Skript zur Algebra

Universität Regensburg

Sommersemester 2016

Zusammenfassung

Dieses Skript entstand anlässlich des Examenskurs für Lehramt Gymnasium an der Universität Regensburg im Sommersemester 2016. Es beinhaltet jedoch nicht nur Basiswissen, sondern auch die zugehörigen Ideen und Beweise, die aus Zeitgründen in der Vorlesung oft ausgelassen werden müssen. Die mit * gekennzeichneten Beispiele sind zum Teil aus früheren Examensaufgaben entnommen.

Inhaltsverzeichnis

Danksagung

Algebra gehört seit langer Zeit schon zu den Basiskursen eines Mathematikstudiums, und ist seit geraumer Zeit auch Teil des Lehrplans für Lehramtsstudenten. Es ist ein faszinierendes Fach, das nicht immer ganz einfach sein kann — aber auf jeden Fall Spaß machen soll. Ich kann mich noch lebhaft an die Algebravorlesung von Professor Wolfgang Zimmermann an der Ludwig-Maximilians-Universität München erinnern, die ich damals hörte, und die mit zu der Wahl meines Themas und meiner Studienrichtung im weiteren Studienverlauf beigetragen hat.

Ich weiß es sehr zu schätzen, daß er in mir die Liebe zur Algebra, und zu abstraktem Denken allgemein, geweckt und gefördert hat und mir eine so umfassende und gute Grundlage für mein weiteres Studium angedeihen hat lassen.

Dieses Skript basiert auf seiner Vorlesung, und will ihm hiermit herzlich dafür danken, daß es mir zur Verfügung steht.

Ich möchte auch David Koniecny danken, der einen großen Beitrag dazu geleistet hat, Schreibfehler aus dem Skript auszumerzen.

Kapitel 1

Gruppentheorie

1.1 Gruppen und Untergruppen

1.1.1 Gruppenaxiome

Definition 1.1.1. Sei M eine Menge und $\cdot : M \times M \to M$; $(x, y) \mapsto x \cdot y = xy$ eine Abbildung. Wir betrachten folgende Axiome:

(a) Assoziativität: $\forall x, y, z \in M$: $(xy)z = x(yz)$.

(b) Neutrales Element: $\exists! e \in M \forall x \in M$: $ex = x = xe$.

(c) Inverses Element: $\forall x \in M \exists! x' \in M$: $xx' = e = x'x$. Wir setzen $x^{-1} := x'$.

(d) Kommutativität: $\forall x, y \in M$: $xy = yx$.

$(M, \cdot)$ heißt Gruppe, falls (a), (b), (c) gelten, abelsche Gruppe, falls zusätzlich (d) gilt. $(M, \cdot)$ heißt Monoid, falls (a), (b) gelten, abelsches Monoid falls zusätzlich (d) gilt.

Ist $(M, \cdot)$ Gruppe, dann gilt $\forall x, y \in M$:

$$\begin{aligned} (xy)^{-1} &= y^{-1}x^{-1} \\ (x^{-1})^{-1} &= x \end{aligned}$$

Definition 1.1.2. Die Zahl $|M| \in \mathbb{N}_0 \cup \{\infty\}$ heißt Ordnung von M.

In abelschen Monoiden $(M, +)$ schreibt man 0 statt e, $+$ statt $\cdot$ und $-x$ statt x^{-1}.

Proposition 1.1.3. *Sei $(M, \cdot)$ ein Monoid und $x_1, \ldots, x_n \in M$. Es gilt für $0 \leqslant m \leqslant n$*

$$\prod_{i=1}^{n} x_i = \prod_{i=1}^{m} x_i \prod_{i=m+1}^{n} x_i.$$

Genauer, multipliziert man $\{x_1, \ldots x_n\}$ in beliebiger sinnvoller Klammerung, dann erhält man stets $\prod_{i=1}^{n} x_i$.

Beweis. Induktion nach n. Die Aussage ist klar für $n = 0, 1$. Sei also $n \geqslant 2$. Berechnet man das Produkt bei einer Klammerung, dann erhält man $u \cdot v$, wobei u das Podukt von $x_1, \ldots, x_m$ und v das Produkt von $x_{m+1}, \ldots, x_n$ ist, jeweils mit einer gewissen Klammerung. Nach Induktionsannahme gilt $u = \prod_{i=1}^{m} x_i$ und $v = \prod_{j=1}^{n-m} x_{m+j}$. Es folgt $u \cdot v = \prod_{i=1}^{n} x_i$. □

Im Falle $x_i = x$ $\forall 1 \leqslant i \leqslant n$ setzt man $x^n := \prod_{i=1}^{n} x$. Dann gilt $x^{n+m} = x^n x^m$ und $(x^n)^m = x^{nm}$ für $n, m \in \mathbb{N}_0$. Ist M eine Gruppe, dann setzt man $x^{-n} := (x^{-1})^n = (x^n)^{-1}$. Also ist $x^a \forall a \in \mathbb{Z}$ erklärt, es gilt $\forall a, b \in \mathbb{Z}$

$$\begin{aligned} x^{a+b} &= x^a x^b \\ (x^a)^b &= x^{ab} = (x^b)^a. \end{aligned}$$

Ist M eine abelsche Gruppe, dann schreibt man ax statt x^a. Dann gilt für alle $x \in M$ und $a, b \in \mathbb{Z}$

$$\begin{aligned}(a+b)x &= ax + bx,\\ a(bx) &= (ab)x.\end{aligned}$$

Proposition 1.1.4. *Sei $(M, \cdot)$ abelsches Monoid. Für $x_1, \dots, x_n \in M$, $n \in \mathbb{N}_0$, $\sigma \in \mathfrak{S}_n$ gilt $\prod_{i=1}^n x_i = \prod_{i=1}^n x_{\sigma(i)}$. Für $x, y \in M$, $n \in \mathbb{N}_0$ gilt $(xy)^n = x^n y^n$. Ist $(M, \cdot)$ eine abelsche Gruppe, $x, y \in M$, $a \in \mathbb{Z}$, dann $(xy)^a = x^a y^a$.*

Beispiele 1.1.5. (a) Sei K ein Körper, dann ist $(K, +)$ abelsche Gruppe, $(K, \cdot)$ abelsches Monoid und $(K\backslash\{0\}, \cdot)$ abelsche Gruppe.

(b) $(\mathbb{Z}, +)$ abelsche Gruppe, $(\mathbb{Z}, \cdot)$ abelsches Monoid, $(\mathbb{Z}\backslash\{0\}, \cdot)$ abelsches Monoid, $(\{1, -1\}, \cdot)$ abelsche Gruppe.

(c) Sei $\mathcal{X} \neq \emptyset$ eine Menge. Die Menge $\mathfrak{S}_\mathcal{X}$ aller Bijektionen von $\mathcal{X}$ nach $\mathcal{X}$ ist bezüglich der Komposition eine Gruppe, die symmetrische Gruppe von $\mathcal{X}$. Ist $\mathcal{X} = \{1, \dots, n\}$, dann setzt man $\mathfrak{S}_n := \mathfrak{S}_\mathcal{X}$. Es gilt $|\mathfrak{S}_n| = n!$. $\mathfrak{S}_n$ ist nur für $n = 1, 2$ abelsch. Die Elemnte der $\mathfrak{S}_n$ werden in der Gestalt $\sigma = \binom{1\dots n}{\sigma(1)\dots\sigma(n)}$ geschrieben.

(d) Ist $(M, \cdot)$ Monoid, dann ist $M^\times = \{x \in M \mid \exists x' \in M : xx' = e =' x\}$ eine Gruppe; sie heißt Einheitengruppe von $(M, \cdot)$. Speziell $(\mathbb{Z}, \cdot)^\times = \{1, -1\}$.

(e) Sind $G_1, \dots, G_n$ Gruppen (Monoide), dann ist das kartesische Produkt $G_1 \times \cdots \times G_n$ mit komponentenweiser Multiplikation eine Gruppe (ein Monoid) $(x_1, \dots, x_n) \cdot (y_1, \dots, y_n) = (x_1 y_1, \dots, x_n y_n)$.

(f) Weitere Beispiele: $\mathbf{GL}_n(K)$, $\mathbf{SL}_n(K)$, $\mathbf{O}_n$, $\mathbf{SO}_n$, $\mathbf{U}_n$, $\mathbf{SU}_n$,...

Definition 1.1.6. Sei $(M, \cdot)$ ein Monoid, seien $\mathcal{X}, \mathcal{Y}, \mathcal{Z} \subset M$ nichtleere Teilmengen.

$$\mathcal{X} \cdot \mathcal{Y} = \mathcal{X}\mathcal{Y} = \{z \in M \mid \exists x \in \mathcal{X}, y \in \mathcal{Y} : z = xy\}$$

heißt Komplexprodukt von $\mathcal{X}$ und $\mathcal{Y}$. Es gilt $(\mathcal{X}\mathcal{Y})\mathcal{Z} = \mathcal{X}(\mathcal{Y}\mathcal{Z})$. Falls $\mathcal{X} = \{x\}$, dann schreibt man $x\mathcal{Y}$ statt $\{x\}\mathcal{Y}$. Ist $(M, \cdot)$ eine Gruppe, dann sei noch

$$\mathcal{X}^{-1} = \{z \in M \mid \exists x \in \mathcal{X} : z = x^{-1}\}.$$

1.1.2 Untergruppen

Definition 1.1.7. Eine Teilmenge H eines Monoids $(M, \cdot)$ heißt Untermonoid, falls

(a) $e \in H$

(b) $\forall x, y \in H$ ist $xy \in H$

Dann ist H wieder ein Monoid.
Eine Teilmenge H einer Gruppe $(M, \cdot)$ heißt Untergruppe, falls zusätzlich gilt

(c) $\forall x \in H : x^{-1} \in H$.

Dann ist $(H, \cdot)$ wieder eine Gruppe.

Proposition 1.1.8. *Sei $(G, \cdot)$ eine Gruppe, $H \subset G$ eine Teilmenge. H ist genau dann Untergruppe, wenn $e \in H$ und $\forall x, y \in H$, gilt $xy^{-1} \in H$. Sei H endlich. H ist genau dann Untergruppe, wenn $e \in H$ und $\forall x, y \in H$ gilt $xy \in H$.*

Beweis. Sei H eine Untergruppe. Dann ist für $x, y \in H$ auch $x, y^{-1} \in H$ und damit $xy^{-1} \in H$, $e \in H$ ist trivial. Es gelte umgekehrt $\forall x, y \in H$, $xy^{-1} \in H$. Insbesondere für $x \in H$, $x^{-1} = ex^{-1} \in H$. Damit auch für $x, y \in H$, $x, y^{-1} \in H$ und $xy = x(y^{-1})^{-1} \in H$.

Sei H endlich, $x \in H$. Sei $\varphi : H \to H$, $y \mapsto xy$, dann ist φ injective: für

$$\begin{aligned}xy_1 &= xy_2 \quad \text{gilt}\\ y_1 = x^{-1}xy_1 &= x^{-1}xy_2 = y_2.\end{aligned}$$

Da H endlich ist, ist φ auch surjektiv, also $\exists z \in H : xz = e$ also $x^{-1} = z$. □

Beachte: die zweite Aussage kann falsch sein, wenn H unendlich ist, z. B. $(\mathbb{N}_0, +) \subset (\mathbb{Z}, +)$.

Proposition 1.1.9. *Sei G eine Gruppe, $(H_i)_{i\in I}$ eine Familie von Untergruppen. Dann ist $\bigcap_{i\in I} H_i$ wieder eine Untergruppe.*

Beweis. $\forall i \in I$ gilt: $e \in H_i$, also $e \in \bigcap_{i\in I} H_i$. Sei $x, y \in \bigcap_{i\in I} H_i$, dann $\forall i \in I$ ist $x, y \in H_i$, also $\forall i \in I$, $xy^{-1} \in H_i$ also $xy^{-1} \in \bigcap_{i\in I} H_i$. □

Proposition 1.1.10. *Sei G eine Gruppe und $X \subset G$ eine Teilmenge.*

$$\langle X\rangle := \bigcap \{H \mid H \text{ Untergruppe von } G \text{ mit } X \subset H\}$$

ist die kleinste (bezüglich Inklusion) Untergruppe von G, die X enthält. Es gilt

$$\langle X\rangle = \{y \in G \mid \exists n \in \mathbb{N}_0, x_1, \dots, x_n \in X \cup X^{-1} : y = x_1 \cdots x_n\}.$$

Beweis. Die erste Aussage ist klar. Für die zweite Aussage, sei K die Menge rechts. Offenbar ist K eine Untergruppe, die X enthält. Also gilt $\langle X\rangle \subset K$. Sei H eine beliebige Untergruppe, die X enthält und $n \in \mathbb{N}_0, x_1, \dots, x_n \in X \cup X^{-1}$, dann ist $\prod_{i=1}^n x_i \in H$ also gilt $K \subset H$. Es folgt $K \subset \langle X\rangle$. □

Es gilt $\langle\emptyset\rangle = \{e\}$. Für $x \in G$ gilt $\langle x\rangle = \langle\{x\}\rangle = \{x^a \mid a \in \mathbb{Z}\}$; dies ist abelsche Untergruppe von G. Die Ordnung von $\langle x\rangle$ heißt auch Ordnung von x, $\operatorname{ord}(x) = |\langle x\rangle| \in \mathbb{N}_0 \cup \infty$.

Ist $(G, +)$ abelsche Gruppe, $x \in G$, dann ist $\langle x\rangle = \{ax \mid a \in \mathbb{Z}\} = \mathbb{Z}\,x$. Ist $x_1, \dots, x_n \in G$, dann ist $\langle x_1, \dots, x_n\rangle = \langle\{x_1, \dots, x_n\}\rangle = \{y \in G \mid \exists a_1, \dots a_n \in \mathbb{Z} : y = \sum_{i=1}^n a_i x_i\}$. Diese Untergruppe, wird mit $\sum_{i=1}^n \mathbb{Z}\,x_i$ bezeichnet und heißt Summe der $\mathbb{Z}\,x_1, \dots, \mathbb{Z}\,x_n$.

Definition 1.1.11. G heißt endlich erzeugt, bzw. zyklisch, falls es eine endliche Teilmenge $X \subset G$, bzw. $x \in G$, gibt, mit $G = \langle X\rangle$, bzw. $G = \langle x\rangle$.

Beispiele 1.1.12. (a) Die symmetrische Gruppe

$$G = \mathfrak{S}_3 = \left\{e, a = \begin{pmatrix}123\\231\end{pmatrix}, a^2 = \begin{pmatrix}123\\312\end{pmatrix}, b = \begin{pmatrix}123\\132\end{pmatrix}, c = \begin{pmatrix}123\\321\end{pmatrix}, d = \begin{pmatrix}123\\213\end{pmatrix}\right\}$$

mit den Relationen $a^3 = e$, $a^{-1} = a^2$, $b^2 = c^2 = d^2 = e$, $b^{-1} = b$, $c^{-1} = c$, $d^{-1} = d$, $ab = d$, $a^2b = c$.

$$\begin{aligned}\langle a\rangle &= \langle a^2\rangle = \{e, a, a^2\}\\ \langle b\rangle &= \{e, b\}\\ \langle c\rangle &= \{e, c\}\\ \langle d\rangle &= \{e, d\}\end{aligned}$$

ergibt

$$\begin{aligned}\operatorname{ord}(e) &= 1\\ \operatorname{ord}(a) &= 3\\ \operatorname{ord}(b) = \operatorname{ord}(c) = \operatorname{ord}(d) &= 2\end{aligned}$$

Also: $G = \{e, a, a^2, b, ab, a^2b\}$. Kommutatorrelation: $ba = c = a^2b$.

(b) Sei $n \geqslant 2$, $a = \begin{pmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n}\end{pmatrix}$, $b = \begin{pmatrix} 1 & 0 \\ 0 & -1\end{pmatrix}$ in $\mathbf{O}_2$. Es gilt

$$\begin{aligned}a^n &= e\\ a^i &= a^j \quad \text{für } 0 \leqslant i < jn\\ b^2 &= e\end{aligned}$$

Relation: $ba = a^{n-1}b$
Untergruppen:

$$\begin{aligned} \langle a \rangle &= \{e, a, \dots a^{n-1}\} \quad \text{also } \operatorname{ord}(a) = n \\ \langle b \rangle &= \{e, b\} \quad \text{also } \operatorname{ord}(b) = 2 \\ D_n &= \{e, a, a^2 \dots, a^{n-1}, b, a^2 b \dots, a^{n-1} b\} \quad \text{ist Gruppe der Ordnung } 2n \end{aligned}$$

Jede zu D_n isomorphe Gruppe heißt Diedergruppe der Ordnung $2n$.
Für $n = 2$:

$$D_2 = \{e, a, b, ab\} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} \cos\pi & -\sin\pi \\ \sin\pi & \cos\pi \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} \cos\pi & \sin\pi \\ \sin\pi & -\cos\pi \end{pmatrix} \right\}$$

ist abelsche Gruppe der Ordnung 4. Jede dazu isomorphe Gruppe heißt Kleinsche Vierergruppe.
Für $n = 3$:

$$D_3 \cong S_3.$$

(c) Sei $a = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $b = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ in $\mathbf{U}_2$. Dann

$$\begin{aligned} a^2 &= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \\ a^4 &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = e \\ a^3 &= \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} = a^{-1} \\ b^2 &= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = a^2 \\ b^4 &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = e \\ b^3 &= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = b^{-1} \end{aligned}$$

Relationen: $b^2 = a^2$, $ba = a^3 b$

$$Q = \langle a, b \rangle = \{e, a, a^2, a^3, b, ab, a^2 b, a^3 b\}$$

hat Ordnung 8 und heißt Quaternionengruppe.

1.1.3 Die Untergruppen von $\mathbb{Z}$, Teilbarkeit in $\mathbb{Z}$

Für $a \in \mathbb{Z}$ ist

$$\langle a \rangle = \mathbb{Z}\, a = a\, \mathbb{Z} = \{za \mid z \in \mathbb{Z}\}$$

die von a erzeugte Untergruppe von $(\mathbb{Z}, +)$. Für $a, b \in \mathbb{Z}$ gilt

$$\mathbb{Z}\, a \subset \mathbb{Z}\, b \Leftrightarrow \exists c \in \mathbb{Z} : a = cb, \quad b \text{ teilt } a, \text{ in Zeichen } b|a.$$

Es gilt

$$\mathbb{Z}\, a = \mathbb{Z}\, b \Leftrightarrow a|b \wedge b|a \Leftrightarrow b = \pm a.$$

Proposition 1.1.13 (Division mit Rest)**.** *Für alle $a, b \in \mathbb{Z}$, $b \neq 0$, gibt es $q, r \in \mathbb{Z}$ so daß*

$$a = bq + r \quad \text{und } 0 \leqslant r < |b|.$$

Beweis. Sei $\tilde{q}$ die größte ganze Zahl $\leqslant \frac{a}{|b|}$. Dann gilt $0 \leqslant \frac{a}{|b|} - \tilde{q} < 1$. Für $r = a - \tilde{q}|b|$ gilt dann

$$0 \leqslant r < b \quad \text{und} \quad a = |b|\tilde{q} + r = bq + r \quad \text{mit } q = \pm\tilde{q}.$$

Eindeutigkeit: Sei

$$a = bq + r = bq' + r' \quad \text{mit } q', r' \in \mathbb{Z}, 0 \leqslant r' < |b|.$$

Dann

$$b(q - q') = r' - r \Rightarrow |b||q - q'| = |r - r'| < b \Rightarrow q = q', r = r'.$$

□

Satz 1.1.14. *Jede Untergruppe von $(\mathbb{Z}, +)$ ist von der Gestalt $\mathbb{Z}\,n$ mit eindeutigem $n \in \mathbb{N}_0$.*

Beweis. Sei o. E. $H \neq \{0\}$ Untergruppe von $\mathbb{Z}$, sei $0 \neq b \in H$, so daß $|b|$ minimal ist. Dann ist $|b| = \pm b \in H$. Dann gilt $H = \mathbb{Z}\,|b|$.
„$\supset$“Das ist klar.
„$\subset$“Sei $a \in H$. Dann $\exists q, r \in \mathbb{Z} : a = |b|q + r$ und $0 \leqslant r < |b|$. Es folgt $r = a - |b|q \in H$. Da $|b|$ minimal war folgt $r = 0$, also $a = |b|q \in \mathbb{Z}\,|b|$.
Eindeutigkeit: Sei $\mathbb{Z}\,m = \mathbb{Z}\,n$ mit $m, n \in \mathbb{N}_0$. Dann $m|n$ und $n|m \to m = n$. □

Definition 1.1.15. Seien $a_1, \ldots, a_n \in \mathbb{Z}\setminus\{0\}$. Eine Zahl $v \in \mathbb{Z}$ heißt kleinstes gemeinsames Vielfaches (kgV) der a_i, falls

(a) für alle $1 \leqslant i \leqslant n$ gilt $a_i|v$,

(b) für alle $s \in \mathbb{Z}$ gilt: wenn $\forall i : a_i|s$ dann $v|s$.

Eine Zahl $t \in \mathbb{Z}$ heißt größter gemeinsamer Teiler (ggT) der a_i, falls

(a) für alle $1 \leqslant i \leqslant n$ gilt $t|a_i$,

(b) für alle $s \in \mathbb{Z}$ gilt: wenn $\forall i : s|a_i$ dann $s|t$.

Aus (b) folgt jeweils, daß kgV und ggT bis auf Vorzeichen eindeutig bestimmt sind.

Proposition 1.1.16. *Seien $a_1, \ldots, a_n \in \mathbb{Z}\setminus\{0\}$, seien $t, v \in \mathbb{N}_0$ eindeutig bestimmte Zahlen mit $\bigcap_{i=1}^n \mathbb{Z}\,a_i = \mathbb{Z}\,v$, $\sum_{i=1}^n \mathbb{Z}\,a_i = \mathbb{Z}\,t$. Dann ist v kgV und t ggT der $a_1, \ldots, a_n \in \mathbb{Z}\setminus\{0\}$.*

Beweis. Für v: Sei $\bigcap_{i=1}^n \mathbb{Z}\,a_i = \mathbb{Z}\,v$ dann ist $\mathbb{Z}\,v \subset \mathbb{Z}\,a_i$ für alle a_i, das heißt $a_i|v$. Also ist v vielfaches. Sei $s \in \mathbb{Z}$ mit $a_i|s$. Dann $\mathbb{Z}\,s \subset \mathbb{Z}\,a_i$, also $\mathbb{Z}\,s \subset \bigcap_{i=1}^n \mathbb{Z}\,a_i = \mathbb{Z}\,v$. Also $v|s$ und ist somit kleinstes Vielfaches. Analog für t. □

Definition 1.1.17. $a_1, \ldots, a_n$ heißen teilerfremd oder relativ prim, falls $\sum_{i=1}^n \mathbb{Z}\,a_i = \mathbb{Z}$ ist. Äquivalent dazu, falls 1 ein ggT der a_i ist.

Folgerung 1.1.18 (Lemma von Bezout)**.** *$a_1, \ldots, a_n \in \mathbb{Z}\setminus\{0\}$ sind genau dann teilerfremd, wenn es $z_1, \ldots, z_n \in \mathbb{Z}$ gibt mit $\sum_{i=1}^n z_i a_i = 1$*

Beweis. „$\Rightarrow$“Dies folgt aus der Definition.
„$\Leftarrow$“Gilt $\sum_{i=1}^n z_i a_i = 1$, dann ist 1 ein ggT. □

Folgerung 1.1.19 (Lemma von Euklid)**.** *Seien $a, b, c \in \mathbb{Z}\setminus\{0\}$. Sind a, b teilerfremd, und es gilt $a|bc$, dann gilt $a|c$.*

Beweis. Nach Annahme gibt es $z \in \mathbb{Z}$ mit $bc = az$. Nach Bezout existieren $x, y \in \mathbb{Z}$ mit $ax + by = 1$. Multipliziere mit c:

$$c = axc + bcy = axc + azy = a(xc + zy)$$

also $a|c$. □

Definition 1.1.20. $p \in \mathbb{N}$ heißt Primzahl, wenn $p > 1$ ist und in $\mathbb{Z}$ keine Teiler außer ± 1 und $\pm p$ hat.

Folgerung 1.1.21. *$p \in \mathbb{N}\setminus\{0\}$ ist genau dann prim, wenn gilt $\forall a, b \in \mathbb{Z} : p|ab \Rightarrow p|a \vee p|b$.*

Beweis. „⇒“Sei p prim, seien $a, b \in \mathbb{Z}$ mit $p|ab$. Falls $p|a$ fertig. Falls $p \nmid a$, dann sind p und a teilerfremd. Es folgt $p|b$.
„⇐“Sei $p = ab$ mit $a, b \in \mathbb{Z}$. Dann gilt $p|a$ oder $p|b$, also $a = \pm p$ und $b = \pm 1$ oder umgekehrt. □

Satz 1.1.22 (Hauptsatz der Elementaren Zahlentheorie)**.** *Zu jeder Zahl $a \in \mathbb{Z}\setminus\{-1, 0, 1\}$ gibt es eindeutig bestimmte $r \in \mathbb{N}$, Primzahlen $p_1 < \ldots < p_r$ und $v_1, \ldots, v_r \in \mathbb{N}$ mit*

$$a = \pm p_1^{v_1} \cdots p_r^{v_r}.$$

Beweis. Sei ohne Einschränkung $a > 0$. Existenz: Induktion nach a. Wenn a Primzahl ist, dann fertig. Andernfalls gibt es $b, c \in \mathbb{N}\setminus\{1\}$ mit $a = bc$. Da $1 < b, c < a$ sind, und nach Induktionsannahme b, c Produkt von Primzahlen, ist auch a Produkt von Primzahlen.

Eindeutigkeit: Seien $a = q_1 \cdots q_k = q_1' \cdots q_l'$ zwei Zerlegungen in Primzahlen. Behauptung $k = l$ und es existiert $\sigma \in \mathfrak{S}_k$ mit $q_i = q'_{\sigma(i)}$. Induktion nach k. Ist $k = 1$, dann ist $l = 1$ und $q_1 = q_1'$. Sei $k > 1$. Dann $q_k | q_1' \cdots q_l'$ und $\exists 1 \leqslant j \leqslant l$: $q_k | q_j'$, also $q_k = q_j'$. Dann $q_1 \cdots q_{k-1} = \prod_{i \neq j} q_i'$. Nach Induktionsannahme gilt $k - 1 = l - 1$ und es gibt $\sigma : \{1, \ldots, k-1\} \to \{1, \ldots, l\}\setminus\{j\}$ mit $q_i = q'_{\sigma(i)}$ für $1 \leqslant i \leqslant k-1$. Dann ist $k = l$ und setzt man noch $\sigma(k) = j$, dann ist $\sigma \in \mathfrak{S}_k$ mit $q_i = q'_{\sigma(i)}$ für $1 \leqslant i \leqslant k$. □

Flexiblere Schreibweise: Sei $\mathbb{P}$ die Menge aller Primzahlen. Zu jedem $a \in \mathbb{Z}\setminus\{0\}$ existiert eine eindeutig bestimmte Familie $(\nu_p(a))_{p\in\mathbb{P}}$ von Zahlen in $\mathbb{N}_0$, $\nu_p(a) = 0$ für fast alle $p \in \mathbb{P}$, und $\varepsilon \in \{\pm 1\}$, mit

$$a = \varepsilon \prod_{p\in\mathbb{P}} p^{\nu_p(a)}.$$

Folgerung 1.1.23. *Für $a, b \in \mathbb{Z}\setminus\{0\}$ gilt $a|b$ genau dann, wenn $\forall p \in \mathbb{P}$: $\nu_p(a) \leqslant \nu_b(b)$.*
Für $a_1, \ldots a_n \in \mathbb{Z}\setminus\{0\}$ ist

$$\prod_{p\in\mathbb{P}} p^{\max\{v_p(a_i), 1\leqslant i\leqslant n\}}$$

kgV und

$$\prod_{p\in\mathbb{P}} p^{\min\{v_p(a_i), 1\leqslant i\leqslant n\}}$$

ggT.

Beweis. „⇒“Falls $b = ac$, dann ist

$$\varepsilon \prod_{p\in\mathbb{P}} p^{\nu_p(b)} = \varepsilon \prod_{p\in\mathbb{P}} p^{\nu_p(a)} \prod_{p\in\mathbb{P}} p^{\nu_p(c)} = \varepsilon \prod_{p\in\mathbb{P}} p^{\nu_p(a)+\nu_p(c)}.$$

Also gilt für alle p:$\nu_p(b) = \nu_p(a) + \nu_p(c)$, das heißt $\nu_p(b) \geqslant \nu_p(a)$.
„⇐“mit $c = \pm \prod_{p\in\mathbb{P}} p^{\nu_p(b)-\nu_p(a)}$ gilt $b = ac$.
Die zweite Aussage ist klar. □

Beispiel* 1.1.24. Sei $r \in \mathbb{Z}$ Summe zweier Quadrate. Dann ist auch $2r \in \mathbb{Z}\,2$ Summer zweier Quadrate.

1.1.4 Die Ordnung eines Gruppenelements

Satz 1.1.25. *Sei G eine Gruppe, $x \in G$ ein Element mit endlicher Ordnung. Für $n \in \mathbb{N}$ sind äquivalent:*

(a) $n = \mathrm{ord}(x) = |\langle x\rangle|$,

(b) $\langle x\rangle = \{e, x, \ldots, x^{n-1}\}$ *und* $x_i \neq x_j$ *für* $i \neq j$,

(c) $\forall z \in \mathbb{Z} : x^z = e \Leftrightarrow n|z$,

(d) $n = \min\{k \in \mathbb{N} \,|\, x^k = e\}$.

Beweis. Zunächst eine Vorbemerkung. Da $\langle x\rangle$ endlich ist, gibt es $k < l \in \mathbb{Z}$, mit $x^k = x^l$. Es folgt $x^{l-k} = e$. Sei $m \in \mathbb{N}$ die kleinste Zahl mit $x^m = e$. Dann gilt $\langle x\rangle = \{e, x, \ldots, x^{m-1}\}$ und $x_i \neq x_j$ für $0 \leqslant i < j < n$. Die Inklusion „$\supset$“ ist klar. Für die Inklusion „$\subset$“ sei $z \in \mathbb{Z}$. Dann gibt es $q, r \in \mathbb{Z}$ mit $z = mq + r$, $0 \leqslant r < m$, es folgt $x^z = (x^m)^q x^r = x^r$. Für $0 \leqslant i < j < m$ gilt $j - i < m$ also $x^{j-i} \neq e \Rightarrow x^i \neq x^j$.

Gilt (a), dann gilt $n = m$, und (b) und (d) sind gezeigt.

(d) $\Rightarrow$ (c): Sei $z \in \mathbb{Z}$ mit $x^z = e$. Dann gibt es $q, r \in \mathbb{Z}$ mit $z = nq + r$, $0 \leqslant r < n$. Es folgt $e = x^{nq+r} = (x^n)^q x^r = x^r$. Also $r = 0$ und $z = nq$ und weiter $n|z$. Die andere Richtung ist klar.

(c) $\Rightarrow$ (b): Sei $z \in \mathbb{Z}$, $z = nq + r$ mit $q, r \in \mathbb{Z}$, $0 \leqslant r < n$. Dann $x^z = (x^n)^q x^r$. Also $\langle x\rangle = \{e, \ldots, x^{n-1}\}$. Für $0 \leqslant i < j < n$ gilt $n \nmid j - i$, also ist $x^{j-i} \neq e$, es folgt $x^i \neq x^j$.

(b) $\Rightarrow$ (a) Klar. □

Beispiel 1.1.26. Sei $n \in \mathbb{N}$, $\zeta = e^{\frac{2\pi i}{n}} \in \mathbb{C}$. Als Element der Gruppe $\mathbb{C}^\times$ hat ζ die Ordnung n, also ist $\langle\zeta\rangle = \{1, \zeta, \ldots, \zeta^{n-1}\}$ zyklische Gruppe der Ordnung n. $\mu_n(\mathbb{C}) = \langle\zeta\rangle$ heißt Gruppe der n-ten Einheitswurzeln von $\mathbb{C}$. $\mu(\mathbb{C}) = \cup_{n\in\mathbb{N}}\mu_n(\mathbb{C})$ ist ebenfalls Untergruppe von $\mathbb{C}^\times$.

1.2 Operationen von Gruppen auf Mengen

1.2.1 Äquivalenzrelationen

Definition 1.2.1. Sei X eine Menge. Eine Familie $(X_i)_{i\in I}$ von nichtleeren Teilmengen von X heißt Partition, falls $X = \bigcup_{i\in I} X_i$ und $X_i \cap X_j = \emptyset$ für alle $i \notin I$.

Definition 1.2.2. Sei X eine Menge. Eine Teilmenge $R \subset X \times X$ heißt Relation. R heißt Äquivalenzrelation, falls

(a) $\forall x \in X$: $(x, x) \in R$ (Reflexivität)

(b) $\forall x, y \in X$: $(x, y) \in R \Leftrightarrow (y, x) \in R$ (Symmetrie)

(c) $\forall x, y, z \in X$: $(x, y) \in R, (y, z) \in R \Rightarrow (x, z) \in R$ (Transitivität)

Statt $(x, y) \in R$ schreibt man $x \sim_R y$ oder $x \sim y$. Für $x \in X$ heißt $\overline{x} = \{y \in X \mid x \sim y\}$ die Äquivalenzklasse von x bei R oder $\sim$. Jedes Element $y \in \overline{x}$ heißt Repräsentant von $\overline{x}$; es gilt $\overline{y} = \overline{x}$.
(Sei nämlich $z \in \overline{y}$ das heißt $z \sim y$. Wegen $y \in \overline{x}$ gilt $y \sim x$, auf Grund der Transitivität also $z \in \overline{x}$. Dies zeigt $\overline{y} \subset \overline{x}$. Die Umkehrung folgt durch Vertauschen von x und y.)

Die Menge der Äquivalenzklassen wird mit X/R oder $X/\sim$ bezeichnet. Die Abbildung

$$\pi : X \to X/\sim, x \mapsto \overline{x}$$

heißt kanonische Abbildung. Sie ist surjektiv. Eine Teilmenge $X \subset X$ heißt Transversale von $X/\sim$, falls jede Äquivalenzklasse genau ein Element von X' enthält.

Proposition 1.2.3. *Ist $(X_i)_{i\in I}$ eine Partition von X, dann definiert*

$$x \sim y :\Leftrightarrow \exists i \in I : x, y \in X_i$$

eine Äquivalenzrelation, deren Äquivalenzklassen genau die X_i sind.

Ist $\sim$ eine Äquvalenzrelation auf X, dann ist $X/\sim$ eine Partition von X, und die dadurch definierte Äquivalenzrelation ist $\sim$.

Beweis. Die erste Aussage ist klar. Für die zweite Aussage: Zeige zuerst: $X/\sim$ ist eine Partition: Für $\in X$ gilt: $x \in \overline{x}$, also ist $X = \bigcup_{\overline{x}\in X/\sim} \overline{x}$. Seien $\overline{x}, \overline{y} \in X/\sim$, $\overline{x} \cap \overline{y} \neq \emptyset$. Sei $z \in \overline{x} \cap \overline{y}$, dann $\overline{x} = \overline{z} = \overline{y}$. Also ist $X/\sim$ eine Partition. Alles andere ist klar. □

Beispiel* **1.2.4.** Sei $X = \mathbb{Z}$. Für $x, y \in \mathbb{Z}$ sei $x \sim y$ genau dann, wenn bei Division mit 5 der gleiche Rest bleibt. Anders gesagt $x \sim y$ genau dann, wenn $x - y \in 5\,\mathbb{Z}$. Eine Transversale, oder Menge von Repsäsentanten ist zum Beispiel $\{0, 1, 2, 3, 4\}$. Die Äquivalenzklassen sind

$$\begin{aligned} \overline{0} &= 5\,\mathbb{Z} \\ \overline{1} &= 1 + 5\,\mathbb{Z} \\ \overline{2} &= 2 + 5\,\mathbb{Z} \\ \overline{3} &= 3 + 5\,\mathbb{Z} \\ \overline{4} &= 4 + 5\,\mathbb{Z} \end{aligned}$$

1.2.2 Operationen von Gruppen auf Mengen

Definition 1.2.5. Sei X eine Menge $\neq \emptyset$, G eine Gruppe. Eine Abbildung

$$G \times X \to X, (g, x) \mapsto g \cdot x = gx$$

heißt (Links)Operation von G auf X, falls

(a) für alle $x \in X$ gilt $ex = x$;

(b) für alle $x \in X$ und $g_1, g_2 \in G$ gilt $g_2(g_1 x) = (g_1 g_2)x$.

Die Operation heißt transitiv, falls es für alle $x, y \in X$ ein $g \in G$ gibt mit $y = gx$.

Aus den Axiomen folgt, daß eine Operation gesehen werden kann als Gruppenhomomorphismus

$$\psi : G \to \mathfrak{S}_X$$

zwischen G und der Symmetriegruppe der Menge X.

Proposition und Definition 1.2.6. *Sei $\cdot : G \times X \to X$ eine Operation.*

(a) Durch

$$x \sim y \Leftrightarrow \exists g \in G : gx = y$$

wird auf X eine Äquivalenzrelationrelation definiert. Die Äquivalenzklasse von $x \in X$ ist $\overline{x} = Gx = \{gx \mid g \in G\}$. Sie heißt Bahn von x bei $\sim$ oder $\cdot$. Eine Transversale von $X/\sim$ heißt auch Transversale der Operation $\cdot$.

(b) Für $x \in X$ ist $G_x = \mathrm{Stab}_G(x) = \{g \in G \mid gx = x\}$ eine Untergruppe von G. Sie heißt Stabilisatoruntergruppe oder Isotropieuntergruppe von x. $x \in X$ heißt Fixpunkt der Operation, falls für alle $g \in G$ gilt $gx = x$
($\Leftrightarrow Gx = \{x\} \Leftrightarrow G = G_x$)
Ist $X' \subset X$ eine Teilmenge von X, dann heißt $G_{X'} = \mathrm{Stab}_G(X') = \bigcap_{x \in X'} G_x$ Stabilisatoruntergruppe von X'.

Beweis. **Zu (a): $\sim$ ist Äquivalenzrelation:** Reflexivität: Da $ex = x$ gilt $x \sim x$.
Symmetrie: $x \sim y$ genau dann, wenn es $g \in G$ gibt mit $gx = y$. Dann ist $x = (g^{-1}g)x = g^{-1}(gx) = g^{-1}y$ also $y \sim x$.
Transitivität: $x \sim y$ und $y \sim z$ genau dann wenn es $g, h \in G$ gibt mit $gx = y$ und $hy = z$. Dann ist $(hg)x = h(gx) = hy = z$, also $x \sim z$.
Äquivalenzklasse von x: $y \in \overline{x} \Leftrightarrow x \sim y \Leftrightarrow \exists g \in G : gx = y \Leftrightarrow y \in Gx$.
Zu (b): G_x ist Untergruppe: Da $ex = x$ ist, ist $e \in G_x$. Sei $g, h \in G_x$, dann ist $gx = x = hx$, also $(gh)x = g(hx) = gx = x$. Damit ist also $gh \in G_x$. Ist $g \in G_x$, dann ist $gx = x$, und $x = g^{-1}x$, also $g^{-1} \in G_x$. □

Die Operation ist genau dann transitiv, wenn es genau eine Bahn gibt.

Beispiele 1.2.7. (a) Sei $X \neq \emptyset$ eine Menge, $G \subset \mathfrak{S}_X$ eine Untergruppe. Dann ist

$$G \times X \to X, (\sigma, x) \mapsto \sigma(x)$$

eine Operation.
Speziell $X = \{1, 2, 3\}$, $G = S_3$. Dann ist $G.1 = G.2 = G.3 = X$, also ist die Operation transitiv. Sie ist fixpunktfrei.

$$\begin{aligned} G_1 &= \left\{e, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\right\} \\ G_2 &= \left\{e, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\right\} \\ G_3 &= \left\{e, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\right\} \end{aligned}$$

(b) $X = \mathbb{R}^2$, $G = \mathbf{SO}_2 = \left\{ \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix} \mid 0 \leqslant \varphi < 2\pi \right\}$. Dann ist

$$\mathbf{SO}_2 \times \mathbb{R}^2 \to \mathbb{R}^2, (A, x) \mapsto Ax$$

eine Operation mit $G_0 = G$, $G_x = e$ für $x \neq 0$.

1.2.3 Der Satz von Lagrange

Sei G eine Gruppe, H eine Untergruppe von G. Wir betrachten die Rechtsoperation

$$G \times H \to G, (x, h) \mapsto xh$$

von H auf G. Die Äquivalenzrelation auf G dazu ist:

$$x \sim y \Leftrightarrow \exists h \in H : xh = y \Leftrightarrow x^{-1}y \in H \Leftrightarrow y^{-1}x \in H.$$

Die Bahn von x ist $\overline{x} = xH$; sie heißt Linksnebenklasse von H in G repräsentiert durch x. Es gilt also

$$xH = yH \Leftrightarrow x \sim y \Leftrightarrow x^{-1}y \in H.$$

Die Menge aller Linksnebenklassen von H in G wird mit G/H bezeichnet. Eine Transversale von G/H oder $\sim$ heißt Linkstransversale von H in G.

Bei der Linksoperation

$$H \times G \to G, (h, x) \mapsto hx$$

erhält man die Äquivalenzrelation

$$x \sim y \Leftrightarrow \exists h \in H : hx = y \Leftrightarrow yx^{-1} \in H \Leftrightarrow xy^{-1} \in H.$$

Die Bahn von x ist $\overline{x} = Hx$, sie heißt Rechtsnebenklasse von H in G represäntiert durch x. Es gilt

$$Hx = Hy \Leftrightarrow x \sim y \Leftrightarrow yx^{-1} \in H.$$

Die Menge aller Rechtsnebenklassen von H in G wird mit $H\backslash G$ bezeichnet. Eine Transversale von $H\backslash G$ heißt Rechtstransversale von H in G.

Proposition und Definition 1.2.8. *Die Zuordnung*

$$G/H \to H\backslash G, xH \mapsto Hx^{-1}$$

ist eine bijektive Abbildung. Die Zahl $[G : H] = |G/H| = |H\backslash G| \in \mathbb{N} \cup \{\infty\}$ *heißt Index von* H *in* G.

Beweis. **Wohldefiniert und injektiv:** $xH = yH \Leftrightarrow x^{-1}y \in H \Leftrightarrow Hx^{-1} = Hy^{-1}$.
Surjektiv: Ist klar. □

Ist $H = \{e\}$, dann ist $xH = \{x\}$ für alle $x \in G$, also

$$G/H = \{\{x\}, x \in G\},$$

und $G \to G/H, x \mapsto \{x\}$, ist bijektiv. Insbesondere ist $[G : H] = |G|$. Ferner ist $[G : H] = 1 \Leftrightarrow H = G$.

Satz 1.2.9 (Lagrange)**.** *Sei G endliche Gruppe, $H \subset G$ Untergruppe. Dann gilt*

$$|G| = [G : H] \cdot |H|.$$

Insbesondere sind $[G : H]$ und $|H|$ Teiler von $|G|$.

Beweis. Sei $x_1, \ldots, x_n$ Transversale der Linksnebenklassen von H in G, das heißt

$$G = \bigcup_{i=1}^{n} x_i H$$

disjunkte Vereinigung. Es gilt: für alle i ist die Abbildung $H \to x_i H, h \mapsto x_i h$ bijektiv. Es folgt

$$|G| = \sum_{i=1}^{n} |x_i H| = \sum_{i=1}^{n} |H| = n|H| = [G : H] \cdot |H|.$$

□

Folgerung 1.2.10. *Seien H, K Untergruppen von G mit $K \subset H$. Dann gilt*

$$[G : K] = [G : H][H : K].$$

Genauer: Ist $x_1, \ldots, x_n$ bzw. $y_1, \ldots y_m$ eine Linkstransversale von H in G bzw. von K in H, dann ist $(x_i y_j)_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant m}}$ eine Linkstransversale von K in G.

Beweis. Es gilt $G = \bigcup_{i=1}^{n} x_i H$ und $H = \bigcup_{j=1}^{m} y_j K$, also

$$G = \bigcup_{i=1}^{n} x_i (\bigcup_{j=1}^{m} y_j K) = \bigcup_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant m}} x_i y_j K$$

disjunkt, denn Linksmultiplikation mit x_i ist injektiv. □

Folgerung 1.2.11. *Sei G eine endliche Gruppe, $x \in G$. Dann gilt* $\operatorname{ord}(x) \big| |G|$. *Insbsondere $x^{|G|} = e$.*

Beweis. Es gilt $\operatorname{ord}(x) = |\langle x \rangle| \big| |G|$. □

Folgerung 1.2.12. *Sei G Gruppe, deren Ordnung eine Primzahl p ist. Dann hat G keine Untergruppe außer $\{e\}$ und G. Außerdem ist G zyklisch und für alle $e \neq x \in G$ gilt $G = \langle x \rangle = \{e, x, \ldots, x^{p-1}\}$.*

Beweis. Ist $H \subset G$ eine Untergruppe, dann

$$|H| \big| |G| = p.$$

Also gilt $|H| = 1$ oder $|H| = p$, also $H = \{e\}$ oder $H = G$. Sei $e \neq x \in G$, dann ist $\langle x \rangle \neq \{e\}$, also

$$G = \langle x \rangle = \{e, x, \ldots, x^{p-1}\}.$$

□

1.2.4 Die Bahnengleichung

Satz 1.2.13. *Sei X endliche Menge, G endliche Gruppe, $G \times X \to X$, $(g,x) \mapsto gx$ eine Operation.*

(a) Für alle $x \in X$ ist die Abbildung

$$G/G_x \to Gx, gG_x \mapsto gx$$

bijektiv. Insbesondere gilt $|Gx| = [G : G_x]$.

(b) (Bahnengleichung) Ist $T \subset X$ eine Transversale der Bahnen, dann gilt

$$|X| = \sum_{x \in T} [G : G_x].$$

Ist X_0 die Menge der Fixpunkte, dann gilt

$$|X| = |X_0| + \sum_{x \in T \setminus X_0} [G : G_x].$$

Beweis. **Zu (a):** Wohldefiniert und injektiv:

$$gG_x = g'G_x \Leftrightarrow g^{-1}g' \in G_x \Leftrightarrow g^{-1}g'x = x \leftrightarrow g'x = gx.$$

Surjektivität ist klar.

Zu (b): Die Vereinigun $X = \bigcup_{x \in T} Gx$ ist disjunkt, also

$$|X| = \sum_{x \in T} |Gx| = \sum_{x \in T} [G : G_x].$$

Es gilt,

$$x \in X_0 \Leftrightarrow |Gx| = [G : G_x] = 1$$

also

$$|X| = |X_0| + \sum_{x \in T \setminus X_0} [G : G_x].$$

□

Folgerung 1.2.14. *Voraussetzungen und Bezeichnungen wie im Satz. Wenn alle $[G : G_x]$, $x \in T \setminus X_0$ durch eine Zahl $d \in \mathbb{N} \setminus \{1\}$ teilbar sind, dann ist $|X| - |X_0|$ durch d teilbar.*

1.2.5 Konjugation

Sei G eine Gruppe, $u \in G$. Die Abbildung

$$\kappa_u : G \to G, x \mapsto uxu^{-1}$$

heißt Konjugation mit u. Wir betrachten die Operation

$$G \times G \to G, (u,x) \mapsto uxu^{-1}.$$

Es gilt $exe^{-1} = x$ und $v(uxu^{-1})v^{-1} = (vu)x(vu)^{-1}$ für alle $u, v \in G$, also definiert dies in der Tat eine Operation. Die Äquivalenzrelation dazu ist:

$$x \sim y \Leftrightarrow \exists u \in G : uxu^{-1} = y;$$

dann heißen x und y konjugiert. Die Äquivalenzklasse von x ist

$$C_x = \{uxu^{-1} : u \in G\}.$$

Sie heißt Konjugationsklasse von x. Allgemein heißen $X, Y \subset G$ konjugiert, wenn es $u \in G$ gibt mit $uXu^{-1} = Y$.

Die Stabilisatoruntergruppe von $x \in G$ ist

$$\{u \in G : uxu^{-1} = x\} = \{u \in G : ux = xu\}.$$

Sie heißt Zentralisator von x in G und wird mit $C_G(x)$ bezeichnet.

$x \in G$ ist genau dann Fixpunkt obiger Operation, wenn $C_G(x) = G$, dh. $ux = xu$ für alle $u \in G$.

Definition 1.2.15. $x \in G$ heißt zentrales Element, falls für alle $u \in G$ gilt $ux = xu$. Die Menge aller zentralen Elemente $Z(G)$ ist eine Untergruppe (denn $Z(G) = \bigcap_{x \in G} C_G(x)$). Sie heißt Zentrum von G.

Beispiel 1.2.16. $\mathfrak{S}_3 = \{e, a, a^2, b, ab, a^2b\}$ mit $a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ und $b = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $ba = a^2b$.

Konjugationsklassen:

$$\begin{aligned} C_e &= \{e\} \\ C_a &= \{a, a^2\} \quad \text{denn } bab = a^2\text{; das sind die Elemente der Ordnung 3} \\ C_b &= \{b, ab, a^2b\} \quad \text{denn } a^{-1}ba = ab,\ a^{-2}ba^2 = ba = a^2n\text{, dies sind die Elemente der Ordnung 2} \end{aligned}$$

Zentralisatoren: Diese sind Untergruppen von $\mathfrak{S}_3$, haben also Ordnung $1, 2, 3$ oder 6.

$$\begin{aligned} C_{\mathfrak{S}_3}(e) &= \mathfrak{S}_3 \\ C_{\mathfrak{S}_3}(a) &= \{e, a, a^2\} \quad \text{nicht-triviale echte Untergruppe, denn } a \text{ vertauscht mit sich selbst, aber nicht mit } b \\ &= C_{\mathfrak{S}_3}(a^2) \\ C_{\mathfrak{S}_3}(b) &= \{e, b\} \quad \text{nicht-triviale echte Untergruppe, denn } b \text{ vertauscht mit sich selbst, aber nicht mit } a \\ C_{\mathfrak{S}_3}(ab) &= \{e, ab\} \quad \text{nicht-triviale echte Untergruppe, denn } ab \text{ vertauscht mit sich selbst, aber nicht mit } a \\ C_{\mathfrak{S}_3}(a^b) &= \{e, a, a^2\} \quad \text{nicht-triviale echte Untergruppe, denn } a^2b \text{ vertauscht mit sich selbst, aber nicht mit } a \end{aligned}$$

Zentrum: $Z(G) = \{e\}$.

