Teil (a) dass dann $N(P)$ die ganze Gruppe G sein muss. Damit hat G nur eine einzige p-Sylow Gruppe. Dies gilt fuer jedes p und es folgt aus Lemma 1.9.8, dass das Produkt H der p-Sylowgruppen direkt sein muss. Dieses Produkt hat aber ebensoviele Elemente wie G selbst. □

Definition 1.9.11. 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.

Beispiele 1.9.12.

Nilpotente Gruppen sind aufloesbar.

Die Gruppe der oberen Dreiecksmatrizen in $\mathrm{M}_n(K)$ ist aufloesbar.

Satz 1.9.13. (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 aufloesbar, wenn N und G/N aufloesbar sind.*

Beweis. (a) Sei G aufloesbar 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. Fuer $j = 0$ ist dies klar. Sei es fuer j bewiesen, dann folgt
$G^{(j+1)} = [G^{(j)}, G^{(j)}] \subset [U_j, U_j] \subset U_{j+1}$.

(b) Sei $U \subset G$ eine Untergruppe einer aufloesbaren Gruppe G. Wir zeigen induktiv $U^{(j)} \subset G^{(j)}$. Fuer $j = 0$ 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 aufloesbar. Ist $\phi : G \to H$ surjektiv, so folgt ebenso induktiv, dass $\phi(G^{(j)}) = H^{(j)}$ und damit ist H aufloesbar.

(c) Ist G aufloesbar, dann sind N und G/N aufloesbar nach Teil (b). Seien umgekehrt N und G/N aufloesbar. Da G/N aufloesbar, gibt es ein n so dass $G^{(n)} \subset N$ gilt. Damit folgt dann induktiv $G^{(n+k)} \subset N^{(k)}$ und da N aufloesbar ist, muss auch G aufloesbar sein. □

1.10 Semidirekte Produkte

Aus Lemma 1.9.8 wissen wir, dass aus $G = MN$ mit Normalteilern M, N und $M \cap N = \{1\}$ folgt $G \cong M \times N$. Jetzt schwaechen wir die Bedingung ab, indem wir nur von einer der beiden Untergruppen die Normalteilereigenschaft verlangen.

Lemma 1.10.1 (Semidirektes Produkt)**.** *Sei G eine Gruppe, U eine Untergruppe und N ein Normalteiler von G. Gilt $G = NU$ und $N \cap U = 1$, dann ist die Abbildung $\phi : N \times U \to G$ bijektiv. Auf der Menge $N \times U$ definiert die Vernknuepfung*

$$(n, u)(n_1, u_1) = (n \cdot un_1u^{-1}, uu_1)$$

eine Gruppenstruktur so dass ϕ ein Isomorphismus wird.

Man sagt in diesem Fall, dass G das **semidirekte Produkt** von N und U ist, Schreibweise:

$$G \cong N \rtimes U.$$

Merke: Der Fisch schwimmt vom Normalteiler zum Quotienten.

Beweis. Ist $nu = n'u'$, dann folgt $u(u')^{-1} = n^{-1}n' \in N \cap U = 1$, also $u = u'$ und $n = n'$ und die Abbildung ist injektiv. Surjektiv war sie eh schon. Es gilt nun

$$\phi(n, u)\phi(n_1, u_1) = nun_1u_1 = \underbrace{n \cdot un_1u^{-1}}_{\in N} \cdot \underbrace{uu_1}_{\in U} = \phi(n \cdot un_1u^{-1}, uu_1).$$

Wegen der Bijektivitaet von ϕ definiert die Vorschrift damit eine Grupppenstruktur, die ϕ zum Isomorphismus macht. □

Definition 1.10.2. Eine Sequenz von Gruppenhomomorphismen

$$A \xrightarrow{\alpha} B \xrightarrow{\beta} C$$

heisst **exakt** and der Stelle A, wenn $\text{Bild}(\alpha) = \ker(\beta)$ gilt. Insbesondere gilt dann $\beta \circ \alpha = 1$.

Lemma 1.10.3. *Sei die Sequenz*

$$1 \to N \xrightarrow{\alpha} G \xrightarrow{\beta} Q \to 1$$

ueberall exakt. Ein Gruppenhomomorphismus $s : Q \to G$ heisst **Schnitt** *zu β, falls $\beta \circ s = \text{Id}_Q$. Existiert ein solcher Schnitt, sagt man, die Sequenz* **spaltet**.

$$1 \longrightarrow N \xrightarrow{\alpha} G \underset{s}{\overset{\beta}{\rightleftarrows}} Q \longrightarrow 1$$

Dann gilt: Jede Spaltung induziert einen Isomorphismus $G \cong N \rtimes Q$ und umgekehrt, d.h. ist G das semidirekte Produkt, so gibt es eine spaltende Sequenz.

Beweis. Sei s eine Spaltung der Sequenz und betrachte die Abbildung $\phi : N \times Q \to G$, $(n, q) \mapsto ns(q)$. Sei $U = s(Q)$, wir zeigen $N \cap U = 1$. Sei hierzu $x \in N \cap U$, also $x = s(q)$ fuer ein $q \in Q$ und $x = \alpha(n)$ fuer ein $n \in N$. Da $\beta \circ \alpha = 1$, andererseits s aber ein Schnitt ist, folgt $q = \beta(s(q)) = \beta(\alpha(n)) = 1$, also ist auch $x = 1$. Die Behauptung folgt. □

Lemma 1.10.4. *Sind N, Q Gruppen und operiert Q auf N durch Gruppenhomomorphismen, $(q, n) \mapsto q * n$, dann definiert die Verknuepfung*

$$(n, q)(n_1, q_1) = (n \cdot q * n_1, qq_1)$$

eine Gruppenstruktur auf $G = N \times Q$, die diese Gruppe zu einem semi-direkten Produkt macht. Die Abbildungen $\alpha : N \to G$, $n \mapsto (n, 1)$, $\beta : G \to Q$, $(n, q) \mapsto q$ und $s : Q \to G$, $q \mapsto (1, q)$ definieren eine spaltende exakte Sequenz:

$$1 \longrightarrow N \xrightarrow{\alpha} G \underset{s}{\overset{\beta}{\rightleftarrows}} Q \longrightarrow 1$$

Beweis. Zunaechst muss man die Gruppenaxiome nachrechnen. Wir machen das mal mit der Assoziativitaet. Seien $a = (n, q), b = (n_1, q_1), c = (n_2, q_2) \in G$. Dann gilt

$$\begin{aligned}
(ab)c &= [(n, q)(n_1, q_1)](n_2, q_2) \\
&= (n(q * n_1), qq_1)(n_2, q_2) \\
&= \left(n(q * n_1)(qq_1) * n_2 \ , \ qq_1q_2\right) \\
&= \left(n(q * n_1)(q * (q_1 * n_2)) \ , \ qq_1q_2\right) \\
&= \left(n(q * (n_1(q_1 * n_2)) \ , \ qq_1q_2\right) \\
&= (n, q)(n_1(q_1 * n_2) \ , \ q_1q_2) \\
&= (n, q)(n_1(q_1 * n_2) \ , \ q_1q_2) \\
&= a(bc).
\end{aligned}$$

Das neutrale Element ist $(1, 1)$ und das Inverse zu (n, q) ist $((q^{-1} * n^{-1}), q^{-1})$. Der Rest ist klar. □

Beispiel 1.10.5. Die Diedergruppe D_{2n} der Ordnung $2n$ ist isomorph zum semidirekten Produkt $(\mathbb{Z}/n\mathbb{Z}) \rtimes \{\pm 1\}$, wobei ± 1 auf $\mathbb{Z}/n\mathbb{Z}$ durch Multiplikation operiert.

Satz 1.10.6. *Seien $p < q$ Primzahlen und G eine Gruppe der Ordnung pq. Gilt $q \not\equiv 1 \mod p$, dann ist G zyklisch. Andernfalls ist G entweder zyklisch oder isomorph zum semidirekten Produkt $(\mathbb{Z}/q\mathbb{Z}) \rtimes (\mathbb{Z}/p\mathbb{Z})$, wobei die Operation von $\mathbb{Z}/p\mathbb{Z}$ auf $\mathbb{Z}/q\mathbb{Z}$ nichttrivial ist. Alle diese semidirekten Produkte sind isomorph.*

Proof. Ist $q \not\equiv 1 \mod p$, so seien s_p und s_q die Anzahl der p- und q-Sylowgruppen von G. Es gilt dann $s_p \mid q$ und $s_p \equiv 1 \mod p$, so dass $s_p = 1$ folgt. Ebenso gilt $s_q \mid p$ und $s_q \equiv 1 \mod q$. Wegen $q > p$ muss dann auch $s_q = 1$ sein. Aus Anzahlgruenden G das Produkt seiner Sylowgruppen und nach Lemma

1.9.8 ist G isomorph zum direkten Produkt welches nach dem chinesischen Restsatz wiederum zyklisch ist.

Betrachte nun den Fall $q \equiv 1 \mod p$. Die Anzahl der q-Sylowgruppen ist wieder 1, also ist die q-Sylowgruppe N ein Normalteiler. Die Anzahl der p-Sylowgruppen ist ein Teiler von q also gleich 1 oder q. Im ersten Fall ist G wie oben zyklisch. Im zweiten Fall sei U eine p-Sylowgruppe. Da die Ordnungen von N und U teilerfremd sind, folgt $N \cap U = 1$. Dann ist die Abbildung $N \times U \to G$, $(n, u) \mapsto nu$ injektiv und weil beide Seiten die gleich Ordnung haben, auch surjektiv, so dass $G = NU$ gilt. Damit gilt $G \cong N \rtimes U$ mit einer nichttrivialen Operation, denn U ist kein Normalteiler, also G nicht abelsch. Die Operation ist gegeben durch einen Gruppenhomomorphismus $\phi : U \to \mathrm{Aut}(N) \cong \mathbb{F}_q^\times$, wobei $\mathbb{F}_q$ der Koerper mit q Elementen ist. Die Gruppe $\mathbb{F}_q^\times$ ist nach Satz 3.8.1 zyklisch, hat also genau eine Untergruppe A der Ordnung p. Ist ϕ nichttrivial, muss $\mathrm{Bild}(\phi) = A$ sein. Je zwei solche Homomorphismen ϕ, ϕ' erfuellen $\phi' = \phi \circ \alpha$ mit $\alpha \in \mathrm{Aut}(U)$. Die zugehoerigen semidirekten Produkte sind isomorph vermoege der Abbildung

$$N \rtimes_{\phi'} U \xrightarrow{\mathrm{Id} \times \alpha} N \rtimes_{\phi} U,$$

wie man direkt nachrechnet. □

Korollar 1.10.7. *Sei p eine ungerade Primzahl und G eine Gruppe der Ordnung $2p$, dann ist G entweder zyklisch oder eine Diedergruppe.*

2 Ringe

2.1 Definition

Definition 2.1.1. Ein **kommutativer Ring mit Eins** ist eine abelsche Gruppe $(R, +)$ mit einer weiteren Verknüpfung $\times$, die assoziativ ist,

$$(ab)c = a(bc)$$

und kommutativ

$$ab = ba$$

und das Distributivgesetz erfüllt:

$$a(b + c) = ab + ac.$$

Ferner existiert ein Element $1_R \in R$ mit

$$1_R a = a$$

für jedes $a \in R$. Dieses Element ist dann eindeutig bestimmt und wird 1 geschrieben.

Wenn wir im Folgenden **Ring** schreiben, meinen wir immer einen kommutativen Ring mit Eins.

Ein Ring ist also dasselbe wie ein Körper, bis auf die Tatsache, dass nicht jedes Element $\neq 0$ invertierbar sein muss.

Beispiele 2.1.2.

- $(\mathbb{N}, +, \times)$ ist **kein** Ring, da es keine inversen Elemente der Addition gibt.
- $(\mathrm{M}_n(K), +, \times)$ ist kein kommutativer Ring für $n \geq 2$, da Matrixmultiplikation nicht kommutativ ist.
- Jeder Körper ist ein Ring.
- $\mathbb{Z}$ ist ein Ring, der kein Körper ist.
- 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

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

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

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

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

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

- 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 Unbekannten**,

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

  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.

- Im Polynomring $R[x]$ gilt

  $$(a_0 + a_1 x + \cdots + a_n x^n)(b_0 + b_1 x + \cdots + b_m x^m) = c_0 + c_1 x + \cdots + c_{n+m} x^{n+m},$$

  wobei $c_0 = a_0 b_0, c_1 = a_0 b_1 + a_1 b_0$ und allgemein

  $$c_k = \sum_{i+j=k} a_i b_j.$$

  Also hängt der Koeffizient c_k nur von den Koeffizienten $a_0, \ldots, a_k$ und $b_0, \ldots b_k$ ab und nicht von denen höheren Grades. Dasselbe gilt für die Addition. Also kann man Addition und Multiplikation des Polynomrings $R[x]$ auch auch die Menge aller Koeffizientenfolgen $(a_0, a_1, \ldots)$ ausdehnen, die nicht notwendigerweise endlich sind. Alternativ kann man diese Menge $R^{\mathbb{N}_0} = \mathrm{Abb}(N_0, R)$ auch als Menge aller formalen Reihen

  $$\sum_{j=0}^{\infty} a_j x^j$$

  beschreiben. Der so entstehende Ring wird der Ring der **formalen Potenzreihen** genannt und als

  $$R[[x]]$$

  geschrieben.