Beachte: In einer Konjugationsklasse haben alle Elemente die gleiche Ordnung, denn

$$(uxu^{-1})^k = e \Leftrightarrow x^k = e.$$

Satz 1.2.17. *Ist C_x die Konjugationsklasse von x, dann gilt*

$$|C_x| = [G : C_G(x)].$$

Klassengleichung: Sei S eine Transversale der Konjugationsklassen in $G \backslash Z(G)$, dann gilt

$$|G| = |Z(G)| + \sum_{s \in S} [G : C_G(s)].$$

Beweis. Dies ist ein Spezialfall von der Bahnengleichung, Satz 1.2.13. □

Definition 1.2.18. Sei p eine Primzahl. Eine endliche Gruppe heißt p-Gruppe, falls es $n \in \mathbb{N}$ gibt mit $|G| = p^n$.

Beispiel 1.2.19. Die Quaternionengruppe der Ordnung 8, die Diedergruppen $D_{2n}, n \geqslant 1$ sind 2-Gruppen.

Satz 1.2.20. *Sei G eine p-Gruppe. Ist $G \neq \{e\}$, dann ist $Z(G) \neq \{e\}$.*

Beweis. Mit den Bezeichnungen des vorherigen Satzes gilt

$$|G| = |Z(G)| + \sum_{s \in S} [G : C_G(s)].$$

Für $s \in S$ gilt $1 \neq [G : C_G(s)] \big| |G|$, also $p \big| [G : C_G(s)]$. Da auch $p \big| |G|$ gilt, folgt $p \big| Z(G)$. Da $e \in Z(G)$ gilt $|Z(G)| \geqslant 1$, also $|Z(G)| \geqslant p$. □

Proposition 1.2.21. *Sei G eine Gruppe. Wenn es $x \in G$ gibt mit $G = \langle Z(G) \cup \{x\} \rangle$, dann ist G abelsch.*

Beweis. Nach Voraussetzung hat jedes Element von G die Gestalt yx^a mit $y \in Z(G)$ und $a \in \mathbb{Z}$. Hieraus folgt die Behauptung. □

Folgerung 1.2.22. *Sei p eine Primzahl. Jede Gruppe der Ordnung p^2 ist abelsch.*

Beweis. Sei G eine Gruppe der Ordnung p^2. Nach Satz 1.2.20 ist $Z(G) \neq \{e\}$. Es folgt $|Z(G)| \in \{p, p^2\}$. Falls $|Z(G)| = p^2$, dann ist $Z(G) = G$ also G abelsch. Falls $|Z(G)| = p$, dann sei $x \in G \backslash Z(G)$. Dann gilt $Z(G) \subsetneq \langle Z(G), x \rangle$, also gilt $G = \langle Z(G), x \rangle$ und nach Proposition 1.2.21 G abelsch. □

1.3 Homomorphismen, Faktorgruppen

1.3.1 Homomorphismen, Normalteiler

Definition 1.3.1. Seien G und G' Monoide. Eine Abbildung $f : G \to G'$ heißt (Monoid)homomorphismus, falls

(a) $f(e) = e'$,

(b) für alle $x, y \in G$: $f(xy) = f(x)f(y)$.

Ein Homomorphismus $f : G \to G'$ heißt Isomorphismus (Endomorphismus, Automorphismus), falls f bijektiv ($G = G'$, $G = G'$ und bijektiv) ist. G und G' heißen isomorph, in Zeichen $G \cong G'$, wenn es einen Isomorphismus $G \to G'$ gibt.

Proposition 1.3.2. *Ein Homomorphismus $f : G \to G'$ ist genau dann Isomorphismus, wenn es einen Homomorphismus $f' : G' \to G$ gibt mit $f \circ f' = \mathrm{id}_{G'}$ und $f' \circ f = \mathrm{id}_G$. Dann gilt $f' = f^{-1}$.*

Beweis. Die Richtung „⇐“ist klar.
Für die Implikation „⇒“zeigen wir, daß die Umkehrabbildung $f' : G' \to G$ ein Homomorphismus ist. Zunächst gilt

$$f'(e') = f'(f(e)) = e$$

Weiterhin gilt für all $x', y' \in G'$

$$f(f'(x') \cdot f'(y')) = f(f'(x')) \cdot f(f'(y')) = x'y' = f(f'(x'y')).$$

Da f injektive ist, ergibt das $f'(x') \cdot f'(y') = f'(x'y')$. □

Proposition 1.3.3. *Seien G, G' Gruppen. $f : G \to G'$ ist genau dann Homomorphismus, wenn für alle $x, y \in G$ $f(xy) = f(x)f(y)$. Dann gilt auch für alle $x \in G$ $f(x^{-1}) = f(x)^{-1}$.*

Beweis. „⇐“: Das ist klar.
„⇒“: Es gilt $f(e) = f(e \cdot e) = f(e)f(e)$, also $f(e) = e'$.
Dann gilt für $x \in G$: $f(e) = f(xx^{-1}) = f(x)f(x^{-1})$ also $f(x^{-1}) = f(x)^{-1}$. □

Ein Monoidhomomorphismus zwischen Gruppen heißt auch Gruppenhomomorphismus.

Proposition 1.3.4. *Sei $f : G \to G'$ Gruppenhomomorphismus.*

(a) Ist H Untergruppe von G, dann ist $f(H)$ Untergruppe von G'. Ist H' Untergruppe von G', so ist $f^{-1}(H')$ Untergruppe von G. Insbesondere ist $\mathrm{im}(f) = f(G)$, das Bild von f Untergruppe von G', und $\ker(f) = f^{-1}(e)$, der Kern von f Untergruppe von G. Außerdem ist für alle $x \in G$, $x \ker(f)x^{-1} = \ker(f)$.

(b) f ist genau dann injektiv, wenn $\ker(f) = e$. f ist genau dann surjektiv, wenn $\mathrm{im}(f) = G$.

Beweis. **Zu (a):** $f^{-1}(H')$ ist Untergruppe von G: $f(e) = e' \in H'$ also $e \in f^{-1}(H')$.
Sei $x, y \in f^{-1}(H')$, also $f(x), f(y) \in H'$ und

$$f(xy^{-1}) = f(x)f(y^{-1}) = f(x)f(y)^{-1} \in H'$$

also $xy^{-1} \in f^{-1}(H')$.
Sei $K = \ker(f)$, $x \in G$. Für $y \in K$ gilt

$$f(xyx^{-1}) = f(x)f(y)f(x^{-1}) = f(x)ef(x)^{-1} = e$$

also $xyx^{-1} \in \ker(f)$.
Zu (b): Wie bei Vektorräumen. □

Definition 1.3.5. Sei G Gruppe. Eine Untergruppe $N \subset G$ heißt Normalteiler oder normale Untergruppe, wenn für alle $x \in G$ $xNx^{-1} = N$, geschrieben $N \triangleleft G$.

Nach Proposition sind Kerne von Gruppenhomomorpismen Normalteiler.
Sei $N \subset G$ Untergruppe.

(a) $N \triangleleft G \Leftrightarrow \forall x \in G : xNx^{-1} \subset N \Leftrightarrow \forall x \in G : xN = Nx \Leftrightarrow \forall x \in G : xN \subset Nx$

(b) $N \triangleleft G \Leftrightarrow N$ ist Vereinigung von Konjugationsklassen

Proposition 1.3.6. *Ist $(N_i)_{i\in I}$ eine Familie von Normalteilern, dann ist $\bigcap_{i\in I} N_i$ Normalteiler.*

Beweis. Wie bei Gruppen. □

Proposition 1.3.7. *Sei $f : G \to G'$ Gruppenhomomorphismus.*

(a) Ist $N' \triangleleft G'$, dann ist $f^{-1}(N') \triangleleft G$.

(b) Ist f surjektiv und $N \triangleleft G$, dann ist $f(N) \triangleleft G'$.

Beweis. Für (b): Sei $z \in N$, $y \in G'$, dann existiert $x \in G$ mit $f(x) = y$. Es gilt

$$yf(z)y^{-1} = f(x)f(z)f(x)^{-1} = f(xzx^{-1}) \in f(N)$$

also $yf(N)y^{-1} \subset f(N)$. □

1.3.2 Beispiele, Bemerkungen

Sei $H \subset G$ eine Untergruppe, dann ist $H \to G$, $x \mapsto x$ ein Homomorphismus. Sind G, G' Gruppen, dann heißt $G \to G'$, $x \mapsto e'$ trivialer Homomorphismus.

Sei $\cdot : G \times X \to X$ eine Operation. Für $g \in G$ sei

$$l_g : X \to X, x \mapsto gx.$$

Mit $l_{g^{-1}} = l_g^{-1}$. Damit haben wir die Abbildung

$$l : G \to \mathfrak{S}_X, g \mapsto l_g.$$

Sie ist Gruppenhomomorphismus, das heißt $l_{g_2} \circ l_{g_1} = l_{g_2 g_1}$. Es gilt

$$\ker(l) = \{g \in G | l_g = \mathrm{id}_X\} = \{g \in G | \forall x \in X : gx = x\} = G_X$$

die Stabilisatorgruppe von X. Insbesondere $G_X \triangleleft G$. Wendet man dies auf die Operation

$$G \times G \to G, (g, x) \mapsto gx$$

an, erhält man:

Satz 1.3.8 (Cayley)**.** *Die Abbildung $l : G \to \mathfrak{S}_G, g \mapsto l_g$ ist injektiver Homomorphismus.*

Beweis. Es gilt: $\ker(l) = \{g \in G | \forall x \in G : gx = x\} = \{e\}$. □

Ein weiterer Spezialfall: Für $u \in G$ ist

$$\kappa_u : G \to G, x \mapsto uxu^{-1}$$

ein Automorphismus, denn

$$\kappa_u(xy) = uxyu^{-1} = uxu^{-1}uyu^{-1} = \kappa_u(x)\kappa_u(y)$$

und $\kappa_u^{-1} = \kappa_{u^{-1}}$.

Sei $\mathrm{Aut}(G)$ die Menge aller Automorphismen von G. Dies ist Gruppe bezüglich der Komposition.

$$\kappa : G \to \mathrm{Aut}(G), u \mapsto \kappa_u$$

ist ein Gruppenhomomorphismus. Es gilt $\ker(\kappa) = Z(G)$. Insbesondere ist $Z(G) \triangleleft G$.

Ist $\varphi : G \to \mathfrak{S}_X$ ein Gruppenhomomorphismus, dann ist $G \times X \to X$, $(g, x) \mapsto \varphi(g)(x)$ eine Operation.

Ist G abelsch, dann sind alle Untergruppen von G Normalteiler.

Die Normalteiler von $\mathfrak{S}_3$ sind $\{e\}$, S_3, $\left\langle \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\rangle$.

Ist $H \subset G$ Untergruppe vom Index 2, dann ist $H \triangleleft G$: Für $x \in G \backslash H$ gilt $G = H \cup xH = H \cup Hx$ disjunkt, also $xH = Hx$, für $x \in H$ gilt $xH = H = Hx$.

1.3.3 Faktorgruppen

Satz 1.3.9. *Sei G Gruppe, $N \triangleleft G$.*

(a) G/N ist bei der Verknüpfung

$$G/N \times G/N \to G/N, (xN, yN) \mapsto xNyN = xyN$$

eine Gruppe mit Neutralelement $eN = N$ und Inversem $(xN)^{-1} = x^{-1}N$ für $xN \in G/N$.

(b) Die Abbildung

$$\pi : G \to G/N, x \mapsto xN$$

ist Gruppenhomomorphismus mit $\ker \pi = N$.

G/N mit dieser Verknüpfung heißt Faktorgruppe von G nach N, oder Faktorgruppe von G modulo N. π heißt der kanonische Homomorphismus.

Beweis. **Zu (a):** Es gilt da N Normalteiler ist

$$xNyN = xyNN = xyN.$$

Dies ist unabhängig von den Repräsentanten, da aus$x_1N = x_2N$ und $y_1N = y_2N$ folgt

$$x_1y_1N = x_1Ny_1N = x_2Ny_2N = x_2y_2N$$

und assoziativ da

$$xN(yNzN) = xN(yzN) = x(yz)N = (xy)zN = (xyN)zN = (xNyN)zN.$$

Zu (b): π ist Gruppenhomomorphismus, da

$$\pi(xy) = xyN = xNyN = \pi(x)\pi(y).$$

$\ker \pi = N$, da

$$\pi(x) = N \Leftrightarrow xN = N \Leftrightarrow x \in N.$$

□

Sei $N \triangleleft G$. Es gilt $|G/N| = [G : N]$. Ist G abelsch, dann auch G/N. Für die Äquivalenzrelation

$$x \sim y \Leftrightarrow xN = yN$$

schreibt man oft $x \equiv y \mod N$ sprich „x kongruent zu y modulo N“.

Proposition 1.3.10. *Die Untergruppen (Normalteiler) von G/N sind genau die Teilmengen H/N wobei H Untergruppe (Normalteiler) von G ist mit $N \subset H$.*

Beweis. Sei $\pi : G \to G/N$ der kanonische Homomorphismus. Sei $H \subset G$ Untergruppe von G mit $N \subset H$. Dann ist $N \triangleleft H$ Normalteiler, und $\pi(H) = \{hN : h \in H\} = H/N$ wird Untergruppe von G/N. Ist zusätzlich $H \triangleleft G$, dann ist $H/N \triangleleft G/N$.

Sei andererseits $U \subset G/N$ Untergruppe. Dann ist $\pi^{-1}(U)$ Untergruppe von G mit $N \subset \pi^{-1}(U)$, und es gilt

$$U = \pi\pi^{-1}(U) = \pi^{-1}(U)N,$$

wobei bei der ersten Gleichung „$\supset$“klar ist; für „$\subset$“sei $xN \in U$, dann $\pi(x) = xN \in U \Rightarrow x \in \pi^{-1}(U) \Rightarrow xN = \pi(x) \in \pi\pi^{-1}(U)$. Ist zusätzlich $U \triangleleft G/N$, dann ist $\pi^{-1}(U) \triangleleft G$. □

1.3.4 Die Faktorgruppen von $(\mathbb{Z}, +)$

Proposition 1.3.11. *Sei $n \in \mathbb{N}_0$, $\pi : \mathbb{Z} \to \mathbb{Z}/\mathbb{Z}n$, $z \mapsto z + \mathbb{Z}n$ der kanonische Homomorphismus.*

(a) Für $n = 0$ ist π Gruppenisomorphismus.

(b) Sei $n > 0$. $\mathbb{Z}/\mathbb{Z}n = \langle 1 + \mathbb{Z}n\rangle = \{r + \mathbb{Z}n : 0 \leqslant r < n\}$ ist zyklische Gruppe der Ordnung n. Die Abbildung

$$d \mapsto \mathbb{Z}d/\mathbb{Z}n$$

ist eine Bijektion von der Menge der Teiler $d \in \mathbb{N}$ von n auf die Meng der Untergruppen von $\mathbb{Z}/\mathbb{Z}n$. Gilt $n = dd'$, dann hat $\mathbb{Z}d/\mathbb{Z}n$ die Ordnung d', es gilt

$$\begin{aligned} \mathbb{Z}d/\mathbb{Z}n &= \{z + \mathbb{Z}n : d'(z + \mathbb{Z}n) = 0 = 0 + \mathbb{Z}n\} \\ \mathbb{Z}d/\mathbb{Z}n &\cong \mathbb{Z}/\mathbb{Z}d' \end{aligned}$$

(c) Ist n eine Primzahl, dann hat $\mathbb{Z}/\mathbb{Z}n$ keine Untergruppe außer $\{0\}$ und $\mathbb{Z}/\mathbb{Z}n$.

Beweis. **Zu (a):** Das ist klar.

Zu (b): $\mathbb{Z}/\mathbb{Z}n$ ist zyklisch: Für $z \in \mathbb{Z}$ gilt $z(1 + \mathbb{Z}n) = 0 + \mathbb{Z}n \Leftrightarrow z + \mathbb{Z}n = 0 + \mathbb{Z}n \Leftrightarrow z \in \mathbb{Z}n \Leftrightarrow n|z$. Also ist $n = \operatorname{ord}(1 + \mathbb{Z}n)$ und $\mathbb{Z}/\mathbb{Z}n = \langle 1 + \mathbb{Z}n\rangle = \{r + \mathbb{Z}n : 0 \leqslant r < n\}$.

Die Abbildung $d \mapsto \mathbb{Z}d/\mathbb{Z}n$ ist eine Bijektion: Es gilt $d|n \Leftrightarrow \mathbb{Z}n \subset \mathbb{Z}d$. Für $d|n$ ist $\mathbb{Z}d/\mathbb{Z}n$ Untergruppe von $\mathbb{Z}/\mathbb{Z}n$, und nach der Proposition 1.3.10 ist jede Untergruppe von $\mathbb{Z}/\mathbb{Z}n$ von dieser Gestalt. Also ist die Abbildung definiert und surjektiv. Ist $n = dd'$, dann ist $\operatorname{ord}(d + \mathbb{Z}n) = d'$, denn

$$z(d + \mathbb{Z}n) = 0 + \mathbb{Z}n \Leftrightarrow zd + \mathbb{Z}n = 0 + \mathbb{Z}n \Leftrightarrow n|zd \Leftrightarrow d'|z.$$

Also hat $\mathbb{Z}d/\mathbb{Z}n$ die Ordnung d'. Insbesondere ist die Abbildung injektiv.

Es gilt $\mathbb{Z}d/\mathbb{Z}n = \{z + \mathbb{Z}n : d'(z + \mathbb{Z}n) = 0\}$, denn

$$d'(z + \mathbb{Z}n) = 0 + \mathbb{Z}n \Leftrightarrow n|d'z \Leftrightarrow d|z \Leftrightarrow z + \mathbb{Z}n \in \mathbb{Z}d/\mathbb{Z}n.$$

Die Abbildung $\mathbb{Z}/\mathbb{Z}d' \to \mathbb{Z}d/\mathbb{Z}n$, $z + \mathbb{Z}d' \mapsto zd + \mathbb{Z}n$ ist Isomorphismus.

Zu (c): Dies folgt aus (b). □

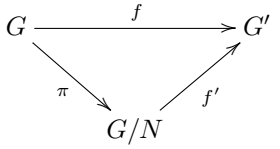
Schreibweise: Sei $a \in \mathbb{Z}$. Statt $x \equiv y \mod \mathbb{Z}a$ ($\Leftrightarrow x - y \in \mathbb{Z}a \Leftrightarrow a|x - y$) schreibt man $x \equiv y \mod a$.

Beispiele 1.3.12. $\mathbb{Z}/\mathbb{Z}4$ hat die Untergruppen $\{0\}$, $\mathbb{Z}2/\mathbb{Z}4 \cong \mathbb{Z}/\mathbb{Z}2$ und $\mathbb{Z}/\mathbb{Z}4$.
$\mathbb{Z}/\mathbb{Z}6$ hat die Untergruppen $\{0\}$, $\mathbb{Z}2/\mathbb{Z}6 \cong \mathbb{Z}/\mathbb{Z}3$, $\mathbb{Z}3/\mathbb{Z}6 \cong \mathbb{Z}/2$, und $\mathbb{Z}/\mathbb{Z}6$.

1.3.5 Die Isomorphiesätze

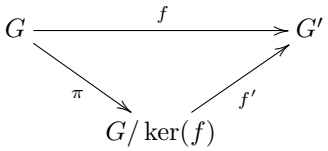
Satz 1.3.13. *Sei $f : G \to G'$ Gruppenhomomorphismus.*

(a) Ist $N \triangleleft G$ mit $N \subset \ker(f)$, dann existiert genau ein Homomorphismus $f' : G/N \to G'$ mit $f = f' \circ \pi$, das heißt, das Diagramm



kommutiert.

(b) (Homomorphiesatz) Es gibt genau einen injektiven Homomorphismus $f' : G/Ker(f) \to G'$ mit $f = f' \circ \pi$ wobei π der kanonische Homomorphismus ist, das heißt, das Diagramm



kommutiert. Insbesondere ist

$$f' : G/\ker(f) \to \mathrm{im}(f), x\ker(f) \mapsto f(x)$$

Isomorphismus.

Beweis. **Zu (a):** Gibt es f' wie behauptet, dann gilt

$$f(x) = f' \circ \pi(x) = f'(x'N). \tag{1.3.1}$$

Wir setzen $f'(xN) = f(x)$ für $x \in G$. Dies ist unabhängig von der Wahl des Repräsentanten, denn

$$xN = yN \Rightarrow x^{-1}y \in N \subset \ker(f) \Rightarrow e = f(x^{-1}y) = f(x^{-1})f(y) = f(x)^{-1}f(y) \Rightarrow f(x) = f(y).$$

f' ist Homomorphismus, da

$$f'(xNyN) = f'(xyN) = f(xy) = f(x)f(y) = f'(xN)f'(yN).$$

Kommutativität des Diagrams:

$$f' \circ \pi(x) = f'(xN) = f(x) \forall x \in G.$$

Zusammen mit (1.3.1) zeigt dies gleichzeitig die Eindeutigkeit.

Zu (b): Wir wenden (a) auf $N = \ker(f)$ an. Dann ist f' injektiv:

$$f'(xN) = e' \Rightarrow f(x) = e' \Rightarrow x \in \ker(f) \to x\ker(f) = \ker(f) = N.$$

Da $\mathrm{im}(f) = \mathrm{im}(f')$ ist dann $f' : G/\ker(f) \to \mathrm{im}(f)$ Isomorphismus. □

Folgerung 1.3.14. *Sei G Gruppe.*
1. Isomorphiesatz: *Sei $H \subset G$ Untergruppe und $N \triangleleft G$ Normalteiler. Dann ist $HN = NH$ Untergruppe von G, $N \triangleleft HN$. $H \cap N \triangleleft H$, und die Abbildung*

$$H/H \cap N \to HN/N, hH \cap N \mapsto hN$$

ist Isomorphismus.
2. Isomorphiesatz: *Seien $M \triangleleft G$, $N \triangleleft G$ Normalteiler mit $M \subset N$. Dann sind $M \triangleleft N$, $N/M \triangleleft G/M$ Normalteiler, und die Abbildung*

$$G/N \to (G/M)/(N/M), xN \mapsto (xM)(N/M)$$

ist Isomorphismus.

Beweis. **1. Isomorphiesatz:** Sei $\pi : G \to G/N$ der kanonische Homomorphismus. Dann gilt

$$\pi^{-1}\pi(H) = HN.$$

„$\supset$“: folgt aus $\pi(HN) = \pi(H)$; „$\subset$“: sei $x \in \pi^{-1}\pi(H)$ dann existiert $h \in H$, so daß $\pi(x) = \pi(h)$, also existiert $h \in H$ mit $xN = hN$, also $x \in HN$. Also ist HN Untergruppe von G. Da für alle $h \in H$ gilt $hN = Nh$, ist $HN = NH$. $N \triangleleft HN$ ist klar. Sei

$$\nu : H \to HN/N, h \mapsto hN.$$

ν ist Homomorphismus mit $\ker \nu = H \cap N$. Insbesondere ist $H \cap N \triangleleft H$. Offenbar ist ν surjektiv. Nach Homomorphiesatz ist dann

$$\nu' : H/H \cap N \to HN/N, hH \cap N \mapsto hN$$

Isomorphismus.
2. Isomorphiesatz: $M \triangleleft N$ und $N/M \triangleleft G/M$ sind klar. Seien

$$G \xrightarrow{\pi} G/M \xrightarrow{\nu} (G/M)/(N/M)$$

sie kanonischen Homomorphismen. $\nu\pi$ ist surjektiv. Es gilt $\ker(\nu\pi) = N$, denn

$$\nu\pi(x) = \nu(xM) = (xM)(N/M) = N/M \Leftrightarrow xM \in M/N \Leftrightarrow x \in N.$$

Nach Homomorphiesatz ist

$$G/N \to (G/M)/(N/M), xN \mapsto (xM)(N/M)$$

Isomorphismus. □

Sind $N_1, \ldots, N_k$ Normalteiler von G, dann auch $N_1 \cdots N_k$: Nach Folgerung und Induktion ist $N_1 \cdots N_k$ Untergruppe von G; für $x \in G$ gilt: $xN_1 \cdots N_k x^{-1} = xN_1x^{-1}xN_2 \cdots x^{-1}xN_kx^{-1} = N_1 \cdots N_k$.

1.3.6 Zyklische Gruppen

Satz 1.3.15. *Sei G Gruppe.*

(a) G ist genau dann zyklisch, wenn es $n \in \mathbb{N}_0$ gibt, mit $G \cong \mathbb{Z}/\mathbb{Z}n$. Ist G zyklisch, dann sind auchdie Unter- und Faktorgruppen von G zyklisch.

(b) Sei $G = \langle g \rangle$ zyklisch von der Ordnung $n \in \mathbb{N}$. Die Abbildung

$$d \mapsto \langle g^d \rangle$$

ist eine Bijektion von der Menge der Teiler $d \in \mathbb{N}$ von n auf die Untergruppen von G. Ist $n = dd'$, dann hat $\langle g^d \rangle$ die Ordnung d', es gilt $\langle g^d \rangle = \{x \in G | x^{d'} = e\}$.

Beweis. **Zu (a):** „⇒“Sei G zyklisch mit $G = \langle g \rangle = \{g^z | z \in \mathbb{Z}\}$. Die Abbildung

$$f : \mathbb{Z} \to G, z \mapsto g^z$$

ist ein surjektiver Homomorphismus, es gibt $n \in \mathbb{N}_0$ mit $\ker(f) = \mathbb{Z}n$. Nach Homomorphiesatz ist

$$f' : \mathbb{Z}/\mathbb{Z}n \to G, z + \mathbb{Z}n \mapsto g^z$$

Isomorphismus.
„⇐“Sei andererseits

$$h : \mathbb{Z}/\mathbb{Z}n \to G$$

ein Isomorphismus. Da $\mathbb{Z}/\mathbb{Z}n$ von $1 + \mathbb{Z}n$ erzeugt wird, wird G von $h(1 + \mathbb{Z}n)$ erzeugt.
Sei $G = \langle g \rangle$, $f : \mathbb{Z} \to G$ wie oben und $H \subset G$ eine Untergruppe. Dann ist $f^{-1}(H)$ eine Untergruppe von $\mathbb{Z}$, also gibt es $m \in \mathbb{N}_0$ mit $f^{-1}(H) = \mathbb{Z}m$. Da f surjektiv ist, gilt

$$H = ff^{-1}(H) = f(\mathbb{Z}m) = \langle g^m \rangle.$$

Ferner $G/H = \langle gH \rangle$.

Zu (b): Sei $G = \langle g \rangle$ von der Ordnung n, sei $f' : \mathbb{Z}/\mathbb{Z}n \to G, z + \mathbb{Z}n \mapsto g^z$ der Isomorphismus aus (a). Unter f' entsprechen die Untergruppen von G genau den Untergruppen von $\mathbb{Z}/\mathbb{Z}n$. Letztere sind genau die $\mathbb{Z}d/\mathbb{Z}n$, wobei $\mathbb{N} \ni d|n$. Da $f'(\mathbb{Z}d/\mathbb{Z}n) = \langle g^d \rangle$ ist, ist die erste Behauptung gezeigt. Für $n = dd'$ hat $\mathbb{Z}d/\mathbb{Z}n$ die Ordnung d', also auch $\langle g^d \rangle$. Für $z \in \mathbb{Z}$ gilt

$$(g^z)^{d'} = e \Leftrightarrow zd' + \mathbb{Z}n = 0 + \mathbb{Z}n \Leftrightarrow n|zd' \Leftrightarrow d|z \Leftrightarrow g^z \in \langle g^d \rangle.$$

□

Folgerung 1.3.16. *Für eine Gruppe $G \neq \{e\}$ sind äquivalent:*

(a) Die Ordnung von G ist eine Primzahl.

(b) Es gibt eine Primzahl p mit $G \cong \mathbb{Z}/\mathbb{Z}p$.

(c) G besitzt keine Untergruppen außer $\{e\}$ und G.

Beweis. **(a)⇒(c):** Das ist gezeigt (Lagrange).
(c)⇒(b): Für $e \neq g \in G$ gilt $\{e\} \neq \langle g\rangle \subset G$, also $\langle g\rangle = G$. Nach dem vorhergehenden Satz ist $|G| = p$ eine Primzahl. Dann ist $G \cong \mathbb{Z}/\mathbb{Z}p$.
(b)⇒(a): Das ist klar. □

Definition 1.3.17. Eine Gruppe G heißt einfach, wenn $G \neq \{e\}$ und G außer G und $\{e\}$ keine Normalteiler enthält.

Folgerung 1.3.18. *Die einfachen abelschen Gruppen sind bis auf Isomorphie genau die $\mathbb{Z}/\mathbb{Z}p$, p prim.*

Folgerung 1.3.19. *Sei p prim, G Gruppe der Ordnung p^2. Dann gilt entweder $G \cong \mathbb{Z}/\mathbb{Z}p^2$, oder $\mathbb{Z} \cong \mathbb{Z}/\mathbb{Z}p \times \mathbb{Z}/\mathbb{Z}p$.*

Beweis. Wir wissen, daß G abelsch ist nach Folgerung 1.2.22. Falls für alle $e \neq x \in G$ gilt $\mathrm{ord}(x) = p$: sei $e \neq x, y \in G$ mit $y \in G\backslash\langle x\rangle$. Da $\langle x\rangle$ und $\langle y\rangle$ die Ordnung p haben, gilt

$$\langle x\rangle \cap \langle y\rangle = \{e\}.$$

Wir zeigen: die Abbildung

$$h : \mathbb{Z}/\mathbb{Z}p \times \mathbb{Z}/\mathbb{Z}p \to G, (\overline{a}, \overline{b}) \mapsto x^a y^b$$

ist Isomorphismus, dabei ist $\overline{a} = a + \mathbb{Z}p$ und $\overline{b} = b + \mathbb{Z}p$.

$$\begin{aligned} h((\overline{a}_1, \overline{b}_1) + (\overline{a}_2, \overline{b}_2)) &= h(\overline{a}_1 + \overline{a}_2, \overline{b}_1 + \overline{b}_2) \\ &= h(\overline{a_1 + a_2}, \overline{b_1 + b_2}) \\ &= x^{a_1+a_2} y^{b_1+b_2} \\ &= x^{a_1} x^{a_2} y^{b_1} y^{b_2} \\ &= x^{a_1} y^{b_1} x^{a_2} y^{b_2} = h(\overline{a}_1 \overline{b}_1) h(\overline{a}_2, \overline{b}_2). \end{aligned}$$

h ist injektiv: Aus $h(\overline{a}, \overline{b}) = e$ folgt $x^a y^b = e$ also $x^a = y^{-b} \in \langle x\rangle \cap \langle y\rangle = \{e\}$, das heißt $x^a = y^b = e$ und es muß gelten $p|a, b$ in anderen Worten $a, b \in \mathbb{Z}p$ oder $a = \overline{b} = \overline{0}$. Also $(\overline{a}, \overline{b}) = (\overline{0}, \overline{0})$.
Da beide Seiten p^2 Elemente haben, ist h Isomorphismus.

Gibt es $x \in G$ der Ordnung p^2, dann ist $G = \langle x\rangle$ und es gibt einen Ismorphismus

$$\mathbb{Z}/\mathbb{Z}p^2 \to \langle x\rangle.$$

□

1.3.7 $\mathbb{Z}/\mathbb{Z}a$ als Ring, prime Restklassen

Proposition 1.3.20. *Sei $a \in \mathbb{Z}$.*

(a) $\mathbb{Z}/\mathbb{Z}a$ ist bezüglich der Multiplikation

$$\mathbb{Z}/\mathbb{Z}a \times \mathbb{Z}/\mathbb{Z}a \to \mathbb{Z}/\mathbb{Z}a, (x + \mathbb{Z}a, y + \mathbb{Z}a) \mapsto xy + \mathbb{Z}a$$

abelsches Monoid mit neutralem Element $1 + \mathbb{Z}a$.

(b) $\mathbb{Z}/\mathbb{Z}a$ ist bezüglich $+, \cdot$ ein kommutativer Ring mit Einselement (abelsche Gruppe bezüglich $+$, abelsches Monoid bezüglich $\cdot$, und es gilt das Distributivgesetz).

Beweis. **Zu (a):** Wohldefiniert: Sei $x_1 + \mathbb{Z}a = x_2 + \mathbb{Z}a$ und $y_1 + \mathbb{Z}a = y_2 + \mathbb{Z}a$, dann folgt $x_1 - x_2$ und $y_1 - y_2 \in \mathbb{Z}a$, also

$$x_1 y_1 - x_2 y_2 = (x_1 - x_2) y_1 + (y_1 - y_2) x_2 \in \mathbb{Z}a,$$

also

$$x_1 y_1 + \mathbb{Z}a = x_2 y_2 \ + \mathbb{Z}a.$$

Das Prüfen der Axiome ist Routine.
Zu (b): Distributivgesetz:

$$\overline{x}(\overline{y} + \overline{z}) = \overline{x}(\overline{y + z}) = \overline{x(y + z)} = \overline{xy + xz} = \overline{xy} + \overline{xz}.$$

□

Proposition 1.3.21. *Seien $a_1, \dots a_r \in \mathbb{Z}\setminus\{0\}$ paarweise relativ prim.*

(a) (Chinesischer Restsatz) Die Abbildung

$$\mathbb{Z}/\mathbb{Z}\,a_1\cdots a_r \to \prod_{i=1}^{r} \mathbb{Z}/\mathbb{Z}\,a_i, \overline{z} \mapsto (\overline{z}, \dots, \overline{z})$$

ist ein Ringisomorphismus.

(b) $\mathbb{Z}\,a_1\cdots a_r \cong \bigcap_{i=1}^{r} \mathbb{Z}\,a_i$. Insbesondere ist $a_1\cdots a_r$ ein kgV der $a_1, \dots, a_r$.

Beweis. Sei

$$\psi : \mathbb{Z} \to \prod_{i=1}^{r} \mathbb{Z}/\mathbb{Z}\,a_i, z \mapsto (\overline{z}, \dots, \overline{z}).$$

Dies ist Homomorphismus bezüglich + und ·, es gilt $\ker\psi = \bigcap_{i=1}^{r} \mathbb{Z}\,a_i$. Es gilt auch $\ker\psi = \mathbb{Z}\,a_1\cdots a_r$:
„$\supset$“ ist klar.
„$\subset$“ Induktion nach r. Der Fall $r = 1$ ist klar. Sei $r > 1$ und $\psi(z) = (\overline{z}, \dots, \overline{z}) = (\overline{0}, \dots, \overline{0})$. Nach Induktionsannahme ist $z \in \mathbb{Z}\,a_2\cdots a_r$, d.h. es gibt $x \in \mathbb{Z}$ mit $z = xa_2\cdots a_r$. Außerdem $z \in \mathbb{Z}\,a_1$, d.h. es gibt $y \in \mathbb{Z}$ mit $z = ya_1$. OBdA. sei $z \neq 0$. Es folgt

$$ya_1 = xa_2\cdots a_r$$

also

$$a_1 \big| xa_2\cdots a_r$$

und mit Euklid $a_1 \big| x$, d.h. es gibt $x' \in \mathbb{Z}$ mit $x = x'a_1$. Dann ist

$$z = x'a_1\cdots a_r \in \mathbb{Z}\,a_1\cdots a_r.$$

Nach Homomorphiesatz ist die Abbildung

$$\psi' : \mathbb{Z}/\mathbb{Z}\,a_1\cdots a_r \to \prod_{i=1}^{r} \mathbb{Z}/\mathbb{Z}\,a_i, \overline{z} \mapsto (\overline{z}, \dots, \overline{z})$$

injektiver Gruppenhomomorphismus. ψ' ist auch Monoidhomomorphismus bezüglich ·. Da beide Seiten $|a_1\cdots a_r|$ Elemente haben, ist ψ' auch surjektiv. □

Definition 1.3.22. Für $a \in \mathbb{Z}/\{0\}$ sei $(\mathbb{Z}/\mathbb{Z}\,a)^\times$ die Einheitengruppe des Monoids $(\mathbb{Z}/\mathbb{Z}\,a, \cdot)$. $(\mathbb{Z}/\mathbb{Z}\,a)^\times$ heißt prime Restklassengruppe modulo a.

Proposition 1.3.23. *Sei $a \in \mathbb{Z}\setminus\{0\}$. Die Abbildung*

$$h : \mathrm{Aut}(\mathbb{Z}/\mathbb{Z}\,a) \to (\mathbb{Z}/\mathbb{Z}\,a)^\times, \alpha \mapsto \alpha(\overline{1})$$

ist ein Gruppenisomorphismus.

Beweis. Für $\alpha \in \mathrm{Aut}(\mathbb{Z}/\mathbb{Z}\,a)$ sei $h(\alpha) = \alpha(\overline{1}) = \overline{x}$, $\alpha^{-1}(\overline{1}) = \overline{y}$. Dann ist $\overline{1} = \alpha^{-1}\alpha(\overline{1}) = \alpha^{-1}(\overline{x}) = \alpha^{-1}(\overline{x}\,\overline{1}) = x\alpha^{-1}(\overline{1}) = \overline{xy}$. Also ist $h(\alpha) \in (\mathbb{Z}/\mathbb{Z}\,a)^\times$.
Um zu zeigen h ist Homomorphismus: seien α und $\beta \in \mathrm{Aut}(\mathbb{Z}/\mathbb{Z}\,a)$, $h(\alpha) = \alpha(\overline{1}) = \overline{x}$, $h(\beta) = \beta(\overline{1}) = \overline{y}$. Dann $h(\beta\circ\alpha) = (\beta\circ\alpha)(\overline{1}) = \beta(\overline{x}) = x\beta(\overline{1}) = x\overline{y} = \overline{xy} = \overline{yx} = h(\beta)h(\alpha)$.
Inverses von h: Für $\overline{x} \in (\mathbb{Z}/\mathbb{Z}\,a)^\times$ sei $l_{\overline{x}} : \mathbb{Z}/\mathbb{Z}\,a \to \mathbb{Z}/\mathbb{Z}\,a, \overline{z} \mapsto \overline{zx}$. Dies ist ein Automorphismus, und die Abbildung $\overline{x} \mapsto l_{\overline{x}}$ ist invers zu h. □

Folgerung 1.3.24 (Aus dem chinesischen Restsatz)**.** *Seien $a_1, \dots, a_r \in \mathbb{Z}\setminus\{0\}$ paarweise Teilerfremd. Dann ist die Abbildung*

$$\psi : (\mathbb{Z}/\mathbb{Z}\,a_1\cdots a_r)^\times \to \prod_{i=1}^{r} (\mathbb{Z}/\mathbb{Z}\,a_i)^\times, \overline{z} \mapsto (\overline{z}, \dots, \overline{z})$$

Gruppenisomorphismus.

Beweis. Sei ψ' die Abbildung aus dem Chinesischen Restsatz. Es gilt $\overline{z} \in (\mathbb{Z}/\mathbb{Z}\,a_1 \cdots a_r)^\times$ genau dann, wenn es $z' \in \mathbb{Z}$ gibt mit $zz' \equiv 1 \mod a_1 \cdots a_r$ genau dann, wenn für alle i gilt $zz' \equiv 1 \mod a_i$. Also $\psi'(\overline{z}) = (\overline{z}, \ldots, \overline{z}) \in \prod_{i=1}^r (\mathbb{Z}/\mathbb{Z}\,a_i)^\times$. Klar ist ψ' injektiver Gruppenhomomorphismus.
ψ' ist auch surjektiv: Sei $(\overline{x}_1, \ldots, \overline{x}_r) \in \prod_{i=1}^r (\mathbb{Z}/\mathbb{Z}\,a_i)^\times$. Dann gibt es $(\overline{x}'_1, \ldots, \overline{x}'_r) \in \prod_{i=1}^r (\mathbb{Z}/\mathbb{Z}\,a_i)^\times$ mit $\overline{x}_i\overline{x}'_i = 1$ in $\mathbb{Z}/\mathbb{Z}\,a_i$. Nach Restsatz existiert $\overline{zz'} \in \mathbb{Z}/\mathbb{Z}\,a_1 \cdots a_r$ mit $\psi'(\overline{z}) = (\overline{x}_1, \ldots, \overline{x}_r)$ und $\psi'(\overline{z}') = (\overline{x}'_1, \ldots, \overline{x}'_r)$. Es folgt

$$\psi'(\overline{zz'}) = \psi'(\overline{z})\psi(\overline{z}') = (\overline{x}_1, \ldots, \overline{x}_r)(\overline{x}'_1, \ldots, \overline{x}'_r) = (\overline{1}, \ldots, \overline{1}) = \psi'(\overline{1})$$

also $\overline{zz'} = \overline{1}$. Also ist $\overline{z} \in (\mathbb{Z}/\mathbb{Z}\,a_1 \cdots a_r)^\times$, $\psi(\overline{z}) = (\overline{x}_1, \ldots, \overline{x}_r)$. □

Proposition und Definition 1.3.25. *Sei $n \in \mathbb{N}$. Für $x \in \mathbb{Z}$ sind äquivalent*

(a) $x + \mathbb{Z}\,n \in (\mathbb{Z}/\mathbb{Z}\,n)^\times$,

(b) $x + \mathbb{Z}\,n$ *erzeugt die Gruppe* $(\mathbb{Z}/\mathbb{Z}\,n, +)$,

(c) $\operatorname{ord}(x + n\,\mathbb{Z}) = n$,

(d) n *und* x *sind teilerfremd.*

Die Anzahl der $x \in \mathbb{N}$, $1 \leqslant x \leqslant n$ die (a)-(d) genügen, wird mit $\varphi(n)$ bezeichnet. Die Abbildung $\varphi : \mathbb{N} \to \mathbb{N}$ heißt Eulersche Funktion.

Beweis. „(a) ⇔ (d) ": Es gilt $x + \mathbb{Z}\,n \in (\mathbb{Z}/\mathbb{Z}\,n)^\times$ genau dann, wenn es $x' \in \mathbb{Z}$ gibt mit $xx' \equiv 1 \mod n$ genau dann, wenn es $x', y \in \mathbb{Z}$ gibt, mit $xx' + yn = 1$. Nach Bezout äquivalent zu $(x, n) = 1$.
„(b) ⇔ (c) ": Klar.
„(a) ⇔ (b) ": Es gilt $\overline{x} \in (\mathbb{Z}/\mathbb{Z}\,n)^\times$ genau dann, wenn es $x' \in \mathbb{Z}$ gibt mit $x'\overline{x} = \overline{1}$, genau dann, wenn $\overline{1} \in \langle\overline{x}\rangle$ genau dann, wenn $\mathbb{Z}/\mathbb{Z}\,n \subset \langle\overline{x}\rangle$ genau dann, wenn $\langle\overline{x}\rangle = \mathbb{Z}/\mathbb{Z}\,n$. □

Beispiel 1.3.26.

$$\begin{aligned}
\varphi(1) &= 1\\
\varphi(2) &= 1\\
\varphi(3) &= 2\\
\varphi(4) &= 2\\
\varphi(5) &= 4\\
\varphi(6) &= 2\\
\varphi(7) &= 6\\
\varphi(8) &= 4\\
\varphi(9) &= 6\\
\varphi(10) &= 4
\end{aligned}$$

Also $\mathbb{Z}/\mathbb{Z}\,4$ erzeugt durch $\overline{1}, \overline{3}$, $\mathbb{Z}/\mathbb{Z}\,6$ erzeugt durch $\overline{1}, \overline{5}$. Für $n \geqslant 2$ ist $\varphi(n)$ gerade. $\varphi(n) = n - 1$ genau dann, wenn n prim („⇐ ": Das ist klar. „⇒ ": sein n nicht prim, dann gibt es $k, l \in \mathbb{N}\setminus\{1\}$: $n = kl$, also $\varphi(n) \leqslant n - 2$.)

Satz 1.3.27. *(a) Sind $a_1, \ldots, a_r \in \mathbb{N}$ paarweise teilerfremd, dann gilt*

$$\varphi(a_1 \cdots a_r) = \prod_{i=1}^r \varphi(a_i).$$

(b) Ist $n = p_1^{\nu_1} \cdots p_r^{\nu_r}$ mit $p_1 < \ldots < p_r$ und $\nu_i \in \mathbb{N}$, dann ist

$$\varphi(n) = \prod_{i=1}^r p_i^{\nu_i - 1}(p_i - 1) = n \prod_{i=1}^r (1 - \frac{1}{p_i}).$$

(c) Für $n \in \mathbb{N}$ gilt

$$n = \sum_{0<d|n} \varphi(d).$$

Beweis. **(a)** Nach der Folgerung zum Restsatz gilt $(\mathbb{Z}/\mathbb{Z}\,a_1 \cdots a_r)^\times \cong \prod_{i=1}^r (\mathbb{Z}/\mathbb{Z}\,a_i)^\times$, also gilt $\varphi(a_1 \cdots a_r) = \varphi(a_1) \cdots \varphi(a_r)$.
(b) Sei zuerst $n = p^\nu$ mit p Primzahl, $\nu \in \mathbb{N}$. Für $x \in \mathbb{N}$, $1 \leqslant x \leqslant p^\nu$, gilt: x, p^ν sind nicht teilerfremd, genau dann, wenn $p|x$ genau dann, wenn es $1 \leqslant y \leqslant p^{\nu-1}$ gibt mit $x = py$. Es folgt

$$\varphi(p^\nu) = p^\nu - p^{\nu-1}.$$

Ist $n = p_1^{\nu_1} \cdots p_r^{\nu_r}$ dann

$$\varphi(n) = \prod_{i=1}^r p_i^{\nu_i - 1}(p_i - 1) = n \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right).$$

(c) Für $n \in \mathbb{N}$ und $d \in \mathbb{N}$ mit $d|n$ sei X_d die Menge aller Elemente der Ordnung d von $\mathbb{Z}/\mathbb{Z}\,n$. Dann $\mathbb{Z}/\mathbb{Z}\,n = \bigcup_{d|n} X_d$ disjunkt. Da $\mathbb{Z}/\mathbb{Z}\,n$ zu jedem $d|n$ genau eine Untergruppe der Ordnung d enthält, ist $|X_d| = \varphi(d)$. Es gilt

$$n = \sum_{d|n} |X_d| = \sum_{d|n} \varphi(d).$$

□

Proposition 1.3.28. *(a) (Euler) Sind $n \in \mathbb{N}$ und $a \in \mathbb{Z}\setminus\{0\}$ teilerfremd, dann gilt*

$$a^{\varphi(n)} \equiv 1 \mod n.$$

(b) (Kleiner Satz von Fermat) Ist p prim, $a \in \mathbb{Z}$, dann gilt

$$a^p \equiv a \mod p.$$

Falls $p \big| a$ ist letzteres trivial.

Beweis. **(a)** Sind n, a teilerfremd, dann gilt $a + \mathbb{Z}\,n \in (\mathbb{Z}/\mathbb{Z}\,n)^\times$, also gilt

$$(a + \mathbb{Z}\,n)^{\varphi(n)} = 1 + \mathbb{Z}\,n$$

das heißt $a^{\varphi(n)} \equiv 1 \mod n$.
(b) Falls $p \nmid a$, dann gilt

$$a^{p-1} \equiv 1 \mod p$$

nach (a). Es folgt

$$a^p \equiv a \mod p.$$

Falls $p|a$ ist letzteres trivial. □

Wenn $n \in \mathbb{N}$ und $a \in \mathbb{Z}\setminus\{0\}$ teilerfremd sind, dann setzt man $\mathrm{ord}_n(a) = \mathrm{ord}(a + \mathbb{Z}\,n)$. Nach Proposition gilt $\mathrm{ord}_n(a) \big| \varphi(n)$.

Proposition 1.3.29. *Sei $n \in \mathbb{N}$. $\mathbb{Z}/\mathbb{Z}\,n$ ist genau dann Körper, wenn n Primzahl ist.*

Beweis. „$\Leftarrow$“: Sei n Primzahl. Dann ist $\mathbb{Z}/\mathbb{Z}\,n$ kommutativer Ring mit $\overline{1} \neq \overline{0}$, und $(\mathbb{Z}/\mathbb{Z}\,n)^\times = (\mathbb{Z}/\mathbb{Z}\,n)\setminus\{0\}$ ist Gruppe. Also ist $\mathbb{Z}/\mathbb{Z}\,n$ Körper.
„$\Rightarrow$“: Sei $\mathbb{Z}/\mathbb{Z}\,n$ Körper. Dann ist $n > 1$. Wäre $n = kl$ mit $k, l \in \mathbb{N}\setminus\{1\}$, dann wäre $\overline{k} \neq \overline{0} \neq \overline{l}$, aber $\overline{kl} = \overline{n} = \overline{0}$, Widerspruch. □

1.4 Direkte und semi-direkte Produkte

1.4.1 Direkte Produkte

Seien $G_1, \dots, G_r$ Gruppen, $G := \prod_{i=1}^r G_i$ das kartesische Produkt. Für $1 \leqslant i \leqslant r$ hat man die Homomorpismen

$$\begin{aligned} p_i &: G \to G_i; \qquad (x_1, \dots, x_r) \mapsto x_i \quad \text{(Projektion)} \\ q_i &: G_i \to G; \quad x \mapsto (e, \dots, e, x, e, \dots e) \quad \text{(Inklusion)} \end{aligned}$$

Sei $\widetilde{G}_i = q_i(G_i)$.

Proposition 1.4.1. *(a) Die $\widetilde{G}_i = q_i(G_i)$ sind Normalteiler von G.*

(b) Für $i < j$ ist jedes Element von $\widetilde{G}_i$ mit jedem Element von $\widetilde{G}_j$ vertauschbar.

(c) $G = \widetilde{G}_1 \cdots \widetilde{G}_r$

(d) $\widetilde{G}_i \cap (\widetilde{G}_1 \cdots \widetilde{G}_{i-1}\widetilde{G}_{i+1} \cdots \widetilde{G}_r) = \{e\}$ für $1 \leqslant i \leqslant r$.

Beweis. **Zu (a):** Es gilt $\widetilde{G}_i = \bigcap_{j \neq i} \ker(p_j)$.
Zu (b): Für $i < j$ gilt: $q_i(x)q_j(y) = (e, \dots, e, x, e \dots, e, y, e, \dots, e) = q_j(y)q_i(x)$.
Zu (c): $(x_1, \dots, x_r) = q_1(x_1) \cdots q_1(x_r)$.
Zu (d): Das ist klar. □

Proposition 1.4.2. *Für eine Gruppe G und Untergruppen $H_1, \dots, H_r$ sind äquivalent:*

(a) $H_1, \dots, H_r$ sind Normalteiler mit

$$G = H_1 \cdots H_r \quad \text{und} \quad H_i \cap (H_{i+1} \dots H_r) = \{e\}$$

für $1 \leqslant i \leqslant r$.

(b) Die Abbildung

$$f : \prod_{i=1}^r H_i \to G, (x_1, \dots, x_r) \mapsto x_1 \cdots x_r$$

ist Gruppenisomorphismus.

(c) Für $1 \leqslant i < j \leqslant r$, $x_i \in H_i$, $x_j \in H_j$ gilt:

$$x_i x_j = x_j x_i$$

und jedes Element $x \in G$ hat eine eindeutige Darstellung

$$x = x_1 \cdots x_r \quad \text{mit } x_i \in H_i.$$

Definition 1.4.3. Gelten diese Aussagen, dann heißt G direktes Produkt der H_i, man schreibt

$$G = H_1 \times \cdots \times H_r = \times_{i=1}^r H_i.$$

Im Fall einer abelschen Gruppe $(G, +)$, schreibt man

$$G = H_1 \oplus \cdots \oplus H_r = \bigoplus_{i=1}^r H_i.$$

Beweis. „$(a) \Rightarrow (c)$ “: Für $1 \leqslant i < j \leqslant r$, $x_i \in H_i$, $x_j \in H_j$ gilt

$$\begin{aligned} x_i^{-1}x_j^{-1}x_ix_j &= (x_i^{-1}x_j^{-1}x_i)x_j \in H_j \text{ da beide Summanden in } H_j \text{ (Normalteiler)} \\ &= x_i^{-1}(x_j^{-1}x_ix_j) \in H_i \text{ da beide Summanden in } H_i \text{ (Normalteiler)}, \end{aligned}$$

das heißt

$$x_i^{-1}x_j^{-1}x_ix_j \in H_i \cap H_j \subset H_i \cap (H_{i+1} \dots H_r) = \{e\}.$$

Also

$$x_ix_j = x_jx_i.$$

Sei $x \in G$, dann gibt es $x_i \in H_i$ mit $x = x_1 \cdots x_r$. Ist auch $x = x_1' \cdots x_r'$ mit $x_i' \in H_i$, dann ist

$$\begin{aligned} x_1' \cdots x_r' &= x_1 \cdots x_r \\ x_1^{-1}x_1' &= (x_2 \cdots x_r)({x_r'}^{-1} \cdots {x_2'}^{-1}) = x_2{x_2'}^{-1} \cdots x_r{x_r'}^{-1} \in H_1 \cap (H_2 \cdots H_R) = \{e\} \end{aligned}$$

Also $x_1 = x_1'$. Induktiv folgt $x_i = x_i'$ für alle i.
„$(c) \Rightarrow (b)$ “: Das ist klar.
„$(b) \Rightarrow (a)$ “: Sei $H = \prod_{i=1}^r H_i$, seien die $\widetilde{H}_i$ wie vorher. Sei $f : \prod_{i=1}^r H_i \to G, (x_1, \dots, x_r) \mapsto x_1 \cdots x_r$ ein Isomorphismus. Dann sind die $H_i = f(\widetilde{H}_i)$ ebenfalls Normalteiler von G. Ferner gilt

$$G = f(H) = f(\widetilde{H}_1 \cdots \widetilde{H}_r) = f(\widetilde{H}_1) \cdots f(\widetilde{H}_r) = H_1 \cdots H_r$$

und

$$H_i \cap (H_{i+1} \cdots H_r) = f(\widetilde{H}_i) \cap \left(f(\widetilde{H}_{i+1}) \cdots f(\widetilde{H}_r)\right) = f\left(\widetilde{H}_i \cap (\widetilde{H}_{i+1} \cdots \widetilde{H}_r)\right) = f(\{e\}) = \{e\}.$$

□

1.4.2 Der Hauptsatz für endliche abelsche Gruppen

Definition 1.4.4. Sei $(A, +)$ abelsche Gruppe, p eine Primzahl. Dann ist

$$A_p := \{x \in A \mid \exists k \in \mathbb{N} : p^k x = 0\}$$

eine Untergruppe von A. Sie heißt p-Komponente von A.

Proposition 1.4.5. *Sei A endliche abelsche Gruppe, $|A| = n = p_1^{\nu_1} \cdots p_r^{\nu_r}$ mit $r \in \mathbb{N}_0$, $p_1 < \cdots < p_r$ prim, $\nu_1, \dots, \nu_r \in \mathbb{N}$. Sei $A_i = A_{p_i}$ jeweils die p_i-Komponente. Dann $A = A_1 \oplus \cdots \oplus A_r$ (Primarzerlegung).*

Beweis. Die Zahlen $q_i = \prod_{j \neq i} p_j^{\nu_j}$ sind teilerfremd, also gibt es $u_i \in \mathbb{Z}$ mit $\sum_{i=1}^r u_iq_i = 1$. Für $x \in A$ gilt

$$x = \sum_{i=1}^r u_iq_ix$$

und es gilt:

$$p_i^{\nu_i}u_iq_ix = u_inx = 0,$$

also $u_iq_ix \in A_i$. Somit $A = A_1 + \cdots + A_r$. Sei $1 \leqslant i < r$, $x \in A_i \cap (A_{i+1} + \ldots + A_r)$. Dann gibt es $k \in \mathbb{N}$ mit $p_i^k x = 0$, ferner $l \in \mathbb{N}$ mit $(p_{i+1} \cdots p_r)^l x = 0$. Es gibt $u, v \in \mathbb{Z}$ mit $p_i^k u + (p_{i+1} \cdots p_r)^l v = 1$. Es folgt

$$x = p_i^k ux + (p_{i+1} \cdots p_r)^l vx = 0.$$

Es folgt $A = A_1 \oplus \cdots \oplus A_r$. □

Proposition 1.4.6. *Sei A endliche abelsche Gruppe, $A = B \oplus C$ mit Untergruppen B, C. Es gebe p prim und $\nu \in \mathbb{N}$ mit $p^\nu B = 0$, $p \nmid |C|$. Dann ist $B = A_p$.*

Beweis. „$\subset$ “: Klar.
„$\supset$ “: Sei $x \in A_p$, $p^l x = 0$. Es gibt $\xi, \mu \in \mathbb{Z}$ mit $p^l\xi + |C|\mu = 1$. Sei $x = b + c$ mit $b \in B$, $c \in C$. Dann

$$x = p^l\xi x + |C|\mu x = 0 + |C|\mu(b + c) = |C|\mu b \in B.$$

□

Proposition 1.4.7. *Sei A eine endliche abelsche Gruppe, p prim, mit $A_p = A$. Ferner sei $B = \mathbb{Z}\,b$ eine zyklische Untergruppe maximaler Ordnung p^n von A. Dann gibt es eine Untergruppe C von A mit $A = B \oplus C$.*

Beweis. **Induktion nach** $[A : B]$**.** Falls $[A : B] = 1$, dann setze $C = 0$. Sei also $[A : B] > 1$ und $c \in A \backslash B$. Dann gilt

$$\operatorname{ord}(c + B) \big| \operatorname{ord}(c) \big| p^n$$

also gibt es $r \in \mathbb{N}$, $1 \leqslant r \leqslant n$ mit $\operatorname{ord}(c + B) = p^r$. Wir zeigen: es gibt eine Untergruppe D, der Ordnung p von A mit $B \cap D = 0$.
Beweis dazu: Da $p^r c \in B$, gibt es $s \in \mathbb{Z}$ mit $p^r c = sb$. Es gilt

$$0 = p^n c = p^{n-r} sb \Rightarrow p^n \big| p^{n-r} s \Rightarrow p^r \big| s \Rightarrow p \big| s \Rightarrow \exists s' \in \mathbb{Z} : s = ps'.$$

Es folgt

$$p^r c = ps'b \text{ also } p(p^{r-1} c - s'b) = 0.$$

Wegen $c \notin B$ gilt

$$d := p^{r-1} c - s'b \notin B,$$

insbesondere $d \neq 0$, also $\operatorname{ord}(d) = p$. Sei $D = \mathbb{Z}\,d$, dann $|D| = p$ und $B \cap D = 0$.
Induktionsschritt: Es gilt $(B + D)/D \cong B/B \cap D \cong B$, also ist $(B + D)/D$ Untergruppe der Ordnung p^n von A/D. Für $x \in A$ gilt

$$\operatorname{ord}(x + D) \big| \operatorname{ord}(x) \big| p^n.$$

Es gilt $[A/D : (B + D)/D] < [A : B]$, also gibt es nach Induktionsannahme eine Untergruppe $C \subset A$ mit $D \subset C$ mit

$$A/D = (B + D)/D \oplus C/D.$$

Es folgt $A = C + B + d = B + C$. Außerdem folgt $(B + D) \cap C = D$, es folgt $B \cap C \subset B \cap D = 0$. Damit ist $A = B \oplus C$ gezeigt. □

Proposition 1.4.8. *Sei A eine endliche abelsche Gruppe, p prim mit $A = A_p$. Es gibt $s \in \mathbb{N}_0$, $b_1, \ldots, b_s \in A$ und natürliche Zahlen $k_1 \geqslant \cdots \geqslant k_s \geqslant 1$ mit*

$$A = \mathbb{Z}\,b_1 \oplus \cdots \oplus \mathbb{Z}\,b_s \quad \operatorname{ord}(b_i) = p^{k_i}.$$

Hat man auch $s' \in \mathbb{N}_0$, $b'_1, \ldots, b'_{s'} \in A$ und $k'_1 \geqslant \cdots \geqslant k'_{s'} \in \mathbb{N}$ mit $A = \mathbb{Z}\,b'_1 \oplus \cdots \mathbb{Z}\,b'_{s'}$ und $\operatorname{ord}(b'_i) = p^{k'_i}$, dann gilt $s = s'$ und $k_i = k'_i$. Insbesondere gilt $\mathbb{Z}\,b_i = \mathbb{Z}\,b'_i$.

Beweis. Sei ohne Einschränkung $A \neq 0$, $\mathbb{Z}\,b_1$ zyklische Untergruppe maximaler Ordnung p^{k_1}. Nach Proposition 1.4.7 gibt es eine Untergruppe $C \subset A$ mit $A = \mathbb{Z}\,b_1 \oplus C$ Fertig falls $C = 0$. Andernfalls gibt es wegen $|C| < |A|$ nach Induktionsannahme Elemente $b_2, \ldots, b_s \in C$, und natürliche Zahlen $k_2 \geqslant \cdots \geqslant k_s$ mit $C = \mathbb{Z}\,b_2 \oplus \cdots \oplus \mathbb{Z}\,b_s$ und $\operatorname{ord}(b_i) = p^{k_i}$, $2 \leqslant i \leqslant s$. Es folgt $A = \mathbb{Z}\,b_1 \oplus \cdots \oplus \mathbb{Z}\,b_s$ und $k_1 \geqslant \cdots \geqslant k_s$ und $\operatorname{ord}(b_i) = p^{k_i}$. Die Eindeutigkeit folgt aus Proposition 1.4.9. □

Proposition 1.4.9. *Sei A endliche abelsche Gruppe $A = \bigoplus_{i=1}^{s} \mathbb{Z}\,x_i = \bigoplus_{i=1}^{s'} \mathbb{Z}\,x'_i$ mit $\operatorname{ord}(x_i) = a_i \in \mathbb{N}\backslash\{1\}$, mit $a_s \big| a_{s-1} \big| \ldots \big| a_1$, $\operatorname{ord}(x'_i) = a'_i \in \mathbb{N}\backslash\{1\}$, mit $a'_s \big| a'_{s-1} \big| \ldots \big| a'_1$. Dann gilt $s = s'$, $a_i = a'_i$. Insbesondere $\mathbb{Z}\,x_i \cong \mathbb{Z}\,x'_i$.*

Beweis. **Rechenregel:** Sei $0 \neq x \in A$, $0 \neq a \in \mathbb{Z}$, $d = \gcd(a, \operatorname{ord}(x))$. Dann gilt $\operatorname{ord}(ax) = \frac{\operatorname{ord}(x)}{d}$. (Beweis davon: Sei $a = da'$, $\operatorname{ord}(x) = dm$. Dann sind a' und m teilerfremd. Für $z \in \mathbb{Z}$ gilt: $zax = 0$ genau dann, wenn $\operatorname{ord}(x) \big| za$ genau dann, wenn $m \big| za'$ genau dann, wenn (nach Euklid) $m \big| z$.)
Es gilt $a_1 A = 0$, insbesondere $a_1 x'_1 = 0$, also $a'_1 \big| a_1$. Da ebenso $a_1 \big| a'_1$, folgt $a_1 = a'_1$. Es folgt $s = 1$ genau dann, wenn $s' = 1$. Sei $s, s' > 1$ und ohne Einschränkung $s \leqslant s'$.
Behauptung: $a_i = a'_i$. Beweis durch Induktion. Es gilt $a_1 = a'_1$. Es gelte $a_i = a'_i$ für $1 \leqslant i \leqslant l \leqslant s$. Dann

$$a_{l+1} A = \bigoplus_{i=1}^{s} \mathbb{Z}\,a_{l+1} x_i = \bigoplus_{i=1}^{s'} \mathbb{Z}\,a_{l+1} x'_i.$$

Nach Induktionsannahme und der Rechenregel oben gilt $\operatorname{ord}(a_{l+1} x_i) = \operatorname{ord}(a_{l+1} x'_i)$ für $1 \leqslant i \leqslant l$. Also $a_{l+1} x'_i = 0$ für $l + 1 \leqslant i \leqslant s$, insbesondere $a_{l+1} x'_{l+1} = 0$ also $a'_{l+1} \big| a_{l+1}$. Da ebenso $a_{l+1} \big| a'_{l+1}$ folgt $a'_{l+1} = a_{l+1}$.
Insgesamt folgt $a_i = a'_i$ und $s = s'$. □

Satz 1.4.10 (Hauptsatz für endliche abelsche Gruppen)**.** *Sei A endliche abelsche Gruppe, $|A| = n = p_1^{\nu_1} \cdots p_r^{\nu_r}$, $r \in \mathbb{N}_0$, Primzahlen $p_1 < \cdots < p_r$, und $\nu_i \in \mathbb{N}$. Dann gibt es $b_{ij} \in A$, $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant s_i$, und natürliche Zahlen $k_{i1} \geqslant \ldots \geqslant k_{is_i} \geqslant 1$ mit*

$$A = \bigoplus_{i=1}^{r} \bigoplus_{j=1}^{s_i} \mathbb{Z}\, b_{ij} \quad \text{und } \operatorname{ord}(b_{ij}) = p_i^{k_{ij}} \text{ für } 1 \leqslant i \leqslant r, 1 \leqslant j \leqslant s_i.$$

Diese Zerlegung ist eindeutig.

Beweis. Die Existenz der Zerlegung folgt aus den Propositionen 1.4.5 und 1.4.8. Die Eindeutigkeit folgt aus den Propositionen 1.4.6 und 1.4.9. □

Proposition und Definition 1.4.11. *Sei G eine beliebige endliche Gruppe. Die Zahl $m = \min\{k \in \mathbb{N} \mid \forall x \in G : x^k = e\}$ ist kgV der Zahlen $\operatorname{ord}(x)$, $x \in G$. Insbesondere ist m Teiler von $|G|$. Die Zahl m heißt Exponent von G.*

Beweis. Es gilt $x^m = e$, also $\operatorname{ord}(x) \mid m$ für alle $x \in G$. Sei $z \in \mathbb{Z}$ mit $x^z = e$ für alle $x \in G$, dann ist $z = mq + r$ mit $q, r \in \mathbb{Z}$, $0 \leqslant r < m$, und es folgt $x^r = e$ für alle $x \in G$, also wegen Minimalität von m $r = 0$ und $z = mq$, dh. $m \mid z$. □

Beispiele 1.4.12. Der Exponent von $\mathfrak{S}_3$ ist 6. Der Exponent von $\mathbb{Z}/\mathbb{Z}2 \times \mathbb{Z}/\mathbb{Z}2$ ist 2.

Folgerung 1.4.13. *Sei A endliche abelsche Gruppe, m der Exponent von A.*

(a) Es gibt $a \in A$ mit $\operatorname{ord}(a) = m$.

(b) A ist genau dann zyklisch, wenn $|A| = m$.

(Beide Aussagen sind für nichtabelsche Gruppen falsch.)

Beweis. **Zu (a):** Mit den Bezeichnungen des Hauptsatzes gilt: $m = p_1^{k_{1,1}} \cdots p_r^{k_{r,1}}$. Sei $a = b_{11} + \cdots + b_{r1}$. Es gilt $\operatorname{ord}(a) = m$, denn für $z \in \mathbb{Z}$ gilt

$$za = 0 \Leftrightarrow \forall i \in \{1, \ldots, r\} : zb_{i1} = 0 \Leftrightarrow \forall i : p_i^{k_{i1}} \mid z \Leftrightarrow m \mid z.$$

Zu (b): „⇒ “: Das ist klar. „⇐ “: Sei $a \in A$ mit $\operatorname{ord}(a) = m$. Dann folgt $A = \langle a \rangle$. □

Folgerung 1.4.14. *Sei A endliche abelsche Gruppe der Ordnung n, sei $d \in \mathbb{N}$ mit $d \mid n$. Dann besitzt A eine Untergruppe der Ordnung d.*

Beweis. Sei $A = \bigoplus_{i=1}^{t} \mathbb{Z}\, x_i$ mit $\operatorname{ord}(x_i) = p_i^{w_i}$, wobei die p_i nicht notwendig verschiedene Primzahlen sind, $w_i \in \mathbb{N}$. Sei $d \in \mathbb{N}$, $d \mid n$. Es gibt $u_i \in \mathbb{N}_0$, $0 \leqslant u_i \leqslant w_i$ mit $d = \prod_{i=1}^{t} p_i^{u_i}$. Sei $B = \bigoplus_{i=1}^{t} \mathbb{Z}\, p_i^{w_i - u_i} x_i$. Da $\operatorname{ord}(p_i^{w_i - u_i} x_i) = p_i^{u_i}$, gilt $|B| = \prod_{i=1}^{k} p_i^{u_i} = d$. □

Beispiele 1.4.15. Abelsche Gruppen bis auf Isomorphie:

$$\begin{aligned}
n = 4 \quad & \mathbb{Z}/\mathbb{Z}2 \times \mathbb{Z}/\mathbb{Z}2 \quad , \quad \mathbb{Z}/\mathbb{Z}4 \\
n = 6 \quad & \mathbb{Z}/\mathbb{Z}2 \times \mathbb{Z}/\mathbb{Z}3 \cong \mathbb{Z}/\mathbb{Z}6 \\
n = 8 \quad & \mathbb{Z}/\mathbb{Z}2 \times \mathbb{Z}/\mathbb{Z}2 \times \mathbb{Z}/\mathbb{Z}2 \quad , \quad \mathbb{Z}/\mathbb{Z}4 \times \mathbb{Z}/\mathbb{Z}2 \quad , \quad \mathbb{Z}/\mathbb{Z}8 \\
n = 12 \quad & \mathbb{Z}/\mathbb{Z}2 \times \mathbb{Z}/\mathbb{Z}2 \times \mathbb{Z}/\mathbb{Z}3 \cong \mathbb{Z}/\mathbb{Z}2 \times \mathbb{Z}/\mathbb{Z}6 \quad , \quad \mathbb{Z}/\mathbb{Z}4 \times \mathbb{Z}/\mathbb{Z}3 \cong \mathbb{Z}/\mathbb{Z}12
\end{aligned}$$

Beachte: in einer zyklischen Gruppe A der Ordnung p^ν, p prim, $\nu \in \mathbb{N}$ gibt es keine Untergruppen $B \neq 0$, $C \neq 0$ mit $A = B \oplus C$.

1.4.3 Einige Anwendungen

Satz 1.4.16. *Sei K ein Körper. Jede endliche Untergruppe von $(K\backslash\{0\},\cdot)$ ist zyklisch.*

Beweis. Sei G endliche Untergruppe von $(K\backslash\{0\},\cdot)$, m der Exponent von G. Es gilt $x^m = 1$ für alle $x \in G$. Da das Polynom $X^m - 1 \in K[X]$ höchstens m Nullstellen in K hat, gilt $|G| \leqslant m$. Da auch $m \big| |G|$ ist, folgt $|G| = m$, also ist G zyklisch. □

Folgerung 1.4.17. *Sei p Primzahl. $\mathbb{Z}/\mathbb{Z}p$ ist Körper, $(\mathbb{Z}/\mathbb{Z}p)^\times$ ist zyklisch von der Ordnung $p-1$.*

Beispiele 1.4.18.

$$
\begin{aligned}
(\mathbb{Z}/\mathbb{Z}2)^\times &= \{\overline{1}\}\\
(\mathbb{Z}/\mathbb{Z}3)^\times &= \{\overline{1},\overline{2}\} = \langle\overline{2}\rangle\\
(\mathbb{Z}/\mathbb{Z}4)^\times &= \{\overline{1},\overline{3}\} = \langle\overline{3}\rangle\\
(\mathbb{Z}/\mathbb{Z}5)^\times &= \{\overline{1},\overline{2},\overline{3},\overline{4}\} = \langle\overline{2}\rangle \cong \mathbb{Z}/\mathbb{Z}4 \text{ hat } \varphi(4)=2 \text{ Erzeugende: } \overline{2},\overline{2}^3 = \overline{3}\\
(\mathbb{Z}/\mathbb{Z}7)^\times &= \{\overline{1},\dots,\overline{6}\} = \langle\overline{3}\rangle \text{ hat } \varphi(6)=2 \text{ Erzeugende: } \overline{3},\overline{3}^5 = \overline{5}\\
(\mathbb{Z}/\mathbb{Z}8)^\times &= \{\overline{1},\overline{3},\overline{5},\overline{7}\} \cong \mathbb{Z}/\mathbb{Z}2 \times \mathbb{Z}/\mathbb{Z}2 \text{ ist nicht zyklisch, da alle Element} \neq \overline{1} \text{ Ordnung 2 haben}
\end{aligned}
$$

Satz 1.4.19 (Satz von Wilson)**.** *Ist p Primzahl, dann gilt $(p-1)! \equiv -1 \mod p$.*

Beweis. Die Elemente in $(\mathbb{Z}/\mathbb{Z}p)^\times$ sind genau die Nullstellen des Polynoms $X^{p-1} - \overline{1} \in \mathbb{Z}/\mathbb{Z}p[X]$. Also gilt

$$X^{p-1} - \overline{1} = \prod_{\overline{x}\in(\mathbb{Z}/\mathbb{Z}p)^\times} (X - \overline{x})$$

Es folgt $-\overline{1} = \prod_{\overline{x}\in(\mathbb{Z}/\mathbb{Z}p)^\times} \overline{x}$, also $(p-1)! \equiv -1 \mod p$. □

Folgerung 1.4.20. *Sei p prim. Ist $p > 2$, dann gilt*

$$\left((\frac{p-1}{2})!\right)^2 \equiv (-1)^{\frac{p+1}{2}} \mod p.$$

Ist $p = 2$, oder $p \equiv 1 \mod 4$, dann gibt es $x \in \mathbb{Z}$ mit $x^2 \equiv -1 \mod p$.

Beweis. Sei $p > 2$. Es gilt

$$-1 \equiv (p-1)! = 1\cdot 2\cdots\left(\frac{p-1}{2}\right)\cdot\left(\left(p-\left(\frac{p-1}{2}\right)\right)\cdots(p-2)\cdot(p-1) \equiv (-1)^{\frac{p-1}{2}} 1^2\cdots\left(\frac{p-1}{2}\right)^2 = (-1)^{\frac{p-1}{2}}\left((\frac{p-1}{2})!\right)^2 \quad \text{mo}$$

also $\left((\frac{p-1}{2})!\right)^2 \equiv (-1)^{\frac{p+1}{2}} \mod p$.
Sei $p = 2$, dann ist $1 \equiv -1 \mod 2$. Ist $p \equiv 1 \mod 4$, dann ist $\frac{p+1}{2}$ ungerade, also $\left((\frac{p-1}{2})!\right)^2 \equiv (-1) \mod p$, wähle $x := \left(\frac{p-1}{2}\right)!$. □

1.4.4 Semidirekte Produkte

Beobachtung: Ist G eine Gruppe, $H \subset G$ eine Untergruppe und $N \triangleleft G$ Normalteiler, dann ist $NH = HN$ Untergruppe. Für $x, x' \in N$ und $y, y' \in H$, gilt

$$xyx'y' = xyx'y^{-1}yy'$$

und es gilt $yx'y^{-1} \in N$, also $xyx'y^{-1} = x\kappa_y(x') \in N$, und $yy' \in H$.

Proposition und Definition 1.4.21. *Seien F, G Gruppen und $\tau : G \to \mathrm{Aut}(F)$ ein Homomorphismus. Die Menge $F \times G$ ist Gruppe bezüglich der Multiplikation*

$$(x,y)(x',y') = (x\tau(y)(x'), yy').$$

Dabei ist (e,e) das neutrale Element, es gilt $(x,y)^{-1} = (\tau(y^{-1})(x^{-1}), y^{-1})$. Die so definierte Gruppe heißt äußeres Semidirektes Produkt von F und G bezüglich τ. Sie wird mit $F \times_\tau G$ bezeichnet.

Beweis. Assoziativität der Multiplikation:

$$\begin{aligned}((x,y)(x'y'))\,(x'',y'') &= (x\tau(y)(x'),yy')\,(x'',y'')\\ &= (x\tau(y)(x')\tau(yy')(x''),(yy')y'')\\ &= (x\tau(y)(x')\tau(y)(\tau(y')(x'')),y(y'y''))\\ &= (x\tau(y)\,(x'\tau(y')(x'')),y(y'y''))\\ &= (x,y)\,(x'\tau(y')(x''),y'y'') = (x,y)\,((x',y')(x'',y''))\end{aligned}$$

Für das Inverse:

$$(x,y)(\tau(y^{-1})(x^{-1}),y^{-1}) = \left(x\tau(y)(\tau(y^{-1})(x^{-1})),yy^{-1}\right) = (xx^{-1},yy^{-}) = (e,e).$$

□

Es gilt: $F\times_\tau G = F\times G$ genau dann, wenn τ trivial ist, das heißt für alle $y\in G$ ist $\tau(y)=\mathrm{id}_F$.
Man hat die Gruppenhomomorphismen

$$\begin{aligned}q_1 : F &\to F\times_\tau G, \quad x\mapsto (x,e)\\ q_2 : G &\to F\times_\tau G, \quad y\mapsto (e,y)\\ p : F\times_\tau G &\to G, \quad (x,y)\mapsto y\end{aligned}$$

Dann ist

$$\begin{aligned}\widetilde{F} &= q_1(F) = F\times\{e\} = \ker(p)\triangleleft F\times_\tau G \text{ Normalteiler}\\ \widetilde{G} &= q_2(G) = \{e\}\times G\subset F\times_\tau G \text{ Untergruppe}\end{aligned}$$

und es gilt $F\times_\tau G = \widetilde{F}\cdot\widetilde{G} = \widetilde{G}\cdot\widetilde{F}$ und $\widetilde{F}\cap\widetilde{G} = \{(e,e)\}$, denn $(x,y) = (x,e)(e,y)$. Ferner gilt $q_2(y)q_1(x)q_2(y)^{-1} = q_1(\tau(y)(x))$ für alle $x\in F$ und $y\in G$.

Umgekehrt gilt:

Proposition 1.4.22. *Sei G eine Gruppe, $N\triangleleft G$, $H\subset G$ Untergruppe mit $G=NH=HN$ und $N\cap H=\{e\}$, sei $H\to\mathrm{Aut}(N)$ definiert durch $\kappa(y)(x)=yxy^{-1}$ für $x\in N$, $y\in H$. Dann ist*

$$f : N\times_\kappa H\to G, (x,y)\mapsto xy$$

ein Gruppenisomorphismus. Deshalb heißt G inneres semidirektes Produkt von N und H.

Beweis. κ ist sinnvoll, denn für $y\in H$, $x\in N$, gilt $\kappa(y)(x)=yxy^{-1}\in N$. Es gilt: $\kappa(y)=\kappa_y\big|_N$.
f ist Homomorphismus, denn

$$f\left((x,y)(x',y')\right) = f\left(x\kappa(y)(x'),yy'\right) = f(xyx'y^{-1},yy') = xyx'y^{-1}yy' = xyx'y' = f(x,y)f(x',y').$$

f ist injektiv:

$$f(x,y)=e\Rightarrow xy=e\Rightarrow x=y^{-1}\in N\cap H=\{e\}\Rightarrow x=y=e \text{ dh. } (x,y)=(e,e).$$

f ist surjektiv:

$$\forall g\in G\exists x\in N, y\in H : g=xy=f(x,y).$$

□

Beispiel 1.4.23. Konstruktion äußerer semidirekter Produkte. Sei $m,n\in\mathbb{N}\backslash\{1\}$, $r\in\mathbb{Z}$ mit $r^m\equiv 1 \mod n$, dh. $\mathrm{ord}_n(r)\big|m$. Dann ist

$$\rho : \mathbb{Z}/\mathbb{Z}n\to\mathbb{Z}/\mathbb{Z}n, \overline{z}\mapsto\overline{rz}$$

Homomorphismus mit $\rho^m=\mathrm{id}_{\mathbb{Z}/\mathbb{Z}n}$. Also ist $\rho\in\mathrm{Aut}(\mathbb{Z}/\mathbb{Z}n)$ und $\mathrm{ord}(\rho)\big|m$. Die Abbildung

$$\tau : \mathbb{Z}/\mathbb{Z}m\to\mathrm{Aut}(\mathbb{Z}/\mathbb{Z}n), \overline{y}\mapsto\rho^y$$

ist Gruppenhomomorphismus, explizit

$$\tau(\overline{y})(\overline{x}) = \rho^y(\overline{x}) = \overline{r}^y\overline{x}$$

für $\overline{y} \in \mathbb{Z}/\mathbb{Z}m$, $\overline{x} \in \mathbb{Z}/\mathbb{Z}n$. Sei

$$G = \mathbb{Z}/\mathbb{Z}n \times_\tau \mathbb{Z}/\mathbb{Z}m.$$

In G gilt

$$(\overline{x},\overline{y})(\overline{x}',\overline{y}') = (\overline{x} + \overline{r}^y\overline{x}', \overline{y} + \overline{y}'),$$

neutrales Element ist $(0,0)$, Inverses ist $(\overline{x},\overline{y})^{-1} = (-\overline{r}^{-y}\overline{x}, -\overline{y})$. Seien $a = (\overline{1},\overline{0})$, $b = (\overline{0},\overline{1})$, dann ist $\mathrm{ord}(a) = n$ und $\mathrm{ord}(b) = m$, ferner $bab^{-1} = a^r$ (äquivalent dazu: $ba = a^rb$). Es folgt $G = \{a^ib^j \mid 0 \leqslant i \leqslant n-1, 0 \leqslant j \leqslant m-1\}$. Außerdem $\langle a\rangle \triangleleft G$, $G = \langle a\rangle\langle b\rangle = \langle b\rangle\langle a\rangle$, $\langle a\rangle \cap \langle b\rangle = \{e\}$. G ist genau dann abelsch, wenn $r \equiv 1 \mod n$, dh. wenn τ trivial ist. Spezialfall: $1 \neq n \in \mathbb{N}$, $m = 2$ und $r = -1$. Dann ist

$$\mathbb{Z}/\mathbb{Z}n \times_\tau \mathbb{Z}/\mathbb{Z}2 = \{e, a, \ldots, a^{n-1}, b, ab, \ldots, a^{n-1}b\} \text{ mit } \mathrm{ord}(a) = n, \mathrm{ord}(b) = 2, ba = a^{n-1}b$$

die bereits bekannte Diedergruppe der Ordnung $2n$.

1.5 Einige Tatsachen über die $\mathfrak{S}_n$

1.5.1 Zykelzerlegung von Permutationen

Definition 1.5.1. $\sigma \in \mathfrak{S}_n$ heißt Zykel der Länge k oder k-Zykel, wenn es paarweise verschiedene Elemente $a_1, \ldots, a_k \in \{1, \ldots, n\}$ gibt, so daß

$$\begin{aligned} \sigma(a_i) &= a_{i+1} \quad \text{für } 1 \leqslant i < k, \\ \sigma(a_k) &= a_1, \\ \sigma(x) &= x \quad \text{für } x \in \{1,\ldots,n\}\backslash\{a_1,\ldots,a_k\} \end{aligned}$$

Man schreibt jetzt dafür

$$\sigma = (a_1 \ldots a_k).$$

Die Menge der $a_1, \ldots, a_k$ heißt Träger des Zykels σ. Zweizykel heißen Transpositionen.

Beispiel 1.5.2. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 4 & 2 & 1 & 6 \end{pmatrix} = (13425) \in \mathfrak{S}_6$

Es gilt $\sigma = (a_1 \ldots a_k) = (a_i, \ldots a_k a_1 \ldots a_{i-1})$ für $1 \leqslant i \leqslant k$, sowie $\sigma^{-1} = (a_k \ldots a_1)$. Zwei Zykel heißen disjunkt, falls ihre Träger disjunkt sind; dann gilt $\sigma\tau = \tau\sigma$. Ein k-Zykel hat die Ordnung k, denn

$$\sigma = (a_1\sigma(a_1)\ldots\sigma^{k-1}(a_1))$$

also ist $\sigma^k = \mathrm{id}$ und $\sigma^i \neq \sigma^j$ für $0 \leqslant i < j < k$.

Für $\sigma = (a_1 \ldots a_k)$ gilt

$$\sigma = (a_1a_k)\cdots(a_1a_2).$$

Also ist σ Produkt von $k-1$ Transpositionen. Für $\tau \in \mathfrak{S}_n$ gilt

$$\tau\sigma\tau^{-1} = (\tau(a_1)\ldots\tau(a_k)),$$

denn

$$\tau\sigma\tau^{-1}\tau(a_i) = \begin{cases} \tau\sigma(a_i) = \tau(a_{i+1}) & \text{für } i < k \\ \tau\sigma(a_k) = \tau(a_1) & \text{für } i = k \end{cases}$$

Satz 1.5.3. *Sei $\sigma \in \mathfrak{S}_n$.*

(a) Es gibt $r \in \mathbb{N}_0$ und disjunkte Zyklen $\sigma_1, \ldots, \sigma_r$ mit $\sigma = \sigma_1 \ldots \sigma_r$. Eine solche Darstellung ist eindeutig bis auf Reihenfolge.

(b) $\mathrm{ord}(\sigma)$ *ist kgV der* $\mathrm{ord}(\sigma_i)$, $1 \leqslant i \leqslant r$.

Beweis. **Zu (a):** Die Identität ist Produkt von 0 Zyklen. Sei also $\sigma \neq \mathrm{id}$. Wir betrachten die Operation

$$\langle\sigma\rangle \times \{1,\dots,n\} \to \{1,\dots,n\}, (\sigma^z, i) \mapsto \sigma^z(i).$$

Seien $B_1,\dots,B_r$ die Bahnen mit mehr als einem Element, $|B_i| = k_i$, $b_i \in B_i$ und $G_i \subset \langle\sigma\rangle$ die Stabilisatoruntergruppe von b_i, $1 \leqslant i \leqslant r$.
Wir untersuchen zunächst die Behauptung $B_i = \{b_i, \sigma(b_i), \dots, \sigma^{k_i-1}(b_i)\}$: Wir wissen, daß die Abbildung $\langle\sigma\rangle/G_i \to B_i$, $\sigma^z G_i \mapsto \sigma^z(b_i)$ bijektiv ist. Also ist $[\langle\sigma\rangle : G_i] = k_i$ und $\langle\sigma\rangle/G_i = \{G_i, \sigma G_i, \dots \sigma^{k_i-1}G_i\}$. Die Behauptung trifft also zu.
Sei $\sigma_i = (b_i\sigma(b_i)\dots\sigma^{k_i-1}(b_i))$ für $1 \leqslant i \leqslant r$. Dies sind disjunkte Zyklen, es gilt $\sigma = \sigma_1\cdots\sigma_r$, den beide Seiten bewirken auf $\{\sigma^l(b_i) \mid 1 \leqslant i \leqslant r, 0 \leqslant l < k_i\}$ und auf $\{1,\dots,n\}\backslash\bigcup B_i$ dasselbe.
Eindeutigkeit: Sei auch $\sigma = \rho_1\cdots\rho_s$ eine Zerlegung mit paarweise disjunkten Zyklen $\rho_1,\dots,\rho_s$, sei C_j der Träger von ρ_j, $m_j = |C_j|$, $c_j \in C_j$, $1 \leqslant j \leqslant s$. Dann $\rho_j = (c_j\rho_j(c_j)\dots\rho^{m_j-1}(c_j)) = (c_j\sigma(c_j)\dots\sigma^{m_j-1}(c_j))$, also ist C_j eine Bahn unter der Operation von $\langle\sigma\rangle$. mit mehr als einem ELement. Also sind die C_j genau die Bahnen mit mehr als einem Element. Es folgt $r = s$ und nach eventueller Umindizierung gilt $B_i = C_i$, $1 \leqslant i \leqslant r$, und damit $\sigma_i = \rho_i$.

Zu (b): Sei $\sigma = \sigma_1\dots\sigma_r$ wie in (a), sei $m \in \mathbb{N}$ kgV der $\mathrm{ord}(\sigma_i)$. Für $z \in \mathbb{Z}$ gilt $\sigma^z = \sigma_1^z\dots\sigma_r^z$ und σ^z bewegt höchstens die Elemente des Trägers von σ_i. Es folgt, $\sigma^z = \mathrm{id}$ genau dann, wenn für alle $i \in \{1,\dots,r\}$ $\sigma_i^z = \mathrm{id}$, genau dann, wenn $\mathrm{ord}(\sigma)\big|z$ genau dann, wenn $\mathrm{ord}(\sigma_i)\big|z$ genau dann, wenn $m\big|z$. Es folgt $m = \mathrm{ord}(\sigma)$. □

Folgerung 1.5.4. *Sei $\sigma \in \mathfrak{S}_n$, $\sigma = \sigma_1\dots\sigma_r$ Zerlegung in paarweise disjunkte Zykel, die Länge von σ_i sei k_i. Dann ist σ Produkt von $\sum_{i=1}^r (k_i - 1)$ Transpositionen.*

Beweis. σ_i ist Produkt von $k_i - 1$ Transpositionen. □

Beispiele 1.5.5. (a) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 1 & 4 & 7 & 9 & 3 & 8 & 6 & 5 & 10 \end{pmatrix} = (12)(34786)(59)$

(b) Sei p prim, $\sigma = (a_1\dots a_p)$ ein p-Zykel. Dann sind auch $\sigma^2,\dots,\sigma^{p-1}$ p-Zyklen, denn diese Elemente haben alle Ordnung p. Dagegen: für $\sigma = (1234)$ ist $\sigma^2 = (13)(24)$.

Definition 1.5.6. Sei $\sigma = \sigma_1\cdots\sigma_r$ Zerlegung in paarweise disjunkte Zyklen, $k_i = \mathrm{ord}(\sigma_i)$, $k_1 \geqslant \cdots \geqslant k_r$. Dann heißt $(k_1,\dots,k_r)$ Typ von σ.

Satz 1.5.7. *Zwei Permutationen sind genau dann konjugiert, wenn sie denselben Typ haben.*

Beweis. **Eine Richtung ist klar:** Sei $\sigma = \sigma_1\cdots\sigma_r$ Zerlegung in disjunkte Zyklen, $\rho \in \mathfrak{S}_n$, dann ist

$$\rho\sigma\rho^{-1} = \rho\sigma_1\rho^{-1}\rho\sigma_2\rho^{-1}\rho\cdots\rho\sigma_r\rho^{-1}$$

ebenfalls Zerlegung in disjunkte Zykel, es gilt $\mathrm{ord}(\rho\sigma_i\rho^{-1}) = \mathrm{ord}(\sigma_i)$ für alle i.
Umgekehrt: Seien $\sigma, \tau \in \mathfrak{S}_n$ mit Zerlegung in disjunkte Zyklen $\sigma = \sigma_1\cdots\sigma_r$ und $\tau = \tau_1\cdots\tau_r$ mit $\mathrm{ord}(\sigma_i) = \mathrm{ord}(\tau_i)$. Sei $\sigma_i = (a_{i1}\dots a_{ik_i})$, $\tau_i = (b_{i1}\dots b_{ik_i})$ Wir definieren $\alpha \in \mathfrak{S}_n$ durch

$$\begin{aligned} \alpha : \{a_{ij} \mid 1 \leqslant i \leqslant r, 1 \leqslant j \leqslant k_i\} &\to \{b_{ij} \mid 1 \leqslant i \leqslant r, 1 \leqslant j \leqslant k_i\} \\ \alpha(a_{ij}) &= b_{ij} \\ \alpha : \{1,\dots,n\}\backslash\{a_{ij} : i,j\} &\to \{1,\dots,n\}\backslash\{a_{ij} : i,j\} \quad \text{eine beliebige Bijektion} \end{aligned}$$

Dann gilt $\alpha\sigma\alpha^{-1} = \tau$, denn

$$\begin{aligned} \alpha\sigma\alpha^{-1}(b_{ij}) &= \left\{\begin{matrix} \alpha\sigma(a_{ij}) = \alpha(a_{i,j+1}) = b_{i,j+1}, & j < k_i \\ \alpha\sigma(a_{ik_i}) = \alpha(a_{i1}) = b_{i1}, & j = k_i \end{matrix}\right\} = \tau(b_{ij}) \quad \text{für alle } i,j \\ \alpha\sigma\alpha^{-1}(x) &= x = \tau(x) \quad \text{sonst} \end{aligned}$$

Es folgt, daß alle k-Zyklen, $k > 1$ zueinander konjugiert sind. (Es gibt $\frac{1}{k}n(n-1)\cdots(n-(k-1))$ k-Zyklen.) □

1.5.2 Signum einer Permutation

Satz 1.5.8. *Es gibt genau einen surjektive Gruppenhomomorphismus $\varepsilon : \mathfrak{S}_n \to \{-1,1\} \subset \mathbb{Z}$. Für alle Transpositionen gilt $\varepsilon(\tau) = -1$.*

Beweis. Für $\sigma \in \mathfrak{S}$ sei

$$\varepsilon(\sigma) = \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(j) - \sigma(i)}{j - i}.$$

Es ist klar, daß $\varepsilon(\sigma) \in \{-1,1\}$. Es gilt

$$\varepsilon(\sigma\tau) = \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma\tau(j) - \sigma\tau(i)}{j - i} = \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma\tau(j) - \sigma\tau(i)}{\tau(j) - \tau(i)} \cdot \prod_{1 \leqslant i < j \leqslant n} \frac{\tau(j) - \tau(i)}{j - i} = \varepsilon(\sigma)\varepsilon(\tau).$$

Also ist ε Gruppenhomomorphismus. Es gilt $\varepsilon(\mathrm{id}) = 1$, und $\varepsilon((12)) = -1$, also ist ε surjektiv. Da alle Transpositionen zueinander konjugiert sind, ist $\varepsilon(\tau) = -1$ für jede Transposition τ.
Sei $\varepsilon' : \mathfrak{S}_n \to \{-1,1\}$ auch surjektiver Gruppenhomomorphismus. Dann gibt es $\sigma \in \mathfrak{S}_n$ mit $\varepsilon(\sigma) = -1$, also gibt es eine Transposition mit $\varepsilon'(\tau) = -1$, und dann gilt dies für alle Transpositionen. Da jede Permutation Produkt von Transpositionen ist, folgt $\varepsilon' = \varepsilon$. □

$\varepsilon(\sigma)$ heißt Vorzeichen oder Signum von σ. Ist $\sigma = \tau_1 \cdots \tau_n$ Produkt von Transpositionen, dann gilt

$$\varepsilon(\sigma) = (-1)^n.$$

Ist $\sigma = \sigma_1 \cdots \sigma_r$ Produkt von disjunkten Zyklen, $\mathrm{ord}(\sigma_i) = k_i$, dann gilt

$$\varepsilon(\sigma) = (-1)^{\sum(k_i - 1)}.$$

Ein Paar (i,j) mit $1 \leqslant i < j \leqslant n$ heißt Inversion von σ, falls $\sigma(i) > \sigma(j)$. Ist $\nu(\sigma)$ die Anzahl der Inversionen von σ, dann ist

$$\varepsilon(\sigma) = (-1)^{\nu(\sigma)}.$$

σ heißt gerade (bzw. ungerade) falls $\varepsilon(\sigma) = 1$ (bzw. $\varepsilon(\sigma) = -1$).

Man setzt

$$A_n = \ker \varepsilon.$$

Dies ist die Menge der geraden Permutationen und der einzige Normalteiler vom Index 2 von $\mathfrak{S}_n$. A_n heißt alternierende Gruppe von n Elementen. Es gilt

$$\begin{aligned} \mathfrak{S}_n / A_n &\cong \{-1,1\} \\ |A_n| &= \frac{n!}{2}. \end{aligned}$$

$\mathfrak{S}_n$ ist semidirektes Produkt von A_n und jeder von einer Transposition erzeugten Untergruppe.

1.5.3 Beispiele

Wir beginnen mit der Gruppe $\mathfrak{S}_3$. Es gilt $|\mathfrak{S}_3| = 6$, $|A_3| = 3$. Man macht sich leicht klar, daß

$$\begin{aligned} \mathfrak{S}_3 &= \{\mathrm{id}, (123), (132), (12), (13), (23)\} \\ A_3 &= \{\mathrm{id}, (123), (132)\} \lhd \mathfrak{S}_3 \end{aligned}$$

Als nächstes betrechten wir die Gruppe $\mathfrak{S}_4$. Analog zu oben gilt $|\mathfrak{S}_4| = 24$, $|A_4| = 12$. Es ist nun bereits weit aufwendiger, die Gruppen auszurechenen:

$$\begin{aligned} \mathfrak{S}_4 &= \{\mathrm{id}, (12), (13), (14), (23), (24), (34), (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (134), \\ &\quad (143), (234), (243), (1234), (1243), (1324), (1342), (1423), (1432)\} \\ A_4 &= \{\mathrm{id}, (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (134), (143), (234), (243)\} \lhd \mathfrak{S}_4 \\ V &= \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\} \lhd A_4 \lhd \mathfrak{S}_4 \quad \text{die Klein'sche Vierergruppe} \end{aligned}$$

Also ist A_4 semidirektes Produkt aus V und den Untergruppen der Ordnung 3.
$\mathfrak{S}_4$ enthält Diedergruppen der Ordnung 8: Sei $a = (1234)$, $b = (13)$, dann $\operatorname{ord}(a) = 4$ und $\operatorname{ord}(b) = 2$, $bab^{-1} = (3214) = a^{-1} = a^3$. Also ist $\langle a, b\rangle = \{\mathrm{id}, a, a^2, a^3, b, ab, a^2b, a^3b\}$ Diedergruppe der Ordnung 8.
A_4 enthält keine Untergruppe der Ordnung 6: Annahme A_4 enhält Untergruppe H der Ordnung 6. Dann ist $H \triangleleft A_4$. Da $V \nsubseteq H$, gilt $A_4 = VH = HV$, $V \cap H \triangleleft H$, $A_4/V \cong HV/V \cong H/H \cap V$ ist zyklische Gruppe der Ordnung 3, $|H \cap V| = 2$. Sei $h \in H\backslash(H \cap V)$. Wegen $3 = \operatorname{ord}(hH \cap V) \big| \operatorname{ord}(h)$ ist $\operatorname{ord}(h) \in \{3, 6\}$. In beiden Fällen ist H zyklisch: Das ist klar, wenn $\operatorname{ord}(h) = 6$. Falls $\operatorname{ord}(h) = 3$, dann gilt $[H : \langle h\rangle] = 2$, also $\langle h\rangle \triangleleft H$. Es folgt $H = \langle h\rangle \times (H \cap V)$, also $H \cong \mathbb{Z}/\mathbb{Z}3 \times \mathbb{Z}/\mathbb{Z}2 \cong \mathbb{Z}/\mathbb{Z}6$. Da $\mathfrak{S}_4$ kein Element der Ordnung 6 enthält, hat man einen Widerspruch. Die Gruppe $\mathfrak{S}_4$ enthält Diedergruppen der Ordnung 6 aber keine zyklischen Gruppen der Ordnung 6.

Wir wenden den vorangehenden Abschnitt an, um eine Untergruppe der Ordnung 21 von $\mathfrak{S}_7$ zu konstruieren. Wir brauchen $a, b \in \mathfrak{S}_7$ mit $\operatorname{ord}(a) = 7$, $\operatorname{ord}(b) = 3$, und einen nichttrivialen Homomorphismus $\tau : \langle b\rangle \to \operatorname{Aut}(\langle a\rangle)$.
Da $\operatorname{Aut}(\langle a\rangle) \cong (\mathbb{Z}/\mathbb{Z}7)^\times$ hat $\operatorname{Aut}(\langle a\rangle)$ ein Element der Ordnung 3, also gibt es so ein τ. Es gibt aber keinen nicht-trivialen Homomorphismus $\langle a\rangle \to \operatorname{Aut}(\langle b\rangle)$.
Sei $a = (1234567)$, $a^2 = (1357246)$, $b = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 5 & 7 & 2 & 4 & 6 \end{pmatrix} = (235)(476)$, dann gilt $bab^{-1} = a^2$, dh. $ba = a^2b$. Sei

$$\tau : \langle b\rangle \to \operatorname{Aut}(\langle a\rangle), \tau(b^z) = (\kappa_b)^z = \kappa_{b^z}.$$

Resultat: $G = \langle a, b\rangle = \{\mathrm{id}, a, \ldots, a^6, b, ab, \ldots, a^6b, b^2, \ldots, a^6b^2\}$ ist semidirektes Produkt von $\langle a\rangle \triangleleft G$ und $\langle b\rangle \subset G$.