- Statt nur endlich vieler Unbestimmten, kann man auch Polynomringe in beliebig vielen

Unbestimmten betrachten. Ist I eine Indexmenge, so sei

$$R[x_i : i \in I]$$

der Ring aller formalen Ausdruecke der Form

$$\sum_{i \in I^k} c_i x_{i_1} \cdots x_{i_k},$$

wobei $c_i \in R$ und die Summe endlich ist, d.h., fast alle c_i sind Null, die Summe laeuft ueber alle $k \in \mathbb{N}$ und alle $i \in I^k$. In dieser Beschreibung ist zugelassen, dass $i_\nu = i_\mu$ fuer $\nu \neq \mu$.

- 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 $\mathbb{Q}$.
- Für $m \in \mathbb{N}$ ist die Menge $\mathbb{Z}/m$ der Restklassen $\{0, 1, 2, \ldots, m-1\}$ 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 2.1.3. 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 2.1.4.

- 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. □
- 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 2.1.5. 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

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

Bemerkung 2.1.6. Der Begriff des Nullteilers beißt sich mit der Teilbarkeitsrelation in Definition 2.4.1, denn demnach gilt $a \mid 0$ fuer jedes $a \in R$, auch wenn a kein Nullteiler ist. Der Grund wird sein, dass man frueher Teilbarkeit anders definiert hat, dann aber aus Praktikabilitaetsgruenden zur heutigen

Definition gefunden hat, wobei der Nullteiler hinten runtergefallen ist. Wir werden mit dieser Widerspruechlichkeit leben muessen.

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 Integrigtätsring, 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. □

Definition 2.1.9. Seien R, S Ringe. Ein **Ringhomomorphismus** ist eine Abbildung $\phi : R \to S$ so dass

- ϕ ist ein Gruppenhomomorphismus $(R, +) \to (S, +)$,
- $\phi(1) = 1$,
- $\phi(ab) = \phi(a)\phi(b)$.

Beispiele 2.1.10.
- Die Inklusionen $\mathbb{Z} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C}$ sind Ringhomomorphismen.
- Sei $m \in \mathbb{N}$. Die Projektion $\mathbb{Z} \to \mathbb{Z}/m$, 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 Abbildung $\delta_\alpha : K[x] \to K$, 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 Teilmenge $I \subset R$ mit den folgenden Eigenschaften

- I ist eine additive Untergruppe von R und
- ist $r \in R$ und $a \in I$, dann ist $ra \in I$. Kurz geschrieben lautet diese Bedingung

$$RI \subset I.$$

Proposition 2.2.2. (a) *Ist $\phi : R \to S$ ein Ringhomomorphismus, dann ist* $\ker(\phi) = \left\{x \in R : \phi(x) = 0\right\}$ *ein Ideal.*

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

Beweis. (a) Da ϕ ein additiver Gruppenhomomorphismus ist, ist der Kern eine Untergruppe. Sei also $a \in I$ und $r \in R$. Dann folgt $\phi(ar) = \phi(a)\phi(r) = 0\phi(r) = 0$, also ist $ar \in I$.

(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. □

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
$$rR = \left\{rx : x \in R\right\}$$
ein Ideal. Ein solches Ideal nennt man **Hauptideal**. Manche Autoren schreiben auch (a) für aR.
- Ist $a \in R$, so ist die Menge
$$\mathrm{Ann}(a) := \left\{r \in R : ra = 0\right\}$$
ein Ideal, genannt der **Annullator** von a.

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 $k = p \in m\mathbb{Z}$. □

- 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 $\operatorname{grad}(f) \geq \operatorname{grad}(g)$, also existieren nach der **Division mit Rest** Polynome q, r mit

  $$f = qg + r$$

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

- 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! □

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

Definition 2.2.6. Ein Integritätsring R heißt **euklidischer Ring**, falls es eine Abbildung $\delta : R \setminus 0 \to \mathbb{N}_0$ gibt, so dass zu je zwei $a, b \in R \setminus \{0\}$ zwei Elemente $q, r \in R$ existieren mit

$$a = bq + r$$

und $r = 0$ oder $\delta(r) < \delta(b)$. Man nennt δ die **Gradabbildung** des euklidischen Rings.

Proposition 2.2.7. *Jeder euklidische Ring ist ein Hauptidealring.*

Beweis. Sei $I \neq 0$ ein Ideal und sei $g \in I \setminus \{0\}$ ein Element von minimalem Grad, also $\delta(g)$ minimal unter allen $\delta(f)$ mit $f \in I \setminus \{0\}$. Da $g \in I$, folgt $(g) \subset I$. Sei $f \in I$ beliebig, dann ist also $\delta(f) \geq \delta(g)$, also existieren Elemente q, r mit

$$f = qg + r$$

und $\delta(r) < \delta(g)$. Dann ist $r = f - qg \in I$ und da der Grad von g minimal war, ist $r = 0$, also $f = gq \in (g)$. □

Beispiele 2.2.8.

- $\mathbb{Z}$ ist ein euklidischer Ring mit $\delta(k) = |k|$.
- Sei K ein Körper, dann ist der Polynomring $K[x]$ euklidisch mit $\delta(f) = \operatorname{grad}(f)$.

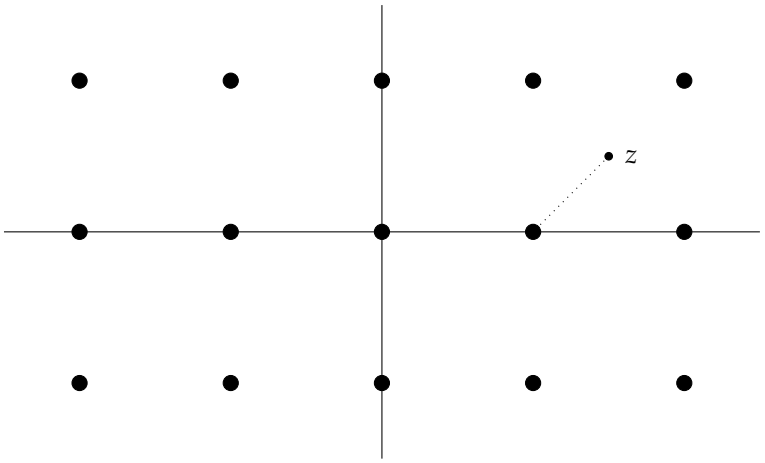
- Der Ring $R = \mathbb{Z}[i] = \mathbb{Z} \oplus \mathbb{Z}i$ aller komplexer Zahlen $m + ni$ mit $m, n \in \mathbb{Z}$ ist ein euklidischer Ring mit

$$\delta(m + ni) = m^2 + n^2, \quad \text{also} \quad \delta(z) = |z|^2 = z\bar{z}.$$

Beweis. Beachte zunächst, dass die Funktion δ auf ganz $\mathbb{C}$ definiert ist und mutliplikativ ist, d.h., für $z, w \in \mathbb{C}$ gilt stets

$$\delta(zw) = \delta(z)\delta(w).$$

Wir stellen fest, dass für jedes $z \in \mathbb{C}$ der Abstand zum nächsten Punkt $c \in R$ stets $\leq \frac{1}{\sqrt{2}}$ ist.



Mit anderen Worten, zu jedem $z \in \mathbb{C}$ existiert ein $c \in R$ mit $\delta(z - c) \leq \frac{1}{2}$. Seien nun $a = m + ni$ und $b = k + li$ in $\mathbb{Z}[i] \setminus \{0\}$ und sei $z = \frac{a}{b} \in \mathbb{C}$. Dann existiert also ein $c \in \mathbb{Z}[i]$ mit $\delta(z - c) \leq \frac{1}{2}$. Setze $r = a - bc \in R$. Dann ist

$$\delta(r) = \delta(b)\delta\left(\frac{a}{b} - c\right) \leq \delta(b)\frac{1}{2} < \delta(b).$$

Damit ist $R = \mathbb{Z}[i]$ ein euklidischer Ring, also insbesondere ein Hauptidealring. □

Definition 2.2.9. Sei R ein Hauptidealring und seien $a, b \in R$. Ein **größter gemeinsamer Teiler** ggT(a, b) ist ein Erzeuger des Ideals $aR + bR$. Ein ggT ist bis auf Multiplikation mit einer Einheit eindeutig festgelegt.

Beispiel 2.2.10. 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 $10\mathbb{Z} + 15\mathbb{Z}$. □

Proposition 2.2.11. *In einem euklidischen Ring (R, δ) kann man die Koeffizienten x, y, also einen ggT von a und b wie folgt berechnen: Man schreibt $a = r_0$ und $b = r_1$ und*

$$a = r_0 = q_1 r_1 + r_2$$

mit $\delta(r_2) < \delta(r_1)$. Dann

$$r_1 = q_2 r_2 + r_3$$

mit $\delta(r_3) < \delta(r_2)$ und so fort. Der allgemeine Schritt ist

$$r_{n-1} = q_n r_n + r_{n+1}$$

mit $\delta(r_{n+1}) < \delta(r_n)$. Da die $\delta(r_n)$ immer kleiner werden, erreichen sie irgendwann die Null, es gibt also ein N mit $r_N \neq 0 = r_{N+1}$, also

$$r_{N-1} = q_N r_N.$$

Es folgt: r_N teilt r_{N-1}. Wegen

$$r_{N-2} = q_{N-1} r_{N-1} + r_N$$

teilt r_N auch r_{N-2} und so fort bis $r_1 = b$ und $r_0 = a$, damit ist r_N ein gemeinsamer Teiler von a und b. Nun ist aber

$$\begin{aligned} r_N &= r_{N-2} - q_{N-1} r_{N-1} \\ &= r_{N-2} - q_N (r_{N-3} - q_{N-2} r_{N-2}) \\ &= (1 + q_N q_{N-2}) r_{N-2} - q_N r_{N-3} \end{aligned}$$

Wir setzen hier wieder $r_{N-2} = r_{N-4} - q_{N-2} r_{N-3}$ ein und so fort, bis wir am Ende $r_N = r_0 x + r_1 y = ax + by$ erhalten.

Bei dem obigen Verfahren gilt also: der letzte nichttriviale Rest ist der ggT.

Beweis. (a) ist klar und die Tatsache in (b), dass r_N ein ggT ist, folgt aus (a). □

Beispiel 2.2.12. Wir bestimmen den ggT von 173 und 435.

$$\begin{aligned} 435 &= 2 \cdot 173 + 89 \\ 173 &= 1 \cdot 89 + 84 \\ 89 &= 1 \cdot 84 + 5 \\ 84 &= 16 \cdot 5 + 4 \\ 5 &= 1 \cdot 4 + 1 \\ 4 &= 1 \cdot 1. \end{aligned}$$

Damit ist der ggT gleich 1.

Definition 2.2.13. Sei R ein Ring und $I \subset R$ ein Ideal. Wir zeigen gleich, dass die Relation

$$x \sim y \quad :\Leftrightarrow \quad x - y \in I$$

eine Äquivalenzrelation auf R ist. Die Menge der Äquivalenzklassen $R/\sim$ schreiben wir als R/I. Die Äquivalenzklasse der Null ist I.

Satz 2.2.14. (a) *Die Relation $\sim$ zu einem gegebenen Ideal ist eine Äquivalenzrelation.*

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

Kern eines Ringhomomorphismus.

(c) *Sei $\sim$ eine Äquivalenzrelation so dass es auf der Quotientenmenge $R/\sim$ eine Ringstruktur gibt so dass die Projektion $\pi : R \to R/\sim$ ein Ringhomomorphismus ist, dann gibt es genau ein Ideal I mit*

$$x \sim y \quad \Leftrightarrow \quad x - y \in I.$$

Beweis. (a) Da I eine Untergruppe ist, sind Reflexivität und Symmetrie klar. Für die Transitivität sei $x \sim y$ und $y \sim z$, also $x - y, y - z \in I$. Dann ist die Summe dieser beiden Elemente, also $x - z$ ebenfalls in I, also $x \sim z$.

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

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

also folgt $(a + b) \sim (a' + b')$ 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.

(c) Sei $\sim$ eine solche Äquivalenzrelation und sei $I = \ker(\pi)$. Dann ist I ein Ideal und es gilt

$$\begin{aligned} x \sim y &\Leftrightarrow \pi(x) = \pi(y) \\ &\Leftrightarrow \pi(x - y) = 0 \\ &\Leftrightarrow x - y \in I. \end{aligned}$$

□

Beispiel 2.2.15. 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 2.2.16.

(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. □

Definition 2.2.17. 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 2.2.18. *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 $I_1, \ldots, I_r$ 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*

$$R/I \cong \prod_{\nu=1}^{r} R/I_\nu.$$

Beweis. Da $I_\nu \supset I$ für jedes ν, gibt es kanonische Projektionen $\pi_\nu : R/I \to R/I_\nu$, also einen Ringhomomorphismus

$$\pi : R/I \to \prod_{\nu=1}^{r} R/I_\nu.$$

Injektivität: Sei $\pi(\bar{x}) = 0$, und $x \in R$ ein Urbild von $\bar{x}$. Dann ist $x \in I_\nu$ für jedes ν. Nun sind die I_ν 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 $I_3, \ldots, I_r$, 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. □

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 **assoziiert**, 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)⇒(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)⇒(ii) Es sei $a = bu$ mit einer Einheit u. Wegen $uR = R$ folgt dann $aR = buR = bR$.