1.5.4 Die Einfachheit von A_n, $n \geqslant 5$

Satz 1.5.9. *(a) Sei $n \geqslant 2$. Folgende Mengen erzeugen $\mathfrak{S}_n$:*

$$\{(ii+1) \ : \ 1 \leqslant i \leqslant n-1\}$$
$$\{(1i) \ : \ 2 \leqslant i \leqslant n\}$$
$$\{(12), (1 \ldots n)\}$$

(b) Für $n \geqslant 3$ liegen alle 3-Zyklen in A_n. A_n wird erzeugt von $\{(12i) \ : \ 3 \leqslant i \leqslant n\}$.

(c) Für $n \geqslant 5$ sind alle 3-Zyklen in A_n zueinander konjugiert.

Beweis. **Zu (a):** Für $1 \leqslant i < k \leqslant n$ ist $(ik) = (ii+1)(i+1i+2)\cdots(k-1k)(k-1k-2)\cdots(i+1i)$. Also wird $\mathfrak{S}_n$ von der ersten Menge erzeugt. Da $(1i)(1i+1)(1i) = (ii+1)$ für $2 \leqslant i \leqslant n$, ist die zweite Menge Erzeugendensystem. Da $(1 \cdots n)(ii+1)(1 \cdots n)^{-1} = (i+1i+2)$ für $1 \leqslant i \leqslant n-2$, ist auch die dritte Menge Erzeugendensystem.
Zu (b): Die erste Aussage ist klar. Da $(ij)(jk) = (ijk)$ und $(ij)(kl) = (ij)(jk)(jk)(kl) = (ijk)(jkl)$ wird A_n von den 3-Zyklen erzeugt. Da $(12j)(12k)(12j)^{-1} = (2jk)$ für $j \neq k$ und $(12i)(2jk)(12i)^{-1} = (ijk)$, wird A_n von den $(12i)$, mit $3 \leqslant i \leqslant n$ erzeugt.
Zu (c): Sei $n \geqslant 5$, und σ, τ Dreizyklen. Es gibt $\alpha \in \mathfrak{S}_n$ mit $\sigma = \alpha\tau\alpha^{-1}$. Da $n \geqslant 5$ ist, gibt es eine zu σ disjunkte Transposition β. Es folgt

$$\sigma = \beta\sigma\beta^{-1} = \beta\alpha\sigma\alpha^{-1}\beta^{-1} = (\beta\alpha)\sigma(\beta\alpha)^{-1}.$$

Entweder α oder $\beta\alpha$ ist gerade. □

Wir wissen $A_2 = \{\mathrm{id}\}$, $A_3 = \langle(123)\rangle$, A_4 ist nicht einfach, A_3 schon.

Satz 1.5.10. *Für $n \geqslant 5$ ist A_n einfach.*

Beweis. Für $\sigma \in \mathfrak{S}_n$ sei α_σ die Anzahl der Elemente, die von σ bewegt werden. Sei $\{\mathrm{id}\} \neq N \triangleleft A_n$ und $\mathrm{id} \neq \sigma \in N$, so daß α_σ minimal ist. Sei $\sigma = \sigma_1 \cdots \sigma_r$ Zerlegung in disjunkte Zyklen, $k_i = \operatorname{ord}(\sigma_i)$ und $k_1 \geqslant \cdots \geqslant k_r$. Wir zeigen, daß σ Dreizykel und $\alpha_\sigma = 3$ ist.
Nach dem vorhergehenden Satz liegen dann alle Dreizykel in N, also folgt $N = A_n$.

Da $\sigma \neq \mathrm{id}$ und gerade ist, muß $\alpha_\sigma \geqslant 3$ sein. Annahme: $\alpha_\sigma \geqslant 4$. Unterannahme: $\alpha_\sigma = 4$. Dann ist $r \geqslant 2$, denn bei $r = 1$ wäre σ Vierzykel, also ungerade. Dann ist $\sigma = \sigma_1\sigma_2$, etwa $\sigma_1 = (ij)$ und $\sigma_2 = (kl)$. Wegen $n \geqslant 5$ gibt es $m \in \{1, \ldots, n\}\backslash\{i, j, k, l\}$. Sei $\tau = (klm)$. Dann ist $\widetilde{\sigma} = \tau\sigma\tau^{-1} = (ij)(lm) \in N$, $\sigma^{-1}\widetilde{\sigma} = (ij)(kl)(ij)(lm) = (kl)(ml) \in N$, also $\alpha_{\sigma^{-1}\widetilde{\sigma}} = 3$ Widerspruch zur Minimalität von α_σ. Also muß $\alpha_\sigma \geqslant 5$ sein. Dann sind folgende Fälle möglich:

(a) $k_1 \geqslant 4$. Dann sei $\sigma_1 = (ijkla_5 \ldots a_{k_1})$

(b) $k_1 = 3$. Dann muß $r \geqslant 2$ sein, $k_1 \geqslant k_2 \geqslant 2$. Außerdem muß $\alpha_\alpha > 5$ sein, denn bei $\alpha_\sigma = 5$ wäre σ ungerade. Also ist etwa $\sigma_1 = (ijk)$ $\sigma_2 = (lm)$ oder (lmp).

(c) $k_1 = 2$. Dann muß $r \geqslant 3$ sein, etwa $\sigma_1 = (ij)$, $\sigma_2 = (kl)$, $\sigma_3 = (mq)$.

In allen Fällen sei $\tau = (jkl)$, $\widetilde{\sigma} = \tau\sigma\tau^{-1} \in N$. Dann gilt jeweils:

(a) $\widetilde{\sigma} = (iklja_5 \ldots a_{k_1})\sigma_2 \cdots \sigma_r$ und $\sigma^{-1}\widetilde{\sigma} = (a_{k_1} \ldots a_5lkji)(iklja_5 \ldots a_{k_1}) = (ijl)$

(b) $\widetilde{\sigma} = (ikl)\begin{Bmatrix}(jm)\\(jmp)\end{Bmatrix}\sigma_3 \cdots \sigma_r$ und $\sigma^{-1}\widetilde{\sigma} = (kjl)\begin{Bmatrix}(lm)\\(pml)\end{Bmatrix}(ikl)\begin{Bmatrix}(jm)\\(jmp)\end{Bmatrix} = \begin{Bmatrix}(ijlkm)\\(ijlkp)\end{Bmatrix}$

(c) $\widetilde{\sigma} = (ik)(lj)(mq)\sigma_4 \cdots \sigma_r$ und $\sigma^{-1}\widetilde{\sigma} = (ij)(kl)(mq)(ik)(lj)(mq)$

In allen Fällen gilt $\sigma^{-1}\widetilde{\sigma} \in N$ und $\alpha_{\sigma^{-1}\widetilde{\sigma}} < \alpha_\sigma$, Widerspruch. □

1.6 Die Sätze von Sylow

1.6.1 Beweis der Sätze, Folgerungen

Definition 1.6.1. Seien G eine endliche Gruppe, p eine Primzahl, $|G| = p^a m$ mit $a \in \mathbb{N}_0$, $m \in \mathbb{N}$ und $p \nmid m$. Eine Untergruppe der Ordnung p^a von G heißt p-Sylowuntergruppe.

Beispiele 1.6.2. (a) $G = \mathfrak{S}_3$. 2-Sylowuntergruppen: $\langle(12)\rangle$, $\langle(13)\rangle$, $\langle(23)\rangle$. 3-Sylowuntergruppe: $\langle(123)\rangle$.

(b) Die Sylowuntergruppen einer endlichen abelschen Gruppe sind genau die p-Komponenten.

Proposition und Definition 1.6.3. *Sei G eine endliche Gruppe, $H \subset G$ eine Untergruppe.*

(a) $N_G(H) = \{x \in G \mid xHx^{-1} = H\}$ ist eine Untergruppe von G; sie heißt Normalisator von H in G. $N_G(H)$ ist die größte Untergruppe von G, in der H als Normalteiler enthalten ist.

(b) Die Anzahl der zu H konjugierten Untergruppen von G ist $[G : N_G(H)]$.

Beweis. Sei $\mathcal{C} = \{yHy^{-1} \mid y \in G\}$. Auf $\mathcal{C}$ betrachten wir die Operation

$$G \times \mathcal{C} \to \mathcal{C}, (g, yHy^{-1}) \mapsto gyHy^{-1}g^{-1}.$$

Die Stabilisatoruntergruppe von H ist $N_G(H)$. Da die Operation transitiv ist, gilt

$$|\mathcal{C}| = [G : N_G(H)].$$

Alles andere ist klar. □

Satz 1.6.4 (Sylow)**.** *Sei G eine endliche Gruppe, p Primzahl, $|G| = p^a m = n$ mit $p \nmid m$.*

(a) G enthält mindestens eine p-Sylowuntergruppe, und jede p-Untergruppe ist in einer solchen enthalten.

(b) Je zwei p-Sylowuntergruppen sind zueinander konjugiert.

(c) Sei s_p die Anzahl der p-Sylowgruppen, sei P eine p-Sylowgruppe. Dann gilt

$$s_p = [G : N_G(P)] \quad , \quad s_p \big| m \quad \text{und} \quad s_p \equiv 1 \mod p.$$

Beweis. **Zu (a):** Sei ohne Einschränkung $a \geqslant 1$.
Existenz einer p-Sylowuntergruppe: Sei

$$\mathcal{T} = \{X \mid X \subset G \text{ mit } |X| = p^a\}.$$

Es gilt $|\mathcal{T}| = \binom{n}{p^a}$. Weiter gilt $p \nmid |\mathcal{T}|$, denn

$$|\mathcal{T}| \cdot p^a! = |\mathcal{T}| \cdot p^a \cdot 1 \cdots (p^a - 1) = n(n-1) \cdots (n - (p^a - 1))$$

und in jedem der Paare (p^a, n) und $(l, n-l)$ mit $1 \leqslant l \leqslant (p^a - 1)$ sind die Zahlen durch die gleiche maximale p-Potenz teilbar.

Wir betrachten die Operation

$$G \times \mathcal{T} \to \mathcal{T}, (g, X) \mapsto gX.$$

Da $p \nmid |\mathcal{T}|$ gibt es eine Bahn $G \cdot Y = \{gY \mid g \in G\}$ mit $p \nmid |G \cdot Y|$. Sei P die Stabilisatoruntergruppe von Y, dann gilt

$$|G \cdot Y| = [G : P]$$

also gilt $p \nmid [G : P]$. Es folgt

$$p^a \big| |P|.$$

Für $g \in P$, $y \in Y$ gilt $gy \in Y$, also $g \in Yy^{-1}$. Es folgt $P \subset Yy^{-1}$. Da

$$p^a \leqslant |P| \leqslant |Yy^{-1}| = |Y| = p^a$$

folgt $|P| = p^a$.

Jede p-Untergruppe ist in einer Sylowuntergruppe enthalten: Sei P eine p-Sylowuntergruppe und H eine p-Untergruppe von G. Dann gibt es $x \in G$ mit $H \subset xPx^{-1}$. Beweis dazu: Sei o. E. $H \neq \{e\}$. Für $\mathcal{L} = G/P$ betrachte die Operation

$$H \times \mathcal{L} \to \mathcal{L}, (h, gP) \mapsto hgP$$

mit der Fixpunktmenge $\mathcal{L}_0$. Aus der Bahnengleichung folgt

$$|\mathcal{L}| \equiv |\mathcal{L}_0| \mod p.$$

Wegen $p \nmid [G : P] = |\mathcal{L}|$ folgt $|\mathcal{L}_0| \neq 0$, also $\mathcal{L}_0 \neq \emptyset$. Für $xP \in \mathcal{L}_0$ und $h \in H$ gilt $hxP = xP$, also $Hx \subset xP$, es folgt $H \subset xPx^{-1}$.
Da xPx^{-1} ebenfalls p-Sylowuntergruppe ist, ist auch die zweite Aussage von (a) gezeigt.

Zu (b): Seien P, P' p-Sylowuntergruppen von G. Nach (a) gibt es $x \in G$ mit $P' \subset xPx^{-1}$. Es folgt $P' = xPx^{-1}$.

Zu (c): Sei $\mathcal{S}$ die Menge aller p-Sylowuntergruppen von G, und $P \in \mathcal{S}$. Nach (a) ist $\mathcal{S}$ die Menge der zu P konjugierten Untergruppen von G. Nach Proposition 1.6.3 gilt

$$s_p = |\mathcal{S}| = [G : N_G(P)].$$

Wegen $[G : N_G(P)] \big| [G : P] = m$ folgt $s_p \big| m$.
Wir betrachten die Operation

$$P \times \mathcal{S} \to \mathcal{S}, (g, Q) \mapsto gQg^{-1}.$$

Dann gilt $\mathcal{S}_0 = \{P\}$. Es ist klar, daß $P \in \mathcal{S}_0$. Sei umgekehrt $Q \in \mathcal{S}_0$. Für $g \in P$ gilt $gQg^{-1} = Q$, also $g \in N_G(Q)$. Es folgt $P \subset N_G(Q)$. Da P und Q p-Sylowuntergruppen von $N_G(Q)$ sind, gibt es nach (b) $n \in N_G(Q)$ mit $P = nQn^{-1} = Q$. Nach der Bahnengleichung gilt

$$|\mathcal{S}| \equiv |\mathcal{S}_0| \mod p \equiv 1 \mod p.$$

□

Proposition 1.6.5. *(a) G hat eine Untergruppe der Ordnung p^b für alle $0 \leqslant b \leqslant a$.*

(b) (Cauchy) Ist $a > 0$, dann enthält G ein Element der Ordnung p.

Beweis. Sei o. E. $a \geqslant 1$, P eine p-Sylowuntergruppe von G.
Zu (a): Induktion nach a. Der Fall $a = 1$ ist klar. Sei $a > 1$. Dann ist $Z(P) \neq \{e\}$, sei also $e \neq y \in Z(P)$, $\mathrm{ord}(y) = p^k$ und sei $x = y^{p^{k-1}}$. Dann hat x Ordnung p, es gilt $\langle x\rangle \triangleleft P$. Da $|P/\langle x\rangle| = p^{a-1}$ gibt es nach Induktionsannahme für alle $0 \leqslant b \leqslant a-1$ Untergruppen $H_b \subset P$ mit $\langle x\rangle \subset H_b$ so daß $H_b/\langle x\rangle$ Ordnung p^b hat. Die Ordnung von H_b ist p^{b+1}, $0 \leqslant b \leqslant a-1$.
Zu (b): Dies folgt aus (a). □

Folgerung 1.6.6. *Sei G eine endliche Gruppe, p Primzahl; dann sind folgende Aussagen äquivalent:*

(a) G ist p-Gruppe.

(b) Für alle $x \in G$ ist $\mathrm{ord}(x)$ p-Potenz.

Beweis. **(a) ⇒ (b):** Dies ist klar.
(b) ⇒ (b): Sei q Primteiler von $|G|$. Nach Cauchy besitzt G ein Element der Ordnung q. Wegen (b) folgt $q = p$. Somit ist $|G|$ p-Potenz. □

Folgerung 1.6.7. *Sei G endliche Gruppe, p prim. Äquivalent sind:*

(a) G hat genau eine p-Sylowuntergruppe.

(b) Ist P p-Sylowuntergruppe von G, dann ist $P \triangleleft G$.

Beweis. Sei P p-Sylowuntergruppe. Dann ist

$$s_p = [G : N_G(P)] = 1 \quad \Leftrightarrow \quad G = N_G(P) \quad \Leftrightarrow \quad P \triangleleft G.$$

□

Folgerung 1.6.8. *Sei $H \subset G$ Untergruppe, P p-Sylowgruppe von H. Dann gibt es eine p-Sylowgruppe Q von G mit $P = H \cap Q$.*

Beweis. Es gibt eine p-Sylowgruppe von G mit $P \subset Q$. Es folgt $P \subset H \cap Q$. Da P p-Sylowgruppe von H ist, $H \cap Q$ eine p-Gruppe folgt $P = H \cap Q$. □

Folgerung 1.6.9. *Sei $N \triangleleft G$ und Q p-Sylowuntergruppe von G.*

(a) $N \cap Q$ ist p-Sylowuntergruppe von N.

(b) QN/N ist p-Sylowuntergruppe von G/N und jede p-Sylowuntergruppe von G/N ist von dieser Gestalt.

Beweis. **Zu (a):** Sei P' p-Sylowgruppe von N. Dann gibt es $g \in G$ mit

$$P' \subset gQg^{-1} \quad \text{und} \quad g^{-1}P'g \subset Q.$$

Es gilt

$$g^{-1}P'g \subset g^{-1}Ng = N;$$

es folgt

$$g^{-1}P'g \subset N \cap Q.$$

Da $g^{-1}P'g$ eine p-Sylowgruppe von N ist, $N \cap Q$ eine p-Untergruppe von N, folgt $g^{-1}P'g = N \cap Q$.
Zu (b): Offenbar ist QN/N p-Untergruppe von G/N. Ferner gilt

$$[G/N : QN/N] = [G : N]/[QN : N] = |G|/|QN| = [G : QN]\big|[G : Q].$$

Also $p \nmid [G/N : QN/N]$. Also ist QN/N p-Sylowuntergruppe von G/N. Ist R eine p-Sylowgruppe von G/N, dann gibt es $g \in G$ mit

$$R = \overline{g}(QN/N)\overline{g}^{-1} = gQg^{-1}N/N,$$

und gQg^{-1} ist ebenfalls p-Sylowuntergruppe von G. □

Folgerung 1.6.10. *Sei $|G| = p^a m$ wie im Satz, sei $O_p(G)$ der Durchschnitt aller p-Sylowuntergruppen von G.*

(a) $O_p(G)$ *ist die größte normale* p*-Untergruppe von* G*.*

(b) $[G : O_p(G)] \big| m!$

Beweis. Sei P eine p-Sylowuntergruppe von G. Die Abbildung

$$\varphi : G \to \mathfrak{S}_{G/P}, \varphi(y)(xP) \quad \text{für } y \in G, xP \in G/P$$

ist Homomorphismus; es gilt

$$\ker(\varphi) = \bigcap_{x \in G} xPx^{-1} = O_p(G).$$

Also ist $O_p(G)$ eine normale p-Untergruppe von G. Nach Homomorphiesatz existiert ein injektiver Homomorphismus

$$G/O_p(G) \to \mathfrak{S}_{G/P};$$

es folgt $[G : O_p(G)] \big| m!$. Ist H normale p-Untergruppe von G, dann gibt es $y \in G$ mit $H \subset yPy^{-1}$; es folgt

$$H = xHx^{-1} \subset xyPy^{-1}x^{-1}$$

und damit

$$H \subset \bigcap_{x \in G} xPx^{-1} = O_p(G).$$

□

1.6.2 Anwendungen

Satz 1.6.11. *Sei* G *Gruppe der Ordnung* pq*, wobei* $p < q$ *prim, sei* P *eine* p*- und* Q *eine* q*-Sylowuntergruppe von* G*.*

(a) $Q \triangleleft G$ *ist Normalteiler und* $G = QP = PQ$*,* $Q \cap P = \{e\}$*, dh.* G *ist semidirektes Produkt von* P *und* Q*.*

(b) Ist auch $P \triangleleft G$ *Normalteiler, dann ist* G *zyklisch. Dieser Fall tritt ein, wenn* $p \nmid (q-1)$*.*

Beweis. **Zu (a):** Sei s_q die Anzahl der q-Sylowuntergruppen von G. Dann gilt $s_q \big| p$, also $s_q \in \{1, p\}$ und $s_q \equiv 1 \mod q$. Da $p < q$, muß $s_q = 1$ sein. Also ist $Q \triangleleft G$. Alles andere ist klar.
Zu (b): Ist auch $P \triangleleft G$, dann ist $Q = P \times Q \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/pq\mathbb{Z}$. Gelte $p \nmid (q-1)$, und sei s_p Anzahl der p-Sylowuntergruppen. Dann $s_p \in \{1, q\}$, und $s_p \equiv 1 \mod p$. Wegen $p \nmid q-1$ muß $s_p = 1$ sein. □

Was ist, wenn $p \big| (q-1)$?

Proposition 1.6.12. *Seien* p, q *Primzahlen mit* $p < q$ *und* $p \big| (q-1)$*. Dann gibt es einen nichttrivialen Homomorphismus* $\tau : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$*.*

Beweis. $\mathrm{Aut}(\mathbb{Z}/q) \cong (\mathbb{Z}/\mathbb{Z}q)^\times$ ist zyklisch von der Ordnung $q-1$. Da $p \big| (q-1)$, gibt es (genau) eine Untergruppe der Ordnung p, also gibt es einen nichttrivialen Homomorphismus τ wie gewünscht. □

Satz 1.6.13. *Seien* $p < q$ *prim mit* $p \big| (q-1)$*, sei* $\tau : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ *ein nichttrivialer Homomorphismus.*

(a) $\mathbb{Z}/q\mathbb{Z} \times_\tau \mathbb{Z}/p\mathbb{Z}$ *ist nicht-abelsche Gruppe der Ordnung* pq*.*

(b) Jede nicht-abelsche Gruppe der Ordnung pq *ist isomorph zu* $\mathbb{Z}/q\mathbb{Z} \times_\tau \mathbb{Z}/p\mathbb{Z}$*.*

Beweis. **Zu (a):** Dies ist klar.
Zu (b): Dies folgt aus der nächsten Proposition. □

Proposition 1.6.14. *Sind* $p < q$ *Primzahlen mit* $p \big| (q-1)$*, dann sind je zwei nicht-abelsche Gruppen der Ordnung* pq *isomorph.*

Beweis. Seien G, G' nichtabelsche Gruppen der Ordnung pq, seien $Q \triangleleft G$, $Q' \triangleleft G'$ Normalteiler der Ordnung q, $P \subset G$ und $P' \subset G'$ Untergruppen der Ordnung p, seien $\kappa : P \to \mathrm{Aut}(Q)$, $\kappa' : P' \to \mathrm{Aut}(Q')$ die Konjugationshomomorphismen. κ und κ' sind injektiv. Sei $g : Q \to Q'$ Isomorphismus. Dann ist

$$\gamma : \mathrm{Aut}(Q) \to \mathrm{Aut}(Q'), \alpha \mapsto g \circ \alpha \circ g^{-1}$$

Isomorphismus.

$$\begin{array}{ccc} Q & \xrightarrow{g} & Q' \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\gamma(\alpha)} \\ Q & \xrightarrow{g} & Q' \end{array}$$

Die Gruppe $\mathrm{Aut}(Q')$ ist zyklisch von der Ordnung $q-1$. Wegen $p \mid (q-1)$hat $\mathrm{Aut}(Q')$ genau eine Untergruppe der Ordnung p. Da $\mathrm{im}(\kappa')$ und $\mathrm{im}(\gamma \circ \kappa)$ Untergruppen der Ordnung p von $\mathrm{Aut}(Q')$ sind, folgt

$$\mathrm{im}(\kappa') = \mathrm{im}(\gamma \circ \kappa).$$

Der Isomorphismus $f : P \to P'$ sei definiert durch $f = {\kappa'}^{-1} \circ \gamma \circ \kappa$; dann ist $\kappa' \circ f = \gamma \circ \kappa$

$$\begin{array}{ccc} P & \xrightarrow{\kappa} & \mathrm{Aut}(Q) \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle\gamma} \\ P' & \xrightarrow{\kappa'} & \mathrm{Aut}(Q') \end{array}$$

Für $x \in P$ gilt

$$(\gamma \circ \kappa)(x) = g \circ \kappa(x) g^{-1} = \kappa' \circ f(x) = \kappa'(f(x))$$

also $g \circ \kappa(x) = \kappa'(f(x)) \circ g$. Sei $h : G \to G'$ definiert durch

$$h(yx) = g(y)f(x) \quad \text{für } y \in Q, x \in P.$$

Das ist wohldefiniert, und außerden Homomorphismus:

$$\begin{aligned} h(y_1x_1y_2x_2) &= h(y_1x_1y_2x_1^{-1}x_1x_2) \\ &= g(y_1x_1y_2x_1^{-1})f(x_1x_2) \\ &= g(y_1)\left(g \circ \kappa(x_1)\right)(y_2)f(x_1)f(x_2) \\ &= g(y_1)\left(\kappa'(f(x_1)) \circ g\right)(y_2)f(x_1)f(x_2) \\ &= g(y_1)\left(f(x_1)g(y_2)f(x_1)^{-1}\right)f(x_1)f(x_2) \\ &= g(y_1)f(x_1)g(y_2)f(x_2) = h(y_1x_1)h(y_2x_2) \end{aligned}$$

□

Folgerung 1.6.15. *Seien $p < q$ prim. Eine Gruppe der Ordnung pq ist entweder isomorph zu $\mathbb{Z}/pq\mathbb{Z}$ oder zu $\mathbb{Z}/q \times_\tau \mathbb{Z}/p$, wobei $\tau : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ nichttrivialer Homomorphismus ist.*

Beweis. Ist schon bewiesen. □

Folgerung 1.6.16. *Eine Gruppe der Ordnung $2p$, wobei $p > 2$ Primzahl ist, ist isomorph zu $\mathbb{Z}/2p\mathbb{Z}$ oder zu $D_p = \mathbb{Z}/p\mathbb{Z} \times_\tau \mathbb{Z}/2\mathbb{Z}$, wobei*

$$\tau : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z}), \tau(\overline{1}) = -\mathrm{id}_{\mathbb{Z}/p\mathbb{Z}}$$

ist.

Beispiele 1.6.17. (a) Eine Gruppe der Ordnung 6 ist isomorph zu $\mathbb{Z}/6\mathbb{Z}$ oder zu $D_3 \cong \mathfrak{S}_3$.

(b) Die Sylowuntergruppen von $\mathfrak{S}_4$:

(i) $p = 2$: $\mathfrak{S}_4$ enthält eine Diedergruppe der Ordnung 8, diese ist 2-Sylowuntergruppe. Also sind die 2-Sylowuntergruppen von $\mathfrak{S}_4$ genau die Diedergruppen der Ordnung 8, die in $\mathfrak{S}_4$ enthalten sind. Für deren Anzahl s_2 gilt, $s_2 | 3$ und $s_2 \equiv 1 \mod 2$. Also $s_2 \in \{1, 3\}$. Da $\mathfrak{S}_4$ mehr als 8 Elemente enthält, deren Ordnung 2-Potenz ist, folgt $s_2 = 3$.
V ist in jeder 2-Sylowuntergruppe enthalten, offenbar ist dann $V = O_s(\mathfrak{S}_4)$.

(ii) $p = 3$: Die 3-Sylowuntergruppen von $\mathfrak{S}_4$ sind genau die Untergruppen der Ordnung 3. Für deren Anzahl gilt $s_3 = 4$.

(c) Die Sylowuntergruppen von A_4:

(i) $p = 2$: V.

(ii) $p = 3$: Wie in $\mathfrak{S}_4$.

Folgerung 1.6.18. *(a) Jede Untergruppe der $\mathfrak{S}_4$ ist genau zu einer der folgenden Gruppen isomorph:*

$$\{e\}, \quad \mathbb{Z}/2\mathbb{Z}, \quad \mathbb{Z}/3\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z}, \quad V \cong D_2, \quad S_3 \cong D_3, \quad D_4, \quad A_4, \quad \mathfrak{S}_4.$$

(b) Die einzigen Normalteiler von $\mathfrak{S}_4$ sind $\{e\}$, V, A_4, $\mathfrak{S}_4$.

Beweis. **Zu (a):** Diese Gruppen kommen vor. Sei umgekehrt $\{e\} \neq H \neq \mathfrak{S}_4$ Untergruppe. Dann gilt $|H| \in \{2, 3, 4, 6, 8, 12\}$. Ist $|H| = 12$, dann ist $[\mathfrak{S}_4 : H] = 2$, also H Normalteiler vom Index 2, somit $H = A_4$. Ist $|H| = 8$, dann $H \cong D_4$, hiervon gibt es drei Stück. Ist $|H| = 6$, dann ist $H \cong \mathbb{Z}/6$, was aber unmöglich ist, oder $H \cong D_3$, hiervon gibt es 4 Stück. Ist $|H| = 4$, so ist $H \cong \mathbb{Z}/4\mathbb{Z}$ oder $H \cong \mathbb{Z}/2 \times \mathbb{Z}/2 \cong V$. Ist $|H| = 3$, dann ist $H \cong \mathbb{Z}/3\mathbb{Z}$.Ist $|H| = 2$, dann ist $H \cong \mathbb{Z}/2\mathbb{Z}$.
Zu (b): Dies folgt aus (a). □

Beispiel* 1.6.19. Sei G eine Gruppe der Ordnung 105. Dann hat G einen Normalteiler der Ordnung 5 oder 7.

Beweis. Die Primfaktorzerlegung von 105 ist $3 \cdot 5 \cdot 7$. Ist s_p die Anzahl der p-Sylowgruppen von G, so gilt $s_7 | 3 \cdot 5 = 15$, also $s_7 \in \{1, 3, 5, 15\}$. Außerdem gilt $s_7 \equiv 1 \mod 7$, das schränkt s_7 ein auf 1 oder 15. Die gleich Argumentation liefert, da $s_5 | 3 \cdot 7$, $s_5 \in \{1, 3, 7, 21\}$, und wegen $s_5 \equiv 1 \mod 5$ also $s_5 \in \{1, 21\}$.

Da 5 und 7 in der Primfaktorzerlegung von 105 gemnau einmal vorkommen, ist jede Untergruppe der Ordnung 5, bzw. 7, auch 5-Sylowuntergruppe, bzw. 7-Sylowuntergruppe. Wir nehmen nun an, daß G weder einen Normalteiler der Ordnung 5, noch einen Normalteiler der Ordnung 7 hat, insbesondere sind die 5- und 7-Sylowuntergruppen keine Normalteiler. Es folgt daß nicht nur jeweils eine 5-u und eine 7-Sylowuntergruppe geben kann, dh. $s_5 = 21$ und $s_7 = 15$.

Wir zählen nun Elemente um zu zeigen, daß dies nicht der Fall sein kann. Jedes Element $g \neq e$ der Ordnung 5 liegt in einer 5-Sylowuntergruppe, nämlich in der von g erzeugten. Andererseits enthält jede 5-Sylowuntergruppe, da sie zyklisch ist $\varphi(5) = 4$ Elemente $\neq e$ der Ordnung 5. Das heißt, es gibt insgesamt

$$\varphi(5) \cdot s_5 = 4 \cdot 21 = 84$$

nicht-triviale Elemente der Ordnung 5. Genauso gibt es

$$\varphi(7) \cdot s_7 = 6 \cdot 15 = 90$$

nicht-triviale Elemente der Ordnung 7. Dies sind insgesamt bereits $84 + 90 = 174$ Elemente. Widerspruch zu $|G| = 105$.

Es folgt, daß entweder $s_7 = 1$ oder $s_5 = 1$, und G einen Normalteiler der Ordnung 7 oder 5 haben msß. □

1.6.3 Nilpotente Gruppen

Für $x, y \in G$ heißt $[x, y] = xyx^{-1}y^{-1}$ Kommutator von x und y. Es gilt

$$[x, y] = e \quad \Leftrightarrow \quad xy = yx.$$

Ferner ist

$$[x,y]^{-1} = [y,x].$$

Für $z \in G$ gilt

$$z[x,y]z^{-1} = [zyz^{-1}, zyz^{-1}].$$

Für Untergruppen H, K von G sei $[H,K]$ die von allen $[x,y]$ mit $x \in H$, und $y \in K$, erzeugte Untergruppe. Es gilt

$$[H,K] = [K,H].$$

Proposition 1.6.20. *Sei $H \subset G$ Untergruppe.*

(a) $H \triangleleft G$ genau dann, wenn $[H,G] \subset H$.

(b) Aus $H \triangleleft G$ folgt $[H,G] \triangleleft G$ und $H/[H,G] \subset Z(G/[H,G])$.

(c) Ist $N \triangleleft G$ mit $HN/N \subset Z(G/N)$, dann gilt $[H,G] \subset N$.

Beweis. **Zu (a):** Für $x \in H$ $y \in G$ gilt $[x,y] = xyx^{-1}y^{-1} \in H$ genau dann, wenn $yx^{-1}y^{-1} \in H$.
Zu (b): Sei $H \triangleleft G$. Für $x \in H$, $y, z \in G$ gilt:

$$z[x,y]z^{-1} = [zyz^{-1}, zyz^{-1}] \in [H,G]$$

und damit $z[H,G]z^{-1} = [H,G]$, also $[H,G] \triangleleft G$.
In $G/[H,G]$ gilt

$$[\overline{x},\overline{y}] = \overline{xyx^{-1}y^{-1}} = e \quad \text{für } x \in H, y \in G,$$

also $H/[H,G] \subset Z(G/[H,G])$.
Zu (c): Sei $N \triangleleft G$. Für $x \in H$ und $y \in G$ gilt in G/N:

$$\overline{[x,y]} = [\overline{x},\overline{y}] = e,$$

da $\overline{x} \in Z(G/N)$. Also $[x,y] \in N$. Es folgt $[H,G] \subset N$. □

Seien

$$\begin{aligned} C^1(G) &= G \\ C^{i+1}(G) &= [C^i(G), G] \end{aligned}$$

Nach der Proposition sind die $C^i(G)$, $i \geqslant 1$, Normalteiler von G und es gilt

$$G = C^1(G) \supset C^2(G) \supset \dots$$

Da $C^i(G)/C^{i+1}(G) \subset Z(G/C^{i+1}(G))$ ist, ist $C^i(G)/C^{i+1}(G)$ abelsch. Die Folge $\left(C^i(G)\right)_{i\geqslant 1}$ heißt absteigende Zentralreihe von G. $C^2(G) = [G,G]$ heißt Kommutatoruntergruppe.

Proposition und Definition 1.6.21. *Eine endliche Gruppe heißt nilpotent, falls folgende Bedingungen erfüllt sind:*

(a) Es gibt $n \in \mathbb{N}$ mit $C^n(G) = \{e\}$.

(b) Es gibt eine Folge von Untergruppen $G = H_1 \supset H_2 \supset \dots \supset H_m = \{e\}$ mit $[H_i, G] \subset H_{i+1}$, $1 \leqslant i \leqslant m-1$. (Dann gilt $H_i \triangleleft G$.)

Diese Bedingungen sind äquivalent.

Beweis. **„(a) ⇒ (b)“:** Die Folge $\left(C^i(G)\right)_{i\in\mathbb{N}}$ ist wie gewünscht.
„(b) ⇒ (a)“: Es gilt $C^i(G) \subset H_i$. Das ist klar für $i = 1$. Sei $1 \leqslant i < m$ und $C^i(G) \subset H_i$, dann

$$C^{i+1}(G) = [C^i(G), G] \subset [H_i, G] \subset H_{i+1}.$$

Da $H_m = \{e\}$, folgt $C^m(G) = \{e\}$.
Wegen $[H_i, G] \subset H_{i+1} \subset H_i$, ist H_i Normalteiler von G nach Proposiiton 1.6.20. □

Satz 1.6.22. *Sei p prim, P eine p-Gruppe, $|P| = p^n$ mit $n \in \mathbb{N}_0$.*

(a) Es gibt eine Folge $P = P_1 \supset P_2 \supset \ldots \supset P_{n+1} = \{e\}$ von Normalteilern $P_i \triangleleft P$ mit $[P_i, P] \subset P_{i+1}$ und $|P_i| = p^{n+1-i}$.

(b) P ist nilpotent.

Beweis. **Zu (a)**: Induktion über n. Der Fall $n = 1$ ist klar. Sei $n > 1$. Es gilt $Z(P) \neq \{e\}$, sei $x \in Z(P)$ ein Element der Ordnung p. Dann $\langle x \rangle \triangleleft P$. Sei $\overline{P} = P/\langle x \rangle$. Nach Induktionsvoraussetzung gibt es Normalteiler $\overline{P} = H_1 \supset H_2 \supset \ldots \supset H_n = \{e\}$ wie behauptet. Es gibt $P_i \triangleleft P$ mit $\langle x \rangle \subset P_i$ und $H_i = P_i/\langle x \rangle$ für $1 \leqslant i \leqslant n$. Sei $P_{n+1} = \{e\}$. Es gilt $[P_i, P] \subset P_{i+1}$ für $1 \leqslant i \leqslant n-1$, denn für $x \in P_i$ und $y \in P$, gilt $\overline{[x,y]} = [\overline{x}, \overline{y}] \in H_{i+1}$, also $[x, y] \in P_{i+1}$. Ferner gilt $[P_n, P] = [\langle x \rangle, P] = \{e\} = P_{n+1}$. Da $|H_i| = p^{n-i}$, $1 \leqslant i \leqslant n$, folgt $|P_i| = p^{n+1-i}$, $1 \leqslant i \leqslant n+1$.
Zu (b): Daß P nilpotent ist, folgt aus der Definition. □

Satz 1.6.23 (Burnside)**.** *Für eine endliche Gruppe sind äquivalent:*

(a) G ist nilpotent.

(b) Für jede Untergruppe $H \subsetneq G$ gilt $H \subsetneq N_G(H)$.

(c) Jede maximale Untergruppe von G ist Normalteiler.

(d) Jede Sylowuntergruppe von G ist Normalteiler.

(e) G ist direktes Produkt von p-Gruppen. (Genauer G ist direktes Produkt der Sylowuntergruppen $\neq \{e\}$).

(f) Für jeden echten Normalteiler $H \triangleleft G$ gilt $Z(G/H) \neq \{e\}$.

Eine Untergruppe $H \subset G$ heißt maximal, falls $H \subsetneq G$ echt ist, und es keine Untergruppe $H \subsetneq H' \subsetneq G$ gibt. Zum Beispiel sind A_3 und $\{\mathrm{id}, (12)\}$, $\{\mathrm{id}, (13)\}$, $\{\mathrm{id}, (23)\}$ die maximalen Untergruppen von $\mathfrak{S}_3$.

Lemma 1.6.24 (Fratiniargument)**.** *Sei G endliche Gruppe.*

(a) Ist $M \triangleleft G$ und P eine p-Sylowuntergruppe von M, dann gilt $G = M \cdot N_G(P)$.

(b) Ist P p-Sylowuntergruppe von G mit $N_G(P) \subset H$, dann $N_G(H) = H$. Insbesondere gilt $N_G(N_G(H)) = N_G(H)$.

Beweis. **Zu (a)**: Sei $g \in G$. Dann ist $gPg^{-1} \subset gMg^{-1} = M$ ebenfalls p-Sylowuntergruppe von M, also gibt es $x \in M$ mit $xPx^{-1} = gPg^{-1}$. Es folgt $P = x^{-1}gPg^{-1}x$ also $x^{-1}g \in N_G(P)$. Damit ist $g = x(x^{-1})g \in M \cdot N_G(P)$.
Zu (b): Wende (a) auf die Gruppe $N_G(H)$ an. Da $H \triangleleft N_G(H)$ und P p-Sylowuntergruppe von H ist, gilt nach (a), $N_G(H) = H \cdot N_{N_G(P)}(P) \subset H \cdot N_G(P) = H$, also $N_G(H) = H$. □

Beweis des Satzes von Burnside. **(a) ⇒ (b):** Sei $G = H_1 \supset H_2 \supset \ldots \supset H_m = \{e\}$ mit $[H_i, G] \subset H_{i+1}$ für $1 \leqslant i \leqslant m-1$, und sei $H \subsetneq G$ eine Untergruppe. Sei j maximal mit $H_j \nsubseteq H$, für $j < m$. Dafür gilt $[H_j, G] \subset H_{j+1} \subset H$. Dann gilt $H_j \subset N_G(H)$: Für $x \in H_j$, $y \in H$, gilt $[x, y] = xyx^{-1}y^{-1} \in H$, somit $xyx^1 \in H$; es folgt $xHx^{-1} \subset H$, ebenso $x^{-1}Hx \subset H$, also $x^{-1}Hx = H$, und deshalb $x \in N_G(H)$. Wegen $H_j \nsubseteq H$, $H_j \subset N_G(H)$ folgt $H \subsetneq N_G(H)$.
(b) ⇒ (c): Sei $H \subsetneq G$ maximale Untergruppe. Dann ist $H \subsetneq N_G(H) \subset G$, also $N_G(H) = G$, und damit $H \triangleleft G$.
(c) ⇒ (d): Annahme: Es gibt eine nicht-normale Sylowuntergruppe P. Dann gilt $P \subset N_G(P) \subsetneq G$. Es gibt eine maximale Untergruppe $H \subset G$ mit $N_G(P) \subset H$. (Es gibt eine Untergruppe $H \subset G$ mit $N_G(P) \subset H$, so daß $[G : H] > 1$ und minimal ist.) Nach (c) ist $H \triangleleft G$. Nach dem Frattiniargument ist aber $N_G(H) = H$, Widerspruch.
(d) ⇒ (e): Sei ohne Beschränkung der Allgemeinheit $|G| > 1$, sei $|G| = p_1^{\nu_1} \cdots p_r^{\nu_r}$ mit Primzahlen $p_1 < \ldots < p_r$ und $\nu_i \in \mathbb{N}$, sei P_i die p_i-Sylowuntergruppe von G, $1 \leqslant i \leqslant r$. Damit ist $P_i \cap (P_{i+1} \cdots P_r) = \{e\}$ für $1 \leqslant i < r$, und $G = P_1 \cdots P_r$. Nach Abschnitt 1.4.1 ist G direktes Produkt von $P_1, \ldots, P_r$.
(e) ⇒ (f): Sei $G = P_1 \times \ldots \times P_r$ direktes Produkt der p_i-Gruppen mit Primzahlen $p_1 < \ldots < p_r$ und sei $H \triangleleft G$ echter Normalteiler. Dann ist $\overline{G} = G/H = (P_1H/H) \times \ldots \times (P_rH/H)$ ebenalls direkte Produktzerlegung, P_iH/H ist p_i-Untergruppe. Es gibt $1 \leqslant j \leqslant r$ mit $P_jH/H \neq \{e\}$. Es gilt: $\{e\} \neq$

$Z(P_jH/H) \subset Z(\overline{G})$.
(f) $\Rightarrow$ (a): Induktion nach $|G|$. Der Fall $|G| = 1$ ist klar. Sei $|G| > 1$. Dann ist $Z(G) \neq \{e\}$; sei $\overline{G} = G/Z(G)$. Es gilt $C^i(\overline{G}) = C^i(G)Z(G)/Z(G)$ für $i \geqslant 1$. Nach Induktionsannahme gibt es $n \in \mathbb{N}$ mit $C^n(\overline{G}) = \{e\}$. Es folgt $C^n(G) \subset Z(G)$ und $C^{n+1}(G) = [C^n(G), G] = \{e\}$. □

Proposition 1.6.25. *(a) Untergruppen, Faktorgruppen und endliche direkte Produkte endlicher nilpotenter Gruppen sind nilpotent.*

(b) Ist G endlich, $H \subset Z(G)$ eine Untergruppe und ist G/H nilpotent, dann ist G nilpotent.

(c) Ist G endlich und nilpotent, $d \in \mathbb{N}$ ein Teiler von $|G|$, dann hat G einen Normalteiler der Ordnung d.

Beweis. **Zu (a):** Dies folgt aus folgenden einfachen Rechenregeln: Ist $H \subset G$ Untergruppe, dann $C^i(H) \subset C^i(G)$, für $i \geqslant 1$. Ist $N \triangleleft G$, $\overline{G} = G/N$, dann ist $C^i(\overline{G}) = C^i(G)N/N$, für $i \geqslant 1$. Ist $G_1 \times \ldots \times G_r$ direktes Produkt von Gruppen, dann gilt $C^i(G) = C^i(G_1) \times \ldots \times C^i(G_r)$.
Zu (b): Dies sieht man wie „(f) $\Rightarrow$ (a)“im Beweis des Satzes von Burnside.
Zu (c): Sei G nilpotent, $G = P_1 \times \ldots \times P_r$ mit $|P_i| = p_i^{\nu_i}$, wobei die p_i prim sind mit $p_1 < \ldots < p_r$ und $\nu_i \in \mathbb{N}$. Sei d Teiler von $|G|$, dann gibt es $0 \leqslant w_i \leqslant \nu_i$ mit $d = \prod_{i=1}^r p_i^{w_i}$. Nach Satz 1.6.22 gibt es Normalteiler $P_i' \triangleleft P_i$ mit $|P_i'| = p_i^{w_i}$, $1 \leqslant i \leqslant r$. Für $N = P_1' \times \ldots \times P_r'$ gilt dann $N \triangleleft G$, $|N| = d$. □

Folgerung 1.6.26. *Sei G nilpotent, $\{e\} \neq N \triangleleft G$. Dann gilt $N \cap Z(G) \neq \{e\}$.*

Beweis. Sei $N_1 = N$, $N_{i+1} = [N_i, G]$ für $i \geqslant 1$. Es gilt $N_i \subset N$ nach Proposition 1.6.20, und $N_i \subset C^i(G)$, für $i \geqslant 1$. Es gibt $n \in \mathbb{N}$ mit $C^n(G) = \{e\}$, also folgt $N_n = \{e\}$. Es gibt eine maximales $k \geqslant 1$ mit $N_k \neq \{e\}$. Dafür gilt $N_{k+1} = [N_k, G] = \{e\}$. Es folgt $\{e\} \neq N_k \subset Z(G) \cap N$. □

Beispiele 1.6.27. Endliche abelsche Gruppen sind nilpotent.
$\mathfrak{S}_3$ ist nicht nilpotent. Allgemein gilt: D_n ist genau dann nilpotent, wenn n Potenz von 2 ist.

Kapitel 2

Ringtheorie

2.1 Allgemeine Tatsachen

2.1.1 Ringe, Unterringe, Ideale

Definition 2.1.1. Eine Menge R zusammen mit zwei Abbildungen $+ : R \times R \to R, (r,s) \mapsto r+s$ und $\cdot : R \times R \to R, (r,s) \mapsto rs$, heißt Ring mit Einselement, wenn gilt:

(a) $(R,+)$ ist abelsche Gruppe; neutrales Element sei 0, Inverses von $r \in R$ sei $-r$.

(b) $(R,\cdot)$ ist Monoid; neutrales Element sei 1.

(c) Für alle $r,s,t \in R$ gilt: $(r+s)t = rt+st$ und $r(s+t) = rs+rt$.

Ist R ein Ring, dann heißt die Einheitengruppe $R^\times$ des Monoids $(R,\cdot)$ auch Einheitengruppe des Rings R. R heißt kommutativ, wenn $(R,\cdot)$ kommutatives Monoid ist. R heißt Körper, wenn R kommutativ ist mit $1 \neq 0$ und $R^\times = (R\backslash\{0\})$. Ein Ring heißt Schiefkörper, wenn $1 \neq 0$ und $R^\times = (R\backslash\{0\})$.

Proposition und Definition 2.1.2. *Sei R ein Ring. Eine Teilmenge $S \subset R$ heißt Unterring, wenn S Untergruppe von $(R,+)$ und Untermonoid von $(R,\cdot)$ ist. Dann ist S bezüglich $+$ und $\cdot$ ein Ring. R heißt dann auch Oberring von S. S ist genau dann Unterring von R, wenn gilt $1 \in S$ und für alle $s,t \in S$ ist $s-t \in S$ und $st \in S$.*

Beweis. Wegen $1 \in S$ gilt $0 = 1-1 \in S$. Der Rest folgt wie bei Gruppen. □

Beispiele 2.1.3. (a) $\mathbb{Z}$, $\mathbb{Z}/\mathbb{Z}a$ für $a \in \mathbb{Z}$ sind kommutative Ringe. $\mathbb{Z}$ ist Unterring von $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. $\mathbb{Q}$ ist Unterring von $\mathbb{R}$, $\mathbb{C}$.

(b) Sei $d \in \mathbb{Z}\setminus\{0,1\}$.

$$R = \{a + b\sqrt{d} \mid a,b \in \mathbb{Q}\}$$

ist Unterring von $\mathbb{C}$, sogar Körper.

$$S = \{a + b\sqrt{d} \mid a,b \in \mathbb{Z}\}$$

ist Unterring von R.

(c) Sei R ein Ring, $n \in \mathbb{N}$. Die Menge $R^{n\times n}$ der (n,n)-Matrizen mit Koeffizienten in R ist Ring bezüglich der üblichen Addition und Multiplikation von Matrizen. $(R^{n,n})^\times = \mathbf{GL}_n(R)$ ist die Gruppe der invertierbaren Matrizen in $R^{n\times n}$.

(d) Sei R Ring. Dann ist das Zentrum

$$Z(R) = \{r \in R \mid \forall s \in R : rs = sr\}$$

ein kommutativer Unterring von R

Beispiel* 2.1.4. Ein Ring R mit Einselement heißt idempotent, wenn für alle $a \in R$ gilt $a \cdot a = a$. Jeder idempotente Ring ist kommutativ und es gilt $-1 = 1$.

Beweis. Für beliebige $x, y \in R$ gilt wie in jedem Ring $xy = (-x)(-y)$, denn

$$(-x)y + xy = ((-x) + x) \cdot y = 0 \cdot y = 0 = x \cdot 0 = x \cdot ((-y) + y) = x(-y) + xy.$$

dh. $-xy = (-x)y = x(-y)$, und damit

$$xy = -(-xy) = -(x(-y)) = (-x)(-y).$$

Also insbesondere $1 \cdot 1 = (-1)(-1)$ und wegen Idempotenz folgt

$$1 = 1 \cdot 1 = (-1)(-1) = -1.$$

Um die Kommutativität zu zeigen, betrachten wir für $x, y \in R$

$$x + y = (x + y)^2 = x^2 + xy + yx + y^2 = x + xy + yx + y.$$

Nach Subtraktion von x und y auf beiden Seiten erhält man $0 = xy + yx$, also $yx = -xy = (-1)xy = 1 \cdot xy$. □

Beispiel* **2.1.5.** Sei $\mathscr{C}^\infty(\mathbb{R})$ der Ring der beliebig oft differenzierbaren Funktionen unter punktweiser Addition und Multiplikation. Dies ist auch ein $\mathbb{R}$-Vektorraum, also insbesondere eine $\mathbb{R}$-Algebra. Eine Funktion $f \in \mathscr{C}^\infty(\mathbb{R})$ heißt D-finit, falls der von allen Ableitungen $f', f'', \ldots$ erzeugte $\mathbb{R}$-Untervektorraum $D(f)$ endlich-dimensional ist. Die D-finiten Funktionen bilden einen Unterring von $\mathscr{C}^\infty(\mathbb{R})$.

Beweis. Das Einselement in $\mathscr{C}^\infty(\mathbb{R})$ ist die konstante Abbildung $1 : \mathbb{R} \to \mathbb{R}, y \mapsto 1$. Der zugehörige Unterrraum ist sogar eindimensional, da alle Ableitungen $= 0$ sind. Es ist zu zeigen, daß für D-finite Funktionen $f, g \in \mathscr{C}^\infty(\mathbb{R})$, die Funktionen $f \cdot g$ und $f - g$ auch D-finit sind. Nach Voraussetzung sind die Unterräume $D(f)$ und $D(g)$ endlich erzeugt, das heißt

$$D(f) = \langle f^{(i)} \mid 1 \leqslant i \leqslant m \rangle \text{ und } \langle g^{(i)} \mid 1 \leqslant i \leqslant m \rangle$$

für geeignetes m. Dann ist wegen elementaren Rechenregeln

$$D(f - g) \subset \langle f^{(i)}, g^{(j)} \mid 1 \leqslant i, j \leqslant m \rangle$$

und mit Induktion zeigt man

$$D(fg) \subset \langle f^{(i)} \cdot g^{(j)} \mid 1 \leqslant i, j \leqslant m \rangle.$$

□

Definition 2.1.6. Sei R ein Ring.

(a) Eine Teilmenge $A \subset R$ heißt Linksideal von R, wenn A Untergruppe von $(R, +)$ ist, und für alle $a \in A$, $r \in R$ gilt $ra \in A$.

(b) Eine Teilmenge $A \subset R$ heißt Rechtsideal von R, wenn A Untergruppe von $(R, +)$ ist, und für alle $a \in A$, $r \in R$ gilt $ar \in A$.

(c) Eine Teilmenge $A \subset R$ heißt (zweiseitiges) Ideal von R, wenn A Linksideal und Rechtsideal ist.

Ist R kommutativ, dann fallen die drei Begriffe zusammen.

Bemerkung 2.1.7. (a) In einem Ring R sind $\{0\}$ und R selbst stets Ideale.

(b) Ist $(A_i)_{i \in I}$ Familie von (Links-/Rechts-)Idealen, dann ist auch

$$\bigcap_{i \in I} A_i$$

(Links-/Rechts-)Ideal. Sind $A_1, \ldots A_n$ (Links-/Rechts-)Ideale, dann ist

$$A_1 + \ldots + A_n = \left\{ x \in R \;\middle|\; \exists a_i \in A_i, 1 \leqslant i \leqslant n : x = a_1 + \ldots + a_n \right\}$$

(Links-/Rechts-)Ideal.

(c) Ist $X \subset R$ Teilmenge, dann ist

$$ {}_R(X) = \bigcap \{A \mid A \text{ Linksideal von } R \text{ mit } X \subset A\} $$

das kleinste Linksideal, das X enthält; es heißt das von X erzeugte Linksideal. Es gilt

$$ {}_R(X) = \left\{ r \in R \mid \exists n \in \mathbb{N}_0, x_1, \ldots, x_n \in X, r_1, \ldots, r_n \in R : r = \sum_{i=1}^{r} r_i x_i \right\}. $$

Für $a \in R$ setzt man

$$ Ra = {}_R(a) = {}_R(\{a\}) = \{ra \mid r \in R\}. $$

Allgemeiner: Sind $a_1, \ldots, a_r \in R$, dann setzt man

$$ Ra_1 + \ldots + Ra_n = {}_R(a_1, \ldots, a_n) = {}_R(\{a_1, \ldots, a_n\}) = \left\{ r \in R \mid \exists r_1, \ldots, r_n \in R : r = \sum_{i=1}^{n} r_i a_i \right\}. $$

Analog definiert man $(X)_R$.
Ist R kommutativ, dann setzt man $(a_1, \ldots, a_n)$ statt ${}_R(a_1, \ldots, a_n)$.

(d) Sei R ein Ring, A (Links-/Rechts-)Ideal mit $R^\times \cap A \neq \emptyset$. Dann gilt $A = R$. Für Linksideal sieht man das wie folgt: Sei $a \in R^\times \cap A$. Dann gibt es $a' \in R$ so daß $a'a = 1$. Damit gilt für alle $r \in R$: $r = ra'a \in A$.

(e) Sei R kommutativer Ring. R ist genau dann Körper, wenn $1 \neq 0$ und $\{0\}$ und R die einzigen Ideale von R sind. Dies sieht man folgendermaßen:
„$\Rightarrow$“: Sei $0 \neq A \subset R$ Ideal, dann ist $A \cap R^\times \neq \emptyset$. Wir haben gerade gesehen, daß dann $A = R$.
„$\Leftarrow$“: Sei $0 \neq a \in R$. Dann ist $Ra \neq 0$ Ideal von R, also $R = Ra$. Also gibt es $a' \in R$ mit $a'a = 1$.

(f) Die Ideale von $\mathbb{Z}$ sind genau die Untergruppen: Nach Definition sind Ideale Untergruppen. Sei andererseits $A \subset \mathbb{Z}$ Untergruppe. Dann gibt es $a \in \mathbb{Z}$ mit $A = \mathbb{Z}\,a$. Dies ist Ideal von $\mathbb{Z}$.

Definition 2.1.8. Sei R ein Ring. $A \subset R$ heißt Linkshauptideal, wenn es $a \in A$ gibt, mit $A = Ra = {}_R(a)$. Analog definiert man Rechtshauptideale und Hauptideale.

Beispiel* 2.1.9. Seien R und S kommutative Ringe mit 1. Die Ideale des direkten Produkts $R \times S$ haben die Form $I \times J$, wobei I ein Ideal von R und J ein Ideal von S ist.

2.1.2 Ringhomomorphismen

Definition 2.1.10. Eine Abbildung $\varphi : R \to R'$ zwischen zwei Ringen heißt Ringhomomorphismus, falls $\varphi : (R, +) \to (R', +)$ Gruppenhomomorphismus ist, und $\varphi : (R, \cdot) \to (R', \cdot)$ Monoidhomomorphismus ist.

Wie bei Gruppen definiert man Iso-, Endo- und Automorphismen sowie Isomorphie zwischen zwei Ringen. Die Umkehrabbildung eines bijektiven Homomorphismus ist wieder ein Homomorphismus.

Proposition 2.1.11. *Bei einem Ringohmomorphismus sind Bilder und Urbilder von Unterringen wieder Unterringe. Ferner sind Urbilder von (Links-/Rechts-)Idealen wieder (Links-/Rechts-)Ideale. Ist der Homomorphismus surjektiv, dann gilt dies auch für Bilder. Insbesondere gilt: Ist $\varphi : R \to R'$ ein Ringhomomorphismus, dann ist* $\mathrm{im}(\varphi)$ *ein Unterring von R' und* $\ker(\varphi) = \varphi^{-1}(0)$ *ein Ideal von R. φ ist genau dann injektiv, wenn* $\ker(\varphi) = 0$ *ist.*

Beweis. Wie bei Gruppen. □

Definition 2.1.12. Sei R ein kommutativer Ring. Ein Ring R' heißt R-Algebra, wenn es einen Ringhomomorphismus $\varphi : R \to R'$ gibt mit $\mathrm{im}(\varphi) \subset Z(R')$. Man definiert dann eine Skalarmultiplikation von R auf R' durch

$$ r.r' = \varphi(r)r' \quad \text{für } r \in R, r' \in R'. $$

Dafür gelten dieselben Axiome wie für die Skalarmultiplikation auf einem Vektorraum. Ferner gilt für $r \in R$, $r'_1, r'_2 \in R'$

$$(rr'_1)r'_2 = r'_1(rr'_2) = r(r'_1r'_2).$$

Sei R'' ebenfalls eine R-Algebra bezüglich $\psi : R \to R''$. Ein Ringhomomorphismus $\rho : R' \to R''$ heißt R-Algebrenhomomorphismus, falls $\psi = \rho \circ \varphi$. Dies gilt genau dann, wenn für alle $r \in R$, $r' \in R'$

$$\rho(r.r') = r.\rho(r').$$

Dies sieht man wie folgt: Falls $\psi = \rho \circ \varphi$, dann

$$\rho(r.r') = \rho(\varphi(r)r') = \rho(\varphi(r))\rho(r') = \psi(r)\rho(r') = r.\rho(r').$$

Umgekehrt gilt für alle $r \in R$

$$\rho(\varphi(r)) = \rho(\varphi(r)1_{R'}) = \rho(r.1_{R'}) = r.\rho(1_{R'}) = r.1_{R''} = \psi(r)1_{r''}.$$

Beispiele 2.1.13. (a) Sei R ein kommutativer Ring, $n \in \mathbb{N}$. Dann ist $R^{n,n}$ eine R-Algebra bezüglich

$$\varphi : R \to R^{n,n}, r \mapsto \begin{pmatrix} r & 0 & \cdots & 0 \\ 0 & r & & \vdots \\ \vdots & & \ddots & \\ 0 & \cdots & & r \end{pmatrix}.$$

Die Skalarmultiplikation dazu ist $r.(r_{ij}) = (rr_{ij})$.

(b) Sei R ein Ring. Dann ist

$$\varphi : \mathbb{Z} \to R, z \mapsto z.1$$

ein Ringhomomorphismus mit $\mathrm{im}(\varphi) \subset Z(R)$. Also ist R eine $\mathbb{Z}$-Algebra. Die Skalarmultiplikation dazu ist die von den abelschen Gruppen her bekannte.

2.1.3 Faktorringe

Satz 2.1.14. *Sei R ein Ring, $A \subset R$ ein zweiseitiges Ideal. Die abelsche Gruppe $(R/A, +)$ ist mit der Multiplikation*

$$R/A \times R/A \to R/A, (r + A, s + A) \mapsto rs + A$$

ein Ring. Die Abbildung

$$\pi : R \to R/A, r \mapsto r + A$$

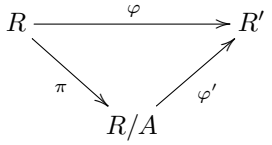
ist ein surjektiver Ringhomomorphismus mit $\ker(\pi) = A$. R/A heißt Faktorring von R modulo A.

Beweis. Wohldefiniertheit: Sei $r + A = r' + A$ und $s + A = s' + A$. Dann ist $r - r' \in A$ und $s - s' \in A$. Also ist $rs - r's' = (r - r')s + r'(s - s') \in A$.
Einselement ist $1 + A$. Der Rest ist klar. □

Die Unterringe, (Links-/Rechts-)Ideale von R/A sind die Teilmengen B/A, wobei B Unterring, (Links-/Rechts-)Ideal von R mit $A \subset B$. Ist R kommutativ, so auch R/A.

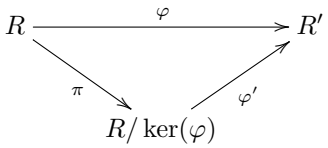
Satz 2.1.15. *Sei $\varphi : R \to R'$ ein Ringhomomorphismus.*

(a) Ist A Ideal von R mit $A \subset \ker(\varphi)$, dann gibt es genau einen Ringhomomorphismus $\varphi' : R/A \to R$ mit $\varphi = \varphi' \circ \pi$, wobei $\pi : R \to R/A$ der kanonische Homomorphismus ist. Das heißt das Diagramm



kommutiert.

(b) (Homomorphiesatz) Es gibt genau einen injektiven Ringhomomorphismus $\varphi' : R/\ker(\varphi) \to R'$ mit $\varphi = \varphi' \circ \pi$, wobei $\pi : R \to R/Ker(\varphi)$ der kanonische Homomorphismus ist. Das heißt das Diagramm



kommutiert. Insbesondere ist die Abbildung

$$\varphi : R/\ker(\varphi) \to \mathrm{im}(\varphi), r + \ker(\varphi) \mapsto \varphi(r)$$

ein Ringisomorphismus.

Beweis. Analog zu Gruppen. □

Folgerung 2.1.16. *Sei R ein Ring.*
1. Isomorphiesatz: *Sei $S \subset R$ ein Unterring, $A \subset R$ ein Ideal. Dann ist $S \cap A \subset S$ ein Ideal, $S + A \subset R$ Unterring, $A \subset S + A$ ein Ideal, und die Abbildung*

$$S/S \cap A \to S + A/A, s + S \cap A \mapsto s + A$$

ein Ringisomorphismus.
2. Isomorphiesatz: *Seien A, B Ideale von R mit $A \subset B$. Dann ist $B/A \subset R/A$ ein Ideal, und die Abbildung*

$$R/B \to (R/A)/(B/A), r + B \mapsto (r + A) + B/A$$

ein Ringisomorphismus.

Beweis. Wie bei Gruppen. □

2.2 Polynomalgebren

Vorbemerkung* 2.2.1. Sei R ein komutativer Ring. Ein Polynom über R in einer Variablen (oder Unbekannten) ist ein Ausdruck der Form

$$f = a_n X^n + \ldots + a_1 X + a_0$$

wobei X ein Symbol ist, das man Variable des Polynoms nennt, und welches unabhängig von jedem Element des Rings R ist; die Koeffizienten a_i sind Elemente in R; n ist eine natürliche Zahl. Manchmal schreibt man auch

$$f = \sum_{i \geqslant 0} a_i X^i$$

und fordert, daß die Koeffizienten a_i fast alle gleich Null sind. Dies bedeuted insbesondere, daß die Summe endlich ist.

Die Menge

$$R[X] = \left\{ f = \sum_{i \geqslant 0} a_i X^i \;\middle|\; \text{fast alle } a_i = 0 \right\}$$

ist ein kommutativer Ring vermöge der Verknüpfungen

$$\begin{aligned} (\sum_{i \geqslant 0} a_i X^i) + (\sum_{i \geqslant 0} b_i X^i) &= \sum_{i \geqslant 0} (a_i + b_i) X^i \\ (\sum_{i \geqslant 0} a_i X^i) \cdot (\sum_{i \geqslant 0} b_i X^i) &= \sum_{i \geqslant 0} (\sum_{k+l=i} a_k b_l) X^i \end{aligned}$$

und des additiven beziehungsweise multiplikativen Inversen

$$\begin{aligned} 1_{R[X]} &= 1X^0 = 1 \\ 0_{R[X]} &= 0X^0 = 0 \end{aligned}$$

Via dem injektiven Homomorphismus

$$R \hookrightarrow R[X], a \mapsto aX^0$$

fassen wir R als Unterring von $R[X]$ auf.

Es ist auch möglich, Polynomringe in mehreren Variablen zu betrachten. Dies lässt sich rekursiv wie folgt definieren

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

Man betrachtet hier also Polynome in der Variablen X_n mit Koeffizienten in dem kommutativen Ring $R[X_1, \ldots, X_{n-1}]$. Wir werden später noch eine Definition via Multipotenzen kennen lernen.

In diesem Abschnitt werden wir die oben genannten Konzepte formalisieren.

2.2.1 Monoidalgebren, Polynomalgebren

Sei R ein kommutativer Ring, $(M, \cdot)$ ein Monoid mit neutralem Element e. Wir konstruieren einen Ring $R[M]$, so daß ein injektiver Ringhomomorphismus $R \to Z(R[M])$ und ein injektiver Monoidhomomorphismus $M \to (R[M], \cdot)$ existieren und $R[M]$ von ihren Bildern erzeugt wird.

Sei $R[M]$ die Menge aller Abbildungen $f : M \to R$ mit $f(i) = 0$ für fast alle $i \in M$

$$R[M] := \left\{ f : M \to R \;\middle|\; f(i) = 0 \text{ für fast alle } i \in M \right\}.$$

Spezielle Elemente in $R[M]$ sind b_i, $i \in M$ mit

$$b_i(j) = \delta_{ij} \quad \text{für } j \in M.$$

$R[M]$ ist ein Ring bezüglich

$$\begin{aligned} (f + f')(i) &= f(i) + f'(i), \quad \text{mit Nullelement } 0_{R[M]}(i) = 0 \\ ff'(i) &= \sum_{j,k \in M; jk = i} f(j) f'(k), \quad \text{mit Einselement } 1_{R[M]} = b_e = \delta_{e-}. \end{aligned}$$

Man hat einen injektiven Ringhomomorphismus

$$\varphi : R \to Z(R[M]), \varphi(r) = \delta_{-e} r$$

das heißt definiert durch $\varphi(r)(i) = \delta_{ie} r$. Es gilt $\varphi(1_R) = 1_{R[M]}$, denn $\varphi(1_R)(i) = \delta_{ie} = b_e(i)$ für alle $i \in M$. Es gilt $\varphi(r) \in Z(R[M])$, denn

$$(f\varphi(r))(i) = \sum_{jk=i} f(j)\varphi(r)(k) = \sum_{jk=i} f(j) r \delta_{ke} = f(i) r = r f(i) = (\varphi(r) f)(i)$$

für alle $i \in M$. Außerdem

$$\varphi(r)\varphi(r')(i) = \varphi(r)(i) r' = r \delta_{ie} r' = r r' \delta_{ie} = \varphi(rr')(i).$$

Damit ist $R[M]$ eine R-Algebra. Man definiert wieder $rf = \varphi(r) f$ für $r \in R$, $f \in R[M]$ und $(rf)(i) = r f(i)$ für alle $i \in M$. Ferner hat man den injektiven Monoidhomomorphismus

$$M \to R[M], i \mapsto b_i$$

Jedes Element $f \in R[M]$ hat eine eindeutige Darstellung $f = \sum_{i \in M} f(i) b_i$, denn es gilt

$$\sum_{i \in M} f(i) b_i(j) = \sum_{i \in M} f(i) \delta_{ij} = f(j)$$

für alle $j \in M$ und ist andererseits $f = \sum_{i \in M} r_i b_i$ mit $r_i \in R$ fast alle 0, dann

$$f(j) = (\sum_{i \in M} r_i b_i)(j) = \sum_{i \in M} r_i \delta_{ij} = r_j$$

für alle $j \in M$. Man schreibt auch f_i statt $f(i)$ und erhällt $f = \sum_{i\in M} f_i b_i$. Ist auch $f' = \sum_{i\in M} f'_i b_i$, dann gilt also

$$\begin{aligned} f + f' &= \sum_{i\in M} (f_i + f'_i) b_i \\ f \cdot f' &= \sum_{i,j\in M} f_i f'_j b_i b_j = \sum_{i\in M} (\sum_{j\cdot k=i} f_j f'_k) b_i \end{aligned}$$

Nullelement ist $0 = \sum_{i\in M} 0 b_i$, und Einselement ist $1 = b_e = 1 \cdot b_e$. Der Ring $R[M]$ heißt die Monoidalgebra von M über R und ist genau dann kommutativ, wenn M abelsch ist.

Sei jetzt $n \in \mathbb{N}$ und $M = (\mathbb{N}_0^n, +)$, sei $\varepsilon_k = (0, \ldots, 0, 1, 0, \ldots, 0)$ mit 1 an der k-ten Stelle, $1 \leqslant k \leqslant n$, sei $X_k = b_{\varepsilon_k}$, $1 \leqslant k \leqslant n$. Für $i = (i_1, \ldots, i_n) \in \mathbb{N}_0^n$ gilt

$$i = i_1\varepsilon_1 + \ldots + i_n\varepsilon_n = X_1^{i_1} \cdots X_n^{i_n}.$$

Jedes Element $f \in R[\mathbb{N}_0^n]$ hat eine eindeutige Darstellung

$$f = \sum_{i_1,\ldots,i_n \geqslant 0} f_{i_1\ldots i_n} X_1^{i_1} \cdots X_n^{i_n}$$

mit $f_{i_1\ldots i_n} \in R$ fast alle 0. Man setzt $R[X_1, \ldots, X_n]$ statt $R[\mathbb{N}_0^n]$, und man nennt diese Algebra die Polynomalgebra in den Unbestimmten $X_1, \ldots, X_n$ über R. Man hat folgende Verknüpfungen:

$$\begin{aligned} f + f' &= \sum_{i_1,\ldots,i_n \geqslant 0} (f_{i_1\ldots i_n} + f'_{i_1\ldots i_n}) X_1^{i_1} \cdots X_n^{i_n} \\ f \cdot f' &= \sum_{i_1,\ldots,i_n \geqslant 0} (\sum_{j_l + k_l = i_l} f_{j_1\ldots j_n} f'_{k_1\ldots k_n}) X_1^{i_1} \cdots X_n^{i_n} \\ rf &= \sum_{i_1,\ldots,i_n \geqslant 0} r f_{i_1\ldots i_n} X_1^{i_1} \cdots X_n^{i_n}, r \in R \end{aligned}$$

Die Polynome $X_1^{i_1} \cdots X_n^{i_n}$ heißen Monome. Für $f = \sum_{i_1,\ldots,i_n \geqslant 0} f_{i_1\ldots i_n} X_1^{i_1} \cdots X_n^{i_n}$ und $k \in \mathbb{N}_0$ sei

$$f_{(k)} = \sum_{\substack{i_1,\ldots,i_n \geqslant 0 \\ i_1 + \cdots + i_n = k}} f_{i_1\ldots i_n} X_1^{i_1} \cdots X_n^{i_n}$$

die k-te homogene Komponente von f, es gilt $f = \sum_{k\in\mathbb{N}_0} f_{(k)}$. f heißt homogen, falls es $k \geqslant 0$ gibt mit $f = f_{(k)}$. Die Polynome $r \cdot 1 = r$ heißen konstant.

Definition 2.2.2. Sei $f \in R[X_1, \ldots, X_n]$ und $f = \sum_{k\in\mathbb{N}_0} f_{(k)}$ die Zerlegung in homogene Komponenten. Der (totale) Grad von f ist definiert durch

$$\deg(f) = \begin{cases} \max\{k \in \mathbb{N} \mid f_{(k)} \neq 0\} & \text{falls } f \neq 0 \\ -\infty & \text{falls } f = 0 \end{cases}$$

Beispiel 2.2.3. Sei $f = X^3Y + 2XY^2 - X^2Y + X - 3Y + 1 \in \mathbb{Z}[X, Y]$, dann ist $f_{(0)} = 1$, $f_{(1)} = X - 3Y$, $f_{(2)} = 0$, $f_{(3)} = 2XY^2 - X^2Y$, $f_{(4)} = X^3Y$. Also $\deg(f) = 4$.

Proposition 2.2.4. *Seien $f, f' \in R[X_1, \ldots, X_n]$.*

(a) $\deg(f + f') \leqslant \max\{\deg(f), \deg(f')\}$.

(b) Stets gilt $\deg(ff') \leqslant \deg(f) + \deg(f')$.
Sind $f, f' \neq 0$, $p = \deg(f)$, $f_{(p)} \neq 0$, $q = \deg(f')$, $f'_{(q)} \neq 0$ und $f_{(p)} f'_{(q)} \neq 0$, dann gilt $\deg(ff') = \deg(f) + \deg(f')$.

Beweis. **Zu (a):** Das ist klar.
Zu (b): Es gilt $f = \sum_{i=0}^{p} f_{(i)}$ und $f' = \sum_{j=0}^{q}$, also

$$ff' = \sum_{\substack{0 \leqslant i \leqslant p \\ 0 \leqslant j \leqslant q}} f_{(i)} f'_{(j)} = \sum_{k=o}^{p+q} \Big(\sum_{i+j=k} f_{(i)} f'_{(j)} \Big),$$

und $(ff')_{(p+q)} = f_{(p)} f'_{(q)}$. Wenn dies $\neq 0$, also $\deg(ff') = p + q = \deg(f) + \deg(f')$. □

Sei speziell $n = 1$ und $X = X_1$. Sei $0 \neq f \in R[X]$, $f = \sum_{i=0}^{m} r_i X^i$, mit $r_m \neq 0$. Dann ist $\deg(f) = m$, r_m bzw. r_0 heißt der höchste bzw. konstante Koeffizient von f. Das Polynom f heißt normiert, wenn $r_m = 1$ ist.

Bemerkung 2.2.5. Sei $n > 1$. Wir fassen $R[X_1, \ldots, X_{n-1}]$ als Unterring von $R[X_1, \ldots, X_n]$ auf. Jedes Polynom $f \in R[X_1, \ldots, X_n]$ hat eine eindeutige Darstellung

$$f = \sum_{k \geqslant 0} g_k X_n^k$$

mit $g_k \in R[X_1, \ldots, X_{n-1}]$ fast alle 0. Denn

$$f = \sum_{i_1, \ldots, i_n \geqslant 0} f_{i_1 \ldots i_n} X_1^{i_1} \cdots X_n^{i_n} = \sum_{i_n \geqslant 0} \Big(\sum_{i_1, \ldots, i_{n-1} \geqslant 0} f_{i_1 \ldots i_{n-1} i_n} X_1^{i_1} \cdots X_{n-1}^{i_{n-1}} \Big) X_n^{i_n} = \sum_{i_n \geqslant 0} g_{i_n} X_n^{i_n}$$

mit $g_{i_n} = \sum_{i_1, \ldots, i_{n-1} \geqslant 0} f_{i_1 \ldots i_{n-1} i_n} X_1^{i_1} \cdots X_{n-1}^{i_{n-1}}$. Die Eindeutigkeit ist klar. Also gilt

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

2.2.2 Einsetzen von Elementen

Satz 2.2.6 (Universelle Eigenschaft von Polynomalgebren)**.** *Sei R ein kommutativer Ring, S eine kommutative R-Algebra, sei $n \in \mathbb{N}$ und $(s_1, \ldots, s_n) \in S^n$. Dann gibt es genau einen R-Algebren-Homomorphismus $\rho : R[X_1, \ldots, X_n] \to S$, mit $\rho(X_i) = s_i$, $1 \leqslant i \leqslant n$.*

Beweis. Für $f = \sum_{i_1, \ldots, i_n \geqslant 0} X_1^{i_1} \cdots X_n^{i_n}$ sei

$$\rho(f) = \sum_{i_1, \ldots, i_n \geqslant 0} s_1^{i_1} \cdots s_n^{i_n}.$$

Dies ist wohldefiniert, Ringhomomorphismus und $\rho(rf) = r\rho(f)$ für alle $r \in R$. Ist auch $\rho' : R[X_1, \ldots, X_n] \to S$ ein R-Algebrenhomomorphismus mit $\rho'(X_i) = s_i$, dann gilt

$$\rho'(f) = \sum_{i_1, \ldots, i_n \geqslant 0} r_{i_1 \ldots i_n} \rho'(X_1^{i_1}) \cdots \rho'(X_n^{i_n}) = \sum_{i_1, \ldots, i_n \geqslant 0} r_{i_1 \ldots i_n} \rho'(X_1)^{i_1} \cdots \rho'(X_n)^{i_n} = \sum_{i_1, \ldots, i_n \geqslant 0} r_{i_1 \ldots i_n} s_1^{i_1} \cdots s_n^{i_n} = \rho(f)$$

für alle $f \in R[X_1, \ldots, X_n]$. Also gilt $\rho' = \rho$. □

Man nennt ρ auch Einsetzungshomomorphismus zu $(s_1, \ldots, s_n)$, und man schreibt $f(s_1, \ldots, s_n) = \rho(f)$, sowie $R[s_1, \ldots, s_n] = \mathrm{im}(\rho)$. $R[s_1, \ldots, s_n]$ ist der kleinste Unterring von S, der $R.1$ und $s_1, \ldots, s_n$ enthält. Er heißt der von $s_1, \ldots, s_n$ erzeugte Unterring von S über R. $(s_1, \ldots, s_n)$ heißt Nullstelle von f, falls $f(s_1, \ldots, s_n) = \rho(f) = 0$ ist.

2.2.3 Division mit Rest in $R[X]$

Satz 2.2.7. *Sei R ein kommutativer Ring, $0 \neq f \in R[X]$ ein Polynom, dessen höchster Koeffizient eine Einheit in R ist. Zu jedem $g \in R[X]$ gibt es dann eindeutig bestimmte Polynome $q, h \in R[X]$ mit $g = qf + h$ und $\deg(h) < \deg(f)$.*

Beweis. Sei $m = \deg(f)$, $a \in R^\times$ der höchste Koeffizient von f. Sei $g \in R[X]$. Induktion nach $n = \deg(g)$. Die Behauptung ist klar, wenn $n < m$. Sei $n \geqslant m$, sei r der höchste Keffizient von g, sei $g' = g - ra^{-1}X^{n-m}f$. Dann ist $\deg(g') < \deg(g)$. Nach Induktionsannahme gibt es $q', h \in R[X]$ mit $g' = q'f + h$, $\deg(h) < \deg(f)$. Mit $q = ra^{-1}X^{n-m} + q'$ gilt dann $g = qf + h$.
Sind auch $\widetilde{q}, \widetilde{h} \in R[X]$ mit $g = \widetilde{q}f + \widetilde{h}$, dann $(q - \widetilde{q})f = \widetilde{h} - h$. Da $\deg(h) < \deg(f)$ und der höchste Koeffizient von f eine Einheit ist, muß $q = \widetilde{q}$ sein, es folgt $h = \widetilde{h}$. □

Folgerung 2.2.8. *Seien $f \in R[X]$, $c \in R$.*

(a) Es gibt $g \in R[X]$ mit $f = (X - c)g + f(c)$.

(b) c ist genau dann Nullstelle von f, wenn es $g \in R[X]$ gibt mit $f = (X - c)g$.

Beweis. **Zu (a):** Es gibt $g, h \in R[X]$ mit $f = (X - c)g + h$ mit $\deg(h) < 1$. Es folgt $h = h(c) = f(c)$.
Zu (b): Dies folgt aus (a). □

Folgerung 2.2.9. *Sei K ein Körper, $0 \neq f \in K[X]$. Zu jedem $g \in K[X]$ gibt es eindeutig bestimmte $q, h \in K[X]$ mit $g = qf + h$ und $\deg(h) < \deg(f)$.*

Beweis. Dies folgt aus dem Satz. □

Beispiel* 2.2.10. Seien $p(X) = X^{500} - 2X^{301} + 1$ und $q(X) = X^2 - 1$ in $\mathbb{Q}[X]$. Wir berechnen den Rest von $p(X)$ bei Division mit $q(X)$.
Dazu betrachten wir den Faktorring $\mathbb{Q}[X]/(q)$, und bemerken, daß zwei Elemente $f_1, f_2 \in \mathbb{Q}[X]$ modulo (q) gleich sind, wenn sie bei Division durch q den gleichen Rest haben, bzw. wenn $f_1 - f_2$ durch q teilbar ist. Insbesondere ist jedes Polynom $f \in \mathbb{Q}[X]$ modulo (q) gleich seinem Rest bei Division durch q. Sei nun r der Rest von p bei Division durch q, dh. $p = sq + r$ in $\mathbb{Q}[X]$ mit $\deg(r) < \deg(q) = 2$. Dann gilt

$$r + (q) = p + (q).$$

Wir finden r, indem wir einen bezüglich des Grads minimalen Repräsentanten der Klasse $p+(q)$ berechnen. Dafür bemerken wir noch, dass gilt $x^2 + (q) = 1 + (q)$.

$$\begin{aligned}
p + (q) &= X^{500} - 2X^{301} + 1 + (q) \\
&= (X^{500} + (q)) - (2 + (q)) \cdot (X^{301} + q) + (1 + (q)) \\
&= ((X^2)^{250} + (q)) - (2 + (q)) \cdot ((X^2)^{150} + q)(X + (q)) + (1 + (q)) \\
&= (1^{250} + (q)) - (2 + (q)) \cdot (1^{150} + q)(X + (q)) + (1 + (q)) \\
&= (1 + (q)) - (2 + (q)) \cdot (1 + q)(X + (q)) + (1 + (q)) \\
&= (1 + (q)) - (2X + (q)) + (1 + (q)) = 2 - 2X + (q)
\end{aligned}$$

Also ist die Differenz $r - (2 - 2X)$ durch q teilbar. Da aber beide Grad < 2 haben, gilt $r - (2 - 2X) = 0$ und $r = 2 - 2X$.

Beispiel* 2.2.11. Es seien K ein Körper und $K[X]$ der Polynomring in einer Unbekannten. Sei $n, m \in \mathbb{N}_0$. Ist $m > 1$, dann ist $X^r - 1$ der Rest bei Division von $X^n - 1$ durch $X^m - 1$, wobei r der Rest bei Division von n durch m ist.
Sei $n = qm + r$ im euklidischen Ring $\mathbb{Z}$ mit $r < m$. Und sei $X^n - 1 = g(X^m - 1) + h$ mit $\deg(h) < \deg(X^m - 1) = m$. Diesmal arbeiten wir im Restklassenring $K[X]/(X^m - 1)$. Es gilt wieder $X^n - 1 \equiv h \mod (X^m - 1)$ und $X^m \equiv 1 \mod (X^m - 1)$. Damit berechnen wir einen minimalen Repräsentanten:

$$\begin{aligned}
X^n - 1 &= X^{mq+r} - 1 \\
&= (X^m)^q X^r - 1 \\
&\equiv X^r - 1 \mod (X^m - 1)
\end{aligned}$$

Es folgt für den Rest h, daß $h \equiv X^r - 1 \mod (X^m - 1)$, also ist die Differenz $h - (X^r - 1)$ durch $X^m - 1$ teilbar. Aber da sowohl h, als auch $X^r - 1$ Grad kleiner m haben, gilt $h - (X^r - 1) = 0$, also $h = X^r - 1$.

2.3 Integritätsringe

2.3.1 Definition und Beispiele

Definition 2.3.1. Ein kommutativer Ring heißt Integritätsring oder Integritätsbereich, wenn $1 \neq 0$ und $(R\backslash\{0\}, \cdot)$ Untermonoid von $(R, \cdot)$ ist, das heißt, wenn $1 \neq 0$ und für alle $r, s \in R\backslash\{0\}$ gilt $rs \neq 0$.

Proposition 2.3.2. *(a) Ein kommutativer Ring R ist genau dann Integritätsbereich, wenn $1 \neq 0$ und für alle $r, s, t \in R$ mit $rs = rt$ und $r \neq 0$ folgt $s = t$.*

(b) Ein endlicher Integritätsbereich ist ein Körper.*

Beweis. **Zu (a):** „$\Rightarrow$“Ist $rs = rt$, dann $r(s - t) = 0$. Also $s - t = 0$ falls $r \neq 0$. Damit $s = t$.
„$\Leftarrow$“Ist $r, s \in R\backslash\{0\}$, dann ist $rs \neq r0 = 0$.
Zu (b): Sei R endlicher Integritätsring, $0 \neq s \in R$, dann ist die Abbildung $R \to R$, $r \mapsto rs$, nach (a) injektiv, also auch surjektiv. Dann gibt es $s \in R$ mit $rs = 1$. □

Beispiele 2.3.3. (a) $\mathbb{Z}$ ist ein Integritätsbereich, Körper sind Integritätsbereiche.

(b) Unterringe von Integritätsringen sind Integritätsringe. Insbesondere sind Unterringe von Körpern Integritätsringe.

(c) Sei $n \in \mathbb{N}_0$. $\mathbb{Z}/n\mathbb{Z}$ ist genau dann Integritätsbereich, wenn $n = 0$ oder n Primzahl ist.

Beispiel* 2.3.4. Sei A ein Integritätsring, der nur eine endliche Anzahl von Idealen hat. Dann ist A bereits ein Körper.

Beweis. Sei $x \in A\backslash 0$. Betrachte die Ideale $I_n = (x^n) \subset A$. Da A nur endlich viele Ideale besitzt, muß es $n < m \in \mathbb{N}$ geben, so daß die von x^n und x^m erzeugten Ideale übereinstimmen, dh. $(x^n) = (x^m) \subset A$. Insbesondere ist $x^m \in (x^n)$, das heißt, es gibt $a \in A$ it $x^n = x^m a$. Es folgt

$$x^n(1 - x^q a) = x^n - x^m a = 0,$$

mit $q = m - n > 0$. Da A ein Integritätsring ist, folgt $x^q a = 1$. Also ist x in A invertierbar mit Inversem $x^{q-1}a$. □

Proposition 2.3.5. *Sei R Integritätsring, $n \in \mathbb{N}$.*

(a) $R[X_1, \ldots, X_n]$ ist Integritätsring, für $f, g \in R[X_1, \ldots, X_n]$ gilt $\deg(fg) = \deg(f) + \deg(g)$.

(b) $R[X_1, \ldots, X_n]^\times = R^\times$.

Beweis. **Zu (a):** Induktion nach n: Sei zunächst $n = 1$. Seien $f = \sum_{i=0}^{p} r_i X^i$, $r_p \neq 0$, $g = \sum_{j=0}^{q} s_j X^j$, $s_q \neq 0$, Polynome in $R[X]$. Dann ist $r_p s_q \neq 0$ der höchste Koeffizient von fg, also ist $fg \neq 0$ und $\deg(fg) = p + q = \deg(f) + \deg(g)$. Für $f = 0$ oder $g = 0$ ist diese Gleichung trivial.
Sei nun $n > 1$. Nach Induktionsannahme ist $R[X_1, \ldots, X_{n-1}]$ Integritätsring. Wie oben gezeigt, ist dann $R[X_1, \ldots, X_n] = R[X_1, \ldots, X_{n-1}][X_n]$ ebenfalls Integritätsring.
Seien $f, g \in R[X_1, \ldots, X_n]\backslash\{0\}$, $\deg(f) = p$, $\deg(g) = q$, dann ist $f_{(p)} \neq 0$ und $g_{(q)} \neq 0$, also $f_{(p)} g_{(q)} \neq 0$. Nach Proposition 2.2.4 ist dann $\deg(fg) = \deg(f) + \deg(g)$. Für $f = 0$ und $g = 0$ ist dies klar.
Zu (b): Die Inklusion „$\supset$“ist klar. Für die Inklusion „$\subset$“sei $f \in R[X_1, \ldots, X_n]^\times$. Dann gibt es $g \in R[X_1, \ldots, X_n]$ mit $fg = 1$. Es folgt $0 = \deg(1) = \deg(f) + \deg(g)$, also $\deg(f) = \deg(g) = 0$, also $f, g \in R^\times$. □

Folgerung 2.3.6. *Sei $n \in \mathbb{N}$.*

(a) Für jeden Körper ist $K[X_1, \ldots, X_n]$ Integritätsbereich und $K[X_1, \ldots, X_n]^\times = K^\times$.

(b) $\mathbb{Z}[X_1, \ldots, X_n]$ ist Integritätsbereich und $\mathbb{Z}[X_1, \ldots, X_n]^\times = \mathbb{Z}^\times$.

Proposition 2.3.7. *Sei R Integritätsring.*

(a) Jedes Polynom $0 \neq f \in R[X]$ hat höchstens $\deg(f)$ *Nullstellen.*

(b) Seien $f, g \in R[X]$ Polynome vom Grad $\leqslant n$. Wenn es $a_1, \ldots, a_{n+1} \in R$ gibt mit $f(a_i) = g(a_i)$ für $1 \leqslant i \leqslant n + 1$, dann ist $f = g$.

Beweis. **Zu (a):** Induktion nach $m = \deg(f)$. Ist $\deg(f) = 0$, dann hat f keine Nullstelle. Sei $m > 0$. Falls f keine Nullstelle hat, dann ist das klar. Falls f eine Nullstelle $a \in R$ hat, dann existiert $g \in R[X]$ mit $f = (X-a)g$, dann ist $\deg(g) = m-1$. Ist b Nullstelle von f, $b \neq a$, dann $0 = f(b) = (b-a)g(b)$ und $g(b) = 0$. Also sind die Nullstellen von f ungleich a auch Nullstellen von g. Nach Induktionsannahme hat g höchstens $m-1$ Nullstellen, also hat f höchstens m Nullstellen.
Zu (b): $f-g$ hat $n+1$ Nullstellen, $a_1, \ldots, a_{n+1}$, da $\deg(f-g) \leqslant n$ folgt nach (a) $f-g = 0$, also $f = g$. □

Beispiel* **2.3.8.** Eine kommutative integre $\mathbb{R}$-Algebra A von Dimension $n \geqslant 2$ ist bereits isomorph zu $\mathbb{C}$.

Beweis. Wir identifizieren hier $\mathbb{R}$ mit $\mathbb{R}\cdot 1$, wobei 1 das Einselement von A ist. Um die Aussage zu sehen, zeigt man zunächst, daß jedes Element $a \in A\backslash\{0\}$ invertierbar ist. Dann überlegt man sich, daß für jedes Element $a \in A\backslash(\mathbb{R}\cdot 1)$ die Menge $\{1, a\}$ linear unabhängig über $\mathbb{R}$ ist, aber die Menge $\{1, a, a^2\}$ linear abhängig. Daraus folgert man, daß in dem $\mathbb{R}$-Vektorraum $\langle 1, a\rangle$ ein Element i existiert mit $i^2 = -1$. Man folgert, daß $\dim(A) = 2$ und daß A isomorph zu $\mathbb{C}$ ist. □

2.3.2 Euklidische Ringe

Definition 2.3.9. Ein Integritätsring R heißt euklidisch, wenn es eine Abbildung $\delta : R\backslash\{0\} \to \mathbb{N}_0$ gibt, so daß gilt: Für alle $a, b \in R$, $b \neq 0$, gibt es $q, r \in R$ mit $a = bq + r$ und wenn $r \neq 0$ ist, dann $\delta(r) < \delta(b)$. Eine solche Abbildung heißt euklidische Norm.

Beispiele 2.3.10. (a) $\mathbb{Z}$ ist euklidisch bezüglich $\delta : \mathbb{Z} \to \mathbb{N}_0$, $z \mapsto |z|$.

(b) Sei K ein Körper. $K[X]$ ist euklidisch bezüglich $K[X]\backslash\{0\} \to \mathbb{N}_0$, $f \mapsto \deg(f)$.

(c) $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} = \mathbb{Z} \oplus \mathbb{Z}\, i$ ist Unterring von $\mathbb{C}$, der $\mathbb{Z}$ enthält; er heißt Ring der ganzen Gaußschen Zahlen. $\delta : \mathbb{Z}[i] \to \mathbb{N}_0$, $x = a + bi \mapsto x\overline{x} = a^2 + b^2$ ist euklidische Norm.

Beweis. Seien $x = a + bi \in \mathbb{Z}[i]$ und $y = c + di \in \mathbb{Z}[i]\backslash\{0\}$. Dann ist $\frac{x}{y} = \frac{x\overline{y}}{y\overline{y}} = \frac{x\overline{y}}{c^2+d^2} = s + ti$ mit $s, t \in \mathbb{Q}$. Es gibt $u, v \in \mathbb{Z}$ mit $|s-u| \leqslant \frac{1}{2}$ und $|t-v| \leqslant \frac{1}{2}$; sei $q = u+vi \in \mathbb{Z}[i]$. Dann gilt $x - qy \in \mathbb{Z}[i]$, $x = qy + (x - qy)$, und $|\frac{x}{y} - q|^2 = |s + ti - (u + vi)|^2 = (s-u)^2 + (t-v)^2 \leqslant \frac{1}{2}$. Also ist $|\frac{x}{y} - q|^2 < 1$ und so $|x - qy|^2 < |y|^2$, also $\delta(x - qy) < \delta(y)$. □

Satz 2.3.11. *Sei R euklidischer Ring. Jedes Ideal $A \subset R$ ist Hauptideal, das heißt, es gibt $a \in A$ so daß $A = (a)$.*

Beweis. Sei $\delta : R\backslash\{0\} \to \mathbb{N}_0$ euklidische Norm, $A \neq 0$ ein Ideal, sei $0 \neq a \in A$, so daß $\delta(a)$ minimal ist. Wir zeigen, daß gilt $A = (a)$. Es ist klar, daß $(a) \subset A$. Sei andererseit $x \in A$. Dann gibt es $q, r \in R$ mit $x = qa + r$ und $\delta(r) < \delta(a)$. Falls $r \neq 0$ gilt $r = x - qa \in A$. Widerspruch zur Wahl von a. Also ist $r = 0$. Es folgt $x = qa \in (a)$. □

Definition 2.3.12. Ein Integritätsring R heißt Hauptidealring, wenn jedes Ideal von R Hauptideal ist.

Beispiele 2.3.13. Für Hauptidealringe sind $\mathbb{Z}$, $\mathbb{Z}[i]$, $K[X]$ für einen Körper K: Dagegen sind $\mathbb{Z}[X]$ und $K[X, Y]$ keine Hauptidealringe.

Folgerung 2.3.14. *Sei K ein Körper. Zu jedem Ideal $0 \neq A \subset K[X]$ gibt es genau ein normiertes Polynom $f \in A$ mit $A = (f)$.*

Beweis. Es gibt $g \in A$ mit $A = (g)$. Sei $\alpha \in K$ der höchste Koeffizient von g, dann ist $\alpha^{-1}g$ normiert, und $A = (\alpha^{-1}g)$. Seien $g_1, g_2 \in A$ normiert mit $(g_1) = (g_2) = A$. Dann gibt es $u, v \in K[X]$ so daß $g_1 = ug_2$ und $g_2 = vg_1$. Also ist $g_1 = uvg_1$, damit $1 = uv$ und $u, v \in K^\times$, $u = v = 1$, folglich $g_1 = g_2$. □

Merkregel*: Es gelten folgende Inklusionen für kommutative Ringe:

Körper $\subset$ Euklidische Ringe $\subset$ Hauptidealringe $\subset$ faktorielle Ringe $\subset$ Integritätsringe

2.4 Ringe von Brüchen

2.4.1 Konstruktion des Quotientenrings

Definition 2.4.1. Sei R ein kommutativer Ring. Eine Teilmenge $S \subset R$ heißt multiplikativ abgeschlossen, wenn $\emptyset \neq S$ und S Untermonoid von $(R\backslash\{0\})$ ist.

Beispiele 2.4.2. (a) Ist R Integritätsring, dann ist $R\backslash\{0\}$ multiplikativ abgeschlossen.

(b) Sei R kommutativer Ring, $s \in R$. $S = \{s^n \mid n \in \mathbb{N}_0\}$ ist genau dann multiplikativ abgschlossen, wenn $s^n \neq 0$ für alle $n \in \mathbb{N}$ ist, das heißt, wenn s nicht nilpotent ist. Dies ist in einem Integritätsring für alle $s \neq 0$ erfüllt.

(c) Sei $p \in \mathbb{N}$ Primzahl. Dann ist $\mathbb{Z}\backslash(p)$ multiplikativ abgeschlossene Teilmenge von $\mathbb{Z}$.

Sei R kommutativer Ring, $S \subset R$ multiplikativ abgeschlossene Teilmenge. Wir definieren auf $R \times S$ eine Äquivalenzrelation durch

$$(r, s) \sim (r', s') \text{ genau dann wenn es } t \in S \text{ gibt, so daß } (rs' - r's)t = 0.$$

Transitivität: Sei auch $(r', s') \sim (r'', s'')$, mit $(r's'' - r''s')t' = 0$ für $t' \in S$. Dann ist $(rs'' - r''s)s'tt' = (rs' - r's)s''tt' + (r's'' - r''s')stt' = 0$ und $s'tt' \in S$ also $(r, s) \sim (r'', s'')$. Alles andere ist klar.
Man setzt $R_S = R \times S/\sim$ und bezeichnet die Äquivalenzklasse von (r, s) mit $\frac{r}{s}$. Also gilt $\frac{r}{s} = \frac{r'}{s'}$ genau dann wenn es $t \in S$ gibt mit $(rs' - r's)t = 0$.

Satz 2.4.3. *(a) R_S ist kommutativer Ring bezüglich $\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1s_2+r_2s_1}{s_1s_2}$ und $\frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \frac{r_1r_2}{s_1s_2}$, Nullelement ist $\frac{0}{1}$, Einselement ist $\frac{1}{1}$.*

(b) Die Abbildung $i : R \to R_S$, $r \mapsto \frac{r}{1}$ ist Ringhomomorphismus mit $\ker(i) = \{r \in R \mid \exists s \in S : rs = 0\}$. Für alle $s \in S$ ist $i(s) = \frac{s}{1}$ Einheit von R_S.

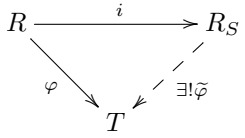
Definition 2.4.4. R_S heißt Quotientenring von R nach S, $i : R \to R_S$ heißt kanonischer Homomorphismus.

Beweis. **Zu (a):** Die Addition ist wohldefiniert: Sei $\frac{r_1}{s_1} = \frac{r_1'}{s_1'}$ und $\frac{r_2}{s_2} = \frac{r_2'}{s_2'}$, dann gibt es $t_1, t_2 \in S$ mit $(r_1s_1' - r_1's_1)t_1 = 0$ und $(r_2s_2' - r_2's_2)t_2 = 0$. Dann

$$((r_1s_2 + s_1r_2)s_1's_2' - (r_1's_2' + r_2's_1')s_1s_2)\, t_1t_2 = ((r_1s_1' - r_1's_1)s_2s_2' + (r_2s_2' - r_2's_2)s_1s_1')\, t_1t_2 = 0$$

und $t_1t_2 \in S$, also $\frac{r_1s_2+r_2s_1}{s_1s_2} = \frac{r_1's_2'+r_2's_1'}{s_1's_2'}$. Genauso für Multiplikation. Die Ringaxiome prüft man nach.
Zu (b): Es gilt $i(r_1 + r_2) = \frac{r_1+r_2}{1} = \frac{r_1}{1} + \frac{r_2}{1} = i(r_1) + i(r_2)$, und $i(1) = \frac{1}{1}$ ist Einselement von R_S. Außerdem $i(r) = 0$ genau dann, wenn $\frac{r}{1} = 0$, genau dann, wenn es $s \in S$ gibt mit $rs = 0$. Für $s \in S$ gilt: $i(s) \cdot \frac{1}{s} = \frac{s}{1} \cdot \frac{1}{s} = \frac{s}{s} = \frac{1}{1}$, also ist $i(s) \in R_S^\times$. □

Satz 2.4.5 (Universelle Eigenschaft des Quotientenrings)**.** *Sei R kommutativer Ring, $S \subset R$ multiplikativ abgeschlossene Teilmenge. Ist T ein kommutativer Ring, $\varphi : R \to T$ Ringhomomorphismus mit $\varphi(S) \subset T^\times$, dann gibt es genau einen Ringhomomorphismus $\widetilde{\varphi} : R_S \to T$ mit $\widetilde{\varphi} \circ i = \varphi$, das heißt, das Diagramm*



kommutiert.