(ii)⇒(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 $b \mid a$. □

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. □

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. □

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)⇒(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. □

Beispiel 2.4.9. In dem Integritätsring $R = \mathbb{Z}[\sqrt{-5}]$ ist das Element 3 irreduzibel, aber kein Primelement. Insbesondere folgt, dass $\mathbb{Z}\left[i\sqrt{5}\right]$ kein Hauptidealring sein kann, was den fehlenden Beweis in Beispiel 2.2.5 liefert.

Beweis. Sei $\alpha = i\sqrt{5}$. Wir zeigen, dass 3 irreduzibel ist. Ist $3 = zw$ in R, dann folgt $9 = |3|^2 = |z|^2|w|^2$. Ist $|z|^2 = 1$, dann ist $z = \pm 1$ eine Einheit. Ist $|z|^2 = 9$, dann ist $|w|^2 = 1$ und w ist eine Einheit. *Angenommen,* $|z|^2 = 3$. Sei $z = a + b\alpha$, dann ist $3 = |z|^2 = a^2 + 5b^2$, also ist $b = 0$, da der Betrag sonst zu gross wäre. Dann ist $3 = a^2$, aber 3 ist kein Quadrat in $\mathbb{Z}$, *Widerspruch!* Also ist 3 irreduzibel.

Wir zeigen, dass 3 kein Primelement ist. Hierzu beachte, dass $3 \mid 9 = (2 + \alpha)(2 - \alpha)$, aber 3 teilt keinen der Faktoren, denn würde 3 etwa $2 + \alpha$ teilen, also $2 + \alpha = 3z$, dann ist $9 = |2 + \alpha|^2 = |3|^2|z|^2$, also $|z| = 1$ und damit ist $z = \pm 1$, was ein Widerspruch ist. □

Korollar 2.4.10. *In einem Hauptidealring R lässt sich jedes Element von $R \setminus \{0\}$, das keine Einheit ist, als endliches Produkt von Primelementen schreiben.*

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

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

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

$$\bigcup_{j\in\mathbb{N}} a_jR$$

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

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

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

Lemma 2.4.11. *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 $r = s$. □

Definition 2.4.12. Ein Integritätsring R heißt **faktoriell**, falls jede Nichteinheit in $R \setminus \{0\}$ als Produkt von Primelementen darstellen lässt, das heißt wenn wir eine sogenannte **Primfaktorzerlegung** haben. Die Faktoren sind dann bis auf Reihenfolge und Assoziiertheit eindeutig bestimmt. Satz 2.4.8 gilt auch für faktorielle Ringe, d.h. in einem faktoriellen Ring gilt

$$p \text{ irreduzibel} \quad \Leftrightarrow \quad p \text{ Primelement.}$$

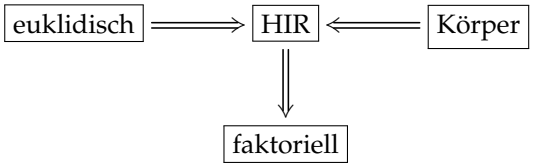
Satz 2.4.13. (a) *In einem faktoriellen Ring ist jedes irreduzible Element ein Primelement und umgekehrt.*

(b) *Jeder Hauptidealring ist faktoriell. Insbesondere ist $\mathbb{Z}$ faktoriell und für jeden Körper K ist der Polynomring $K[x]$ faktoriell.*

Beweis. Ist R faktoriell und $q \in R$ irreduzibel, dann ist $q = p_1 \cdots p_n$ mit Primelementen p_j. Da q irreduzibel ist, muss entweder eines der p_j eine Einheit sein oder $n = 1$. Da keines der p_j eine Einheit ist, folgt $n = 1$, also ist q prim.

(b) Folgt aus Korollar 2.4.10 und Lemma 2.4.11. □

Für einen Integritätsring gilt also



Beispiel 2.4.14. Der Ring $R = \mathbb{Z}[\sqrt{-5}]$ ist nicht faktoriell, denn wir haben schon gesehen, dass nicht jedes irreduzible Element prim ist.

Korollar 2.4.15. *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 Primfakorzerlegung von z nicht vorkommt und damit ist $\mathrm{ggT}(z, p) = 1$. 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.

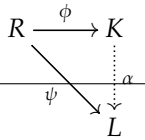
Für die Umkehrung sei R/pR ein Körper und p teile ein Produkt ab. Dann ist $\bar{a}\bar{b} = 0$ und daher $\bar{a} = 0$ oder $\bar{b} = 0$, also $p \mid a$ oder $p \mid b$. □

Beispiel 2.4.16. $\mathbb{Z}/m$ 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

Satz 2.5.1. *Sei R ein Integritaetsring. Dann gibt es einen injektiven Ringhomomorphismus $\phi : R \hookrightarrow K$ in einen Körper K. Es gibt bis auf Isomorphie genau einen Koerper $K = \mathrm{Quot}(R)$ mit der Eigenschaft, dass R nach K eingebettet werden kann, so dass R den Koerper K erzeugt. Man nennt* $\mathrm{Quot}(R)$ *den* **Quotientenkoerper** *von R.*

Ist $\psi : R \hookrightarrow L$ ein injektiver Ringhomomorphismus, wobei L ein Koerper ist, dann ist R ein Integritaetsring und es gibt genau einen Koerperhomomorphismus $\alpha : K = \mathrm{Quot}(R) \to L$, der das Diagramm



kommutativ macht.

Wir brauchen ein Lemma:

Lemma 2.5.2. *Sei $S = R \setminus \{0\}$. Auf der Menge $R \times S$ führen wir eine Äquivalenzrelation ein:*

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

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

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

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

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 f 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 Injektivitaet von f. Ist $f(a) = 0$, 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 f injektiv. □

Beweis des Satzes. Ist nun $\psi : R \hookrightarrow L$ ein Ringhomomorphismus in einen Koerper, so definiere $\alpha : K \to L$ durch

$$\alpha\left(\frac{a}{b}\right) = \frac{\psi(a)}{\psi(b)},$$

wobei auf der rechten Seite die Quotientenbildung in L gemeint ist. Dies ist moeglich, da $b \neq 0$ und daher $\psi(b) \neq 0$. Man rechnet sofort nach, dass α ein Koerperhomomorphismus ist und das α den Homomorphismus ψ fortsetzt. Die Eindeutigkeit von α ist ebenfalls klar, denn die Kommutativitaet des Diagramms erzwingt $\alpha\left(\frac{a}{b}\right) = \frac{\psi(a)}{\psi(b)}$. □

Bemerkung 2.5.3. Es gibt auch eine alternative Konstruktion des Quotientenkoerpers: Fuer jedes $s \in S$ sei X_s eine Unbestimmte. Betrachte dann den Polynomring $P = R[X_s : s \in S]$ in all diesen Unbestimmten. In diesen Ring ist das Ideal

$$I = \bigoplus_{s \in S} (sX_s - 1)P$$

ein maximales Ideal und man erhaelt den Quotientenkoerper K als $K = P/I$.

Beispiele 2.5.4.

- 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.

2.6 Faktorielle Polynomringe

Sei R ein faktorieller Ring und sei $K = \mathrm{Quot}(R)$ sein Quotientenkörper. Fixiere ein Vertretersystem $\mathbb{P}$ der Primelemente modulo Assoziiertheit. Dann ist die Menge

$$V = \left\{ \prod_{p \in \mathbb{P}} p^{k_p} : k_p \in \mathbb{N}_0, \text{ fast alle Null} \right\}$$

ein Vertretersystem von R modulo Assoziiertheit. Mit anderen Worten, jedes $a \in R$ lässt sich eindeutig schreiben in der Form $a = uv$ mit $u \in R^\times$ und $v \in V$. Insbesondere definieren wir für $a_0, a_1, \ldots, a_n \in R$, nicht alle Null, den **größte gemeinsame Teiler** als das eindeutig bestimmte Element $v \in V$ so dass $v \mid a_j$ für jedes $a_j \neq 0$ und ist $w \in V$ ein zweites Element mit dieser Eigenschaft, dann folgt $w \mid v$. Man berechnet den ggT wie folgt: Man schreibt jedes $a_j \neq 0$ als $a_j = u_j \prod_{p \in \mathbb{P}} p^{k_p(a_j)}$ fuer eine Einheit u_j. Dann ist

$$v = \mathrm{ggT}(a_0, \ldots, a_n) = \prod_{p \in \mathbb{P}} p^{m_p},$$

wobei m_p das Minimum über alle $k_p(a_j)$ ist.

Sei $0 \neq f(x) = a_0 + a_1 x + \cdots + a_n x^n$ in $R[x]$. Schreibe dann $v(f) \in V$ für den ggT der Koeffizienten $a_0, \ldots, a_n$.

Ist $0 \neq f(x) \in K[x]$, dann existiert $0 \neq \lambda \in K$ so dass $\lambda f(x) \in R[x]$. Wir definieren dann

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

und stellen fest, dass $v(f)$ nicht von der Wahl von λ abhängt.

Indem man Zaehler wegmultipliziert und durch gemeinsame Teiler teilt, stellt man fest, dass es fuer jedes $0 \neq f \in K[x]$ ein $\lambda \in K^\times$ gibt, so dass λf in $R[x]$ liegt und teilerfremde Koeffizienten hat. Insbesondere ist dann $v(\lambda f) = 1$. Gilt ausserdem, dass $v(f) = 1$, so folgt $1 = v(\lambda f) = \lambda v(f) = \lambda$, also ist dann $f \in R[x]$.

Lemma 2.6.1. *Ist $f \in K[x]$ so dass $v(f)$ in R liegt, dann ist $f \in R[x]$.*

Proof. Indem wir f durch $\frac{1}{v(f)} f$ ersetzen, koennen wir verlangen, dass $v(f) = 1$ ist. In diesem Fall haben wir uns schon ueberlegt, dass $f \in R[x]$ ist. □

Lemma 2.6.2 (Gauß Lemma)**.** *Sei R ein faktorieller Ring und K sein Quotientenkörper. Seien $0 \neq f, g \in K[x]$. Dann gilt*

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

Beweis. Schreibt man $f = cf_1$ und $g = dg_1$ wobei $c = v(f)$ und $d = v(g)$, so wird ersichtlich, dass es reicht,

zu zeigen, dass aus $v(f) = v(g) = 1$ folgt $v(fg) = 1$. Sei

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n,$$
$$g(x) = b_0 + b_1 x + \cdots + b_m x^m$$

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 2.6.3. *Sei R ein faktorieller Ring 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 $R[x]$.*

Beweis. Schreibe $f = cf_1$ und $g = dg_1$, wobei $c = v(f)$ und $d = v(g)$. Dann ist $cd = 1$ und $f_1 = \frac{1}{c} f$ liegt in $R[x]$ und hat Leitkoeffizient $1/c$, so dass $1/c \in R$ gilt und ebenso $c = 1/d \in R$, also ist c eine Einheit in R, also ist $f \in R[x]$ und ebenso g. □

Satz 2.6.4 (Gauß)**.** *Ist R ein faktorieller Ring, dann ist auch der Polynomring $R[x]$ faktoriell.*

Beweis. Sei K der Quotientenkörper von R und sei $0 \neq f \in R[x]$. Da $K[x]$ faktoriell ist, gibt es Primpolynome $p_1, \ldots, p_n$ in $K[x]$ so dass mit dem Gauss-Lemma folgt

$$f = p_1 \cdots p_n = v(f) \frac{p_1}{v(p_1)} \cdots \frac{p_n}{v(p_n)}.$$

Nun ist $v(f) \in R$ und jedes der Polynome $\frac{p_j}{v(p_j)}$ liegt in $R[x]$. Man kann $v(f)$ in R in Primelemente zerlegen und es reicht daher zu zeigen, dass ein Primpolynom $p \in K[x]$, welches $v(p) = 1$ erfüllt, ein Primelement in $R[x]$ ist. Es ist allerdings prim in $K[x]$ und gilt $p \mid ab$ in $R[x]$, so gilt, sagen wir $p \mid a$ in $K[x]$, also $a = pc$ in $K[x]$. Nach dem Gauss-Lemma folgt $v(c) = v(a)/v(p) = v(a) \in R$, also $c \in R[x]$. □

Satz 2.6.5 (Eisenstein Kriterium)**.** *Sei R ein faktorieller Ring, K sein Quotientenkörper. Sei $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ ein Polynom vom Grad $n \geq 1$ in $R[x]$. Sei p ein Primelement von R und nimm an*

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

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

Beweis. Wir können $n \geq 2$ annehmen. Indem wir gemeinsame Primfaktoren herausziehen, können wir annehmen, dass $a_0, \ldots, a_n$ 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 $g(x) = b_0 + b_1x + \cdots + b_kx^k$ und $h(x) = c_0 + \cdots + c_mx^m$. 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!** □

2.7 Moduln

Ein Ring ist wie immer in dieser Vorlesung kommutativ und mit einer Eins versehen.

Definition 2.7.1. Ein **Modul** über dem Ring R ist eine abelsche Gruppe $(M, +)$, deren neutrales Element als 0 geschrieben wird, zusammen mit einer Abbildung

$$\begin{aligned} R \times M &\to M \\ (a, m) &\mapsto am, \end{aligned}$$

dergestalt, dass folgende Axiome erfüllt sind:

$$1m = m \qquad (ab)m = a(bm)$$
$$a(m + n) = am + an \qquad (a + b)m = am + bm.$$

Beispiele 2.7.2.

- Jeder Ring R ist ein Modul über sich selbst.
- Jede abelsche Gruppe ist ein $\mathbb{Z}$-Modul.
- Jedes Ideal von R ist ein Modul über R.
- Ist $R = K$ ein Körper, dann ist ein Modul dasselbe wie ein Vektorraum.

Definition 2.7.3. Ein **Untermodul** ist eine additive Untergruppe $N \subset M$, so dass $aN \subset N$ für jedes $a \in R$ gilt.

Definition 2.7.4. Ein **Modulhomomorphismus** ist eine Abbildung $\phi : M \to M$ zwischen R-Modulen, so dass

$$\phi(m + n) = \phi(m) + \phi(n), \qquad \phi(am) = a\phi(m).$$

Statt Modulhomomorphismus sagt man auch **R-lineare Abbildung**.

Proposition 2.7.5. *Ist $N \subset M$ ein Untermodul, dann wird die Quotientengruppe M/N durch die Vorschrift*

$$a(m + N) = am + N$$

zu einem R-Modul so dass die Projektion $M \to M/N$ ein Modulhomomorphismus ist.

Beweis. Klar. □

Ist $\phi : M \to N$ ein Modulhomomorphismus, dann sind $\ker(\phi)$ und $\text{Bild}(\phi)$ Untermoduln und es gilt der

Satz 2.7.6 (Homomorphiesatz)**.** (a) *Ist $\phi : M \to N$ ein R-Modulhomomorphismus, dann induziert ϕ einen Isomorphismus*

$$M/\ker(\phi) \cong \text{Bild}\,\phi.$$

(b) *Sind $U, W \subset M$ Untermoduln, so ist $U + W = \{u + w : u \in U,\ w \in W\}$ ebenfalls ein Untermodul und die Inklusion $U \to U + W$ induziert einen kanonischen Isomorphismus*

$$U/(U \cap W) \cong (U + W)/W.$$

(c) *Sind $U' \subset U$ Untermoduln von M, dann induziert die Projektion einen kanonischen Isomorphismus*

$$(M/U')/(U/U') \cong M/U.$$

Beweis. Wie die Homomorphiesätze in der Theorie der Gruppen. □

3 Körper

3.1 Adjunktion von Nullstellen

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 oder L einen **Oberkörper** zu K oder $L \supset K$ eine **Körpererweiterung**.

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.

Beispiele 3.1.2.

- $\mathbb{R}/\mathbb{Q}$ und $\mathbb{C}/\mathbb{R}$ sind Körpererweiterungen.
- $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ ist eine Körpererweiterung. Hierbei ist $\mathbb{Q}(\sqrt{2}) = \mathbb{Q} \times \mathbb{Q}$ als Menge mit komponentenweiser Addition und der Multiplikation

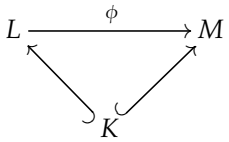
$$(a, b)(c, d) = (ac + 2bd, ad + bc).$$

  Dies ist ein Körper, der $\mathbb{Q}$ via $a \mapsto (a, 0)$ als Unterkörper enthält und in dem es eine Wurzel aus 2 gibt, nämlich das Element $(0, 1)$.

Definition 3.1.3. Sind L/K und M/K Körpererweiterungen, so ist ein **Homomorphismus von Körpererweiterungen**, oder ein Homomorphismus von $L \to M$ *über* K ein Ringhomomorphismus

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

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

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

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

Beispiel 3.1.4. Sei $\phi : \mathbb{Q}\left(\sqrt{2}\right) \to \mathbb{R}$, $\phi(a, b) = a + b\sqrt{2}$, wobei $\sqrt{2}$ die eindeutig bestimmte reelle Zahl $\alpha > 0$ ist mit $\alpha^2 = 2$. Dann ist ϕ ein Homomorphismus von Körpererweiterungen $\mathbb{Q}\left(\sqrt{2}\right)/\mathbb{Q} \to \mathbb{R}/\mathbb{Q}$.

Definition 3.1.5. Sei L/K eine Körpererweiterung und seien $\alpha_1, \ldots, \alpha_n \in L$. Sei

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

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

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

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

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 euklidisch, also faktoriell, 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 3.1.6. *Sei $f \in K[x]$ ein irreduzibles Polynom vom Grad n. Dann ist $fK[x]$ ein Ideal und der Quotient*

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

ein Körper. Die Körpererweiterung K_f/K ist bis auf Isomorphie die einzige Erweiterung vom Grad n, so dass f in K_f eine Nullstelle α_0 hat.

Ist M/K irgendeine Körpererweiterung, so dass f in M eine Nullstelle γ hat, dann gibt es genau einen Homomorphismus von Körpererweiterungen $\phi : K_f \to M$, 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.

Beweis. Nach Korollar 2.4.15 ist der Ring $K_f = K[x]/fK[x]$ ein Körper. Ist $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ mit $a_n \neq 0$, dann ist $1, x, \ldots, x^{n-1}$ eine Basis von K_f über K, also ist die Körpererweiterung K_f/K endlich. Ferner sei $\alpha \in K_f$ die Restklasse von x, dann gilt $f(\alpha) = 0$. Sei nun M/K eine weitere Körpererweiterung in der f eine Nullstelle γ hat. Betrachte den Ringhomomorphismus $\phi : K[x] \to M$ gegeben durch $x \mapsto \gamma$. Dann ist $\phi(f) = 0$, also faktorisiert ϕ über K_f. Beachte, dass ϕ auf K die Identität ist. Haben K_f und M dieselbe Dimension über K, so ist ϕ ein Isomorphismus. □

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

Satz 3.1.7. *Sei K ein Körper und sei $T \subset K[x]$ eine Menge von irreduziblen Polynomen. Dann existiert eine "kleinste" Körpererweiterung K_T/K so dass jedes Polynom $f \in T$ eine Nullstelle α_f in K_T hat.*

Beweis. Wir nehmen $T \neq \emptyset$ an. Sei $R = K[X_f : f \in T]$ der Polynomring mit so vielen Unbestimmten wie T Elemente hat. Sei

$$I = \sum_{f \in T} f(X_f)R$$

das Ideal erzeugt von allen Elementen der Form $f(X_f)$. Nach Satz 2.2.16 existiert ein maximales Ideal $J \supset I$. Sei dann $K_T = R/J$. Dies ist ein Körper. In dem Körper K_T hat jedes $f \in T$ eine Nullstelle, nämlich die Nullstelle $\alpha_f = X_f + J$ und der Körper wird von diesen Nullstellen erzeugt. □

Primkörper

Definition 3.1.8. 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

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

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

Satz 3.1.9. *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

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

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 3.1.10. *Ist* $\mathrm{Char}(K) = 0$, *dann ist die Abbildung* $\mathbb{Z} \to K$, $n \mapsto n \cdot 1$ *injektiv.*

Beweis des Satzes. Sei $\mathrm{Char}(K) = n \neq 0$. 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 $p \geq \mathrm{Char}(K) = n = pq$, 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 $n \cdot 1 = 1 + \cdots + 1$ 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 $\mathrm{Char}(K) = p$ eine Primzahl, dann faktorisiert der Ringhomomorphismus $\mathbb{Z} \to K$ über $\mathbb{Z} \to \mathbb{Z}/p$, 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 $\mathrm{Char}(K) = 0$, dann ist der Ringhomomorphismus $\mathbb{Z} \to K$ 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 $\mathbb{Q} \to K$. Nun hat aber auch $\mathbb{Q}$ keine Unterkörper und damit ist $P \cong \mathbb{Q}$. □

3.2 Algebraische und endliche Körpererweiterungen

Sei L/K eine Körpererweiterung, dann ist L insbesondere ein Vektorraum über K. Die Körpererweiterung heisst **endlich**, falls L endliche Dimension über K hat. Der **Grad** der Koerpererweiterung ist dann diese Dimension:

$$[L : K] := \dim_K(L).$$

Beispiele 3.2.1.

- Der Körper $\mathbb{Q}(\sqrt{2})$ ist zweidimensional über $\mathbb{Q}$, also ist der Index gleich zwei:

$$\left[\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}\right] = 2.$$

- Der Körper der komplexen Zahlen hat Dimension 2 über $\mathbb{R}$, also

$$[\mathbb{C} : \mathbb{R}] = 2.$$

  Der Körper $\mathbb{R}$ hat unendliche Dimension über $\mathbb{Q}$, ja sogar überabzählbare Dimension, denn jeder $\mathbb{Q}$-Vektorraum abzählbarer Dimension ist auch als Menge abzählbar. Also insbesondere

$$[\mathbb{R} : \mathbb{Q}] = \infty.$$

Definition 3.2.2. 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 3.2.3.

- 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.

Definition 3.2.4. Im Folgenden werden wir oft eine Koerpwererweiterung L/K und einen

Zwischenkoerper $L \supset M \supset K$ betrachten. Wir schreiben dann

$$L/M/K.$$

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

Satz 3.2.5.

(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) *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

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

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

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

Das heisst, α ist Nullstelle des Polynoms $f(x) = a_0 + a_1 + \cdots + a_n x^n \in K[x]$.

(b) Die Koerpererweiterungen $L/M/K$ seien beide endlich und sei $v_1, \ldots, v_n$ eine Basis von M über K und sei $w_1, \ldots, w_m$ eine Basis von L über M. Wir behaupten, dass $(v_i w_j)_{i,j}$ eine Basis von L über K ist. Zur Linearen Unabhängigkeit: Sei

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

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

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

Für die Umkehrung schliesslich sei L/K endlich, dann ist M ein K-Unterraum von L und damit selbst endlich-dimensional. Ist schliesslich $v_1, \ldots, v_n$ 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) Seien die beiden Erweiterungen $L/M/K$ algebraisch und sei $\alpha \in L$. Dann existiert ein nichtkonstantes Polynom $f(x) \in M[x]$ so dass $f(\alpha) = 0$. Indem man f gegebenenfalls durch einen seine irreduziblen Faktoren ersetzt, kann man annehmen, dass f selbst irreduzibel ist. Sei nun M_f/M die Körpererweiterung aus Satz 3.1.6 und sei $M(\alpha)$ das Bild des kanonischen Homomorphismus $M_f \to L$. Dann ist $M(\alpha)$ endlich über M. Sei $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, dann ist jedes $a_0, \ldots, a_n$ algebraisch über K, sei $K(a_0, \ldots, a_n)$ der kleinste Zwischenkörper $M \supset K(a_0, \ldots, a_n) \supset K$, der alle Koeffizienten $a_0, \ldots, a_n$ enthält. Dann ist $K(a_0)$ endlich über K, ferner ist $K(a_0)(a_1) = K(a_0, a_1)$ endlich über $K(a_0)$ und so weiter, so das schliesslich nach iterierter Anwendung von (b) der Körper $K(a_0, \ldots, a_n)$ endlich über K ist. Das Element α schliesslich liegt ist algebraisch über $K(a_0, \ldots, a_n)$ und damit ist $K(a_0, a_1, \ldots, a_n, \alpha) = K(a_0, \ldots, a_n)(\alpha)$ endlich über K und enthält α. Also ist α algebraisch über K und damit ist L/K algebraisch.

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. □

3.3 Minimalpolynom

Satz 3.3.1. *Sei L/K eine Körpererweiterung und sei $\alpha \in L$ ein algebraisches Element. Dann existiert genau ein normiertes Polynom $m_\alpha(x) = m(x)$ kleinsten Grades in $K[x]$ mit $m(\alpha) = 0$. Dies wird das* **Minimalpolynom** *von α genannt. Das Minimalpolynom ist irreduzibel in $K[x]$. Ist $f(x) \in K[x]$ irgendein nichtkonstantes Polynom mit $f(\alpha) = 0$, dann ist f ein Vielfaches von $m(x)$. Der Grad des Minimalpolynoms ist gleich dem Körpergrad von $K(\alpha)$ über K, also*

$$\operatorname{grad}(m_\alpha) = [K(\alpha) : K].$$

Beweis. Die Menge I aller Polynome $f \in K[x]$ mit $f(\alpha) = 0$ ist ein Ideal im Hauptidealring $K[x]$. Da α algebraisch ist, ist $I \neq 0$, also gibt es genau ein ein normiertes Polynom m mit $I = mK[x]$. Dieses Polynom m hat den kleinsten Grad unter allen Polynomen, die α annullieren. Wir zeigen, dass das Ideal I prim ist, dann ist m ein Primelement also irreduzibel im Hauptidealring $K[x]$. Ist also $fg \in I$,also $f(\alpha)g(\alpha) = 0$, dann muss einer der beiden schon α annullieren, also in I liegen. Bleibt zu zeigen, dass der Grad von $K(\alpha)$ gleich dem Grad von m ist, was aber wegen $K(\alpha) \cong K[x]/mK[x]$ klar ist. □

Beispiele 3.3.2.