Beweis. **Existenz von $\widetilde{\varphi}$:** Für $\frac{r}{s} \in R_S$ setzt man $\widetilde{\varphi}\left(\frac{r}{s}\right) = \varphi(r)\varphi(s)^{-1}$.
Wohldefiniertheit: Sei $\frac{r}{s} = \frac{r'}{s'}$. Dann gibt es $t \in S$ mit $(rs' - r's)t = 0$, also

$$\begin{aligned}
(\varphi(r)\varphi(s') - \varphi(r')\varphi(s))\varphi(t) &= 0 \quad \text{also} \\
\varphi(r)\varphi(s') &= \varphi(r')\varphi(s) \quad \text{also} \\
\varphi(r)\varphi(s)^{-1} &= \varphi(r')\varphi^{-1}(s') \quad \text{also} \\
\widetilde{\varphi}\left(\frac{r}{s}\right) &= \widetilde{\varphi}\left(\frac{r'}{s'}\right)
\end{aligned}$$

Außerdem

$$\begin{aligned}\widetilde{\varphi}\left(\frac{r_1}{s_1}+\frac{r_2}{s_2}\right) &= \widetilde{\varphi}\left(\frac{r_1s_2+r_2s_1}{s_1s_2}\right)\\ &= \varphi(r_1s_2+r_2s_1)\varphi(s_1s_2)^{-1}\\ &= \left(\varphi(r_1)\varphi(s_2)+\varphi(r_2)\varphi(s_1)\right)\varphi(s_1)^{-1}\varphi(s_2)^{-1}\\ &= \varphi(r_1)\varphi(s_1)^{-1}+\varphi(r_2)\varphi(s_2)^{-1}=\widetilde{\varphi}\left(\frac{r_1}{s_1}\right)+\widetilde{\varphi}\left(\frac{r_2}{s_2}\right)\end{aligned}$$

etc. Wegen $(\widetilde{\varphi}\circ i)(r)=\widetilde{\varphi}\left(\frac{r}{1}\right)=\varphi(r)\varphi(1)^{-1}=\varphi(r)$ für alle $r\in R$ gilt $\widetilde{\varphi}\circ i=\varphi$.
Eindeutigkeit: Sei $\lambda: R_S\to T$ ein Ringhomomorphismus mit $\lambda\circ i=\varphi$. Für $s\in S$ gilt

$$1=\lambda\left(\frac{1}{1}\right)=\lambda\left(\frac{s}{1}\frac{1}{s}\right)=\lambda\left(\frac{s}{1}\right)\lambda\left(\frac{1}{s}\right)=\lambda\circ i(s)\lambda\left(\frac{1}{s}\right)=\varphi(s)\lambda\left(\frac{1}{s}\right)$$

also $\lambda\left(\frac{1}{s}\right)=\varphi(s)^{-1}$. Für $\frac{r}{s}\in R_S$ gilt also

$$\lambda\left(\frac{r}{s}\right)=\lambda\left(\frac{r}{1}\frac{1}{s}\right)=\lambda\left(\frac{r}{1}\right)\lambda\left(\frac{1}{s}\right)=\lambda\circ i(r)\varphi(s)^{-1}=\varphi(r)\varphi(s)^{-1}=\widetilde{\varphi}\left(\frac{r}{s}\right).$$

Es folgt $\lambda=\widetilde{\varphi}$. □

Bemerkung 2.4.6. Seien R, S wie oben. Zu $x_1,\dots,x_n\in R_S$ gibt es $r_1,\dots,r_n\in R$, $s\in S$ mit $x_i=\frac{r_i}{s}$ für alle $1\leqslant i\leqslant n$.

Beweis. Es gibt $c_1,\dots,c_n\in R$ und $s_1,\dots,s_n\in S$ mit $x_i=\frac{c_i}{s_i}$. Sei $s=\prod_{i=1}^n s_i$ und $t_i=\prod_{j\neq i}s_j$, dann ist $s_it_i\in S$ und

$$x_i=\frac{c_i}{s_i}=\frac{c_it_i}{s_it_i}=\frac{c_it_i}{s}$$

für alle $1\leqslant i\leqslant n$. □

Proposition 2.4.7. *Seien R,S wie oben, $i: R\to R_S$ der kanonische Homomorphismus.*

(a) Ist $A\subset R$ Ideal von R, dann ist $\left\{\frac{a}{s}\ ;\ a\in A, s\in S\right\}$ das von $i(A)$ erzeugte Ideal von R_S. Wir bezeichnen es mit $R_S\cdot A$.

(b) Ist $B\subset R_S$ Ideal, dann ist $i^{-1}(B)=:A$ Ideal von R und es gilt $B=R_S\cdot A$.

(c) Ist $A\subset R$ Ideal von R, dann gilt: $R_S\cdot A=R_S$ genau dann wenn $A\cap S\neq\emptyset$.

Beweis. **Zu (a):** Die Menge $B=\left\{\frac{a}{s}\ ;\ a\in A,s\in S\right\}$ ist offenbar ein Ideal von R_S, das $i(A)$ enthält [$i(A)\subset B$ ist klar. Für $\frac{a_1}{s_1},\frac{a_2}{s_2}\in B$ und $\frac{r}{s}\in R_S$ gilt $\frac{a_1}{s_1}-\frac{a_2}{s_2}=\frac{a_1s_2-a_2s_1}{s_1s_2}\in B$ und $\frac{r}{s}\frac{a_1}{s_1}=\frac{ra_1}{ss_1}\in B$]. Ist C ein Ideal von R_S, das $i(A)$ enthält, dann gilt $\frac{a}{s}=\frac{a}{1}\frac{1}{s}=i(a)\cdot\frac{1}{s}\in C$, für alle $\frac{a}{s}\in B$, also $B\subset C$.
Zu (b): Sei $B\subset R_S$ Ideal. Dann ist $A=i^{-1}(B)$ Ideal von R. Behauptung $B=R_S\cdot A$.
„$\subset$ “: Sei $\frac{r}{s}\in B$, dann ist $i(r)=\frac{r}{1}=\frac{r}{s}\frac{s}{1}\in B$, also $r\in A$ und $\frac{r}{s}\in R_SA$.
„$\supset$ “: Sei $x\in R_s\cdot A$, dann gibt es $a\in A$ und $s\in S$ so daß $x=\frac{a}{s}=\frac{a}{1}\frac{1}{s}=i(a)\frac{1}{s}\in B$.
Zu (c): Gilt $R_SA=R_S$, so gibt es $a\in A$ und $s\in S$ mit $\frac{1}{1}=\frac{a}{s}$, das heißt, es gibt $a\in A$ und $s,t\in S$ mit $(a-s)t=0$. Und $at=st\in A\cap S$. Ist andererseits $A\cap S\neq\emptyset$, dann gibt es $a\in A\cap S$, also $\frac{1}{1}=\frac{a}{a}\in R_S\cdot A$ und es folgt $R_S\cdot A=R_S$. □

Beispiel* 2.4.8. Sei $p\in\mathbb{Z}$ eine Primzahl und die multiplikativ abgeschlossenen Teilmenge $S=\mathbb{Z}\setminus(p)\subset\mathbb{Z}$ gegeben. Der Quotientenring $\mathbb{Z}_{(p)}:=\mathbb{Z}_S$ ist gegeben durch

$$\mathbb{Z}_{(p)}:=\left\{\frac{r}{s}\mid r\in R,s\in S\right\}=\left\{\frac{r}{s}\mid r,s\in R,p\nmid s\right\}.$$

Die Ideale $B\subset\mathbb{Z}_{(p)}$ sind gegeben durch $B=\mathbb{Z}_{(p)}\cdot A$, wobei $A\subset\mathbb{Z}$ Ideal ist mit $A\cap\{\mathbb{Z}\setminus(p)\}=\emptyset$, also $A\subset(p)$. Da $\mathbb{Z}$ Hauptidealring ist, ist $A=(a)$ mit $p\big|a$, also $a=np$. Es folgt, dass das von p erzeugte Ideal in $\mathbb{Z}_{(p)}$ maximal bezüglich Inklusion ist, und dies ist das einzige Ideal mit dieser Eigenschaft. Ein solcher Ring heißt lokal, $\mathbb{Z}_{(p)}$ heißt Lokalisierung von $\mathbb{Z}$ bei (p).

Satz 2.4.9. *Sei R Integritätsring.*

(a) Sei S multiplikativ abgeschlossene Teilmenge von R. Es gilt $(r,s) \sim (r',s')$ genau dann, wenn $rs' = r's$. R_S ist Integritätsring und der kanonische Homomorphismus $i : R \to R_S$ ist injektiv. Man schreibt deshalb r statt $\frac{r}{1}$ in R_S.

(b) Ist speziell $S = R\backslash\{0\}$, dann ist R_S sogar ein Körper. R_S heißt Quotientenkörper von R, man setzt $\mathrm{Quot}(R) = R_S$.

Beweis. **Zu (a):** Es gilt $(r,s) \sim (r',s')$ genau dann, wenn es $t \in S$ gibt mit $(rs' - r's)t = 0$ genau dann, wenn $rs' = r's$ da $t \neq 0$. Weiter ist $i(r) = 0$ genau dann, wenn $\frac{r}{1} = 0$ genau dann, wenn es $s \in S$ gibt mit $rs = 0$ genau dann, wenn $r = 0$ da $s \neq 0$. Um zu zeigen, daß R_S wieder Integritätsring ist: Da $1 \neq 0$ in R folgt $\frac{1}{1} \neq \frac{0}{1}$ in R_S. Für $\frac{r}{s}$ und $\frac{r'}{s'} \in R_S\backslash\{0\}$ folgt $r, r' \neq 0$, also $rr' \neq 0$ also $\frac{r}{s}\frac{r'}{s'} \neq 0$.

Zu (b): Sei $S = R\backslash\{0\}$. Sei $0 \neq \frac{r}{s} \in R_S$, dann $r \neq 0$, also $r \in S$. Es folgt $\frac{s}{r} \in R_S$ und $\frac{r}{s}\frac{s}{r} = \frac{rs}{rs} = \frac{1}{1}$. Also ist $\frac{r}{s}$ invertierbar. □

Folgerung 2.4.10. *Sei R ein Unterring eines Körpers, $S \subset R$ multiplikativ abgeschlossene Teilmenge. Dann ist die Abbildung*

$$\varphi : R_S \to K, \frac{r}{s} \mapsto rs^{-1}$$

injektiver Homomorphismus und R_S ist Integritätsring. Man identifiziert R_S mit $\mathrm{im}(\varphi)$ via φ.

Beweis. Da alle $s \in S$ in K invertierbar sind, gibt es einen Homomorphismus φ wie vorgegeben. φ ist injektiv: $\varphi\left(\frac{r}{s}\right) = rs^{-1} = 0$, dann $r = 0$, also $\frac{r}{s} = 0$. Daß R_S Integritätsring ist, ist dann klar. □

Beispiele 2.4.11. (a) $\mathrm{Quot}(\mathbb{Z}) = \mathbb{Q}$

(b) Ist K ein Körper, dann ist $K[X_1, \ldots, X_n]$ Integritätsring. Man setzt

$$K(X_1, \ldots, X_n) = \mathrm{Quot}(K[X_1, \ldots, X_n]).$$

Man nennt diesen Körper den Körper der rationalen Funtionen in den Unbekannten $X_1, \ldots, X_n$ über K.

(c) Sei

$$\mathbb{Z}[i] = \left\{a + bi \in \mathbb{C} \;\middle|\; a, b \in \mathbb{Z}\right\}$$

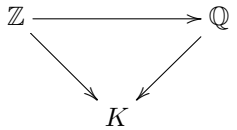
der Ring der ganzen Gaußschen Zahlen, sei

$$\mathbb{Q}[i] = \left\{a + bi \in \mathbb{C} \;\middle|\; a, b \in \mathbb{Q}\right\}$$

der Körper der Gaußschen Zahlen. Ist $S = \mathbb{Z}\backslash\{0\}$, dann gilt $\mathbb{Z}[i]_S = \mathbb{Q}[i] = \mathrm{Quot}(\mathbb{Z}[i])$.

Beispiel* 2.4.12. Der Körper $\mathbb{Q}$ enthält keinen echten Unterkörper.

Beweis. Sei $K \hookrightarrow \mathbb{Q}$ ein Unterkörper von $\mathbb{Q}$. Also sind $0, 1 \in K$. Es folgt, daß $2 = 1 + 1 \neq 0$ ebenfalls in K ist. Angenommen $n \in K$. Dann ist $n + 1 = (1 + \ldots + 1) + 1$ nach Induktion ebenfalls in K. Es folgt $\mathbb{N} \subset K$. Da $(K, +)$ eine abelsche Gruppe ist, ist für $n \in \mathbb{N}$ auch das additive Inverse $-x \in K$. Es folgt $\mathbb{Z} \hookrightarrow K$, und dies ist ein Ringhomomorphismus. Das Bild der multiplikativ abgeschloßenen Menge $S = \mathbb{Z}\backslash\{0\}$ unter diesem Ringhomomorphismus ist in $K\backslash\{0\} = K^\times$ enthalten. Nach der universellen Eigenschaft von Quotientenringen, gibt es also einen eindeutigen Ringhomomorphismus $\mathbb{Q} \to K$, so daß das Diagramm



kommutiert. Dieser ist invers zu $K \hookrightarrow \mathbb{Q}$. Also ist $K = \mathbb{Q}$. □

2.4.2 Primkörper, Charakteristik

Proposition und Definition 2.4.13. *Sei R Integritätsring. $R_0 = \mathbb{Z}\cdot 1$ ist der kleinste Unterring von R, er heißt Primring. Zwei Fälle sind möglich:*

(a) $R_0 \cong \mathbb{Z}$; dies gilt genau dann, wenn $z1 \neq 0$ für alle $z \in \mathbb{Z}\setminus\{0\}$.

(b) Es gibt eine Primzahl $p \in \mathbb{N}$ mit $R_0 \cong \mathbb{Z}/(p)$; p ist die kleinste natürliche Zahl $z \in \mathbb{N}$ mit $z.1 = 0$.

Beweis. Die Abbildung $\varphi : \mathbb{Z} \to R$, $z \mapsto z.1$, ist ein Ringhomomorphismus; $R_0 = \mathrm{im}(\varphi) = \mathbb{Z}.1$ ist der kleinste Unterring von R. Es gibt genau eine Zahl $n \in \mathbb{N}$ mit $\ker(\varphi) = (n)$ und φ induziert den injektiven Homomorphismus

$$\mathbb{Z}/(n) \to R; z + (n) \mapsto z.1$$

Da dann $\mathbb{Z}/(n)$ ebenfalls Integritätsring ist, ist entweder $n = 0$ oder $n = p$ prim. Es gilt $n = 0$ genau dann, wenn $R_0 \cong \mathbb{Z}$ genau dann, wenn für alle $z \in \mathbb{Z}$ gilt $z.1 \neq 0$. Ist $n = p$ Primzahl, dann ist $\mathbb{Z}/(p) \to R_0$, $z + (p) \mapsto z.1$ Isomorphismus. Also ist p die Ordnung von 1 in $(R, +)$, das heißt die kleinste Zahl $z \in \mathbb{N}$ mit $z.1 = 0$. □

Beispiel* 2.4.14. Sei R ein Integritätsring mit Primring $\mathbb{Z}/(p)$, $p > 0$. Dann gilt für alle $x \in R$, daß $px = 0$. Dies folgt leicht aus der Assoziativität von R, denn

$$px = p(1 \cdot x) = (p \cdot 1)x = 0 \cdot x = 0.$$

Beispiel* 2.4.15. Sei R ein Integritätsring mit Primring $\mathbb{Z}/(p)$, $p > 0$. Dann ist die Abbildung

$$F : R \to R, x \mapsto x^p$$

ein Ringhomomorphismus.

Beweis. Es ist klar, daß $F(1) = 1$ ist und für alle $x, y \in R$ gilt $F(xy) = (xy)^p = x^p y^p = F(x)F(y)$, denn R ist kommutativ. Weiterhin berechnet man für $x, y \in R$

$$\begin{aligned} F(x+y) &= (x+y)^p \\ &= \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} = x^p + y^p + \sum_{k=1}^{p-1} \binom{p}{k} x^k y^{p-k} \end{aligned}$$

Es genügt nun nach dem vorherigen Beispiel zu zeigen, daß $p \big| \binom{p}{k}$ für $k = 1, \ldots, p-1$. Nach Definition von $\binom{p}{k}$ gilt die Gleichheit

$$p! = \binom{p}{k} \cdot k! \cdot (p-k)!$$

Da offensichtlich $p|p!$, aber $p \nmid k!$ und $p \nmid (p-k)!$, und p eine Prmzahl ist, muß p $\binom{p}{k}$ teilen. Damit ist $\sum_{k=1}^{p-1} \binom{p}{k} x^k y^{p-k} = 0$ und $F(x+y) = x^p + y^p = F(x) + F(y)$. □

Proposition und Definition 2.4.16. *Sei K ein Körper. K enthält einen kleinsten Unterkörper K_0; er heißt Primkörper von K. Zwei Fälle sind möglich:*

(a) $K_0 \cong \mathbb{Q}$; dies gilt genau dann, wenn $z.1 \neq 0$ für alle $z \in \mathbb{Z}\setminus\{0\}$.

(b) Es gibt eine Primzahl $p \in \mathbb{N}$ mit $K_0 \cong \mathbb{Z}/(p)$; p ist die kleinste natürliche Zahl $z \in \mathbb{N}$ mit $z.1 = 0$.

Beweis. Der Primring von K ist $\mathbb{Z}.1$. Ist $\mathbb{Z}.1 \cong \mathbb{Z}/(p)$ mit p prim, dann ist $K_0 = \mathbb{Z}.1$ der kleinste Unterkörper von K. Ist $\mathbb{Z}.1 \cong \mathbb{Z}$, dann besitzt der injektive Homomorphismus $\varphi : \mathbb{Z} \to K$ eine eindeutige Forsetzung

$$\widetilde{\varphi} : \mathbb{Q} \to K; \widetilde{\varphi}\left(\frac{a}{b}\right) = (a.1)(b.1)^{-1}.$$

$\widetilde{\varphi}$ ist injektiv. Dann ist $K_0 = \mathrm{im}(\widetilde{\varphi}) = \left\{(a.1)(b.1)^{-1} \;\middle|\; a, b \in \mathbb{Z}, b \neq 0\right\}$ der kleinste Unterkörper von K. □

Definition 2.4.17. Sei K ein Körper. Die Charakteristik $\mathrm{char}(K)$ von K ist folgendermaßen definiert:

$$\mathrm{char}(K) = \begin{cases} 0 & \text{falls für alle } 0 \neq z \in \mathbb{Z} : z.1 \neq 0 \\ p & \text{Primzahl, falls } p \text{ die kleinste natürliche Zahl ist mit } z.1 = 0 \end{cases}$$

Folgerung 2.4.18. *Sei p Primzahl. Jeder Körper mit p Elementen ist isomorph zu $\mathbb{Z}/(p)$.*

2.5 Maximale Ideale und Primideale

2.5.1 Das Lemma von Zorn

Sei X eine Menge. Eine Relation $R \subset X \times X$ heißt Ordnung (manchmal teilweise Ordnung), falls

(a) Für alle $x \in X$ gilt $(x, x) \in R$. (Reflexivität)

(b) Ist $(x, y) \in R$ und $(y, x) \in R$, dann gilt $x = y$. (Antisymmetrie)

(c) Ist $(x, y) \in R$ und $(y, z) \in R$ dann ist $(x, z) \in R$. (Transitivität)

Statt $(x, y) \in R$ schreibt man $x \leqslant_R y$ oder $x \leqslant y$. Die Ordnung R oder $\leqslant$ heißt total, wenn für alle $x, y \in X$ entweder $x \leqslant y$ oder $y \leqslant x$ gilt. Sei $(X, \leqslant)$ eine geordnete Menge, dann ist auch $S \subset X$ geordnet bezüglich $s \leqslant t$ für $s, t \in S$, falls dies in X gilt. Ist S bezüglich dieser Ordnung total geordnet, dann heißt S *Kette* von X. Ein Element $x \in X$ heißt *obere Schranke* von $S \subset X$, falls $s \leqslant x$ für alle $s \in S$. Ein Element $x \in X$ heißt größtes Element von X, wenn x obere Schranke von X ist. Ein Element $x \in X$ heißt maximales Element von X, falls für alle $s \in X$ mit $x \leqslant s$ folgt $x = s$. Ebenso definiert man untere Schranke einer Kette, kleinste und minimale Elemente.

Beispiel 2.5.1. Sei $X = \{\{1\}, \{13\}, \{12\}\}$ geordnet bezüglich $\subset$. X ist nicht total geordnet, hat kein größtes Element, aber zwei maximale Elemente.

Lemma von Zorn 2.5.2. *Sei $(X, \leqslant)$ eine nichtleere, geordnete Menge. Wenn jede Kette von X eine obere Schranke in X hat, dann hat X mindestens ein maximales Element.*

2.5.2 Maximale Ideale

Sei R ein Ring. Ein Linksideal $A \subset R$ heißt maximal, wenn $A \neq R$ ist und es kein Linksideal $B \subset R$ gibt, mit $A \subsetneq B \subsetneq R$.

Satz 2.5.3. *Sei R ein Ring $A \subsetneq R$ ein Linksideal. Dann gibt es ein maximales Linksideal B in R, mit $A \subset B$.*

Beweis. Sei $\mathscr{S} = \{C \subset R \mid C \text{ Linksideal von } R \text{ mit } A \subset C \subsetneq R\}$. $\mathscr{S}$ ist nicht leer, und bezüglich $\subset$ geordnet. Sei $\mathscr{T} \subset \mathscr{S}$ eine Kette. Ohne Einschränkung sei $\mathscr{T} \neq \emptyset$. Sei $T = \bigcup_{C \in \mathscr{T}} C$. T ist Linksideal: $0 \in T$ ist klar; seien $x, y \in T$, dann existieren $C_1, C_2 \in \mathscr{T}$ mit $x \in C_1$ und $y \in C_2$. Es gilt $C_1 \subset C_2$ oder $C_2 \subset C_1$. Dann ist $x - y \in C_2 \subset T$ oder $x - y \in C_1 \subset T$, also ist T Untergruppe von $(R, +)$; für $r \in R$ gilt $rx \in C_1 \subset T$, also ist T Linksideal von R; offenbar ist $A \subset T$. Angenommen $T = R$, dann gibt es $C \in \mathscr{T}$ mit $1 \in C$, also $C = R$, unmöglich. Also ist $T \subsetneq R$ und damit $T \in \mathscr{S}$. Da für alle $C \in \mathscr{T}$ gilt $C \subset T$, ist T obere Schranke von $\mathscr{T}$. Nach dem Lemma von Zorn besitzt $\mathscr{S}$ ein maximales Element B. Behauptung: B ist maximales Linksideal von R. Sicher ist $B \neq R$. Gäbe es ein Linksideal D in R mit $B \subsetneq D \subsetneq R$, dann wäre $D \in \mathscr{S}$ und B kein maximales Element von $\mathscr{S}$. Also ist B maximales Ideal von R. □

Folgerung 2.5.4. *Sei R ein kommutativer Ring.*

(a) Ist $A \subsetneq R$ ein Ideal, dann gibt es in R ein maximales Ideal B mit $A \subset B$.

(b) Ist $R \neq 0$, dann besitzt R ein maximales Ideal (Krull).

Proposition 2.5.5. *Sei R ein kommutativer Ring, A ein Ideal in R. A ist genau dann maximal, wenn R/A ein Körper ist.*

Beweis. R/A ist Körper, genau dann, wenn $A \neq R$ und R/A keine Ideale außer 0 und R/A hat. Dies gilt genau dann, wenn $A \neq R$ und für alle Ideal $B \subset R$ mit $A \subset B$ gilt $B/A = 0$ oder $B/A = R/A$. Dies gilt genau dann, wenn $A \neq R$ und für alle Ideale $B \subset R$ mit $A \subset B$ gilt $B = A$ oder $B = R$. Dies ist äquivalent zu der Aussage, daß A maximales Ideal von R ist. □

Beispiele 2.5.6. (a) Die maximalen Ideale von $\mathbb{Z}$ sind die Ideale (p), wobei p eine Primzahl ist. (Denn für $n \in \mathbb{N}_0$ gilt: (n) maximal genau dann, wenn $\mathbb{Z}/(n)$ Körper, genau dann, wenn n Primzahl.)

(b) Sei K Körper, dann ist $(X) = K[X]X$ maximales Ideal. (Denn $K[X]/X \to K, f + (X) \mapsto f(0) =$ konstanter Koeffizient von f ist Ringisomorphismus.)

Beispiel* 2.5.7. Sei R ein (unitärer) kommutativer Ring, $\mathfrak{m} \subset R$ ein maximales Ideal. Sei $1+a$ invertierbar für jedes Element $a \in \mathfrak{m}$. Zeigen Sie, daß $\mathfrak{m}$ das einzige maximale Ideal von R ist.

Beweis. Wir zeigen zunächst, daß jedes Element $b \in R\backslash\mathfrak{m}$ invertierbar in R ist. Sei $0 \neq \overline{b} \in R/\mathfrak{m}$ die Klasse von b modulo $\mathfrak{m}$. Da $R/\mathfrak{m}$ ein Körper ist, gibt es $c \in R$ mit $\overline{b}\overline{c} = \overline{1}$. Es folgt, daß es $a \in \mathfrak{m}$ gibt mit $bc = 1 + a$. Da $1 + a$ nach Voraussetzung invertierbar ist, ist $b \cdot (c \cdot (1 + a)^{-1}) = 1$, also ist b invertierbar. Angenommen $\mathfrak{n} \subset R$ ist ein weiteres maximales Ideal. Dann gibt es $b \in \mathfrak{n}\backslash(\mathfrak{n} \cap \mathfrak{m})$. Wir haben gesehen, daß b in R invertierbar ist. Also ist $1 = b^{-1} \cdot b \in \mathfrak{n}$, also $\mathfrak{n} = R$, Widerspruch. □

2.5.3 Primideale

Definition 2.5.8. Sei R ein kommutativer Ring. Ein Ideal $P \subset R$ heißt Primideal, wenn $P \neq R$ und wenn für alle $r, s \in R$ gilt: ist $rs \in P$, dann ist $r \in P$ oder $s \in P$.

Proposition 2.5.9. *Sei R ein kommutativer Ring. Für ein Ideal $P \subset R$ sind äquivalent:*

(a) P ist Primideal.

(b) $R\backslash P$ ist multiplikativ abgeschlossen.

(c) R/P ist Integritätsbereich.

Beweis. **(a) ⇒ (b):** Wegen $P \neq R$ gilt $1 \in R\backslash P$. Für $r, r' \in R\backslash P$ gilt $rr' \notin P$ wegen (a), also ist $rr' \in R\backslash P$.
(b) ⇒ (c): Wegen $1 \in R\backslash P$ ist $\overline{1} \neq \overline{0}$ in R/P. Für $\overline{r}_1, \overline{r}_2 \in (R/P)\backslash\{0\}$ gilt $r_1, r_2 \in R\backslash P$. Also wegen (b) $r_1 r_2 \in R\backslash P$. Damit $\overline{r}_1\overline{r}_2 = \overline{r_1 r_2} \neq 0$ in R/P.
(c) ⇒ (a): Da $R/P \neq 0$ ist, ist $P \neq R$. Für $r, r' \in R$ mit $rr' \in P$ gilt $\overline{r}\overline{r'} = \overline{rr'} = 0$, also $\overline{r} = 0$ oder $\overline{r'} = 0$. Damit $r \in P$ oder $r' \in P$. □

Folgerung 2.5.10. *In einem kommutativen Ring ist jedes maximale Ideal auch Primideal.*

Beispiele 2.5.11. (a) Die Primideal von $\mathbb{Z}$ sind (0) und die Ideale (p), p eine Primzahl. Das Ideal (0) ist nicht maximal.

(b) Sei R kommutativer Ring. Das Ideal (0) ist genau dann Primideal, bzw. maximales Ideal, wenn R Integritätsring, bzw. Körper, ist.

(c) Sei R Integritätsring. Dann ist $(X) = R[X]X$ Primideal in $R[X]$. (Denn $R[X]/X \to R, f + (X) \mapsto f(0)$ ist Ringisomorphismus.)

Beispiel* 2.5.12. Sei R ein Integritätsbereich und $I \subset R$ ein Primideal, so daß der Index $[R : I]$ der additiven Gruppen $(R, +)$ und $(I, +)$ endlich ist. Zeigen Sie, daß I ein maximales Ideal von R ist.

Beweis. Da I ein Primideal ist, ist nach Proposition 2.5.9 der Faktorring R/I ein Integritätsbereich. Dieser Faktorring ist die Faktorgruppe R/I der additiven Gruppen mit der in Satz 2.1.14 definierten Multiplikation. Also ist R/I ein endlicher Integritätsbereich und damit nach Proposition 2.3.2(b) ein Körper. Proposition 2.5.5 sagt uns dann, daß I ein maximales Ideal ist. □

Satz 2.5.13. *Sei R Hauptidealring. Jedes Primideal ungleich (0) ist maximal.*

Beweis. Sei $(a) \neq 0$ Primideal von R. Es gilt $(a) \neq R$. Sei (b) ein Ideal von R mit $(a) \subset (b) \subset R$. Dann gibt es $c \in R$ mit $a = bc$. Da (a) Primideal ist, folgt $b \in (a)$ oder $c \in (a)$. Ist $b \in (a)$, dann gibt es $x \in R$ mit $b = ax$, also $b = bcx$, also $cx = 1$. Es folgt $c \in R^\times$ und $b = ac^{-1}$. Damit $(b) \subset (a)$ also insbesondere $(b) = (a)$. Ist andererseits $c \in (a)$, dann gibt es $y \in R$ mit $c = ay$, also $c = bcy$ also $by = 1$. Damit ist $b \in R^\times$ und $(b) = R$. Also ist (a) maximales Ideal. □

Proposition 2.5.14. *Seien R, R' kommutative Ringe, $\varphi : R \to R'$ ein Ringhomomorphismus. Für jedes Primideal $Q \subset R'$ ist $\varphi^{-1}(Q)$ Primideal von R. Ist φ surjektiv, $P \subset R$ Primideal mit $\ker(\varphi) \subset P$, dann ist $\varphi(P)$ Primideal von R'.*

Beweis. Sei $Q \subset R'$ Primideal. Wegen $1 \notin Q$ gilt $1 \notin \varphi^{-1}(Q)$. Seien $r, r' \in R$ mit $rr' \in \varphi^{-1}(Q)$. Dann $\varphi(r)\varphi(r') = \varphi(rr') \in Q$. Also ist $\varphi(r) \in Q$ oder $\varphi(r') \in Q$. Damit $r \in \varphi^{-1}(Q)$ oder $r' \in \varphi^{-1}(Q)$. Etc. □

Satz 2.5.15. *Sei R kommutativer Ring, $S \subset R$ multiplikativ abgeschlossene Teilmenge, $i : R \to R_S$ der kanonische Homomorphismus,*

$$\mathscr{A} := \left\{ A \;\middle|\; A \text{ Ideal von } R \text{ mit } A \cap S = \emptyset \right\}.$$

(a) Jedes Ideal $A \in \mathscr{A}$ ist in einem maximalen Element von $\mathscr{A}$ enthalten.

(b) Die maximalen Elemente von $\mathscr{A}$ sind Primideale.

(c) Die Abbildung $P \mapsto R_S P$ vermittelt eine Bijektion von der Menge der maximalen Elemente von $\mathscr{A}$ auf die Menge der maximalen Ideale von R_S. Die inverse Abbildung ist gegeben durch $Q \mapsto i^{-1}(Q)$.

Beweis. **Zu (a):** Für $A \in \mathscr{A}$ ist $R_S A$ Ideal von R_S mit $R_S A \subsetneq R_S$. Es gibt ein maximales Ideal $Q \subset R_S$ mit $R_S A \subset Q$. Für $P = i^{-1}(Q)$ gilt $Q = R_S P$ nach Abschnitt 2.4.1, also gilt $P \in \mathscr{A}$. Wegen $i(A) \subset Q$ gilt $A \subset i^{-1}(Q) = P$. P ist maximales Element von $\mathscr{A}$: Sei $P' \in \mathscr{A}$ mit $P \subset P'$. Dann folgt $Q = R_S P \subset R_S P' \subsetneq R_S$. Da Q maximal ist folgt $Q = R_S P'$. Wegen $i(P') \subset Q$, folgt $P' \subset i^{-1}(Q) = P$, also $P = P'$.
Zu (b): Sei jetzt $A \in \mathscr{A}$ maximales Element von $\mathscr{A}$. In (a) gilt dann $A = P = i^{-1}(Q)$ und $Q = R_S P$. Also ist $A = P$ Primideal und $R_S P = Q$ ist maximales Ideal von R_S.
Zu (c): Nach dem Beweis von (b) ist die Abbildung $P \mapsto R_S P$ sinnvoll, nach dem Beweis von (a) ist sie surjektiv. Sind $P_1 \neq P_2$ maximale Elemente von $\mathscr{A}$, dann gilt $R_S R_1 \neq R_S R_2$. □

Folgerung 2.5.16. *Sei R ein kommutativer Ring, $P \subset R$ ein Primideal, $S = R \backslash P$. Der Ring R_S hat genau ein maximales Ideal, nämlich $R_S P$.*

Beweis. In diesem Fall ist P das größte Element von $\mathscr{A}$, also das einzige Maximale Element von $\mathscr{A}$. □

Unter der Voraussetzung der Folgerung setzt man $R_S = R_P$; R_P heißt Lokalisierung von R in P.

Beispiel* 2.5.17. Für $R = \mathbb{Z}$ und $R = \mathbb{Z}[X]$ untersuche man das durch die Primzahl $2 \in \mathbb{Z}$ erzeugte Hauptideal (2) in R und beweise oder widerlege die folgenden Aussagen:

(a) (2) ist ein Primideal in R.

(b) (2) ist ein maximales Ideal in R.

Ist $R = \mathbb{Z}$, so sind die Primideale genau die von Primelementen und der 0 erzeugten Ideale. Also ist insbesondere (2) Primideal. Explizit sieht man dies wie folgt: Es ist $(2) = 2\,\mathbb{Z} \subsetneq \mathbb{Z}$ eine echte Teilmenge. Sei desweiteren $x, y \in \mathbb{Z}$ mit $xy \in (2)$. Also gibt es $m \in \mathbb{Z}$ mit $xy = 2m$. Da $\mathbb{Z}$ faktorieller Ring ist und 2 Primelement in $\mathbb{Z}$ gilt $2 \big| x$ oder $2 \big| y$. Also ist $x \in (2)$ oder $y \in (2)$. Außerdem ist, da $\mathbb{Z}$ ein Hauptidealring ist, jedes Primideal maximal. Speziell ist (2) ein maximales Ideal.

Betrachten wir nun den Fall $R = \mathbb{Z}[X]$. Zu beachten ist, daß dies zwar ein faktorieller Ring aber kein Hauptidealring ist. Das Element 2 ist hier irreduzibel, also prim. Wie oben sieht man dann, daß das davon erzeugte Ideal (2) Primideal ist. Allerdings ist es nicht maximal, denn es ist zum Beispiel in dem Ideal $A = (2, X)$ enthalten.

Beispiel* 2.5.18. Der Ring $R = \left\{ n + m\sqrt{-2} \,;\, n, m \in \mathbb{Z} \right\}$ ist bekanntlich ein euklidischer Ring bezüglich der Norm $N\left(n + m\sqrt{-2}\right) = n^2 + 2m^2$. Man zeige, daß 11 ein zerlegbares und 13 ein unzerlegbares Element in R ist. Man zeige, daß der Restklassenring $R/13R$ ein Körper ist. Aus wievielen Elementen besteht er?

Für 11 gibt es die Zerlegung $11 = (3 + \sqrt{-2})(3 - \sqrt{-2})$, wobei die Elemente $3 \pm \sqrt{-2}$ keine Einheiten sind, da ihre Norm gegeben ist durch $N(3 \pm \sqrt{-2}) = 11 \neq 1$.

Angenommen das Element 13 wäre zerlegbar, mit $13 = xy$, x, y Nichteinheiten. Da die Norm multiplikativ ist, folgt

$$169 = 13 \cdot 13 = N(13) = N(xy) = N(x)N(y).$$

Da x und y Nichteinheiten sind, muß gelten $N(x) = N(y) = 13$. Aber es gibt keine Elemente $a + b\sqrt{-2} \in R$ mit $a^2 + 2b^2 = 13$. Widerspruch. Also ist 13 nicht zerlegbar. (Hingegen gibt es sehr wohl $a + b\sqrt{-2} \in R$ mit $a^2 + 2b^2 = 11$, siehe oben.)

Da 13 nicht zerlegbar ist, also prim, und R ein Hauptidealring, ist (13) maximales Ideal. Es folgt, daß $R/(13)$ ein Körper ist mit $|R/(13)| = 169$.

2.5.4 Kettenbedingungen

Proposition und Definition 2.5.19. *Für eine geordnete Menge $(X, \leqslant)$ sind äquivalent:*

(a) Für jede Folge $x_1 \leqslant \ldots \leqslant x_n \leqslant \ldots$ in X gilt: es existiert $N \in \mathbb{N}$, so daß für alle $n \geqslant N$ gilt $x_n = x_N$.

(b) Jede nichtleere Teilmenge $X' \subset X$ hat ein maximales Element.

Gelten diese Aussagen, dann sagt man X genügt der aufsteigenden Kettenbedingung oder Maximalbedingung.

Beweis. **(a) ⇒ (b):** Angenommen X besitzt eine nichtleere Teilmenge X' ohne maximales Element. Wähle $x_1 \in X'$. Da X' kein maximales Element hat, gibt es $x_2 \in X'$ mit $x_1 \lneqq x_2$. Da x_2 nicht maximal ist gibt es $x_3 \in X'$ mit $x_2 \lneqq x_3$. Rekursiv findet man eine Kette $x_1 \lneqq x_2 \lneqq x_3 \lneqq \ldots$ im Widerspruch zu (a).
(b) ⇒ (a): Sei $x_1 \leqslant x_2 \leqslant x_3 \leqslant \ldots$ eine Folge in X. Nach (b) hat $X' = \{x_n \ : \ n \in \mathbb{N}\}$ ein maximales Element x_N. Für $n \geqslant N$ gilt $x_N \leqslant x_n$, also $x_N = x_n$. □

Sei R ein Ring, $\mathscr{S}$ eine Menge von Linksidealen (Rechtsidealen / zweiseitigen Idealen) von R. Man sagt R habe aufsteigende Kettenbedingung oder Maximalbedingung für die Ideale in $\mathscr{S}$, falls $\mathscr{S}$ den Bedingungen (a) und (b) genügt.
Beispiele für Teilmengen $\mathscr{S}$ sind: alle Linksideael, alle endlich erzeugten Linksideale, alle Linkshauptideale. Analog für Rechtsideale.

Proposition und Definition 2.5.20. *Für einen Ring R sind äquivalent:*

(a) R genügt der Maximalbedingung für alle Linksideale.

(b) R genügt der Maximalbedingung für alle endlich erzeugten Linksideale.

(c) Jedes Linksideal ist endlich erzeugt.

Gelten (a), (b) und (c), dann heißt R linksnoethersch. Analog definiert man rechtsnoethersch.

Beweis. **(a) ⇒ (b):** Das ist klar.
(b) ⇒ (c): Annahme: R enthält ein Linksideal A, das nicht endlich erzeugt ist. Wähle $a_1 \in A$. Dann gilt $Ra_1 \subsetneq A$. Wähle $a_2 \in A \backslash Ra_1$, dann gilt $Ra_1 \subsetneq (Ra_1 + Ra_2) \subsetneq A$. Wähle $a_3 \in A \backslash (Ra_1 + Ra_2)$, dann $Ra_1 \subsetneq (Ra_1 + Ra_2) \subsetneq (Ra_1 + Ra_2 + Ra_3) \subsetneq A$. Rekursiv findet man eine Folge $(a_k)_{k\in\mathbb{N}}$ in A mit

$$\sum_{i=1}^{k} Ra_i \subsetneq \sum_{i=1}^{k+1} Ra_i \text{ für alle } k \geqslant 1.$$

Dies widerspricht (b).
(c) ⇒ (a): Sei $A_1 \subset A_2 \subset A_3 \subset \ldots$ eine Folge von Linksidealen von R, sei $A = \bigcap_{n\in\mathbb{N}} A_n$. Dann ist A Linksideal. Nach (c) gibt es also $x_1, \ldots, x_m \in A$ mit $A = \sum_{i=1}^{m} Rx_i$. Für alle $1 \leqslant k \leqslant m$ gibt es $i_k \in \mathbb{N}$ so daß $x_k \in A_{i_k}$. Mit $N = \max\{i_1, \ldots, i_m\}$ gilt dann $A_{i_1}, \ldots, A_{i_m} \subset A_N$, also $x_1, \ldots x_m \in A_N$. Somit ist $A \subset A_N$, und es folgt $A = A_N$, insbesondere $A_n = A_N$ für alle $n \geqslant N$. □

Proposition 2.5.21. *Ist R linksnoethersch, $A \subset R$ ein zweiseitiges Ideal, dann ist auch R/A linksnoethersch.*

Beweis. Sei B/A ein Linksideal von R/A, wobei B Linksideal von R ist mit $A \subset B$. Es gibt $b_1, \ldots, b_n \in R$ mit $B = \sum_{i=1}^{n} Rb_i$. Es folgt $B/A = \sum_{i=1}^{n} R/A(b_i + A)$. □

Folgerung 2.5.22. *Jeder Hauptidealring ist noethersch.*

Beweis. Denn jedes Ideal ist endlich (von einem Element) erzeugt. □

Hilberts Basissatz 2.5.23. *Sei R ein kommutativer Ring. Ist R noethersch, $n \in \mathbb{N}$, dann ist auch $R[X_1, \ldots, X_n]$ noethersch.*

Beweis. Es genügt die Behauptung für $n = 1$ zu zeigen. Die allgemeine Aussage folgt induktiv, denn für $n > 1$ ist $R[X_1, \ldots, X_n] = R[X_1, \ldots, X_{n-1}][X_n]$. Sei also $n = 1$, $X = X_1$ und R noethersch.

Annahme: Es gibt ein Ideal A in $R[X]$, das nicht endlich erzeugt ist. Wähle $0 \neq f_1 \in A$ mit minimalem Grad und seien $(f_k)_{k\in\mathbb{N}}$ rekursiv so ausgewählt, daß f_{k+1} Polynom minimalen Grades in $A\backslash(f_1, \ldots, f_k)$ ist. Sei $n_k = \deg(f_k)$ und $a_k \in R$ der höchste Koeffizient von f_k. Es gilt $n_1 \leqslant n_2 \leqslant n_3 \leqslant \ldots$. Wir zeigen, daß $(a_1, \ldots, a_k) \subsetneq (a_1, \ldots, a_{k+1})$ für alle $k \geqslant 1$. Dies widerspricht der Voraussetzung, daß R noethersch ist.

Annahme: Es gibt $k \geqslant 1$ so daß $(a_1, \ldots, a_k) = (a_1, \ldots, a_{k+1})$. Dann gibt es $b_1, \ldots, b_k \in R$ mit

$$a_{k+1} = \sum_{j=1}^{k} b_j a_j.$$

Sei

$$g = f_{k+1} - \sum_{j=1}^{k} b_k X^{n_{k+1}-n_j} f_j.$$

Es gilt $g \in A\backslash(f_1, \ldots, f_k)$ und $\deg(g) < \deg(f_{k+1})$, unmöglich. □

Beispiele 2.5.24. (a) Sei K ein Körper. Für alle $n \in \mathbb{N}$ ist $K[X_1, \ldots, X_n]$ noethersch aber für $n > 1$ ist $K[X_1, \ldots, X_n]$ kein Hauptidealring.

(b) Für $n \in \mathbb{N}$ ist $\mathbb{Z}[X_1, \ldots, X_n]$ noethersch aber kein Hauptidealring.

Folgerung 2.5.25. *Sei R ein kommutativer, noetherscher Ring, S eine kommutative R-Algebra, $s_1, \ldots, s_n \in S$. Dann ist $R[s_1, \ldots, s_n]$ noethersch.*

Beweis. $R[s_1, \ldots, s_n]$ ist das Bild des Einsetzungshomomorphismus

$$R[X_1, \ldots, X_n] \to S, f \mapsto f(s_1, \ldots, s_n).$$

Da also $R[s_1, \ldots, s_n]$ isomorph zu einem Faktorring von $R[X_1, \ldots, X_n]$ ist, ist $R[s_1, \ldots, s_n]$ noethersch. □

2.6 Teilbarkeit in Integritätsringen

2.6.1 Teilbarkeit, irreduzible Elemente

Proposition und Definition 2.6.1. *Sei R ein kommutativer Ring, $r, s \in R$.*

(a) r heißt Teiler von s, geschrieben $r\big|s$, wenn $\exists t \in R$ mit $s = rt$, das heißt, wenn $(s) \subset (t)$.

(b) r, s heißen zueinander assoziiert, geschrieben $r \sim s$, wenn $r\big|s$ und $s\big|r$, d.h. wenn $(s) = (r)$. Dadurch wird auf R eine Äquivalenzrelation definiert. Die Äquivalenzklasse von 1 ist $R^\times$, die von 0 ist $\{0\}$.

(c) r heißt echter Teiler von s, wenn $r\big|s$, $r \notin R^\times$ und r nicht zu s assoziiert ist, d.h. $(s) \subsetneq (r) \subsetneq R$.

Beweis. Die Beweise dazu sind klar. □

Ab jetzt sei R ein Integritätsring. Es gilt, $r \sim s$ genau dann, wenn es $u \in R^\times$ gibt mit $r = us$.

Beweis. Ist $(r) = (s)$, dann gibt es $u, v \in R$ mit $r = us$ und $s = vr$. Also $r = uvr$, also $uv = 1$ und insbesondere $u, v \in R^\times$. Die andere Richtung folgt aus der Definition. □

Die Äquivalenzrelation $\sim$ gehört zur Operation

$$\begin{aligned} R^\times \times R &\to R \\ (ru, r) &\mapsto ur. \end{aligned}$$

Definition 2.6.2. r heißt irreduzibel oder unzerlegbar, wenn $r \notin R^\times \cup \{0\}$ und r keine echten Teiler hat, d.h. wenn $r \neq 0$ und (r) maximales Element in der Menge der Hauptideale ungleich R ist.

Mit r ist auch jedes dazu assoziierte Element irreduzibel.

Beispiele 2.6.3. (a) Die irreduziblen Elemente von $\mathbb{Z}$ sind genau die Zahlen $\pm p$, wobei $p \in \mathbb{Z}$ eine Primzahl ist.

(b) Die irreduziblen Polynome von $\mathbb{C}[X]$ sind genau diejenigen vom Grad 1.

(c) Die irreduziblen Elemente von $\mathbb{R}[X]$ sind die vom Grad 1 und die Polynome aX^2+bX+c mit $a \neq 0$ und $b^2 - 4ac < 0$. (Um dies zu sehen überlege man sich, daß wenn $z \in \mathbb{C}$ Nullstelle eines Polynoms $f \in \mathbb{R}[X]$ ist, so auch $\overline{z}$. Ist $z \in \mathbb{R}$, also insbesondere $z = \overline{z}$, dann spaltet f den Linearfaktor $X - z$ ab. Ist dagegen $z = a + ib \in \mathbb{C} \setminus \mathbb{R}$, dann ist $(X - z)(X - \overline{z}) = X^2 - 2aX + (a^2 + b^2) \in \mathbb{R}[X]$ ein Teiler von f.)

Satz 2.6.4 (Euklid)**.** *Hat R Maximalbedingung für Hauptideale, dann ist jedes Element $r \in R\backslash(R^\times \cup \{0\})$ Produkt von irreduziblen Elementen. Insbesondere gilt das, wenn R noethersch ist.*

Beweis. Angenommen es gibt $r \in R\backslash(R^\times \cup \{0\})$, das nicht Produkt von irreduziblen Elementen ist. Sei $\mathcal{S}$ die Menge aller Hauptideale, die von solchen Elementen erzeugt sind. Da $\mathcal{S} \neq \{0\}$ ist, hat nach Voraussetzung $\mathcal{S}$ ein maximales Element (a). a ist nicht irreduzibel, also gibt es $b, c \in R$ mit $a = bc$ und $(a) \subsetneq (b) \subsetneq R$, $(a) \subsetneq (c) \subsetneq R$. Da $b, c \in R\backslash(R^\times \cup \{0\})$ und (a) maximales Element von $\mathcal{S}$ ist, sind beide Produkte von irreduziblen Elementen, also ist auch $a = bc$ Produkt von irreduziblen Elementen, Widerspruch. □

Man hätte gerne folgende Eigenschaft für solche Zerlegungen:

Definition 2.6.5. Sie $0 \neq r \in R$, $r = a_1 \cdots a_n = b_1 \cdots b_m$ mit irreduziblen Elementen a_i, b_j und $n, m \in \mathbb{N}$. Die beiden Zerlegungen heißen äquivalent, wenn $n = m$ und es $\sigma \in \mathfrak{S}_n$ gibt, so daß für alle $1 \leqslant i \leqslant a_i \sim b_{\sigma(i)}$.

Beispiel 2.6.6. Sei K ein Körper, R der Unterring von $K[X]$ bestehend aus den Polynomen $f = \sum_{i=0}^{n} a_i X^i$, mit $a_1 = 0$. Es gilt $R = K[X^2, X^3]$, also ist R noethersch. Außerdem gilt $R^\times = K^\times$. Die Elemente X^2 und X^3 sind in R irreduzibel: Sei $X^2 = fg$ mit $f, g \in R$, dann gilt $\deg(f), \deg(g) \in \{0, 2\}$, also $f \in R^\times$ oder $g \in R^\times$. Ebenso für X^3. Es gilt $X^6 = X^2 \cdot X^2 \cdot X^2 = X^3 \cdot X^3$, und $X^2 \nmid X^3$ bzw. $X^3 \nmid X^2$. Also hat man zwei nicht-äquivalente Zerlegungen von X^6 in irreduzible Elemente gefunden.