- 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 $\overline{K}/K$, so dass $\overline{K}$ algebraisch abgeschlossen ist. Man nennt $\overline{K}$ den* **algebraischen Abschluss** *von K.*

Beweis. Nach Satz 3.1.7 existiert zu jeder Teilmenge $T \subset K[x]$ von irreduziblen Polynomen eine algebraische Körpererweiterung K_T/K in der jedes $f \in T$ eine Nullstelle besitzt. Wir wenden dies auf die Menge T aller irreduziblen Polynome $f \in K[x]$ an und erhalten einen Körper K_1 in dem jedes irreduzible Polynom f aus $K[x]$ eine Nullstelle besitzt. Wir wiederholen den Schritt und erhalten einen Körper K_2/K_1 in dem jedes irreduzible Polynom aus K_1 eine Nullstelle besitzt und so weiter. Wir erhalten eine Kette von Körpern $K \subset K_1 \subset K_2 \subset \ldots$, so dass jedes irreduzible Polynom aus $K_n[x]$ eine Nullstelle in K_{n+1} besitzt. Sei

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

Dann ist $\overline{K}$ wieder ein Körper und er ist algebraisch abgeschlossen, denn jedes irreduzible $f \in \overline{K}[x]$ hat Koeffizienten in einem K_n, so dass f in $K_{n+1} \subset \overline{K}$ eine Nullstelle hat. Ferner ist $\overline{K}$ 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 $\phi : \overline{K} \xrightarrow{\cong} L$ gibt, der auf K die Identität ist.

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

$$\big(\phi : M \to L\big) \;\leq\; (\psi : P \to L)$$

$$:\Leftrightarrow$$

$$M \subset P \;\text{ und }\; \psi|_M = \phi.$$

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 $\phi : M \to L$. Wir müssen zeigen, dass $M = \overline{K}$ und Bild$(\phi) = L$ ist. Sei $\alpha \in \overline{K}$. Da $\overline{K}/M$ 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 $M(\alpha) \cong M_f \to L$, der ϕ fortsetzt. Da ϕ maximal ist, folgt $M(\alpha) = M$, also $\alpha \in M$. Wir haben also $M = \overline{K}$. Es bleibt zu zeigen, dass das Bild B von ϕ gleich L ist. Nun ist $B \cong \overline{K}$ 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 $\alpha \in B$. □

Satz 3.4.3. *Sei L/K eine algebraische Erweiterung und sei $\sigma : K \to \Omega$ 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 $\overline{K}$ die Menge aller $\omega \in \Omega$, die algebraisch über K sind. Dann ist $\overline{K}$ ein algebraischer Abschluss von K. Sei $\overline{L}$ ein algebraischer Abschluss von L. Da L algebraisch über K ist, ist $\overline{L}$ ebenfalls ein algebraischer Abschluss von K, also gibt es einen Isomorphismus $\overline{L} \xrightarrow{\cong} \overline{K} \subset \Omega$, dessen Einschränkung nach L das Gewünschte leistet. □

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 $\overline{\mathbb{Q}}$ 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 $\overline{\mathbb{Q}}$ 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

$$f(x) = c(x - \lambda_1) \cdots (x - \lambda_n)$$

  mit $\lambda_1, \ldots, \lambda_n \in L$ und $c \in K^\times$ und
- L von den Nullstellen erzeugt wird, also

$$L = K(\lambda_1, \ldots, \lambda_n).$$

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 $\phi : E \to L$ über K.*

Ist $L \subset \overline{K}$ für einen algebraischen Abschluss $\overline{K}$ von K, so hat jeder Körperhomomorphismus $\sigma : E \to \overline{K}$ über K das Bild L und induziert einen Isomorphismus $E \xrightarrow{\cong} L$.

Beweis. Sei $\overline{L}$ ein algebraischer Abschluss von L, dann ist dies auch ein algebraischer Abschluss von K. Ebenso ist $\overline{E}$ ein algebraischer Abschluss von K. Also gibt es einen K-Isomorphismus $\phi : \overline{E} \to \overline{L}$. Sei $f(x) = a_0 + \cdots + a_n x^n$ mit $a_j \in K$. Ist $\alpha \in E$ eine Nullstelle von f, dann gilt

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

also wird jede Nullstelle von f auf eine Nullstelle von f abgebildet. 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. □

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 $\overline{E}$ 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 $\overline{K}$ ein algebraischer Abschluss von K. Dann sind die folgenden Bedingungen äquivalent:*

Nor 1. *Alle Homomorphismen $L \to \overline{K}$ über K haben dasselbe Bild.*

Nor 2. *L ist der Zerfällungskörper einer Familie von Polynomen.*

Nor 3. *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 Nor 1 erfüllt ist. Sei f ein irreduzibles Polynom in $K[x]$, das in L eine Nullstelle α hat. Sei β eine Nullstelle von f in $\overline{K}$. Indem wir α auf β werfen, erhalten wir einen Homomorphismus $K(\alpha) \to \overline{K}$ über K. Dieser lässt sich nach L fortsetzen, es folgt also, dass β in dem gemeinsamen Bild $\tilde{L}$ aller Homomorphismen von L nach $\overline{K}$ liegt. Da f über $\overline{K}$ 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 Nor 3.

Aus Nor 3 folgt Nor 2 indem man die Familie aller Minimalpolynome von Elementen in L nimmt.

Nor 2 schliesslich liefert Nor 1 mit demselben Beweis wie Satz 3.5.2. □

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. □

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 $\varepsilon = e^{2\pi i/3}$ die primitive dritte Einheitswurzel 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 Koerpererweiterung L/K heisst **multiquadratische Erweiterung**, falls es eine Kette von Zwischenkoerpern

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

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

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 $\sigma_1, \ldots, \sigma_k$ die verschiedenen K-Einbettungen von L in einen algebraischen Abschluss $\overline{K}$ von K. Dann ist der von den Bildern $\sigma_1(L), \ldots, \sigma_k(L)$ erzeugte Unterkoerper von $\overline{K}$ 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. Eine algebraische Körpererweiterung L/K heisst **separabel**, falls jedes irreduzible Polynom $f(x) \in K[x]$ höchstens einfache Nullstellen in L hat.

Dies ist äquivalent dazu, dass jedes $\alpha \in L$ nur einfache Nullstelle seines Minimalpolynoms $m_\alpha \in K[x]$ 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*

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

Sei $D : K[x] \to K[x]$ der formale Ableitungsoperator, also $D(f) = f'$. Dann ist D linear und erfüllt die **Leibniz-Regel***:*

$$D(fg) = D(f)g + fD(g).$$

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

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

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

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

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 folgt

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

so dass $f'(\alpha) \neq 0$ folgt. □

Beispiel 3.6.4. 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 $L = K\left(\sqrt{T}\right) = K[x]/x^2 - T$ eine Körpererweiterung vom Grad 2. Wie in Satz 3.1.6 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!

Proposition 3.6.5. *Seien $L/F/K$ algebraische Körpererweiterungen. Dann gilt*

$$L/K \text{ separabel} \quad \Rightarrow \quad \left\{ \begin{array}{c} L/F \text{ separabel und} \\ F/K \text{ separabel.} \end{array} \right\}$$

Beweis. Sei L/K separabel. Dann ist offensichtlich auch F/K separabel. Sei nun $\alpha \in L$ und sei $f \in F[x]$ das Minimalpolynom über F und $g \in K[x]$ das Minimalpolynom über K. Dann gilt $f \mid g$ in $F[x]$, also gibt es

ein Polynom $h \in F[x]$ so dass $g = hf$. Da L/K separabel, ist α nur einfache Nullstelle von g und daher auch nur einfache Nullstelle von f. Somit ist L/F ebenfalls separabel. □

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

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

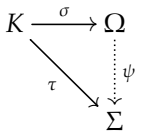
Definition 3.7.1. Sei L/K eine endliche Erweiterung und sei $\sigma : K \hookrightarrow \Omega$ eine Einbettung in einen algebraisch abgeschlossenen Körper Ω. Sei S_σ die Menge aller Fortsetzungen von σ zu einer Einbettung $\sigma^* : L \hookrightarrow \Omega$.

Lemma 3.7.2. *S_σ ist endlich und die Kardinalität $|S_\sigma|$ haengt 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 zunaechst, 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 $v_1, \ldots, v_n$ eine Basis von L als K-Vektorraum, so gibt es auch nur endlich viele Moeglichkeiten fuer $\sigma^*(v_1), \ldots, \sigma^*(v_n)$ 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 $\Omega \to \Sigma$ so dass das Diagramm



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

Beispiele 3.7.3.

- Sei $K = \mathbb{Q}$ und $L = \mathbb{Q}[T]/T^2 - 2 \cong \mathbb{Q}(\sqrt{2})$. In $\Omega = \mathbb{C}$ gibt es genau zwei Zaghlen 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 Separabilitaetsgrad $[L : K]_s$ gleich 2.

- Seien $K = \mathbb{Q}$ und $L = \mathbb{Q}[T]/(T^3 - 2) \cong \mathbb{Q}(\sqrt[3]{(2)})$. 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.

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

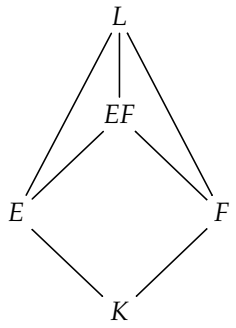
Beweis. Sei $\sigma : K \to \Omega$. Für jede Fortsetzung $\tau : E \to \Omega$ ist jede Fortsetzung von τ nach L eine Fortsetzung von σ nach L. Also erhalten wir eine Bijektion $S_\sigma(L) = \bigsqcup_{\tau \in S_\sigma(E)} S_\tau(L)$. Ferner haben alle S_τ dieselbe Kardinalität und damit folgt die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

Für die zweite Behauptung schreibe $L = K(\alpha_1, \ldots, \alpha_n)$ und beachte, dass man nach der ersten Behauptung die zweite nur für die Zwischenerweiterungen $K(\alpha_1, \ldots, \alpha_{j+1})/K(\alpha_1, \ldots, \alpha_j)$ 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 $\alpha_1, \ldots, \alpha_n$. 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 $\tau : K \to \Omega$ 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 $L \to \Omega$ über K. Umgekehrt wirft jeder Homomorphismus $L \to \Omega$ 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 $L \to \Omega$ 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. □

Definition 3.7.6. 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.



Satz 3.7.7.

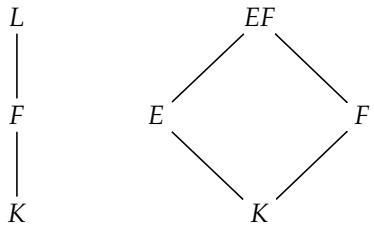
(a) *Seien $L/F/K$ Körpererweiterungen. Es gilt*

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

(b) *Ist L/K eine Körpererweiterung, sind E, F Zwischenkörper und ist E/K separabel, dann ist EF/F separabel.*

(c) *Ist L/K eine Körpererweiterung, sind E, F Zwischenkörper und sind E/K und F/K separabel, dann ist EF/K separabel.*

Die Diagramme zu diesen Situationen sind:



Beweis. (a) Ist L/K separabel, so sind L/F und F/K separabel nach Proposition 3.6.5.

Seien also L/F und F/K separabel und sei $\alpha \in L$. Sei $m(x) = m_F(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n$ das Minimalpolynom von α in $F[x]$. Da L/F separabel ist, gilt $m'(\alpha) \neq 0$. Sei $M = K(a_0, \ldots, a_{n-1})$. Dann ist M/K separabel, da es eine Untererweiterung von F/K ist. Ausserdem ist M/K endlich. Das Polynom m

ist auch das Minimalpolynom von α über M und damit ist $M(\alpha)/M$ separabel und endlich. Es folgt

$$\begin{aligned}\infty > [M(\alpha) : K]_s &= [M(\alpha) : M]_s[M : K]_s \\ &= [M(\alpha) : M][M : K] \\ &= [M(\alpha) : K]\end{aligned}$$

und damit ist $M(\alpha)/K$ separabel, also $p'(\alpha) \neq 0$, wobei p das Minimalpolynom von α über K ist. Da α beliebig ist, ist L/K separabel.

(b) Sei $\alpha \in EF$ und sei $E = K((\alpha_i)_{i\in I})$. Dann lässt sich jedes $x \in E$ als in der Form p/q darstellen, wobei $p, q \in K[(\alpha_i)_{i\in I}]$ Polynome in den α_i sind. Ferner lässt sich ein gegebenes $\alpha \in EF$ in der Form p_1/q_1 schreiben mit $p_1, q_1 \in F[(\alpha_i)_{i\in I}]$. Das bedeutet aber, dass in dieser Darstellung von α nur endlich viele der α_i vorkommen. Es reicht also anzunehmen, dass E endlich erzeugt über K ist und da es algebraisch über K ist, nehmen wir an, dass E/K endlich ist. Nach dem Satz vom primitiven Element können wir dann annehmen, dass $E = K(\beta)$ für ein Element β. Es folgt, dass $EF = F(\beta)$. Bette EF in einen algebraisch abgeschlossenen Körper Ω ein. Dort hat das Minimalpolynom $m(x) \in K[x]$ von β keine mehrfache Nullstelle, also hat auch das Minimalpolynom von β in $F[x]$ keine mehrfache Nullstelle in EF.