2.6.2 Primelemente

Definition 2.6.7. Sei R Integritätsring. Ein Element $p \in R$ heißt Primelement, wenn $p \in R\backslash(R^\times \cup \{0\})$ und für alle $r, s \in R\backslash\{0\}$ gilt: falls $p \mid rs$, dann $p \mid r$ oder $p \mid s$, das heißt, wenn $p \neq 0$ und (p) Primideal ist.

Mit p ist auch jedes dazu assoziierte Element ein Primelement.

Proposition 2.6.8. *Sei R Integritätsring.*

(a) Ist $p \in R$ ein Primelement, $p \mid r_1 \cdots r_n$, dann gibt es $1 \leqslant i \leqslant n$ so daß $p \mid r_i$.

(b) Jedes Primelement ist irreduzibel.

(c) Ist R sogar Hauptidealring, dann ist ein Element genau dann Primelement, wenn es irreduzibel ist.

Beweis. **Zu (a):** Induktion nach n.
Zu (b): Sei p Primelement, $p = rs$ mit $r, s \in R$. Dann gilt $p \mid r$ oder $p \mid s$, also $p \sim r$ oder $p \sim s$.
Zu (c): Sei R Hauptidealring, $r \in R$ irreduzibel, dann ist (r) maximal in der Menge der Hauptideale $\neq R$. Also ist (r) maximales Ideal somit Primideal, also ist r Primelement. Die Umkehrung gilt allgemein in Integritätsringen. □

Beispiel 2.6.9. Sei wieder $R = K[X^2, X^3]$. Dann sind X^2 und X^3 irreduzibel aber keine Primelemente.

Proposition 2.6.10 (Eindeutigkeit)**.** *Sei R Integritätsring, seien $r = p_1 \cdots p_m$ und $s = q_1 \cdots q_n$ mit Primelementen p_i und q_j, und $m, n \in \mathbb{N}$.*

(a) Genau dann gilt $r \mid s$, wenn $m \leqslant n$ und es eine Injektion $\sigma : \{1, \ldots, m\} \to \{1, \ldots, n\}$ gibt mit $p_i = q_{\sigma(i)}$ für $1 \leqslant i \leqslant m$.

(b) Genau dann gilt $r \sim s$, wenn die Zerlegungen äquivalent sind.

Beweis. **Zu (a):** Gibt es eine solche Injektion σ, ist klar, daß $r|s$. Gilt andererseits $r|s$, dann existiert $t \in R$ mit $s = tr$. Induktion nach m: Ist $m = 1$, dann $p_1|s$. Da p_1 prim ist, gibt es also $1 \leqslant i \leqslant n$ mit $p_1|q_i$, also $p_1 \sim q_i$. Der Schritt von $m-1$ nach m: aus $r|s$ folgt $p_m|s$. Wie oben existiert $1 \leqslant i \leqslant n$ mit $p_m \sim q_i$. Das heißt, es gibt $u \in R^\times$ mit $p_m = uq_i$, also $\prod_{j \neq i} q_j = p_1 \cdots p_{m-1} ut$ für ein $t \in R$. Nach Induktionsannahme ist $m - 1 \leqslant n - 1$ und es gibt eine Injektion $\sigma : \{1, \ldots, n-1\} \to \{1, \ldots, n\} \backslash \{i\}$ mit $p_j \sim q_{\sigma(j)}$ für $1 \leqslant j \leqslant m-1$. Setze noch $\sigma(m) = i$.
Zu (b): Das folgt aus (a). □

2.6.3 Faktorielle Ringe

Definition 2.6.11. Ein Integritätsring heißt faktoriell oder ZPE-Ring, wenn jedes Element $r \in R \backslash (R^\times \cup \{0\})$ Produkt von Primelementen ist.

Satz 2.6.12. *Für einen Integritätsring R sind folgende Aussagen äquivalent.*

(a) R ist faktoriell.

(b) Jedes Element $r \in R \backslash (R^\times \cup \{0\})$ ist Produkt von irreduziblen Elementen, und je zwei solche Zerlegungen sind äquivalent.

(c) Es gibt eine Teilmenge $P \subset R \backslash \{0\}$ mit der Eigenschaft, daß es zu jedem Element $r \in R \backslash \{0\}$ eine eindeutig bestimmte Einheit $u_r \in R^\times$ und eine eindeutig bestimmte Familie $(\nu_p(r))_{p \in P}$ von Zahlen in $\mathbb{N}_0$, fast alle Null, gibt, mit $r = u_r \prod_{p \in P} p^{\nu_p(r)}$.

(d) R hat Maximalbedingung für Hauptideale, und jedes irreduzible Element in R ist Primelement.

Beweis. **(a⇒b):** Nach (a) ist jedes Element $r \in R \backslash (R^\times \cup \{0\})$ Produkt von Primelementen, also von irreduziblen Elementen. Insbesondere ist jedes irreduzible Element Primelement. Nach der Eindeutigkeitsproposition sind also je zwei Zerlegungen von r in irreduzible Elemente äquivalent.
(b⇒c): Sei P eine Transversale der Menge aller irreduzibler Elemente von R bezüglich $\sim$. Sei $r \in R \backslash (R^\times \cup \{0\})$. Nach (b) gibt es irreduzible Elemente $q_1, \ldots, q_n \in R$, $n \geqslant 1$, mit $r = q_1 \cdots q_n$. Für $1 \leqslant i \leqslant n$ gibt es eindeutig bestimmte $u_i \in R^\times$, $p_i \in P$ mit $q_i = u_i p_i$. Es folgt $r = q_1 \cdots q_n = u_1 p_1 \cdots u_n p_n = u_1 \cdots u_n \prod_{p \in P} p^{\nu_p(r)}$. Die Eindeutigkeit folgt aus (b).
(c⇒d): Für $r, s \in R \backslash \{0\}$ gilt $(r) \subset (s)$ genau dann, wenn $s|r$. Dies gilt genau dann, wenn für alle $p \in P$ $\nu_p(r) \geqslant \nu_p(s)$ gilt.

Beweis. Gilt $s|r$, dann gibt es $t \in R$ mit $r = st$. Somit $u_r \prod_{p \in P} p^{\nu_p(r)} = u_s \prod_{p \in P} p^{\nu_p(s)} \cdot u_t \prod_{p \in P} p^{\nu_p(t)}$. Also gilt für alle $p \in P$, daß $\nu_p(r) = \nu_p(s) + \nu_p(t) \geqslant \nu_p(s)$. Andererseits gilt mit $t := u_r u_s^{-1} \prod_{p \in P} p^{\nu_p(r) - \nu_p(s)} \in R$, $r = st$. □

Sei $(r_n)_{n \in \mathbb{N}}$ eine Folge in R mit $(r_1) \subset (r_2) \subset (r_3) \subset \cdots$. Dann gibt es $N \in \mathbb{N}$ mit $(r_n) = (r_N)$ für alle $n \geqslant N$.

Beweis. Sei ohne Einschränkung $r_n \neq 0$ für alle $n \in \mathbb{N}$. Dann gilt für alle $p \in P$ und $n \in \mathbb{N}$ $\nu_p(r_n) \geqslant \nu_p(r_{n+1}) \geqslant 0$. Da $\nu_p(r_1) = 0$ für fast alle $p \in P$, gibt es $N \in \mathbb{N}$ mit $\nu_p(r_N) = \nu_p(r_n)$ für alle $p \in P$ und alle $n \geqslant N$. Es folgt $(r_N) = (r_n)$ für alle $n \geqslant N$. □

P ist Transversale der Primelemente bezüglich $\sim$.

Beweis. Für $p \in P$ gilt $p \notin R^\times$, denn andernfalls gilt $p \cdot p^0 = 1 \cdot p$, was unmöglich ist, wegen der Eindeutigkeit der Darstellung. Jedes $p \in P$ ist Primelement: Seien $p \in P$ und $r, s \in R \backslash \{0\}$, mit $p|rs$, dann $1 \leqslant \nu_p(rs) = \nu_p(r) + \nu_p(s)$. Also $\nu_p(s) \geqslant 1$ oder $\nu_p(r) \geqslant 1$, also $p|s$ oder $p|r$. Sei q ein beliebiges Primelement von R, dann $q = u_q \prod_{p \in P} p^{\nu_p(q)}$. Also gibt es $p \in P$ mit $q|p$, also $q \sim p$. Offenbar ist q zu genau einem $p \in P$ assoziiert. □

Sei $r = u_r \prod_{p \in P} p^{\nu_p(r)}$ irreduzibel. Dann gibt es genau ein $p \in P$ mit $\nu_p(r) = 1$ und $\nu_q(r) = 0$ für $q \in P \backslash \{p\}$. Es folgt $r = u_r p$. Also ist r Primelement. **(d⇒a):** Nach dem Satz von Euklid ist jedes Element von $r \in R \backslash (R^\times \cup \{0\})$ Produkt von irreduziblen Elementen. Nach (d) sind irreduzible Elemente in R Primelemente.
Der Zuatz wurde mitbewiesen. □

Folgerung 2.6.13. *Jeder Hauptidealring R ist faktoriell.*

Beweis. R hat Maximalbedingung für (Haupt)ideale. Außerdem wissen wir, daß in R irreduzible Elemente Primelement sind. □

Folgerung 2.6.14. *(a) $\mathbb{Z}$ ist faktoriell, mit $\mathbb{Z}^\times = \{-1, +1\}$, $P = \{p \in \mathbb{N} \mid p \text{ prim}\}$ ist Transversale der Primelemente von $\mathbb{Z}$ bezüglich $\sim$. P ist unendlich.*

(b) Sei K Körper. Dann ist $K[X]$ faktoriell mit $K[X]^\times = K^\times$, $P = \{f \in K[X] \mid f \text{ normiert und irreduzibel }\}$ ist eine Transversale der Primelemente bezüglich $\sim$. P ist unendlich.

Beweis. **Zu (a):** Wir zeigen nur noch, daß P unendlich ist (nach Euklid). Angenommen P ist endlich: $P = \{p_1, \dots p_n\}$, $p_1 \leqslant p_2 \leqslant \dots \leqslant p_n$. Sei $x = p_1 \cdots p_n + 1$. Da $x > 1$ gibt es $p_i \in P$ mit $p_i \big| x$.
Zu (b): Wir werden später sehen: Ist R faktoriell, so ist $R[X]$ faktoriell. Daß P unendlich ist, folgt wie bei $\mathbb{Z}$. □

2.6.4 Kleinstes gemeinsames Vielfaches und größter gemeinsamer Teiler

Definition 2.6.15. Sei R Integritätsring und $r_1, \dots, r_n, v, t \in R \backslash \{0\}$.

(a) v heißt kleinstes gemeinsames Vielfaches, abgekürzt kgV, von $r_1, \dots, r_n$, wenn gilt: v ist Vielfaches der r_i, d.h. $r_i \big| v$ für alle $1 \leqslant i \leqslant n$, und v teilt alle anderen Vielfachen der r_i, d.h. für alle $s \in R \backslash \{0\}$ mit $r_i \big| s$ für alle $1 \leqslant i \leqslant n$ folgt $v \big| s$.

(b) t heißt größter gemeinsamer Teiler, abgekürzt ggT, der $r_1, \dots, r_n$, wenn gilt: t ist Teiler der r_i, d.h. $t \big| r_i$ für alle $1 \leqslant i \leqslant n$, und wird von allen anderen Teilern der r_i geteilt, d.h. falls $s \big| r_i$ für alle $1 \leqslant i \leqslant n$, dann $s \big| t$.

(c) $r_1, \dots, r_n$ heißen teilerfremd bzw. relativ prim, wenn 1 ein ggT von ihnen ist.

Es folgt jeweils aus der Definition, daß ggT und kgV bis auf Assoziiertheit eindeutig bestimmt sind.

Proposition 2.6.16. *Sei R ein Integritätsring, $r_1, \dots, r_n, v, t \in R \backslash \{0\}$.*

(a) v ist genau dann ein kgV *von $r_1, \dots, r_n$, wenn $(v) = \bigcap_{i=1}^n (r_i)$.*

(b) Gilt $(t) = \sum_{i=1}^n (r_i) = (r_1, \dots, r_n)$, dann ist t ein ggT *von $r_1, \dots, r_n$.*

(c) Ist R Hauptidealring, dann gilt:

(i) t ist genau dann ein ggT *von $r_1, \dots, r_n$, wenn $(t) = (r_1, \dots, r_n)$.*

(ii) (Lemma von Bezout) $r_1, \dots, r_n$ sind genau dann teilerfremd, wenn es $s_1, \dots, s_n \in R$ gibt, mit $\sum_{i=1}^n s_i r_i = 1$.

Beweis. **Zu (a):** Sei v ein kgV von $r_1, \dots, r_n$. Dann gilt $x \in \bigcap_{i=r}^n (r_i)$ genau dann, wenn für alle i gilt, $r_i \big| x$, genau dann, wenn $v \big| x$, genau dann, wenn $x \in (v)$. Umgekehrt gilt: Für alle i teilt $r_i \big| x$ genau dann, wenn $x \in \bigcap_{i=1}^n (r_i) = (v)$, genau dann, wenn $v \big| x$.
Zu (b): Ähnlich.
Zu (c,i): Eine Richtung wurde schon in (b) gezeigt. Für die andere Richtung nehmen wir also an, daß t ein ggT von $r_1, \dots, r_n$ ist. Da R Hauptidealring ist, gibt es $t' \in R$ mit $(t') = (r_1, \dots, r_n)$. Nach (b) ist t' ein ggT von $r_1, \dots, r_n$. Also sind t' und t assoziiert, und damit $(t) = (r_1, \dots, r_n)$.
Zu (c,ii): Das folgt aus (i) bzw. ist klar. □

Aus der Proposition folgt, daß in einem Hauptidealring sowohl ggT als auch kgV existieren. In einem beliebigen Integritätsring braucht dies nicht der Fall zu sein.

Folgerung 2.6.17. *Sei R Hauptidealring, $r_1, \dots, r_n \in R\backslash\{0\}$, $t \in R$ ein* ggT *von $r_1, \dots, r_n$, und $c \in R$ beliebig. Die diophantische Gleichung $r_1x_1 + \cdots + r_nx_n = c$ ist in R genau dann lösbar, wenn $t \mid c$.*

Beweis. Angenommendie Gleichung sei lösbar, d.h. es gebe $s_1, \dots, s_n \in R$ mit $\sum_{i=1}^n r_i s_i = c$, dann gilt $t \mid c$. Umgekehrt existiere $d \in R$ mit $c = td$. Da t ggT ist, gibt es $s_1, \dots, s_n \in R$ mit $t = \sum_{i=1}^n r_i s_i$. Es folgt $c = \sum_{i=1}^n r_i(ds_i)$. □

Proposition 2.6.18. *Sei R Integritätsring, $r_1, \dots, r_n \in R\backslash\{0\}$, $n > 1$.*

(a) Ist $v' \in R$ ein kgV *von $r_1, \dots, r_{n-1}$ und v ein* kgV *von v', r_n, dann ist v ein* kgV *von $r_1, \dots, r_n$.*

(b) Ist $t' \in R$ ein ggT *von $r_1, \dots, r_{n-1}$ und t ein* ggT *von t', r_n, dann ist t ein* ggT *von $r_1, \dots, r_n$.*

Beweis. Dies folgt aus der Definition. □

Satz 2.6.19. *Sei R faktoriell, $P \subset R\backslash\{0\}$ eine Transversale der Primelemente bezüglich $\sim$, seien $r_1, \dots, r_n \in R\backslash\{0\}$ mit $n > 1$.*

(a) Das Element

$$v = \prod_{p \in P} p^{\max\{\nu_p(r_i), 1 \leqslant i \leqslant n\}}$$

ist kgV *und*

$$t = \prod_{p \in P} p^{\min\{\nu_p(r_i), 1 \leqslant i \leqslant n\}}$$

ist ggT *von $r_1, \dots, r_n$.*

(b) $r_1, \dots, r_n$ sind genau dann teilerfremd, wenn für alle $p \in P$ gilt $\min\{\nu_p(r_i), 1 \leqslant i \leqslant n\} = 0$.

(c) Im Fall $n = 2$ gilt $r_1r_2 \sim vt$.

Beweis. **Zu (a):** Für $s \in R\backslash\{0\}$ gilt: $r_i \mid s \forall i$ genau dann, wenn für alle $p \in P$ $\nu_p(r_i) \leqslant \nu_p(s) \forall i$, genau dann, wenn für alle $p \in P$ gilt $\max\{\nu_p(r_i) \mid 1 \leqslant i \leqslant n\} = \nu_p(v) \leqslant \nu_p(s)$, genau dann, wenn $v \mid s$.
Ebenso für t.
Zu (b) und (c): Dies folgt aus (a). □

Folgerung 2.6.20 (Lemma von Euklid)**.** *Sei R faktoriell, $r, s, t \in R\backslash\{0\}$. Gilt $r \mid st$ und sind r und s teilerfremd, dann gilt $r \mid t$.*

Beweis. Für $p \in P$ gilt $\nu_p(r) \leqslant \nu_p(st) = \nu_p(s) + \nu_p(t)$. Falls $\nu_p(r) > 0$, dann $\nu_p(s) = 0$, also $\nu_p(r) \leqslant \nu_p(t)$. Falls $\nu_p(r) = 0$, dann gilt trivialerweise $\nu_p(r) \leqslant \nu_p(t)$. Es folgt $r \mid t$. □

Berechnung des ggT **in einem euklidischen Ring** (R, δ)

Seien $r, s \in R\backslash\{0\}$. Dann gibt es $n \in \mathbb{N}_0$, und Folgen

$$r_{-1} = r, r_0 = s, r_1, \dots, r_n \in R\backslash\{0\} \quad \text{und} \quad q_1, \dots q_{n+1} \in R$$

mit

$$\begin{aligned} r &= q_1 s + r_1, \quad \delta(r_1) < \delta(s) \\ s &= q_2 r_1 + r_2, \quad \delta(r_2) < \delta(r_1) \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n, \quad \delta(r_n) < \delta(r_{n-1}) \\ r_{n-1} &= q_{n+1} r_n \end{aligned}$$

Beweis. Die r_i und q_i existieren nach Definition eines euklidischen Rings. Nach endlich vielen Schritten ist ein Rest 0. □

Für $0 \neq c \in R$ gilt

$$c|r, s \Leftrightarrow c|s, r_1 \Leftrightarrow c|r_1, r_2 \Leftrightarrow \cdots \Leftrightarrow c|r_{n-2}, r_{n-1} \Leftrightarrow c|r_n.$$

Durch rekursives Einsetzen im Euklidischen Algorithmus erhält man $a, b \in R$ mit $r_n = ra + sb$.

Beispiel* **2.6.21.** Es seien K ein Körper, $K[X]$ der Polynomring über K und $m, n \in \mathbb{N}$. Sei $g = \mathrm{ggT}(m, n)$ in $\mathbb{Z}$, dann ist $X^g - 1$ ein größter gemeinsamer Teiler von $X^m - 1$ und $X^n - 1$ in $K[X]$.

Beweis. Wir zeigen zuerst, daß $h = X^g - 1$ Teiler von $X^m - 1$ und $X^n - 1$ ist. Da g Teiler von m und Teiler von n ist, gibt es $k, l \in \mathbb{Z}$ mit $m = kg$ und $n = lg$. Wir rechnen im Faktorring $K[X]/(h)$. Hier gilt $X^g \equiv 1 \mod (h)$, also

$$\begin{aligned} X^m + (h) &= (X + (h))^m = (X + (h))^{kg} = ((X + (h))^g)^k = (1 + (h))^k = 1 + (h) \\ X^n + (h) &= (X + (h))^n = (X + (h))^{lg} = ((X + (h))^g)^l = (1 + (h))^l = 1 + (h) \end{aligned}$$

Also $X^m \equiv 1 \mod (h)$, dh. $X^m - 1 \equiv 0 \mod (h)$ und $X^n \equiv 1 \mod (h)$, dh. $X^n - 1 \equiv 0 \mod (h)$. In anderen Worten, $X^g - 1 = h|X^m - 1$ und $X^g - 1 = h|X^n - 1$.

Um zu zeigen, daß $X^g - 1$ ein größter Teiler ist, nehmen wir an, $f \in K[X]$ sei ein weiterer gemeinsamer Teiler von $X^m - 1$ und $X^n - 1$. Wir müssen zeigen, daß dann $f|X^g - 1$. Wir rechnen nun im Faktorring $K[X]/(f)$. Da $f|X^m - 1$ folgt wie oben $X^m + (f) = 1 + (f)$. Ebenso, da $f|X^n - 1$ folgt $X^n + (f) = 1 + (f)$. Nach Proposition 2.6.16 (c,i) (oder dem Lemma von Bézout) angewandt auf den Ring $\mathbb{Z}$, gibt es $k, l \in \mathbb{Z}$ mit $mk + nl = g$. Es folgt

$$\begin{aligned} X^g + (f) &= (X + (f))^g \\ &= (X + (f))^{mk+nl} \\ &= (X + (f))^{mk}(X + (f))^{nl} \\ &= (1 + (f))^k (1 + (f))^l = 1 + (f) \end{aligned}$$

Also $X^g \equiv 1 \mod (f)$, dh. $X^g - 1 \equiv 0 \mod (f)$, in anderen Worten $f|X^g - 1$. □

2.6.5 Primfaktorzerlegung im Quotientenkörper $\mathrm{Frac}(R)$

Satz 2.6.22. *Sei R faktoriell, $P \subset R\backslash\{0\}$ eine Transversale der Primelemente bezüglich $\sim$, und $K = \mathrm{Frac}(R)$.*

(a) Zu jedem Element $0 \neq x \in K$ gibt es bis auf Assoziiertheit eindeutig bestimmte teilerfremde $a, b \in R\backslash\{0\}$ mit $x = \frac{a}{b}$.

(b) Zu jedem $0 \neq x \in K$ gibt es genau eine Einheit $u \in R^*$ und genau eine Familie $(\nu_p(x))_{p \in P}$ von Zahlen in $\mathbb{Z}$, fast alle null, mit $x = u \prod_{p \in P} p^{\nu_p(x)}$.

Beweis. **Zu (a):** Nach Definition gibt es $a', b' \in R\backslash\{0\}$ mit $x = \frac{a'}{b'}$. Sei $t \in R$ ein ggT von a', b', sei $a' = at$ und $b' = bt$. Dann sind a, b teilerfremd, und $x = \frac{a}{b}$. Ist auch $x = \frac{c}{d}$ mit teilerfremden $c, d \in R\backslash\{0\}$, dann $ad = bc$. Mit dem Lemma von Euklid folgt daraus $a|c$, $c|a$, also $a \sim c$. Ebenso $b \sim d$.
Zu (b): Sei $x = \frac{a}{b}$ mit teilerfremden $a, b \in R\backslash\{0\}$, $a = u_a \prod_{p \in P} p^{\nu_p(a)}$ und $b = u_b \prod_{p \in P} p^{\nu_p(b)}$, dann ist $x = u_a u_b^{-1} \prod_{p \in P} p^{\nu_p(a) - \nu_p(b)}$ und

$$\nu_p(a) - \nu_p(b) = \begin{cases} \nu_p(a) & \text{wenn } \nu_p(a) > 0 \\ -\nu_p(b) & \text{wenn } \nu_p(b) > 0 \end{cases}.$$

Sei $x = v \prod_{p \in P} p^{w_p}$ mit $v \in R^*$ und einer Familie $(w_p)_{p \in P}$ in $\mathbb{Z}$, fast alle null, sei $c = \prod_{w_p > 0} p^{w_p}$ und $d = \prod_{w_p < 0} p^{w_p}$, dann $x = v\frac{c}{d}$ und c, d sind teilerfremd. Nach (a) gilt dann $c \sim a$ und $d \sim b$. Für $w_p > 0$ gilt $w_p = \nu_p(a) = \nu_p(a) - \nu_p(b)$ für $w_p < 0$ gilt $w_p = -\nu_p(b) = \nu_p(a) - \nu_p(b)$. Dann folgt auch $v = u_a u_b^{-1}$. □

2.6.6 Faktorielle Polynomringe

Ist $\varphi : R \to R'$ ein Ringhomomorphismus zwischen kommutativen Ringen R, R', dann ist $\widetilde{\varphi} : R[X] \to R'[X], \sum_{i=0}^{n} r_i X^i \mapsto \sum_{i=0}^{n} \varphi(r_i) X^i$ ein R-Algebrenhomomorphismus. Wir setzen $\widetilde{\varphi}(f) = {}^{\varphi}f$.

Proposition 2.6.23. *Sei R ein kommutativer Ring, $A \subset R$ ein Ideal, $\pi : R \to R/A$ der kanonische Homomorphismus.*

(a) Das von A erzeugte Ideal in $R[X]$ ist $\{g \in R[X] \mid \exists n \in \mathbb{N}_0, a_0, \ldots, a_n \in A : g = \sum_{i=0}^{n} a_i X^i\}$. Wir bezeichnen es mit $AR[X]$. Die Abbildung $R[X]/AR[X] \to (R/A)[X]$, $f + AR[X] \mapsto {}^{\pi}f$ ist ein R-Algebrenisomorphismus.

(b) A ist genau dann Primideal, wenn $AR[X]$ Primideal von $R[X]$ ist.

Beweis. **Zu (a):** Die Abbildung $\widetilde{\pi} : R[X] \to (R/A)[X]$, $f \mapsto {}^{\pi}f$ ist ein surjektiver R-Algebrenhomomorphismus, $\ker(\widetilde{\pi})$ ist genau die angegebene Menge. Offenbar ist $\ker(\widetilde{\pi})$ das von A erzeugte Ideal von $R[X]$. Nach Homomorphiesatz ist $R[X]/AR[X] \to (R/A)[X]$, $f + AR[X] \mapsto {}^{\pi}f$ ein R-Algebrenisomorphismus.
Zu (b): A ist Primideal, genau dann, wenn R/A Integritätsring ist, genau dann, wenn $(R/A)[X]$ Integritätsring ist, genau dann, wenn $R[X]/AR[X]$ Integritätsring ist, genau dann, wenn $AR[X]$ Primideal in $R[X]$ ist. □

Folgerung 2.6.24. *Sei R Integritätsring, $0 \neq p \in R$ ist genau dann Primelement in R, wenn es Primelement in $R[X]$ ist.*

Beweis. p ist Primelement in R genau dann, wenn (p) Primideal von R ist, genau dann, wenn $(p)R[X] = pR[X]$ Primideal von $R[X]$ ist, genau dann, wenn p Primelement in $R[X]$ ist. □

Bemerkung 2.6.25. Sei R Integritätsring. Ist $f \in R[X] \backslash R$ irreduzibel, dann sind die nicht trivialen Koeffizienten von f teilerfremd.

Beweis. Ist $0 \neq r \in R$ Teiler der Koeffizienten von f, dann gibt es $g \in R[X]$ mit $f = rg$. Es folgt $r \in R^*$. □

Definition 2.6.26. Sei R Integritätsring, $0 \neq f \in R[X]$.

(a) f heißt primitiv, wenn die Koeffizienten von f teilerfremd sind.

(b) Ist R sogar faktoriell, dann heißt ein ggT der Koeffizienten $\neq 0$ von f ein Inhalt von f.

Beispiel 2.6.27. $f = 3X^3 - 6X^2 + 15 \in \mathbb{Z}[X]$ hat die Inhalte ± 3, $f = 3(X^3 - 2X^2 + 5)$, wobei $X^3 - 2X^2 + 5$ primitiv ist.

Lemma 2.6.28 (Gauß)**.** *Sei R faktoriell, seien $f, g \in R[X] \backslash \{0\}$.*

(a) Sind f und g primitiv, dann auch das Produkt fg.

(b) Ist r bzw. s ein Inhalt von f bzw. g, dann ist rs ein Inhalt von fg.

Beweis. **Zu (a):** Ist fg nicht primitiv, dann gibt es ein Primelement, $p \in R$, das alle Koeffizienten von fg teilt. Es folgt $fg \in pR[X]$. Da $pR[X]$ Primideal von $R[X]$ ist, folgt $f \in pR[X]$ oder $g \in pR[X]$, also ist f oder g nicht primitiv.
Zu (b): Es gibt primitive Polynome $\widetilde{f}, \widetilde{g} \in R[X]$ mit $f = r\widetilde{f}$, $g = s\widetilde{g}$. Dann ist $fg = rs\widetilde{f}\widetilde{g}$. Nach (a) ist $\widetilde{f}\widetilde{g}$ primitiv, also ist rs Inhalt von fg. □

Lemma 2.6.29. *Seien R faktoriell, $K = \mathrm{Frac}(R)$. Zu jedem $0 \neq f \in K[X]$ gibt es x in K und ein primitives Polynom $\widetilde{f} \in R[X]$ mit $f = x\widetilde{f}$. Ist auch $f = yg$ mit $y \in K$ und einem primitive Polynom $g \in R[X]$, dann gibt es $u \in R^*$ so daß $x = uy$, $\widetilde{f} = u^{-1}g$.*

Beweis. Es gibt $0 \neq s \in R$ mit $sf \in R[X]$. Sei r ein Inhalt von sf. Dann gibt es primitive Polynome $\widetilde{f} \in R[X]$ und $sf = r\widetilde{f}$. Es folgt$f = \frac{r}{s}\widetilde{f}$. Ist auch $f = \frac{r'}{s'}g$ mit $r', s' \in R\backslash\{0\}$ und einem primitiven Polynom $g \in R[X]$, dann $rs'\widetilde{f} = r'sg$. Also $rs' \sim r's$, das heißt es gibt $u \in R^*$ so daß $rs' = ur's$ und $\frac{r}{s} = u\frac{r'}{s'}$, $g = u\widetilde{f}$. □

Folgerung 2.6.30. *Sei R faktoriell, $K = \mathrm{Frac}(R)$. $K[X]$ besitzt eine Transversale der irreduziblen Polynome bezüglich $\sim$, bestehend aus primitiven Polynomen in $R[X]$.*

Beweis. In jeder Assoziiertheitsklasse der irreduziblen Polynome von $K[X]$ liegt nach dem vorhergehenden Lemma ein primitives Polynom aus $R[X]$. □

Folgerung 2.6.31. *Sei R faktoriell, $K = \mathrm{Frac}(R)$.*

(a) Seien $f, g \in K[X]$, $f = x\widetilde{f}$, $g = y\widetilde{g}$ mit $x, y \in K$, primitiven $\widetilde{f}, \widetilde{g} \in R[X]$. Gilt $f \mid g$ in $K[X]$, dann $\widetilde{f} \mid \widetilde{g}$ in $R[X]$.

(b) Sind $f, g \in R[X]$, sei f primitiv. Gilt $f \mid g$ in $K[X]$, dann gilt $f \mid g$ auch in $R[X]$.

(c) Besitzen $f, g \in R[X]$ einen gemeinsamen Teiler in $K[X] \backslash K$, dann besitzen sie auch einen solchen in $R[X] \backslash R$.

Beweis. **Zu (a):** Seien $g = fh$ mit $h \in K[X]$, $h = z\widetilde{h}$ mit $z \in K$ und primitivem $\widetilde{h} \in R[X]$. Nach dem vorhergehenden Lemma gibt es $u \in R^*$ mit $uy = xz <$, $\widetilde{g} = u\widetilde{f}\widetilde{h} = \widetilde{f}(u\widetilde{h})$.
Zu (b): Sei y ein Inhalt von g, $\widetilde{g} \in R[X]$ primitiv mit $g = y\widetilde{g}$. Da $f \mid \widetilde{g}$ in $K[X]$ gilt $\widetilde{f} \mid \widetilde{g}$ in $R[X]$. Also existiert $h \in R[X]$ mit $\widetilde{g} = fh$, also $g = f(yh)$.
Zu (c): Sei $h \in K[X] \backslash K$ Teiler von f, g, sei $h = z\widetilde{h}$ mit $z \in K$ und primitivem $\widetilde{h} \in R[X]$. Dann $\widetilde{h} \mid f, g$ in $K[X]$, also nach (b) $\widetilde{h} \mid f, g$ in $R[X]$. □

Folgerung 2.6.32. *Sei R faktoriell, $K = \mathrm{Frac}(R)$, $f \in R[X]$ normiert.*

(a) Sind $g, h \in K[X]$ normiert mit $f = gh$, dann gilt $g, h \in R[X]$.

(b) Ist $x \in K$ eine Nullstelle von f, dann gilt $x \in R$ und x teilt den konstanten Koeffizienten von f.

Beweis. **Zu (a):** Es gibt $a, b, c, d \in R \backslash \{0\}$ und primitive Polynome $\widetilde{g}, \widetilde{h} \in R[X]$ mit $g = \frac{a}{b}\widetilde{g}$, $h = \frac{c}{d}\widetilde{h}$. Sei α bzw. β der höchste Koeffizient von $\widetilde{g}$, $\widetilde{h}$ dann $\frac{a}{b}\alpha = 1 = \frac{c}{d}\beta$. Da $bdf = ac\widetilde{g}\widetilde{h}$ und f, $\widetilde{g}$, $\widetilde{h}$ primitiv sind, gilt $bd \sim ac$. Da auch $bd = ac\alpha\beta$, folgt $\alpha\beta \in R^*$, also $\alpha, \beta \in R^*$. Es folgt $\frac{a}{b} = \alpha^{-1} \in R$, $\frac{c}{d} = \beta^{-1} \in R$, somit $g, h \in R[X]$.
Zu (b): Es gibt $g \in K[X]$ mit $f = (X - x)g$, g normiert. Nach (a) gilt $X - x, g \in R[X]$, also $x \in R$. Hieraus folgen beide Behauptungen. □

Satz 2.6.33 (Gauß)**.** *Sei R faktoriell, $K = \mathrm{Frac}(R)$.*

(a) $R[X]$ ist faktoriell.

(b) Ist $P \subset R \backslash \{0\}$ eine Transversale der Primelemente von R, Q eine Transversale der irreduziblen Polynome $K[X]$, bestehend aus primitiven Polynomen in $R[X]$, dann ist $P \cup Q$ eine Transversale der Primelemente von $R[X]$.

Beweis. Sei $0 \neq f \in K[X]$. Es gibt eindeutige $x \in K$ und $(w_q(f))_{q \in Q} \in \mathbb{N}_0$ fast alle 0, mit $f = x \prod_{q \in Q} q^{w_q(f)}$. Sei $c \in R$ ein Inhalt von f und $\widetilde{f} \in R[X]$ ein primitives Polynom mit $f = c\widetilde{f}$. Es gibt $a, b \in R \backslash \{0\}$ mit $x = \frac{a}{b}$. Es folgt $bc\widetilde{f} = a \prod_{q \in Q} q^{w_q(f)}$. Da $\widetilde{f}$ und das Produkt primitiv sind, folgt $bc \sim a$, also $x = \frac{a}{b} \in R$. Nun gibt es eindeutige $u \in R^*$ und Zahlen $(\nu_p(x))_{p \in P}$ in $\mathbb{N}_0$, fast alle 0 mit $x = u \prod_{p \in P} p^{\nu_p(x)}$. Es folgt $f = u \prod_{p \in P} p^{\nu_p(x)} \prod_{q \in Q} q^{w_q(f)}$. Ist auch $f = u' \prod_{p \in P} p^{\nu'_p} \prod_{q \in Q} q^{w'_q}$ eine solche Zerlegung, dann gilt für alle $q \in Q$: $w'_q = w_q(f)$, dann $u \prod_{p \in P} p^{\nu_p(x)} = u' \prod_{p \in P} p^{v'_p}$. Hieraus folgt $u = u'$ und für alle $p \in P$: $\nu_p(x) = v'_p$. □

Folgerung 2.6.34. *Ist R faktoriell, $n \in \mathbb{N}$, dann ist auch $R[X_1, \ldots, X_n]$ faktoriell.*

Beweis. Durch Induktion nach n. □

Ist R faktoriell aber kein Körper, dann ist $R[X]$ faktoriell, aber kein Hauptidealring.

Folgerung 2.6.35. *Sei R faktoriell, $K = \mathrm{Frac}(R)$, $f \in R[X] \backslash R$.*

(a) Ist f nicht Produkt von nichtkonstanten Polynomen in $R[X]$, dann ist f in $K[X]$ irreduzibel.

(b) Ist f in $R[X]$ irreduzibel, dann ist f auch in $K[X]$ irreduzibel.

(c) Ist f primitiv und irreduzibel in $K[X]$, dann ist f irreduzibel in $R[X]$.

Beweis. **Zu (a):** Sei $f = u\prod_{p\in P} p^{\nu_p(x)}\prod_{q\in Q} q^{w_q(f)}$ wie oben zerlegt. Nach Voraussetzung existiert $q \in Q$: $\nu_q(f) = 1$ und für alle $q' \in Q\backslash\{q\}$: $w_{q'}(f) = 0$.
Zu (b): Dies folgt aus (a).
Zu (c): Ist f wie in (a) zerlegt und primitiv, irreduzibel, dann ist für alle $p \in P$ $\nu_p(x) = 0$ und es existiert $q \in Q$: $\nu_q(f) = 1$ und für alle $q' \in Q\backslash\{q\}$: $w_{q'}(f) = 0$. Es folgt $f = uq$. □

2.6.7 Irreduzibilitätskriterien

Proposition 2.6.36. *Seien R, R' Integritätsringe, $f \in R[X]\backslash R$ primitiv, $\varphi : R[X] \to R'$, der nichtkonstante Faktoren von f auf Nichteinheiten abbildet. Ist $\varphi(f)$ irreduzibel, dann ist auch f irreduzibel.*

Beweis. Seien $g, h \in R[X]$ mit $f = gh$. Falls $g \in R$, dann gilt $g \in R^*$, da f primitiv ist, ebenso für h. Sind g, h nicht konstant, dann sind $\varphi(g)$, $\varphi(h)$ Nichteinheiten in R', also ist $\varphi(f) = \varphi(g)\varphi(h)$ reduzibel. □

Satz 2.6.37. *Sei R Integritätsring.*

(a) Sei $\varphi : R[X] \to R[X]$ ein Automorphismus, $f \in R[X]\backslash R$ primitiv. Ist $\varphi(f)$ irreduzibel, dann ist auch f irreduzibel.

*(b) (**Reduktionskriterium**) Seien $\mathfrak{P} \subset R$ ein Primideal, $\pi : R \to R/\mathfrak{P}$ der kanonische Homomorphismus, sei $f = \sum_{i=0}^{n} r_i X^i \in R[X]\backslash R$ primitiv mit $r_n \notin \mathfrak{P}$. Ist ${}^{\pi}f \in (R/\mathfrak{P})[X]$ irreduzibel, dann ist auch f irreduzibel.*

Beweis. **Zu (a):** φ bildet nur Einheiten auf Einheiten ab. Wende die Proposition an.
Zu (b): Sei $f = gh$ mit $g, h \in R[X]$, $g \notin R$. Dann ist ${}^{\pi}f = {}^{\pi}g\,{}^{\pi}h$. Das bedeutet für den Grad $\deg(f) = \deg({}^{\pi}f) = \deg({}^{\pi}g) + \deg({}^{\pi}h) \leqslant \deg(g) + \deg(h) = \deg(f)$, also $\deg({}^{\pi}g) = \deg(g)$, und ${}^{\pi}g$ kann keine Einheit sein. Nun wende man die Proposition auf $\widetilde{\pi} : R[X] \to (R/\mathfrak{P})[X]$ an. □

Proposition 2.6.38. *Sei R Integritätsring.*

(a) X ist Primelement in $R[X]$.

(b) Gilt $fg = rX^n$ mit $0 \neq r \in R$, $n \in \mathbb{N}$, $f, g \in R[X]$, dann gibt es $k, l \in \mathbb{N}_0$ mit $k + l = n$ und $s, t \in R\backslash\{0\}$ mit $f = sX^k$ und $g = tX^l$.

Beweis. **Zu (a):** Da (X) Primideal ist, ist X Primelement in $R[X]$.
Zu (b): Nach (a) gilt $X \mid f$ oder $X \mid g$. Sei etwa $f = Xf_1$. Dann folgt $f_1 g = rX^{n-1}$. Falls $n = 1$, dann $f, g \in R$. Falls $n > 1$, gibt es nach Induktionsannahme $k, l \in \mathbb{N}_0$ mit $k + l = n - 1$, $s, t \in R\backslash\{0\}$ mit $f_1 = sX^k$, $g = tX^l$. Ebenso wenn $X \mid g$. □

Satz 2.6.39 (Irreduzibilitätskriterium von Eisenstein)**.** *Sei R ein Integritätsring, $0 \neq f = \sum_{i=0}^{n} r_i X^i \in R[X]$ primitiv, $p \in R$ ein Primelement mit $p \nmid r_n$ aber $p \mid r_j$ für alle $0 \leqslant j \leqslant n-1$, und $p^2 \nmid r_0$. Dann ist f in $R[X]$ irreduzibel. Ist R faktoriell, $K = \mathrm{Frac}(R)$, dann ist f auch in $K[X]$ irreduzibel.*

Beweis. Sei $\pi : R \to R/(p)$ der kanonische Homomorphismus, $\widetilde{\pi} : R[X] \to (R/(p))[X], g \mapsto {}^{\pi}g$ davon induziert. Angenommen, es existieren $g, h \in R[X]\backslash R$ mit $f = gh$. Dann ist ${}^{\pi}g\,{}^{\pi}h = {}^{\pi}f = \overline{r}_n X^n$. Wie oben gilt $\deg({}^{\pi}g) = \deg(g)$ und $\deg({}^{\pi}h) = \deg(h)$. Nach Proposition gibt es $k, l \in \mathbb{N}$ mit $k + l = n$ und $s, t \in R\backslash\{0\}$ mit ${}^{\pi}g = \overline{s}X^k$, ${}^{\pi}h = \overline{t}X^l$. Da $k, l \geqslant 1$ sind, sind die konstanten Koeffizienten von g, h durch p teilbar, also ist der konstante Koeffizient von f durch p^2 teilbar. Widerspruch!
Die zweite Aussage folgt aus der Folgerung vorher. □

Beispiele 2.6.40. (a) Sei R ein Integritätsring. Ein normiertes Polynom $f \in R[X]$ vom Grad 2 oder 3 ist genau dann irreduzibel, wenn es in R keine Nullstellen hat (Denn f ist genau dann reduzibel, wenn es einen Faktor $X - a$ mit $a \in R$ hat.)

(b) Sei $f = X^4 + X^3 + X^2 + 1 \in \mathbb{Z}[X]$. Wir zeigen, daß f in $\mathbb{Z}[X]$ irreduzibel ist; dann ist f auch irreduzibel in $\mathbb{Q}[X]$.
f hat keine (normierten) Linearfaktoren in $\mathbb{Z}[X]$: f hat keine Nullstellen in $\mathbb{Z}$, denn die Teiler von 1, nämlich ± 1 sind keine Nullstellen. Wenn f in quadratische Faktoren zerfällt, dann in normierte quadratische Faktoren. Annahme: es existieren $a, b, c, d \in \mathbb{Z}$ so daß $f = (X^2 + aX + b)(X^2 + cX + d)$. Koeffizientenvegleich ergibt:

$$\begin{aligned} a + c &= 1 \\ b + d + ac &= 1 \\ ad + bc &= 0 \\ bd &= 1 \end{aligned}$$

Insbesondere muss dann $b, d \in \{\pm 1\}$. Ist $b = 1$, dann auch $d = 1$ und $ac = -1$, dh. $a = \mp 1$ und $c = \pm 1$ also $a + c = 0$. Widerspruch. Ist andererseits $b = d = -1$, dann $-a - c = 0$. Widerspruch. Also zerfällt f nicht in quadratische Faktoren. Damit ist f in $\mathbb{Z}[X]$ irreduzibel.
Man kann auch mit dem Reduktionskriterium argumentieren. Modulo 2: $\overline{1}$ ist Nullstelle. Modulo 3: f hat keine Nullstelle in $\mathbb{Z}/(3)[X]$, also keine Linearfaktoren. Die quadratischen irreduziblen Polynome in $\mathbb{Z}/(3)[X]$ sind $X^2 + 1$, $X^2 + X + \overline{2}$ und $X^2 + \overline{2}X + \overline{2}$. Division mit Rest in $\mathbb{Z}/(3)[X]$ liefert

$$f = (X^2 + \overline{1})(X^2 + X) - X + 1 = (X^2 + X + \overline{2})(X^2 + \overline{2}) + X = (X^2 + \overline{2}X + \overline{2})(X^2 + \overline{2}X + \overline{1}) + \overline{2},$$

also ist f durch keines der drei Polynome teilbar und folglich in $\mathbb{Z}/(3)[X]$ irreduzibel und damit auch in $\mathbb{Z}[X]$.

(c) Sei R faktoriell, $K = \mathrm{Frac}(R)$. Seien $a \in R$, $p \in R$ Primelement mit $p \mid a$, $p^2 \nmid a$, $n \in \mathbb{N}$. Dann ist $f = X^n - a$ irreduzibel in $R[X]$ nach Eisenstein, damit auch in $K[X]$.

(d) Sei K Körper, $n \in \mathbb{N}$. $f = X^n - Y \in K[X, Y] = K[X][Y]$ ist trivialerweise irreduzibel, oder $f \in K[Y][X]$ ist irreduzibel nach (c), denn Y ist Primelement in $K[Y]$.

(e) Sei K Körper, $\mathrm{char}(K) \neq 2$. $f = X^2 + Y^2$ ist irreduzibel, da f als Polynom in $K[Y]$ keine Nullstelle hat. $g = X^2 + Y^3 + Z^n \in K[X, Y, Z] = K[X, Y][Z]$ ist irreduzibel nach (c).

(f) Sei $p \in \mathbb{N}$ eine Primzahl. Wir zeigen, daß $\Phi_p = X^{p-1} + X^{p-2} + \cdots + X + 1$ in $\mathbb{Z}[X]$ und $\mathbb{Q}[X]$ irreduzibel ist. Die Abbildung $\alpha : \mathbb{Z}[X] \to \mathbb{Z}[X]$, $f \mapsto f(X + 1)$ ist Ringautomorphismus mit Umkehrabbildung $\alpha^{-1}(g) = g(X - 1)$. Es genügt zu zeigen, daß $\alpha(\Phi_p) = \Phi_p(X + 1)$ irreduzibel ist. Es gilt

$$X\Phi_p(X + 1) = ((X + 1) - 1) \sum_{i=0}^{p-1} (X + 1)^i = (X + 1)^p - 1 = \sum_{i=0}^{p-1} \binom{p}{i} X^{p-i}.$$

Also $\Phi_p(X + 1) = \sum_{i=0}^{p-1} \binom{p}{i} X^{p-i-1}$. Es gilt $p \mid \binom{p}{i}$ für $1 \leqslant i < p$, also ist $\Phi_p(X + 1)$ nach Eisenstein irreduzibel.

Beispiele* 2.6.41. (a) Welche der folgenden Polynome in $\mathbb{Q}[X]$ sind irreduzibel?

$$\begin{aligned} &X^7 - 6 \\ &\frac{1}{2}X^5 - 10X^3 + 19 \\ &6X^3 + 3X^2 + 2 \end{aligned}$$

(b) Welche der folgenden Polynome sind irreduzibel in $\mathbb{C}[X, Y]$?

$$\begin{aligned} &X^5 + X^2Y^3 - Y^3 + X + 1 \\ &X^6 + Y^9 \end{aligned}$$

(c) Sei K ein Körper. Seien $n, m \in \mathbb{N}$ teilerfremd. Man zeige, daß das Polynom $f = X^n - Y^m \in K[X, Y]$ irreduzibel ist.

Beweis. Angenommen dies ist nicht der Fall, dann gibt es Polynome $g, h \in K[X,Y]$ mit $X^n - Y^m = f = g \cdot h$. Betrachte den K-Algebrenhomomorphismus

$$K[X,Y] \mapsto K[Z], X \mapsto Z^m, Y \mapsto Z^n.$$

Für das Bild von f unter diesem Homomorphismus gilt

$$0 = (Z^m)^n - (Z^n)^m = f(Z^m, Z^n) = g(Z^m, Z^n)h(Z^m, Z^n).$$

Da $K[Z]$ Integritätsring ist, muß eines der beiden Polynome $g(Z^m, Z^n)$ oder $h(Z^m, Z^n)$ das Nullpolynom sein. Ohne Einschränkung sei dies $g(Z^m, Z^n)$. Mit $g(X,Y) = \sum_{\substack{i,j \\ i<n, j<m}} a_{ij} X^i Y^j$ können wir also schreiben

$$g(Z^m, Z^n) = \sum_{\substack{i,j \\ i<n, j<m}} a_{ij} Z^{mi} Z^{nj} = \sum_k \sum_{\substack{i<n, j<m \\ mi+nj=k}} a_{ij} Z^k.$$

Damit $g(Z^m, Z^n)$ das Nullpolynom ist, müssen alle Koeffizienten der Z^k gleich 0 sein, es muß also für alle k gelten

$$\sum_{\substack{i<n, j<m \\ mi+nj=k}} a_{ij} = 0.$$

Es können jedoch für festes k in einer solche Summe nicht mehrere Summanden vorkommen, denn wäre $mi + nj = mi' + nj'$, so wäre $m(i - i') = n(j' - j)$. Dies bedeutet

$$\begin{aligned} i &\equiv i' \mod n \\ j &\equiv j' \mod m \end{aligned}$$

aber es gilt $i, i' \in \{0, \ldots, n-1\}$ und $j, j' \in \{0, \ldots, m-1\}$, so daß folgt $i = i'$ und $j = j'$. Also besteht die Summe $\sum_{\substack{i<n, j<m \\ mi+nj=k}} a_{ij}$ aus höchstem einem a_{ij}, und dieses muß dann gleich 0 sein. Also ist auch das Polynom $g(X,Y) = \sum_{\substack{i,j \\ i<n, j<m}} a_{ij} X^i Y^j$ gleich 0. Widerspruch. □

2.6.8 Der chinesische Restsatz

Proposition 2.6.42. *Sei $A \subset R$ ein Ideal. Für $x \in R$ sind folgende Aussagen äquivalent:*

(a) $x + A \in (R/A)^*$

(b) $A + (x) = R$

Beweis. $x + A \in (R/A)^*$ genau dann, wenn $y \in R$ existiert mit $(x + A)(y + A) = 1 + A$ genau dann, wenn $y \in R$ und $a \in A$ existieren mit $xy + a = 1$ genau dann, wenn $(x) + A = R$. □

Definition 2.6.43. Zwei Ideale A, B in R heißen fremd oder relativ prim, wenn $A + B = R$, dh. es existieren $a \in A$ und $b \in B$ mit $a + b = 1$.