(c) folgt aus (b) und (a). □

3.8 Primitive Elemente

Satz 3.8.1. *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 hoechstens n Elemente haben kann, so dass

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

Nach Lemma 1.7.4 ist G zyklisch. □

Satz 3.8.2 (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 $L \supset F \supset K$.*

Ist L/K separabel, dann sind diese äquivalenten Bedingungen erfüllt.

Beweis. Ist K endlich, so ist auch L endlich und die multiplikative Gruppe von L ist nach Satz 3.8.1 zyklisch. Ein Erzeuger dieser Gruppe wird dann auch L als Körper erzeugen.

Sei nun also K unendlich. 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 $L = K(\alpha_1, \ldots, \alpha_n)$ und zeigt induktiv, dass L von einem Element erzeugt wird.

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.

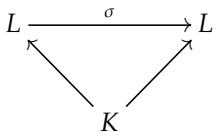
Sei schliesslich L/K separabel. Induktiv reicht es zu zeigen, dass $L = K(\alpha, \beta)$ ein primitives Element hat, falls $K(\alpha)$ und $K(\beta)$ separabel über K sind. Seien $\sigma_1, \ldots, \sigma_n$ die verschiedenen Einbettungen von L in $\overline{K}$ über K. Sei

$$P(x) = \prod_{i \neq j} (\sigma_i\alpha + x\sigma_i\beta - \sigma_j\alpha - x\sigma_j\beta).$$

Dann ist $P(x)$ nicht das Nullpolynom, also existiert ein $c \in K$ mit $P(c) \neq 0$. Die Elemente $\sigma_i(\alpha + c\beta)$ sind also alle verschieden, also hat $K(\alpha + c\beta)$ Grad $\geq n$ über K, so dass $K(\alpha + c\beta) = K(\alpha, \beta)$. □

3.9 Galois-Erweiterungen

Sei L/K eine Körpererweiterung. Ein **Galois-Homomorphismus** von L über K ist ein Isomorphismus $\sigma : L \to L$, der auf K die Identität ist, der also das Diagramm



kommutativ macht. Die **Galois-Gruppe** $\mathrm{Gal}(L/K)$ der Erweiterung L/K ist die Gruppe aller Galois-Homomorphismen von L über K.

Lemma 3.9.1. *Jeder Galois-Homomorphismus $\sigma \in \mathrm{Hom}_K(L, L)$ ist insbesondere eine K-lineare Abbildung.*

Beweis. 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. □

Beispiele 3.9.2.

- Die komplexe Konjugation $z \mapsto \overline{z}$ ist ein Element der Galois-Gruppe $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$.
- 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 Lemma vorgestellt wird.

Lemma 3.9.3. *Sei F ein Körper der Charakteristik p, für eine Primzahl p. Dann ist die Abbildung $F \to F$,*

$$x \mapsto x^p$$

ein Ringhomomorphismus. Man nennt ihn den **Frobenius-Homomorphismus** Fr_p*. Insbesondere ist dann auch die k-fache Hintereinanderschaltung $\mathrm{Fr}_p^k = \mathrm{Fr}_{p^k}$ ein Ringhomomorphismus.*

Beweis. Die Abbildung Fr ist multiplikativ und schickt die Eins auf die Eins. Es bleibt zu zeigen, dass $\mathrm{Fr}(x+y) = \mathrm{Fr}(x) + \mathrm{Fr}(y)$ gilt. Nach den binomischen Formeln ist

$$\mathrm{Fr}(x+y) = (x+y)^p = \sum_{j=0}^{p} \binom{p}{j} x^j y^{p-j}$$

und die Behauptung folgt, wenn wir zeigen, dass die nichttrivialen Binomialkoeffizienten in Charakteristik p verschwinden, also dass der Binomialkoeffizient $\binom{p}{j}$ fuer jedes $1 \le j \le p-1$ von der Primzahl p geteilt wird. Dies ist aber klar, denn $\binom{p}{j} = \frac{p!}{j!(p-j)!}$ und da j und $p-j$ beide $< p$ sind, ist jeder Primteiler von $j!(p-j)!$ echt kleiner als p, also teilt p den Nenner nicht, wohl aber den Zähler. □

In Charakteristik p gilt also insbesondere

$$(x+y)^p = x^p + y^p.$$

Lemma 3.9.4. *Sei L/K eine Körpererweiterung und sei* $\mathrm{Fix}(L/K)$ *die Menge aller Fixpunkte der Gruppe* $\mathrm{Gal}(L/K)$*-Fixpunkte in L, also*

$$\mathrm{Fix}(L/K) = \left\{ x \in L : \sigma(x) = x \ \forall_{\sigma \in \mathrm{Gal}(L/K)} \right\}.$$

Dann ist $F = \mathrm{Fix}(L/K)$ ein Körper, also ein Zwischenkörper $L \supset F \supset K$.

Beweis. Zunächst sind $0, 1 \in F$, da jeder Ringhomomorphismus diese bewahrt. Ferner gilt $x, y \in F \ \Rightarrow \ x+y \in F,\ xy \in F$, denn für jedes $\sigma \in \mathrm{Gal}(L/K)$ gilt

$$\sigma(x+y) = \sigma(x) + \sigma(y) = x + y, \quad \text{und} \quad \sigma(xy) = \sigma(x)\sigma(y) = xy.$$

Ebenso gilt $x \in F \ \Rightarrow \ -x \in F$ und für $x \neq 0$ ist auch $x^{-1} \in F$, also ist F ein Unterkörper von L. Da jedes σ auf K die Identität ist, ist $K \subset F$. □

Definition 3.9.5. Eine Körpererweiterung L/K heisst **Galois-Erweiterung**, falls der Fixkörper gleich K ist, falls also $\mathrm{Fix}(L/K) = K$ gilt.

Beispiele 3.9.6.

- $\mathbb{C}/\mathbb{R}$ ist eine Galois-Erweiterung, da die komplexe Konjugation $\mathbb{R}$ als Fixkörper hat.
- $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ ist galoissch, da der Fixkörper von $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ gleich $\mathbb{Q}$ ist.
- $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ 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 $\tau : L \to L$ 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 $\tau = \mathrm{Id}$, 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. Für einen Galois-Homomorphismus $\tau : L \to L$ gilt aber $\tau(\alpha)^3 = \tau(\alpha^3) = \tau(2) = 2$ und damit folgt $\tau(\alpha) = \alpha$ wie verlangt. □

Lemma 3.9.7. *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! □

Satz 3.9.8 (Artin)**.** *Sei L ein Körper und sei Γ eine endliche Untergruppe von $\mathrm{Aut}(L)$ der Ordnung n. Sei K der Fixkörper*

$$K = L^\Gamma = \left\{x \in L : \gamma(x) = x \ \forall_{\gamma \in \Gamma}\right\}.$$

Dann ist L/K eine endliche Erweiterung vom Grad

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

Die Erweiterung L/K ist normal und separabel.

Beweis. Sei $\alpha \in L$ und sei $\{\gamma_1, \ldots, \gamma_r\}$ eine maximale Teilmenge von Γ so dass die Elemente $\gamma_1\alpha, \ldots, \gamma_r\alpha$ paarweise verschieden sind. Ist $\tau \in \Gamma$, dann unterscheidet sich $(\tau\gamma_1\alpha, \ldots, \tau\gamma_r\alpha)$ von $(\gamma_1\alpha, \ldots, \gamma_r\alpha)$ nur in der Reihenfolge. Daher ist α eine Nullstelle des Polynoms

$$f(x) = \prod_{j=1}^{r} (x - \gamma_j\alpha)$$

und für jedes $\tau \in \Gamma$ 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 3.9.7 folgt ausserdem, dass $[L : K] \leq n$. Andererseits ist aber $n \leq [L : K]_s \leq [L : K]$, so dass Gleichheit folgt. □

Satz 3.9.9 (Hauptsatz der Galois-Theorie)**.** *Sei L/K eine endliche Körpererweiterung und sei $\Gamma = \mathrm{Gal}(L/K)$ ihre Galois-Gruppe.*

(a) *L/K ist genau dann galoissch, wenn die Erweiterung normal und separabel ist.*

(b) *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 $\Sigma = \mathrm{Gal}(L/F)$ ein Normalteiler in Γ ist. In diesem Fall gilt*

$$\mathrm{Gal}(F/K) \cong \Gamma/\Sigma.$$

(c) *Ist L/K galoissch, so ist die Abbildung $F \mapsto \mathrm{Gal}(L/F)$ eine Bijektion*

$$\phi : \{\textit{Zwischenkörper } L \supset F \supset K\} \xrightarrow{\cong} \left\{\textit{Untergruppen von } \Gamma\right\}.$$

Ihre Umkehrabbildung ist $\psi : \Sigma \mapsto L^\Sigma = \left\{x \in L : \sigma(x) = x \ \forall_{\sigma\in\Sigma}\right\}$. Hierbei gehen die normalen Erweiterungen F/K genau auf die normalen Untergruppen von Γ.

Bemerkung: Sind $L/M/K$ Koepererweiterungen so dass beide Teilerweiterungen galoisch sind, so braucht L/K nicht galoisch zu sein. Das Problem ist die Normalitaet. Ein Beispiel ist durch $K = \mathbb{Q}$, $M = \mathbb{Q}(\sqrt{2})$ und $L = \mathbb{Q}(\sqrt[4]{2})$ gegeben, denn $f(x) = x^4 - 2$ ist irreduzibel ueber $\mathbb{Q}$, hat in L aber nur die beiden Nullstellen $\pm\sqrt[4]{2}$ und nicht die beiden anderen Nullstellen $\pm i\sqrt[4]{2}$..

Beweis. (a) Sei L/K galoissch mit Galois-Gruppe Γ. Sei $\alpha \in L$. Seien $\alpha_1, \ldots, \alpha_n$ die verschiedenen Elemente des Γ-Orbits von α. Ist dann $\tau \in \Gamma$, so unterscheidet sich $\tau\alpha_1, \ldots, \tau\alpha_n$ von der ersten Familie nur in der Reihenfolge. Das bedeutet, dass das Polynom

$$f(x) = \prod_{j=1}^{n}(x - \alpha_j)$$

invariant unter Γ ist, also in $K[x]$ liegt. Da $f(\alpha) = 0$, wird f von dem Minimalpolynom geteilt. Da f über L in Linearfaktoren zerfällt, zerfällt jeder Teiler von f und damit zerfällt auch das Minimalpolynom von α in Linearfaktoren. Nach Satz 3.5.5 ist L/K normal. Da die Nullstellen alle verschieden sind, ist L/K auch separabel.

Sei umgekehrt L/K normal und separabel und sei $\alpha \in L^\Gamma$. Sei $\sigma : K(\alpha) \to \overline{L}$ eine Einbettung über K in einen algebraischen Abschluss von L. Wir dehnen σ zu einer Einbettung $L \hookrightarrow \overline{L}$ aus. Dann ist σ ein Automorphismus von L über K, also ein Element von Γ. Deshalb lässt σ das Element α fest, also folgt $|\mathrm{Hom}_K(K(\alpha), \overline{L})| = 1$. Da α separabel über K ist, folgt $1 = [K(\alpha) : K]_s = [K(\alpha) : K]$, also $\alpha \in K$ und (a) ist bewiesen.

(b) L/F ist normal nach Satz 3.5.5 Nor 1 und ist separabel nach Satz 3.7.7, also galoissch. Sei nun F/K ebenfalls galoissch und seien $\sigma \in \mathrm{Gal}(L/F)$ und $\tau \in \mathrm{Gal}(L/K)$. Da F/K normal ist folgt nach Satz 3.5.5, Nor 1, 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 $\tau^{-1}\sigma\tau \in \mathrm{Gal}(L/F)$, diese Gruppe ist also ein Normalteiler. Da jedes $\tau \in \Gamma$ den Körper F fixiert, operiert Γ auf F, man erhält also einen Homomorphismus $\Gamma \to \mathrm{Gal}(F/K)$ mit Kern Σ. Andererseits lässt sich jedes $\eta \in \mathrm{Gal}(F/K)$ zu einer Abbildung $L \to \overline{F} = \overline{L}$ fortsetzen, deren Bild L ist, da L/K normal ist. Damit ist die Abbildung $\Gamma \to \mathrm{Gal}(F/K)$ 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 $\tau : F \to \overline{K} = \overline{F}$ eine

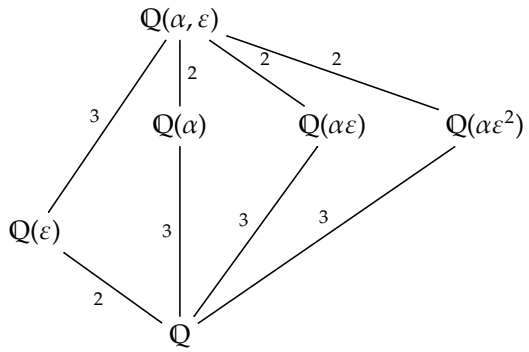
Einbettung, dann kann man τ nach L ausdehnen $\tau : L \to \overline{K} = \overline{L}$, das Bild ist dann L, τ also in Γ. Da Σ ein Normalteiler ist, folgt nach obiger Rechnung, dass $\tau(F)$ ebenfalls von σ punktweise festgehalten wird. Da L/F galoissch ist, folgt, dass $\tau(F) = F$ ist und damit ist F/K normal nach Satz 3.5.5.

(c) 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 $\psi \circ \phi = \mathrm{Id}$. 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). □

Beispiel 3.9.10. 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 galoisch. Da die Galois-Gruppe die drei Nullstellen von f permutiert, ist sie eine Untergruppe von Per(3). Der Zwischenkörper $\mathbb{Q}(\sqrt[3]{2})$ hat die Grade

$$[L : \mathbb{Q}(\sqrt[3]{2})] = 2, \qquad [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3,$$

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 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.

3.10 Norm und Spur

Definition 3.10.1. Sei L/K eine endliche Koerpererweiterung und sei $a \in L$. wir definieren die **Norm** und die **Spur** von a durch

$$N_{L/K}(a) := \det(M_a),$$
$$Sp_{L/K}(a) := \mathrm{tr}(M_a),$$

wobei $M_a : L \to K$ die K-lineare Abbildung $M_a(x) = ax$ bezeichnet.

Lemma 3.10.2. *Für $a, b \in L$ und $\lambda \in K$ gilt*

(a) $N_{L/K}(a) \in K$, $Sp_{L/K}(a) \in K$,

(b) $N_{L/K}(ab) = N_{L/K}(a)N_{L/K}(b)$,

(c) $Sp_{L/K}(a+b) = Sp_{L/K}(a) + Sp_{L/K}(b)$, $Sp(\lambda a) = \lambda Sp(a)$

(d) $N_{L/K}(\lambda) = \lambda^{[L:K]}$, $Sp_{L/K}(\lambda) = [L:K]\lambda$.

Beweis. Diese Eigenschaften sind klar. □

Lemma 3.10.3. *Sei L/K endlich separabel und sei $H = \mathrm{Hom}_K(L, \overline{K})$ fuer einen algebraischen Abschluss $\overline{K}$ von K, dann gilt fuer jedes $a \in L$,*

$$N_{L/K}(a) = \prod_{\tau \in H} \tau(a),$$
$$Sp_{L/K}(a) = \sum_{\tau \in H} \tau(a).$$

Ist L/K galoisch, kann statt H die Galois-Gruppe genommen werden.

Beweis. Sei $\chi(x) = \det(x - M_a)$ das Charakteristische Polynom. Wir zeigen, dass $\chi(x) = P(x)^d$, wobei $d = [L : K(a)]$ und $P(x)$ ist das Minimalpolynom von a. In der Tat, $1, a, a^2, \ldots, a^{m-1}$ ist eine Basis von $K(a)/K$, wobei $m = [K(a) : K]$ der Grad des Minimalpolynoms ist. Ist nun $v_1, \ldots, v_d$ eine Basis von $L/K(a)$ dann ist

$$v_1, v_1 a, \ldots, v_1 a^{m-1}, v_2, \ldots, v_d a^{m-1}$$

eine Basis von L/K. Die Matrix von $M_a : x \mapsto ax$ hat dann auf der Diagonalen Bloecke der Form

$$\begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \\ -c_m & -c_{m-1} & -c_{m-2} & \ldots & -c_1 \end{pmatrix},$$

wobei $P(x) = x^m + c_1 x^{m-1} + \cdots + c_m$. Damit folgt $\chi(x) = P(x)^d$. Die (einfachen) Nullstellen von $P(x)$ werden von den Elementen τ von H auf die entsprechendne Nullstellen in $\overline{K}$ geworfen, wobei alle moeglichen Nullstellen vorkommen. Zwei τ unbd τ' werfen a genau dann auf dasselbe Element, wenn sie auf $K(a)$ uebereinstimmen. Ist $\sigma_1, \ldots \sigma_m$ ein Vertretersystem von H modulo der Aequivalenzrelation $\tau(a) = \tau'(a)$, dann ist

$$P(x) = \prod_{j=1}^{m} (x - \sigma_j(a)).$$

Daher ist $\chi(x) = \prod_{j=1}^{m} (x - \sigma_j(a))^d$ und daher

$$N_{L/K}(a) = (-1)^{dm}\chi(0) = \prod_{j=1}^{'} \sigma_j(a)^d = \prod_{\tau \in H} \tau(a).$$

Ferner ist die Spur das negative des ersten Koeffizienten von $\chi(x)$, also

$$Sp_{L/K}(a) = \sum_{j-1}^{m} d\sigma_j(a) = \sum_{\tau\in H} \tau(a). \qquad \square$$

Lemma 3.10.4. *Sind $L/M/K$ endliche separable Koepererweiterungen, so gilt*

$$N_{M/K}(N_{L/M}(a)) = N_{L/K}(a) \quad \textit{und} \quad Sp_{M/K}(Sp_{L/M}(a)) = Sp_{L/K}(a).$$

Beweis. Die Menge $H = \mathrm{Hom}_K(L, \overline{K})$ zerfaellt unter der Aequivalenzrelation

$$\tau \sim \tau' \quad \Leftrightarrow \quad \tau|_M = \tau'|_M$$

in $m = [M : K]$ Aequivalenzklassen. Ist $\sigma_1, \ldots, \sigma_m$ ein Vertretersystem, so ist $\mathrm{Hom}_K(M, \overline{K}) = \{\sigma_1|_M, \ldots, \sigma_m|_M\}$ und

$$\begin{aligned} Sp_{L/K}(x) \sum_{j=1}^{m} \sum_{\sigma\sim\sigma_j} \sigma(x) &= \sum_{j=1}^{m} Sp_{\sigma_j(L)/\sigma_j(M)}(\sigma_j(x)) \\ &= \sum_{j=1}^{m} \sigma_j(Sp_{L/M}(x)) = Sp_{M/K}(Sp_{L/M}(x)) \end{aligned}$$

und ebenso fuer die Norm. $\square$

Lemma 3.10.5 (Dedekind)**.** *Es seien $\tau_1, \ldots, \tau_n$ verschiedene Homomorphismen von einem Körper K in einen Körper L. Sind $c_1, \ldots, c_n \in L$ mit*

$$c_1\tau_1(x) + \cdots + c_n\tau_n(x) = 0$$

für jedes $x \in K$, dann gilt $c_1 = c_2 = \cdots = c_n = 0$.

Beweis. Durch Induktion nach n. Der Fall $n = 1$ ist klar. Sei also die Behauptung für n gezeigt und sei

$$c_1\tau_1(x) + \cdots + c_n\tau_n(x) + c_{n+1}\tau_{n+1}(x) = 0$$

für jedes $x \in K$. Da $\tau_1 \neq \tau_{n+1}$ gibt es ein $a \in K$ mit $\tau_1(a) \neq \tau_{n+1}(a)$. Indem wir einmal x durch ax ersetzen und zum anderen die obige Gleichung mit $\tau_{n+1}(a)$ multiplizieren erhalten wir

$$\begin{aligned} c_1\tau_1(a)\tau_1(x) + c_2\tau_2(a)\tau_2(x) + \cdots + c_{n+1}\tau_{n+1}(a)\tau_{n+1}(x) = 0, \\ c_1\tau_{n+1}(a)\tau_1(x) + c_2\tau_{n+1}(a)\tau_2(x) + \cdots + c_{n+1}\tau_{n+1}(a)\tau_{n+1}(x) = 0. \end{aligned}$$

Da der letzte Summand in beiden Fällen derselbe ist, gibt die Differenz:

$$c_1\Big(\tau_1(a) - \tau_{n+1}(a)\Big)\tau_1(x) + \cdots + c_n\Big(\tau_n(a) - \tau_{n+1}(a)\Big)\tau_n(x) = 0.$$

Nach Induktionsvoraussetzung folgt insbesondere $0 = c_1(\tau_1(a) - \tau_{n+1}(a))$ und daher $c_1 = 0$. Damit ist aber

$$c_2\tau_2(x) + \cdots + c_n\tau_n(x) + c_{n+1}\tau_{n+1}(x) = 0,$$

so dass eine abermalige Anwendung der Induktionsvoraussetzung $c_2 = c_3 = \cdots = c_{n+1} = 0$ liefert. □

Proposition 3.10.6. *Sei L/K eine endliche Galois-Erweiterung mit Galois-Gruppe G und sei $H \subset G$ eine Untergruppe und sei $F = \mathrm{Fix}(H)$ der Fixkörper. Ist dann $x_1, \ldots, x_n$ ein Erzeugendensystem des K-Vektorraums L, dann ist $Sp_{L/F}(x_1), \ldots, Sp_{L/F}(x_n)$ ein Erzeugendensystem des K-Vektorraums F.*

Proof. Sei $f \in F$. Nach dem Dedekind-Lemma gibt es ein $a \in L$ mit $Sp(a) \neq 0$. Sei $d = \frac{af}{Sp(a)}$. Dann folgt

$$Sp(d) = Sp\left(\frac{f}{Sp(a)}a\right) = \frac{f}{Sp(a)}Sp(a) = f.$$

Schreibe $d = \lambda_1 x_1 + \cdots + \lambda_n x_n$ mit $\lambda_1, \ldots, \lambda_n \in K$, dann folgt

$$f = Sp(d) = Sp(\lambda_1 x_1 + \cdots + \lambda_n x_n) = \lambda_1 Sp(x_1) + \cdots + \lambda_n Sp(x_n).$$ □

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.

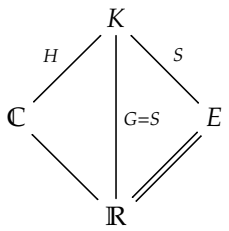
2. Schritt: $\mathbb{C}$ *hat keine Galois-Erweiterung vom Grad 2^k, $k \in \mathbb{N}$.*
Ist $L/\mathbb{C}$ galoisch vom Grad 2^k, dann hat die Galois-Gruppe $G = \mathrm{Gal}(L/\mathbb{C})$ die Ordnung 2^k, also hat sie eine Untergruppe G' vom Index 2. Dann hat $F = \mathrm{Fix}(G')$ den Grad 2 ueber $\mathbb{C}$, 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 $\mathrm{grad}(m_a) = [\mathbb{R}(a) : \mathbb{R}]$ 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 $G = \mathrm{Gal}(K : \mathbb{R})$ und sei S eine 2-Sylow-Gruppe in G. Der Körper $E = \mathrm{Fix}(S)$ 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 $H = \mathrm{Gal}(K : \mathbb{C})$ eine 2-Sylowgruppe. Nach dem zweiten Schritt muss $H = \{1\}$ sein, also $K = \mathbb{C}$. □



3.12 Kreisteilungskörper

Für $n \in \mathbb{N}$ sei

$$C_n(x) = \prod_{\substack{0 \le j \le n-1 \\ ggT(j,n)=1}} (x - e^{2\pi i j/n})$$

das n-te **Kreisteilungspolynom** in $\mathbb{C}[x]$.

Der Grad des n-ten Kreisteilungspolynoms C_n ist gleich

$$\phi(n) = \left|(\mathbb{Z}/n)^\times\right|$$

die **Eulersche ϕ-Funktion**.

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*

$$\phi(p^k) = p^k - p^{k-1}.$$

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 $\mathbb{Z}/p^{k-1} \hookrightarrow \mathbb{Z}/p^k$, $(n + p^{k-1}\mathbb{Z}) \mapsto (np + p^k\mathbb{Z})$. □

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

$$C_n(x) = \prod_{\zeta \in \mu_n^{prim}} (x - \zeta),$$

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. □

Hier eine Liste der ersten Kreisteilungspolynome:

$$\begin{aligned}
C_1(x) &= x - 1 \\
C_2(x) &= x + 1 \\
C_3(x) &= x^2 + x + 1 \\
C_4(x) &= x^2 + 1 \\
C_5(x) &= x^4 + x^3 + x^2 + x + 1 \\
C_6(x) &= x^2 - x + 1 \\
C_7(x) &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\
C_8(x) &= x^4 + 1 \\
C_9(x) &= x^6 + x^3 + 1 \\
C_{10}(x) &= x^4 - x^3 + x^2 - x + 1
\end{aligned}$$

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 2.6.3 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 $\overline{f}, \overline{g}, \overline{h}$ die Bilder in $\mathbb{Z}/p\mathbb{Z}[x]$. Es ist dann $\overline{f}(x)\overline{h}(x) = \overline{g}(x^p) = \overline{g}(x)^p$. Daher folgt über dem endlichen Körper $\mathbb{F}_p$, dass $x^n - 1 = \overline{f}\,\overline{g}$. Jeder irreduzible Faktor von $\overline{f}$ ist wegen $\overline{g}^p = \overline{fh}$ auch ein Faktor von $\overline{g}$ 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 $\tau \in \mathrm{Gal}(K/\mathbb{Q})$ 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 2.6.3, 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 $\mathrm{ggT}(d, n) = 1$. 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 $G = \mathrm{Gal}(K/\mathbb{Q})$. 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 $\tau \in \mathrm{Gal}(K/\mathbb{Q})$, 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

$$\theta : \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \hookrightarrow (\mathbb{Z}/n)^\times,$$

gegeben durch $\tau \mapsto k = k(\tau)$. Ist $\gamma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ 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

$$|\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})| = [\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg(C_n) = |(\mathbb{Z}/n)^\times|.$$

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 $p \equiv a \mod n$. Insbesondere gibt es unendlich viele Primzahlen p mit $p \equiv 1 \mod n$.*

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 $\mathrm{Gal}(K : \mathbb{Q}) \cong G$.

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

$$\begin{aligned} G = \mathrm{Gal}(L/\mathbb{Q}) &\cong (\mathbb{Z}/N)^\times \cong (\mathbb{Z}/p_1)^\times \times \cdots \times (\mathbb{Z}/p_k)^\times \\ &\cong Z_{p_1-1} \times \cdots \times Z_{p_k-1}. \end{aligned}$$

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 $\mathbb{Q}$. □

3.13 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 3.13.1. *Sei* $\mathrm{Char}(K) = p$ *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 3.13.2. (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**

$$\mathrm{Fr}_q : x \mapsto x^q$$

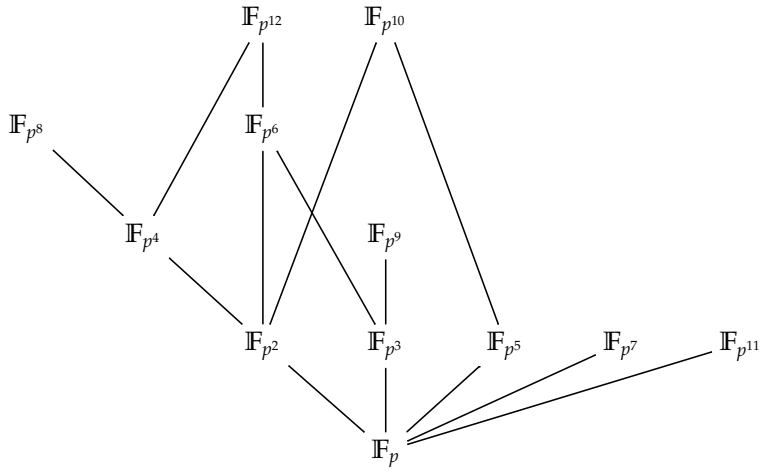
erzeugt

Beweis. Ist F ein endlicher Körper der Kardinalität $q = p^k$, dann ist $F^\times$ eine endliche Gruppe, die nach Satz 3.8.1 zyklisch ist. Das bedeutet, $F^\times$ besteht genau aus den Nullstellen des Polynoms $f(x) = x^{q-1} - 1$ und dieses Polynom hat keine mehrfachen Nullstellen in F nach Lemma 3.13.1. Andererseits bedeutet dies, 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 $\Gamma = \mathrm{Gal}(\mathbb{F}_r/\mathbb{F}_q)$ von Fr_q erzeugt wird, reicht es, einzusehen, dass $\mathbb{F}_q$ genau aus den Fixpunkten von Fr besteht. Dies ist aber klar, denn $\mathrm{Fr}(x) = x$ ist äquivalent mit $x^q = x$ oder $x(x^{q-1} - 1) = 0$. □

Im Bild sieht man den Anfang des Inklusionsbaums der endlichen Körper über $\mathbb{F}_p$.



Proposition 3.13.3 (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 $\mathbb{F}_{p^k}^\times$ ist eine endliche Untergruppe der multiplikativen Gruppe eines Körpers, also zyklisch nach Satz 3.8.1. Ihre Ordnung ist $p^k - 1$, also besteht $\mathbb{F}_{p^k}^\times$ genau aus den Nullstellen des 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. □

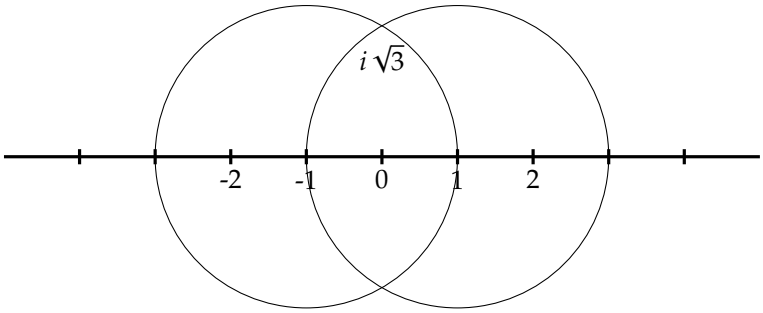
3.14 Konstruktionen mit Zirkel und Lineal

Definition 3.14.1. Wir definieren die Menge $C \subset \mathbb{C}$ der **konstruierbaren Zahlen** induktiv wie folgt:

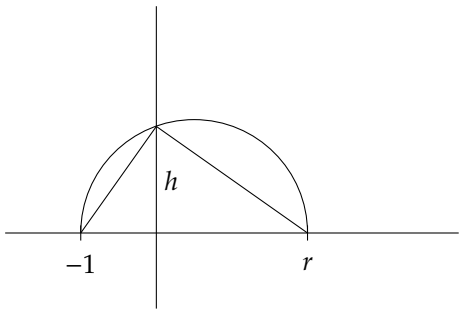
1. $0, 1 \in C$,
2. (Schnittpunkt zweier Geraden) Sind $z_1 \neq z_2$ und $z_3 \neq z_4$ in C und schneiden sich die Geraden durch (z_1, z_2) und durch (z_3, z_4) in genau einem Punkt z, dann liegt z in C.
3. (Schnittpunkte von Gerade und Kreis) Sind $z_1, \ldots, z_5 \in C$ mit $z_1 \neq z_2$ und ist 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 $z \in C$. Hierbei ist es erlaubt, dass die Gerade tangential zum Kreis liegt, es also nur einen Schnittpunkt gibt.
4. (Schnittpunkte zweier Kreise) Sind $z_1, \ldots, z_6$ in 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 $z \in C$. Hierbei wird vorausgesetzt, dass die beiden Kreise verschieden sind.

Beispiele 3.14.2.

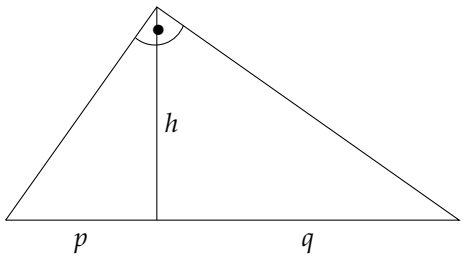
- Man sieht sofort, dass $\mathbb{Z} \subset C$. Aber auch $i\sqrt{3} \in C$



- Man kann Wurzeln ziehen in C. Genauer gilt: Ist $z \in C$ und ist $a \in \mathbb{C}$ mit $a^2 = z$, dann ist $a \in C$. 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 $r \in C$, da man den Kreis um Null mit Radius $r = |z|$ nur an der x-Achse abtragen muss. Da man Winkel durch Konstruktion halbieren kann, reicht es zu zeigen, dass $\sqrt{r}$ in 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 $h = \sqrt{r}$.



Höhensatz:

$h^2 = pq$

Satz 3.14.3. *Die Menge C der konstruierbaren Zahlen ist ein Unterkörper von $\mathbb{C}$. Für eine komplexe Zahl z sind äquivalent:*

(a) $z \in C$.

(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 $j = 0, \ldots, n-1$.*
Mit anderen Worten, z liegt in einer **multiquadratischen Erweiterung** *von $\mathbb{Q}$.*

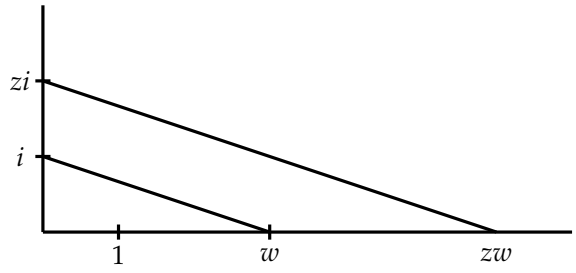
(c) *z liegt in einer Galoiserweiterung $L/\mathbb{Q}$, deren Grad eine Potenz von 2 ist:* $[L : \mathbb{Q}] = 2^m$.

Bemerkung: Damit eine komplexe Zahl z konstruierbar ist, reicht es *nicht* aus, dass sie in einem Körper K/Q vom Grad 2^k über $\mathbb{Q}$ liegt, denn es gibt Körper K/Q vom Grad 4, die nicht galoisch über 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 Per(n) eine Galois-Erweiterung $L/\mathbb{Q}$ gibt mit Gruppe $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathrm{Per}(n)$. Die Gruppe $G = \mathrm{Per}(4)$ hat 24 Elemente und hat $H = \mathrm{Per}(3)$ als nicht-normale Untergruppe vom Index 4. Sei also $K = L^H$, dann ist $K/\mathbb{Q}$ vom Grad 4 und ist nicht galoisch.

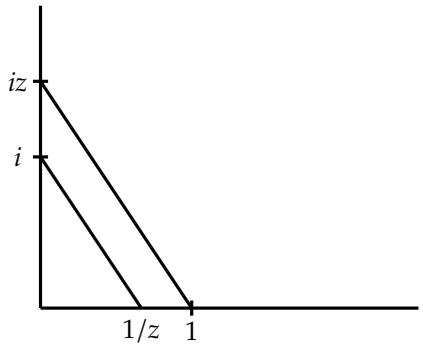
Beweis des Satzes. Indem wir die Schnittpunkte der beiden Kreise in obiger Zeichnung, also $\pm i\sqrt{3}$ verbinden, erhalten wir die imaginäre Achse. Diese schneiden wir mit dem Einheitskreis und erhalten $\pm i \in C$. Ferner gilt: $z \in C \Rightarrow \bar{z} \in C$, was man auf verschiedene Weise 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: $z, w \in C \Rightarrow z \pm w \in C$: 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: $z, w \in C \Rightarrow zw \in C$. 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 zw, siehe Bild.



Wir zeigen: $z \in C, z \neq 0 \Rightarrow \frac{1}{z} \in C$. 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 C ein Körper ist, insbesondere liegt $\mathbb{Q}$ in C. Um (a)⇒(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: 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

$$\mathrm{Re}\left((z(t) - z_3)\overline{i(z_4 - z_3)}\right) = 0.$$

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 $|z|^2 = z\overline{z}$ schreiben, wird daraus eine Gleichung der Form

$$(a + bt)(\overline{a} + \overline{b}t) = c$$

wobei a, b, c in dem Körper K liegen. Das gesuchte t ist eine Lösung der quadratischen Gleichung

$$|a|^2 - c + t(a\overline{b} + \overline{a}b) + |b|^2t^2 = 0,$$

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

$$(z - a)(\overline{z} - \overline{a}) = b$$
$$(z - c)(\overline{z} - \overline{c}) = d$$

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

$$\overline{z} = \frac{b}{z - a} + \overline{a}.$$

Setzen wir dies in die zweite Gleichung ein, erhalten wir

$$(z - c)\left(\frac{b}{z - a} + \overline{a} - \overline{c}\right) = d,$$

was zu einer quadratischen Gleichung über K führt, so dass die Behauptung bewiesen ist.

Damit ist (a)⇒(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 3.14.2 gesehen haben, so dass man auch z konstruieren kann.

(b)⇒(c) Dies folgt aus Lemma 3.5.11, da es besagt, dass mit L auch die normale Huelle von L ueber $\mathbb{Q}$ multiquadratisch ist.

(c)⇒(b): Sei $z \in L$ mit $L/\mathbb{Q}$ galoisch von 2-Potenzgrad. Nach Korollar 1.8.4 gibt es in $G = \mathrm{Gal}(L/\mathbb{Q})$ 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 3.14.4.

- **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 $\mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q}$ 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.

3.15 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

$$P(s_1, \ldots, s_n) = 0, \qquad s_1, \ldots, s_n \in S$$

für ein Polynom $P \in K[x_1, \ldots, x_n]$ 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.

Satz 3.15.2. *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 zunaechst 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 unabhaengig ist. Dann muss $|T_s| < n$ sein. Sei

$K_1 = K(s)$ und $S' = S \setminus \{s\}$. Dann sind T_s und S' algebraisch unabhaengig ueber dem Koerper 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 3.15.3. *Sei K ein algebraisch abgeschlossener Körper und sei $L = K(t) = \mathrm{Quot}(K[t])$ der rationale Funktionenkörper.*

(a) *Es ist $G = \mathrm{Gal}(L/K) \cong \mathrm{PGL}_2(K) := \mathrm{GL}_2(K)/K^\times I$.*

(b) *Sei H die Untergruppe von G isomorph zu $\left\{\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right) : x \in K\right\}$. Dann ist $L^H = K$. Insbesondere ist bei transzendenten Erweiterungen der Hauptsatz der Galois-Theorie verletzt, denn $\mathrm{Gal}(L/L^H) \neq H$.*

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

$$\alpha(\infty) = \begin{cases} 0 & \mathrm{grad}(a) < \mathrm{grad}(b), \\ \infty & \mathrm{grad}(a) > \mathrm{grad}(b), \\ \frac{\text{Leitkoeffizient von } a}{\text{Leitkoeffizient von } b} & \mathrm{grad}(a) = \mathrm{grad}(b) \end{cases}$$

sein. Jedes $\alpha \in K$ liefert dann die konstante Abbildung. Wir behaupten, dass jedes $\alpha \in L \setminus K$ eine surjektive Abbildung $\hat{K} \to \hat{K}$ 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 $\mathrm{grad}(g) \leq 1$. Dasselbe gilt für Nullstellen, so dass $\mathrm{grad}(f) \leq 1$.

(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. □

Index