Definition 2.6.44. Das Produkt von Idealen $A_1, \ldots, A_n$, $n \geqslant 1$, in R ist definiert durch

$$A_1 \cdots A_n = \left\{ x \in R \;\middle|\; \exists m \in \mathbb{N}_0, a_{k,i} \in A_i, 1 \leqslant k \leqslant m, 1 \leqslant i \leqslant n \text{ mit } x = \sum_{k=1}^{m} a_{k,1} \cdots a_{k,n} \right\}.$$

Das ist das kleinste Ideal von R, das alle $a_1 \cdots a_n$, $a_i \in A_i$ enthält.

Proposition 2.6.45. *(a) Sei R Hauptidealring, $a, b \in R \backslash \{0\}$. (a) und (b) sind genau dann fremd, wenn a, b teilerfremd sind.*

(b) Ist $A \subset R$ maximales Ideal, $B \subset R$ ein Ideal mit $B \nsubseteq A$, dann sind A und B fremd. Insbesondere sind zwei verschiedene maximale Ideale fremd.

(c) Sind $A_1, \ldots, A_n$, $B_1, \ldots, B_m$ Ideale von R und A_i und B_j fremd für $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant m$, dann sind $A_1 \cdots A_n$ und $B_1 \cdots B_m$ fremd.

(d) Sind $A_1, \ldots, A_n$ paarweise fremd, dann gilt

$$\bigcap_{i=1}^{n} A_i = A_1 \cdots A_n.$$

Beweis. **Zu (a):** (a) und (b) sind genau dann fremd, wenn $(a) + (b) = R$, genau dann, wenn $r, s \in R$ existieren mit $ra + sb = 1$ genau dann, wenn a und b teilerfremd sind.
Zu (b): Es gilt $A \subsetneq A + B \subset R$, also $A + B = R$.
Zu (c): Es genügt die Aussage für $m = 1$ zu zeigen. Sei $B_1 = B$. Es gilt $A_i + B = R$ für alle $1 \leqslant i \leqslant n$, also gibt es $a_i \in A_i$ und $b_i \in B$ mit $a_i + b_i = 1$ für alle $1 \leqslant i \leqslant n$. Also gilt $1 = \prod_{i=1}^{n}(a_i + b_i) = a_1 \cdots a_n + b$ für ein $b \in B$, dh. $A_1 \cdots A_n + B = R$.
Zu (d): Das ist klar für $n = 1$. Für $n = 2$: $A_1 \cdot A_2 \subset A_1 \cap A_2$ ist klar. Wir zeigen $A_1 \cap A_2 \subset A_1 \cdot A_2$. Es existiert $a_i \in A_i$, $i = 1, 2$ mit $a_1 + a_2 = 1$. Für $x \in A_1 \cap A_2$ gilt $x = xa_1 + xa_2 \in A_1 \cdot A_2$. Die Aussage sei nun bewiesen für $n \geqslant 2$. Nach Voraussetzung sind A_i und A_{n+1} fremd für $1 \leqslant i \leqslant n$. Nach (c) sind $A_1 \cdots A_n$ und A_{n+1} fremd. Nach dem Fall $n = 2$ und nach Induktionsvoraussetzung gilt dann

$$A_1 \cdots A_n \cdot A_{n+1} = (A_1 \cdots A_n) \cap A_{n+1} = (\bigcap_{i=1}^{n} A_i) \cap A_{n+1} = \bigcap_{i=1}^{n+1} A_i.$$

□

Chinesischer Restsatz 2.6.46. *Seien $A_1, \ldots, A_n$ paarweise fremde Ideale von R.*

(a) Die Abbildung

$$\begin{aligned} R/A_1 \cdots A_n &\to \prod_{i=1}^{n} R/A_i \\ r + A_1 \cdots A_n &\mapsto (r + A_1, \ldots, r + A_n) \end{aligned}$$

ist ein R-Algebrenisomorphismus.

(b) Die Abbildung

$$\begin{aligned} (R/A_1 \cdots A_n)^* &\to \prod_{i=1}^{n} (R/A_i)^* \\ r + A_1 \cdots A_n &\mapsto (r + A_1, \ldots, r + A_n) \end{aligned}$$

ist ein Gruppenisomorphismus.

Beweis. **Zu (a):** Die Abbildung

$$\begin{aligned} R &\to \prod_{i=1}^{n} R/A_i \\ r + A_1 \cdots A_n &\mapsto (r + A_1, \ldots, r + A_n) \end{aligned}$$

ist ein R-Algebrenhomomorphismus mit $\ker(\rho) = \bigcap_{i=1}^{n} A_i = A_1 \cdots A_n$. ρ ist surjektiv, denn für alle $1 \leqslant i, j \leqslant n$, $i \neq j$ existieren $x_{ij} \in A_i$ und $y_{ij} \in A_j$ so, daß $x_{ij} + y_{ij} = 1$. Sei $1 \leqslant i \leqslant n$ fest. Dann

$$1 = \prod_{j \neq i} (x_{ij} + y_{ij}) = c_i + d_i,$$

mit $d_i = \prod_{j \neq i} y_{ij}$ und $c_i = 1 - d_i$. Also gilt für alle $j \neq i$ $d_i \in A_j$ und $c_i \in A_i$. Sei $(r_1 + A_1, \ldots, r_n + A_n) \in \prod_{i=1}^{n} R/A_i$, sei $r = \sum_{i=1}^{n} d_i r_i$. In R/A_i gilt

$$r + A_i = d_i + r_i + A_i = r_i + A_i,$$

also gilt $\rho(r) = (r_1 + A_1, \ldots, r_n + A_n)$. Aus dem Homomorphiesatz ergibt sich die Behauptung.
Zu (b): Wegen (a) gilt $r + A_1 \cdots A_n \in (R/A_1 \cdots A_n)^*$ genau dann, wenn $(r + A_1, \ldots, r + A_n) \in (\prod_{i=1}^{n} R/A_i)^*$ genau dann, wenn für alle $1 \leqslant i \leqslant n$ $r + A_i \in (R/A^i)^*$. Mit (a) folgt die Behauptung. □

Folgerung 2.6.47. *Sei R Hauptidealring.*

(a) Sind $a_1, \ldots, a_n \in R\backslash\{0\}$ paarweise teilerfremd, dann ist die Abbildung

$$\begin{aligned} R/(a_1 \cdots a_n) &\to \prod_{i=1}^{n} R/(a_i) \\ r + (a_1 \cdots a_n) &\mapsto (r + (a_1), \ldots, r + (a_n)) \end{aligned}$$

ein R-Algebrenisomorphismus. Zu $b_1, \ldots, b_n \in R$ gibt es also $r \in R$ mit $r \equiv b_i \mod a_i$ für $1 \leqslant i \leqslant n$, und r ist modulo $a_1 \cdots a_n$ eindeutig bestimmt.
Ferner ist die Abbildung

$$\begin{aligned} (R/(a_1 \cdots a_n))^* &\to \prod_{i=1}^{n} (R/(a_i))^* \\ r + (a_1 \cdots a_n) &\mapsto (r + (a_1), \ldots, r + (a_n)) \end{aligned}$$

ein Gruppenisomorphismus.

(b) Sind $p_1, \ldots, p_n$ paarweise nicht zueinander assoziierte Primelemente von R, $\nu_1, \ldots, \nu_n \in \mathbb{N}$, dann gilt (a) für $a_i = p_i^{\nu_i}$, $1 \leqslant i \leqslant n$.

Beweis. **Zu (a):** Sind $a_1, \ldots a_n \in R\backslash\{0\}$ paarweise teilerfremd, dann sind $(a_1), \ldots, (a_n)$ paarweise fremd. Es gilt $(a_1) \cdots (a_n) = (a_1 \cdots a_n)$. Die Behauptung folgt aus dem Satz.
Zu (b): Die $a_i = p_i^{\nu_i}$, $1 \leqslant i \leqslant n$, sind paarweise teilerfremd. □

Beispiel* 2.6.48. Eine natürliche Zahl heißt quadratfrei, wenn sie durch keine Quadratzahl ungleich 1 teilbar ist. Man zeige, daß es beliebig lange Abschnitte direkt aufeinander folgender natürlicher Zahlen gibt, in denen jedes Folgeglied nicht quadratfrei ist.

Beweisskizze. Mithilfe des Chinesischen Restsatzes kann man genauer zeigen: Ist $p_1, p_2, \ldots$ die Folge der positiven Primzahlen, so gibt es für jedes $n \geqslant 1$ eine natürliche Zahl a_n so, daß für alle $1 \leqslant k \leqslant n$ die Zahl $a_n + k - 1$ durch p_k^2 teilbar (und damit nicht quadratfrei) ist. □

Kapitel 3

Körpertheorie

Zur Einstimmung:

Beispiel* **3.0.49.** Sei K ein Körper. Man berechne das Produkt $\prod_{x\in K^*} x$.

3.1 Endliche und algebraische Körpererweiterungen

3.1.1 Definitionen

Sei L ein Körper. Ein Unterring $K \subset L$, der auch ein Körper ist, heißt Unterkörper von L. Dann heißt L auch Oberkörper von K, das Paar $K \subset L$ heißt Körpererweiterung. Man schreibt auch L/K dafür. Ein Unterkörper $E \subset L$ mit $K \subset E$ heißt Zwischenkörper zwischen K und L.

Ist $K \subset L$ eine Körpererweiterung, $A \subset L$ eine Teilmenge, dann ist

$$\begin{aligned} K[A] &= \cap\{R : R \text{ Unterring von } L \text{ mit } K \cup A \subset R\} \\ &= \{x \in L; \exists n \in \mathbb{N}_0, f \in K[X_1, \ldots, X_n], a_1, \ldots, a_n : x = f(a_1, \ldots, a_n)\} \end{aligned}$$

der kleinste Unterring, der $K \cup A$ enthält,

$$K(A) = \cap\{E : E \text{ Unterkörper von } L \text{ mit } K \cup A \subset E\} = \left\{x \in L; \exists y, z \in K[A], z \neq 0, : x = \frac{y}{z}\right\}$$

der kleinste Unterkörper, der $K \cup A$ enthält. $K(A)$ ist der Quotientenkörper von $K[A]$. Man sagt $K(A)$ und $K[A]$ entstehen durch Adjunktion von A an K. Ist $A = \{a_1, \ldots, a_n\}$, dann ist

$$\begin{aligned} K[A] = K[a_1, \ldots, a_n] &= \{f(a_1, \ldots, a_n) : f \in K[X_1, \ldots, X_n]\} \\ K(A) = K(a_1, \ldots, a_n) &= \left\{\frac{f(a_1, \ldots, a_n)}{g(a_1, \ldots, a_n)} : f, g \in K[X_1, \ldots, X_n], g(a_1, \ldots, a_n) \neq 0\right\}. \end{aligned}$$

Eine Körpererweiterung $K \subset L$ heißt endlich erzeugt bzw. einfach, wenn es $a_1, \ldots, a_n \in L$ gibt mit $L = K(a_1, \ldots, a_n)$ bzw. wenn es $a \in L$ gibt mit $L = K(a)$.

3.1.2 Endliche Körpererweiterungen

Definition 3.1.1. Sei $K \subset L$ eine Körpererweiterung. Dann ist L ein K-Untervektorraum.

$$[L : K] := \dim_K L \in \mathbb{N} \cup \{\infty\}$$

heißt Grad von L über K. Die Körpererweiterung L/K heißt endlich, wenn $[L : K]$ endlich ist, andernfalls unendlich.

Proposition 3.1.2. *Seien $K \subset L \subset M$ Körpererweiterungen. Die Erweiterung M/K ist genau dann endlich, wenn L/K und M/L endlich sind. Gilt eine dieser Aussagen, dann ist*

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

Beweis. Aus der Linearen Algebra folgt leicht, dass, wenn M/K endlich ist, auch L/K und M/L endlich sind. Sei andererseits $\{x_1, \dots, x_n\}$ eine K-Basis von L, und $\{y_1, \dots, y_m\}$ eine L-Basis von M. Dann ist $\{x_i y_j : 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m\}$ eine K-Basis von M. □

Ist L/K eine endliche Körpererweiterung, $n = [L : K]$ und $x \in L$, dann sind $1, x, \dots, x^n$ linear abhängig über K, dh. es existieren $\alpha_0, \dots, \alpha_n \in K$ nicht alle Null mit $\sum_{i=0}^{n} \alpha_i x^i = 0$, d.h. x ist Nullstelle des Polynoms $f = \sum_{i=0}^{n} \alpha_i X^i \in K[X] \backslash \{0\}$.

3.1.3 Algebraische Elemente und Erweiterungen

Definition 3.1.3. Sei $K \subset L$ Körpererweiterung. Ein Element $x \in L$ heißt algebraisch über K, wenn es $f \in K[X]$ gibt mit $f(x) = 0$. Es heißt transzendent, wenn es nicht algebraisch ist. Kurz x/K algebraisch bzw. transzendent.

Die Körpererweiterung L/K heißt algebraisch, wenn jedes Element $x \in L$ über K algebraisch ist, sie heißt transzendent, wenn sie nicht algebraisch ist.

Die Bemerkung am Ende von 3.1.2 besagt, daß jede endliche Erweiterung algebraisch ist.

Proposition 3.1.4. *Sei $K \subset L$ Körpererweiterung, $x \in L$ algebraisch über K, sei*

$$\varphi : K[X] \to L, g \mapsto g(x).$$

Dies ist ein K-Algebrenhomomorphismus.

(a) Es gibt genau ein normiertes, irreduzibles Polynom $f \in K[X]$ mit $\ker(\varphi) = (f)$. Die Abbildung

$$K[X]/(f) \to K[x], g + (f) \mapsto g(x)$$

ist K-Algebrenisomorphismus.

(b) Der Ring $K[x]$ ist ein Unterkörper von L mit $[K[x] : K] = \deg(f)$. Ist $n = \deg(f)$, dann ist $1, x, \dots, x^{n-1}$ K-Basis von $K[x]$ über K.

Definition 3.1.5. Das Polynom f in der Proposition heißt Minimalpolynom von x über K.

Beweis. Da x/K algebraisch ist, ist $\ker(\varphi) \neq 0$. Also gibt es genau ein normiertes Polynom $f \in K[X]$ mit $\ker(\varphi) = (f)$. Nach dem Homomorphiesatz ist $K[X]/(f) \to \mathrm{im}(\varphi) = K[x], g + (f) \mapsto g(x)$ ein K-Algebrenisomorphismus. Da $K[X]$ Integritätsring ist, ist (f) Primideal, da $K[X]$ Hauptidealring ist, ist (f) maximales Ideal. Also ist f irreduzibel und $K[X]/(f) \cong K[x]$ ist Körper.

Sei $n = \deg(f)$. Es bleibt zu zeigen, daß $1, x, \cdots, x^{n-1}$ K-Basis von $K[x]$ ist. Lineare Unabhängigkeit sieht man wie folgt. Seien $\beta_0, \dots, \beta_{n-1} \in K$ mit $\sum_{i=0}^{n-1} \beta_i x^i = 0$. Dann gilt $g := \sum_{i=0}^{n-1} \beta_i X^i \in \ker(\varphi)$. Also gilt $f | g$, also $g = 0$ und damit $\beta_i = 0$ für alle $1 \leqslant i \leqslant n$. Um zu zeigen, dass es ein Erzeugendensystem ist, wähle $g \in K[X]$. Dann gibt es $q, r \in K[X]$ mit $g = qf + r$, $\deg(r) < \deg(f)$, $g(x) = r(x)$ und $r(x)$ ist Linearkombination der $1, x, \dots, x^{n-1}$. □

Beispiel* 3.1.6. Sei $d \in \mathbb{N}$ mit $\sqrt{d} \notin \mathbb{Q}$. Man zeige, daß $\mathbb{Q}[\sqrt{d}]$ ein Körper ist.

Proposition 3.1.7. *Sei $K \subset L$ Körpererweiterung. Für $x \in L$ sind äquivalent:*

(a) x ist algebraisch über K.

(b) $K[x] = K(x)$

(c) Es gibt einen Zwischenkörper $K \subset E \subset L$ mit $x \in E$, so daß E/K endlich ist.

Beweis. **(a) ⇒ (b), (c):** Nach der Proposition vorher ist $K[x]$ Körper, also gilt $K[x] = K(x)$. Außerdem ist $K[x]/K$ endlich.
(c) ⇒ (a): Dies folgt aus der Bemerkung am Schluß von 3.1.2.
(b) ⇒ (a): Sei ohne Einschränkung $x \neq 0$. Dann gibt es $0 \neq g \in K[X]$ mit $\frac{1}{x} = g(x)$, also ist x Nullstelle von $Xg - 1 \in K[X] \backslash \{0\}$. □

Proposition 3.1.8. *Sei $K \subset L$ Körpererweiterung, $x \in L$. Für ein normiertes Polynom $f \in K[X]$ mit $f(x) = 0$ sind äquivalent:*

(a) f ist das Minimalpolynom von x.

(b) Für alle $0 \neq g \in K[X]$ gilt: ist $g(x) = 0$, dann $f \mid g$.

(c) Für alle $0 \neq g \in K[X]$ gilt: ist $g(x) = 0$, dann ist $\deg(f) \leqslant \deg(g)$.

(d) f ist irreduzibel.

Beweis. **(a) $\Leftrightarrow$ (b):** Dies gilt nach Definition des Minimalpolynoms.
(b) $\Rightarrow$ (c): Das ist klar.
(c) $\Rightarrow$ (a): Sei h das Minimalpolynom von x. Dann gilt $h \mid f$. Nach (c) gilt $\deg(f) \leqslant \deg(h)$, also sind h und f assoziiert. Da beide normiert sind, folgt $h = f$.
(a) $\Rightarrow$ (d): Das ist gezeigt.
(d) $\Rightarrow$ (a): Sei h das Minimalpolynom von x. Dann gilt $h \mid f$. Da f irreduzibel ist, sind h und f assoziiert, wie oben folgt $h = f$. □

Folgerung 3.1.9. *Seien $K \subset E \subset L$ Körperweiterungen, $x \in L$ algebraisch über K mit Minimalpolynom $f \in K[X]$. Dann ist x auch algebraisch über E. Ist $g \in E[X]$ das Minimalpolynom von x über E, dann gilt $g \mid f$, und $[E(x) : E] \leqslant [K(x) : K]$.*

Beweis. Das ist klar. □

Beispiele 3.1.10. (a) $\mathbb{R} \subset \mathbb{C} = \mathbb{R}[i]$ ist endliche Erweiterung, also algebraisch. Ein Element $x \in \mathbb{C}$ ist Nullstelle von $(X - x)(X - \overline{x}) = X^2 - (x + \overline{x})X + x\overline{x} \in \mathbb{R}[X]$. Für $x \in \mathbb{R}$ ist $X - x$ das Minimalpolynom, für $x \in \mathbb{C} \setminus \mathbb{R}$ ist $X^2 - (x + \overline{x})X + x\overline{x}$ das minimalpolynom. Insbesondere ist $X^2 + 1$ das Minimalpolynom von i über $\mathbb{R}$ und es gilt

$$\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}\,.$$

(b) $\sqrt[3]{2} \in \mathbb{R}$ ist algebraisch über $\mathbb{Q}$ mit Minimalpoynom $X^3 - 2$. Also gilt

$$\mathbb{Q}[X]/(X^3 - 2) \cong \mathbb{Q}[\sqrt[3]{2}] = \mathbb{Q}(\sqrt[3]{2}).$$

(c) $K \subset K(X)$ ist transzendent, denn X/K ist transzendent, $\dim_K K[X] = \infty$, $K[X] \subsetneq K(X)$.

(d) $\mathbb{Q} \subset \mathbb{R}$ ist transzendent, denn zum Beispiel sind e, π transzendent über $\mathbb{Q}$ (Hermite: 187, Lindemann: 1882).

Definition 3.1.11. Sei $K \subset L$ Körpererweiterung, $x \in L$ algebraisch über K, f das Minimalpolynom von x über K. Der Grad von f, $\deg(f) = [K[x] : K]$, heißt auch Grad von x über K.

Beispiel* 3.1.12. Sei $K \subset L$ eine Körpererweiterung und seien $\alpha, \beta \in L$ algebraisch über K. Sei f das Minimalpolynom von α über K und g das Minimalpolynom von β über K. Zeigen Sie, daß f irreduzibel über $K(\beta)$ ist, genau dann, wenn g irreduzibel über $K(\alpha)$ ist.

Proposition 3.1.13. *Sei $K \subset L$ Körpererweiterung.*

(a) Für $x_1, \ldots, x_n$ sind äquivalent:

(i) $x_1, \ldots, x_n$ sind algebraisch über K.

(ii) $K(x_1, \ldots, x_n)$ ist endlich über K.

Gelten (i) und (ii), dann ist $K[x_1, \ldots, x_n] = K(x_1, \ldots, x_n)$ und es gilt $[K(x_1, \ldots, x_n) : K] \leqslant \prod_{i=1}^{n} [K(x_i) : K]$.

(b) Folgende Aussagen sind äquivalent:

(i) L/K ist endlich.

(ii) L/K ist algebraisch und es gibt $x_1, \ldots, x_n \in L$ mit $L = K(x_1, \ldots, x_n)$.

(iii) Es gibt über K algebraische Elemente $x_1, \dots, x_n \in L$ mit $L = K(x_1, \dots, x_n)$.

Beweis. **Zu (a): [(i) ⇒ (ii)]** Induktion nach n. Für $n = 1$ wissen wir, daß $K[x_1] = K(x_1)$ ist, und daß $K(x_1)/K$ endlich ist. Für $n > 1$ nehmen wir an, daß $K[x_1, \dots, x_{n-1}] = K(x_1, \dots, x_{n-1})$ ist, und daß dieser Körper über K endlich ist. Da x_n algebraisch über K ist, ist x_n auch algebraisch über $K(x_1, \dots, x_{n-1})$. Also gilt

$$K(x_1, \dots, x_{n-1})[x_n] = K(x_1, \dots, x_{n-1})(x_n) = K(x_1, \dots, x_n)$$

und dieser Körper ist endlich über $K(x_1, \dots, x_{n-1})$. Dann ist er auch endlich über K.
[(ii) ⇒ (i)] Induktion nach n. Für $n = 1$ gilt $x_i \in K(x_1, \dots, x_n)$ und $K(x_1, \dots, x_n)$ ist endlich über K, also ist x_i algebraisch über K für alle $1 \leqslant i \leqslant n$. Nach Induktionsannahme gilt $K[x_1, \dots, x_{n-1}] = K(x_1, \dots, x_{n-1})$, also

$$K[x_1, \dots, x_n] = K[x_1, \dots, x_{n-1}][x_n] = K(x_1, \dots, x_{n-1})[x_n] = K(x_1, \dots, x_{n-1})(x_n) = K(x_1, \dots, x_n).$$

Ferner gilt

$$[K(x_1, \dots, x_n) : K] = \prod_{i=1}^{n} [K(x_1, \dots, x_i) : K(x_1, \dots, x_{i-1})] \leqslant \prod_{i=1}^{n} [K(x_i) : K].$$

Zu (b): [(i) ⇒ (ii)] Da L/K endlich ist, ist jedes $x \in L$ algebraisch über K. Es gibt $x_1, \dots, x_n \in L$ mit $L = K(x_1, \dots, x_n)$, zum Beispiel eine K-Basis von L.
[(ii) ⇒ (iii)] Das ist klar.
[(iii) ⇒ (i)] Das folgt aus (a). □

Folgerung 3.1.14. *Seien $K \subset L \subset M$ Körpererweiterungen. M/K ist genau dann algebraisch, wenn L/K und M/L algebraisch sind.*

Beweis. Sei zunächst M/K algebraisch. Es ist klar, daß L/K ebenfalls algebraisch ist. Weiterhin ist jedes Element $x \in M$ algebraisch über K, also über L.

Seien andererseits L/K und M/L algebraisch. Sei $x \in M$. Dann gibt es $0 \neq f = \sum_{i=0}^{n} \alpha_i X^i \in L[X]$ mit $f(x) = 0$. Sei $E = K(\alpha_0, \dots, \alpha_n)$. Dann gilt $f \in E[X]$, und x ist algebraisch über E. Dann ist $E(x)/E$ endlich. Da $\alpha_0, \dots, \alpha_n$ über K algebraisch sind, ist E endlich über K. Dann ist $E(x)/K$ endlich, und $x \in E(x)$. Also ist x algebraisch über K. □

Beispiel* 3.1.15. Sei $K \subset L$ eine Körpererweiterung, seien $\alpha, \beta \in L$ gegeben, so daß $\alpha + \beta$ und $\alpha\beta$ algebraisch über K sind. Man zeige, daß α und β algebraisch über K sind.

Beispiel* 3.1.16. Man zeige, daß die Körper $\mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(i\sqrt{2})$ nicht isomorph sind. Hinweis: man überlege sich, daß -1 in $\mathbb{Q}(i\sqrt{2})$ Summe von zwei Quadraten ist.

Beispiel* 3.1.17. Wir haben uns bereits überlegt, daß $\mathbb{Q}[\sqrt{d}] = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{N}$ mit $\sqrt{d} \notin \mathbb{Q}$ ein Körper ist. Sei $\alpha, \beta \in \mathbb{N}$ mit $\sqrt{\alpha}, \sqrt{\beta} \notin \mathbb{Q}$. Man gebe eine notwendige und hinreichende Bedingung dafür, daß die Körper $\mathbb{Q}(\sqrt{\alpha})$ und $\mathbb{Q}(\sqrt{\beta})$ isomorph sind.

Beispiel* 3.1.18. Seien $p, q \in \mathbb{N}$ verschiedene Primzahlen. Man bestimme das Minimalpolynom von $\sqrt{p} + \sqrt{q}$ über $\mathbb{Q}$.

3.1.4 Der algebraische Abschluß eines Körpers in einem Oberkörper

Proposition und Definition 3.1.19. *Sei $K \subset L$ Körpererweiterung. Die Menge $\overline{K}$ aller über K algebraischer Elemente von L sind ein Unterkörper von L, der K enthält. Es gilt $\overline{\overline{K}} = \overline{K}$. Der Körper $\overline{K}$ heißt algebraischer Abschluß von K in L. Der Körper K heißt algebraisch abgeschloßen in L, wenn $K = \overline{K}$.*

Beweis. Es ist klar, daß $K \subset \overline{K}$ ist. Seien $x, y \in \overline{K}$. Dann sind $x + y, x \cdot y \in K(x, y)$. Da $K(x, y)$ endlich über K ist, sind $x + y$ und $x \cdot y$ algebraisch über K, also $x + y, x \cdot y \in \overline{K}$. Damit ist $\overline{K}$ Unterring von L. Sei $0 \neq x \in \overline{K}$, dann ist $K(x)$ endlich über K und $x^{-1} \in K(x)$, also ist $x^{-1} \in \overline{K}$. Damit ist $\overline{K}$ Unterköper von L.

Es ist klar, daß $\overline{K} \subset \overline{\overline{K}}$. Ein Element $x \in \overline{\overline{K}}$ ist algebraisch über $\overline{K}$, welches algebraisch über K ist. Also ist x algebraisch über K, das heißt $x \in \overline{K}$. □

Folgerung 3.1.20. *(a) Der algebraische Abschluß $\overline{\mathbb{Q}}$ von $\mathbb{Q}$ in $\mathbb{C}$ ist eine unendliche algebraische Erweiterung von $\mathbb{Q}$.*

(b) Der Körper $\overline{\mathbb{Q}}$ ist abzählbar unendlich.

(c) Die Mengen $\mathbb{R}\setminus\overline{\mathbb{Q}}$, $\mathbb{C}\setminus\overline{\mathbb{Q}}$ sind überabzählbar.

Beweis. **Zu (a):** Nach Definition ist die Erweiterung $\overline{\mathbb{Q}}/\mathbb{Q}$ algebraisch. Sie ist unendlich, da die Grade der Elemente in $\mathbb{Q}$ unbeschränkt sind, zum Beispiel die Grade der Nullstellen der irreduziblen Polynome $X^n - 2$ für alle $n \in \mathbb{N}$.
Zu (b): Der Körper $\mathbb{Q}$ ist die Menge der Nullstellen aller Polynome $f \in \mathbb{Q}[x]$. Da $\mathbb{Q}[X]$ abzählbar ist, und jedes Element $0 \neq f \in \mathbb{Q}[X]$ höchstens $\deg(f)$ Nullstellen hat, ist $\overline{\mathbb{Q}}$ abzählbar unendlich.
Zu (c): Das folgt aus (b). □

Der Körper $\overline{\mathbb{Q}}$ heißt Körper der algebraischen Zahlen.

Beispiel* 3.1.21. Ist der Körper $\mathbb{C}(t)$ der rationalen Funktionen über $\mathbb{C}$ algebraisch abgeschloßen?

3.2 Zerfällungskörper und normale Körpererweiterungen

Seien K und L Körper und $\varphi : K \to L$ ein Ringhomomorphismus. Man sieht leicht, daß φ injektiv ist: $\ker(\varphi)$ ist ein Ideal, das echt in K enthalten ist, denn es enthält die 1 nicht, also $\ker(\varphi) = (0)$. Man faßt manchmal K via φ als Unterkörper von L auf. Damit ist die induzierte Abbildung von Polynomringen

$$\widetilde{\varphi} : K[X] \to L[X], f = \sum_{i=0}^{n} \alpha_i X^i \mapsto {}^{\varphi}f = \sum_{i=0}^{n} \varphi(\alpha_i) X^i$$

ein injektiver K-Algebrenhomomorphismus.

3.2.1 Adjunktion von Nullstellen

Satz 3.2.1 (Kronecker)**.** *Seien K ein Körper, $f \in K[X]$ ein irreduzibles Polynom.*

(a) Es gibt einen Oberkörper $L \supset K$ und $x \in L$ mit $f(x) = 0$ und $L = K(x)$.

(b) Sind $K(x_i) = L_i$ für $i = 1, 2$ Erweiterungen von K mit $f(x_i) = 0$, dann gibt es genau einen Ringisomorphismus $\sigma : L_1 \to L_2$ mit $\sigma(x_1) = x_2$ und $\sigma\big|_K = \mathrm{id}_K$, das heißt genau einen K-Algebrenisomorphismus $\sigma : L_1 \to L_2$ mit $\sigma(x_1) = x_2$.

Beweis. **Zu (a):** Da f irreduzibel ist, ist (f) ein maximales Ideal von $K[X]$, also ist $L := K[X]/(f)$ ein Körper. Offenbar ist die Abbildung

$$\varphi : K \to L, \alpha \mapsto \alpha + (f)$$

ein injektiver Ringhomomorphismus. Wir fassen K via φ als Unterkörper von L auf. Sei $x = X + (f) \in L$ und $f = \sum_{i=0}^{n} \alpha_i X^i$. Dann gilt

$$f(x) = \sum_{i=0}^{n} \alpha_i (X + (f))^i = \sum_{i=0}^{n} \alpha_i X^i + (f) = f + (f) = 0$$

in L. Also ist x Nullstelle von f. Da $L = K[x]$ ist, folgt $L = K(x)$.
Zu (b): Dies folgt aus dem nächsten Lemma. □

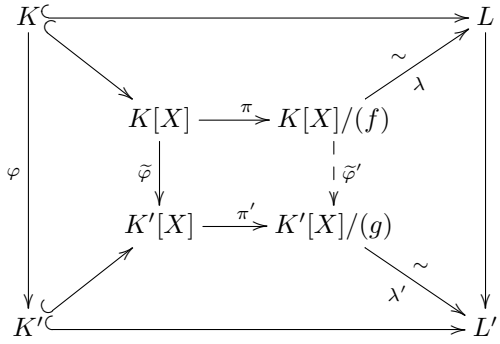
Lemma 3.2.2. *Sei $L = K(x)$ endliche algebraische Erweiterung von K, f das Minimalpolynom von x über K, $\varphi : K \to K'$ ein Ringhomomorphismus in einen Körper K', $g \in K'[X]$ ein irreduzibler Teiler von ${}^{\varphi}f$, $L' = K'(x')$ eine Erweiterung mit $g(x') = 0$.*

(a) Es gibt genau einen Ringhomomorphismus $\psi : L \to L'$ mit $\psi(x) = x'$ und $\psi\big|_K = \varphi$.

$$\begin{array}{ccc} K & \hookrightarrow & L \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\psi} \\ K' & \hookrightarrow & L' \end{array}$$

(b) Ist φ ein Isomorphismus, so auch ψ.

Beweis. **Zu (a):** Es gibt $h \in K'[X]$ mit ${}^{\varphi}f = gh$. Wir haben das kommutative Diagramm von Ringhomomorphismen



wobei π und π' die kanonischen Homomorphismen sind, und λ bzw. λ' gegeben sind durch $\lambda(p+(f)) = p(x)$, $\lambda'(q+(g)) = q(x')$. Da gilt

$$\pi'\widetilde{\varphi}(f) = \pi'({}^{\varphi}f) = \pi'(gh) = 0,$$

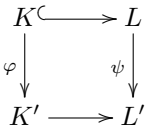
gibt es genau einen Ringhomomorphismus $\widetilde{\varphi}'$ mit $\widetilde{\varphi}' \circ \pi = \pi' \circ \widetilde{\varphi}$. Sei

$$\psi = \lambda' \circ \widetilde{\varphi}' \circ \lambda^{-1},$$

das heißt $\psi(p(x)) = {}^{\varphi}p(x')$ für $p \in K[X]$. Damit gilt $\psi(x) = x'$ und $\psi\big|_K = \mathrm{id}_K$. Ist auch $\overline{\psi} : L \to L'$ ein Homomorphismus mit $\overline{\psi}(x) = x'$ und $\overline{\psi}\big|_K = \mathrm{id}_K$, dann gilt $\overline{\psi}(x^i) = x'^i$ für alle $1 \leqslant i \leqslant \deg(f)$, also ist $\psi = \overline{\psi}$ da die x^i mit $1 \leqslant i \leqslant \deg(f)$ eine K-Basis von L bilden.
Zu (b): Ist φ ein Isomorphismus, dann auch $\widetilde{\varphi}$. Daraus folgt, daß $\widetilde{\varphi}'$ surjektiv ist, und weil dies bereits injektiv ist, ist es ein Isomorphismus. Also ist auch ψ ein Isomorphismus. □

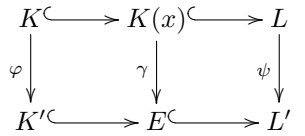
3.2.2 Fortsetzung von Homomorphismen

Fortsetzungssatz 3.2.3. *Sei $K \subset L$ endliche Körpererweiterung, $\varphi : K \to K'$ Ringhomomorphismus in einen Körper K'. Dann gibt es eine endliche Körpererweiterung $K' \subset L'$ und einen Ringhomomorphismus $\psi : L \to L'$ mit $\psi\big|_K = \varphi$.*



Beweis. Induktion nach $n = [L : K]$. Bei $n = 1$ ist nichts zu zeigen. Sei $n > 1$, $x \in L \backslash K$. Dann ist x algebraisch über K. Sei f das Minimalpolynom von x über K, sei $g \in K'[X]$ ein irreduzibler Faktor von ${}^{\varphi}f$. Es gibt eine Erweiterung $K' \subset E = K'(x')$ mit $g(x') = 0$. Nach obigem Lemma (genau) einen Ringhomomorphismus $\gamma : K(x) \to E$ mit $\gamma(x) = x'$ und $\gamma\big|_K = \varphi$.

Im Fall $K(x) = L$ sind wir fertig. Ist $K(x) \subsetneq L$, dann gibt es wegen $[L : K(x)] < n$ nach Induktionsannahme eine endliche Erweiterung $E \subset L'$ und einen Ringhomomorphismus $\psi : L \to L'$ mit $\psi\big|_K = \gamma$. Dann ist L' endlich über K' und $\psi\big|_K = \gamma\big|_K = \varphi$.



□

3.2.3 Der Zerfällungskörper eines Polynoms

Definition 3.2.4. Sei K ein Körper, $f \in K[X]$. Ein Oberkörper L von K heißt Zerfällungskörper von f, wenn:

(a) Es existieren $\alpha \in K$, $n \in \mathbb{N}_0$, $x_1, \ldots, x_n \in L$, so daß $f = \alpha \prod_{i=1}^{n}(X - x_i)$.

(b) Der Körper L ist gegeben durch $K(x_1, \ldots, x_n)$.

Dann ist L endlich über K.

Beispiele 3.2.5. (a) Die komplexen Zahlen $\mathbb{C}$ sind Zerfällungskörper von $X^2 + 1 \in \mathbb{R}[X]$.

(b) Der Körper $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ ist Zerfällungskörper von $(X^2 - 2)(X^2 - 3) \in \mathbb{Q}[X]$.

(c) Sei $K = \mathbb{Z}/(2)$, $f = X^2 + X + 1 \in K[X]$. Das Polynom f ist irreduzibel, also ist $L = K[X]/(f)$ Körpererweiterung von K. L ist Zerfällungskörper von f denn mit $x = X + (f)$ gilt $f = (X + x)(X + x + 1)$ und $L = K(x)$. Es gilt $[L : K] = 2$, also hat L 4 Elemente.

Satz 3.2.6. *Sei K ein Körper und $f \in K[X]$.*

(a) Es gibt einen Zerfällungskörper $L \supset K$ von f.

(b) Ist $f \neq 0$, dann gilt

$$[L : K] \big| \deg(f)!.$$

(c) Sind $K \subset L_i$, $i = 1, 2$, Zerfällungskörper von f, dann gibt es einen Ringisomorphismus $\sigma : L_1 \to L_2$ mit $\sigma\big|_K = \mathrm{id}_K$.

Beweis. **Zu (a):** Wir führen Induktion nach $n = \deg(f)$ durch. Man kann annehmen, daß f nicht konstant ist, und daß $f$über K nicht in Linearfaktoren zerfällt. Dann hat f einen irreduziblen Faktor g mit $\deg(g) > 1$. Nach dem Satz von Kronecker gibt es eine Erweiterung $K \subset E = K(x_1)$ mit $g(x_1) = 0$. Dann gibt es $f_1 \in E[X]$ mit $f = (X - x_1)f_1$. Da $\deg(f_1) = \deg(f) - 1$ ist, gibt es nach Induktionsannahme eine Erweiterung $E \subset L$ und Elemente $\alpha \in E$, $x_2, \ldots, x_n \in L$, (wobei $n = \deg(f)$), mit $f_1 = \alpha \prod_{i=2}^{n}(X - x_i)$, und $L = E(x_2, \ldots, x_n)$. Dann gilt $f = \alpha \prod_{i=1}^{n}(X - x_i)$. Insbesondere $\alpha \in K$ und $L = K(x_1, \ldots, x_n)$.
Zu (b): Wiederum Induktion nach $n = \deg(f)$. Für $n = 0, 1$ ist die Behauptung klar. Sei $n > 1$. Sei zunächst f irreduzibel. Sei $x \in L$ Nullstelle von f und $g \in K(x)[X]$ mit $f = (X - x)g$. Offenbar ist L Zerfällungskörper von g über $K(x)$. Nach Induktionsannahme gilt $[L : K(x)] \big| \deg(g)! = (n - 1)!$. Es folgt

$$[L : K] = [L : K(x)] \cdot [K(x) : K] \big| (n - 1)! \cdot n.$$

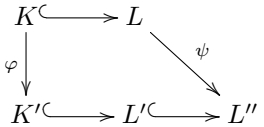
Sei nun f reduzibel, dh. $f = f_1 \cdot f_2$ mit $f_1, f_2 \in K[X] \backslash K$ und $m_i = \deg(f_i)$ für $i = 1, 2$. Es gibt einen Zwischenkörper $K \subset E \subset L$, der Zerfällungskörper von f_1 ist. Dann ist L Zerfällungskörper von f_2 über E. Nach Induktionsannahme gilt $[E : K] \big| m_1!$ und $[L : E] \big| m_2!$. Es folgt

$$[L : K] = [L : E][E : K] \big| m_1! \cdot m_2!.$$

Wegen $m! = m(m - 1) \cdots (m - m_1 + 1)m_2! = \binom{m}{m_1} m_1! m_2!$ folgt $[L : K] \big| m!$.

Zu (c): Zum Beweis von (c) zeigen wir zuerst folgendes Lemma.

Lemma 3.2.7. *Sei $f \in K[X]$, $K \subset L$ ein Zerfällungskörper von f, $\varphi : K \to K'$ ein Ringhomomorphismus in einen Körper K', $L' \supset K'$ ein Zerfällungskörper von ${}^{\varphi}f$, $L' \subset L''$ eine Körpererweiterung, $\psi : L \to L''$ ein Ringhomomorphismus mit $\psi\big|_K = \varphi$.*



Dann gilt:

(a) $\psi(L) \subset L'$.

(b) Ist φ *Isomorphismus, dann* $\psi(L) = L'$.

(c) Zerfällt f *über* L *in lauter verschiedene Linearfaktoren, dann gilt dies auch für* ${}^{\varphi}f$ *über* L'.

Beweis. Sei ohne Einschränkung $f \in K[X]\backslash K$.
Zu (a) und (b): Es gibt $\alpha \in K$ und $x_1, \ldots, x_n \in L$ mit $f = \alpha \prod_{i=1}^{n}(X - x_i)$ und $L = K(x_1, \ldots, x_n)$. Es folgt

$$ {}^{\varphi}f = {}^{\psi}f = \varphi(\alpha) \prod_{i=1}^{n}(X - \psi(x_i)). $$

Also gilt

$$ \psi(L) = \psi(K)(\psi(x_1), \ldots, \psi(x_n)) = \varphi(K)(\psi(x_1), \ldots, \psi(x_n)) \subset K'(\psi(x_1), \ldots, \psi(x_n)) = L' $$

und wenn φ Isomorphismus ist, dann gilt Gleichheit.
Zu (c): Dies gilt, da ψ injektiv ist. □

Kommen wir zurück zu Aussage (c) des Satzes. Seien $K \subset L_1$ und $K \subset L_2$ Zerfällungskörper von f. Nach dem Fortsetzungssatz 3.2.3 gibt es eine endliche Erweiterung $L_2 \subset L''$ und einen Homomorphismus $\psi : L_1 \to L''$, so daß $\psi\big|_K$ die Inklusionsabbildung $K \subset L_2$ ist.

$$\begin{array}{ccccc} K & \hookrightarrow & L_1 & & \\ \| & & & \searrow^{\psi} & \\ K & \hookrightarrow & L_2 & \hookrightarrow & L'' \end{array}$$

Nach dem Lemma gilt $\psi(L_1) = L_2$. □

Folgerung 3.2.8. *Sei* $f \in K[X]$ *irreduzibel vom Grad* n, $K \subset L$ *ein Zerfällungskörper von* f. *Dann gilt*

$$ n \big| [L : K] \big| n!. $$

Beweis. Das ist klar. □

Beispiel 3.2.9. Sei $f = X^3 - 2 \in \mathbb{Q}[X]$. Das Polynom f ist irreduzibel. Sei

$$ \omega = \frac{1}{2}(-1 + \sqrt{-3}) = e^{\frac{2\pi i}{3}} \in \mathbb{C}\,. $$

Es gilt $\omega^2 = \overline{\omega}$ und $\omega^3 = 1$. Die Nullstellen von f sind

$$ \sqrt[3]{2}, \omega\sqrt[3]{2}, \overline{\omega}\sqrt[3]{2}, $$

also ist

$$ f = (X - \sqrt[3]{2})(X - \omega\sqrt[3]{2})(X - \overline{\omega}\sqrt[3]{2}) = (X - \sqrt[3]{2})(X^2 + \sqrt[3]{2}X + \sqrt[3]{2}^2). $$

Also ist $\mathbb{Q}(\sqrt[3]{2}, \omega) = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ Zerfällungskörper von f. Es gilt

$$ [\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 2 \cdot 3 = 6 = 3! $$

Beispiel* 3.2.10. Gegeben sei das Polynom $f = X^4 - 3 \in \mathbb{Q}[X]$. Man beweise, daß $L = \mathbb{Q}(\sqrt[4]{3}, i)$ Zerfällungskörper von f ist und berechne den Grad der Körpererweiterung $L/\,\mathbb{Q}$.

3.2.4 Normale Erweiterungen

Definition 3.2.11. Eine Körpererweiterung $K \subset L$ heißt normal, wenn sie algebraisch ist und jedes irreduzible Polynom in $K[X]$, das in L eine Nullstelle hat, über L in Linearfaktoren zerfällt.

Satz 3.2.12. *Für eine endliche Körpererweiterung $K \subset L$ sind äquivalent:*

(a) L ist normale Erweiterung von K.

(b) L ist Zerfällungskörper eines Polynoms in $K[X]$.

(c) Für alle Oberkörper $L \subset L'$ und alle K-Algebrenhomomorphismen $\sigma : L \to L'$ gilt $\sigma(L) = L'$.

Beweis. **[(a) ⇒ (b)]** Es gibt $x_1, \dots x_n \in L$ mit $L = L(x_1, \dots, x_n)$. Sei $f_i \in K[X]$ das Minimalpolynom von x_i, $1 \leqslant i \leqslant n$. Nach Voraussetzung zerfallen die f_i vollständig in Linearfaktoren, also zerfällt $f = \prod_{i=1}^{n} f_i$ vollständig in Linearfaktoren über L. Wegen $L = K(x_1, \dots, x_n)$ ist L Zerfällungskörper von f.
[(b) ⇒ (c)] Sei L Zerfällungskörper von $f \in K[X]$, $L \subset L'$ eine Körpererweiterung und $\sigma : L \to L'$ ein K-Algebrenhomomorphismus

$$\begin{array}{ccccc} K & \hookrightarrow & L & & \\ \| & & & \searrow^{\sigma} & \\ K & \hookrightarrow & L & \hookrightarrow & L' \end{array}$$

Nach Lemma 3.2.7 gilt $\sigma(L) = L'$.
[(c) ⇒ (a)] Da L/K endlich ist, ist L/K algebraisch. Angenommen, es gibt ein irreduzibles Polynom $f \in K[X]$ mit einer Nullstelle $x \in L$, das über L nicht in Linearfaktoren zerfällt. Dann hat f in $L[X]$ einen irreduziblen Faktor g mit $\deg(g) > 1$. Nach dem Satz von Kronecker und dem Lemma dazu gibt es eine Erweiterung $L \subset L(x')$ mit $[L(x') : L] = \deg(g)$ und $g(x') = 0$ und einen Homomorphismus $\psi : K(x) \to L(x')$, so daß $\psi(x) = x'$ und $\psi\big|_K$ die Inklusion $K \subset L$ ist. Nach dem Fortsetzungssatz 3.2.3 gibt es eine endliche Erweiterung $L(x') \subset L'$ und einen Homomorphismus $\sigma : L \to L'$ mit $\sigma\big|_{K(x)} = \psi$

$$\begin{array}{ccccc} K & \hookrightarrow & K(x) & \hookrightarrow & L \\ \downarrow & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \sigma} \\ L & \hookrightarrow & L(x') & \hookrightarrow & L \end{array}$$

Dann ist σ ein K-Algebrenhomomorphismus, nach (c) gilt also $\sigma(L) = L$. Insbesondere $\sigma(x) = \psi(x) = x' \in L$. Widerspruch. □

Beispiele* 3.2.13. Welche der folgenden Körpererweiterungen sind normal?

$$\mathbb{Q}(\sqrt{3})/\,\mathbb{Q}$$
$$\mathbb{Q}(\sqrt[4]{3})/\,\mathbb{Q}$$
$$\mathbb{Q}(\sqrt[4]{3})/\,\mathbb{Q}(\sqrt{3})$$

Beschreiben Sie die Zerfällungskörper L der folgenden Polynome über dem Grundkörper K:

$$\begin{aligned} K = \mathbb{Q} \quad & f = X^3 - 1 \in \mathbb{Q}[X] \\ K = \mathbb{F}_2 \quad & f = X^3 - 1 \\ K = \mathbb{F}_2(t) \quad & f = X^3 - t \\ K = \mathbb{F}_5 \quad & f = X^3 - 1 \\ K = \mathbb{F}_2(t) \quad & f = X^2 - t \end{aligned}$$

Folgerung 3.2.14. *Ist $K \subset L$ endlich und normal, $K \subset E \subset L$ ein Zwischenkörper, dann ist auch L/E endlich und normal.*

Beweis. Ist L Zerfällungskörper von $f \in K[x]$, dann ist L auch Zerfällungskörper von f über E. □

Dagegen ist im Allgemeinen E/K nicht normal (siehe Beispiel 3.2.9).

Beispiel* 3.2.15. Man gebe ein Beispiel eines Körperturms $K \subset L \subset M$ an, so daß $K \subset L$ und $L \subset M$ normal sind, aber $K \subset M$ nicht.
Lösung: Betrachte die Erweiterungen $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$. Die Erweiterung $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$ ist quadratisch, das Minimalpolynom von $\sqrt{2}$ über $\mathbb{Q}$ ist X^2-2. Die Erweiterung $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$ ist ebenso quadratisch, das Minimalpolynom von $\sqrt[4]{2}$ über $\mathbb{Q}(\sqrt{2})$ ist $X^2-\sqrt{2}$. Aber $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{2})$ ist nicht normal, denn das Minimalpolynom X^4-2 von $\sqrt[4]{2}$ über $\mathbb{Q}$ zerfällt über $\mathbb{Q}(\sqrt[4]{2})$ nicht in Linearfaktoren, sondern nur in $(X-\sqrt[4]{2})(X+\sqrt[4]{2})(X^2+\sqrt{2})$.

Satz 3.2.16. *Sei $K \subset L$ endliche Körpererweiterung.*

(a) Es gibt eine endliche Erweiterung $L \subset N$ mit folgenden Eigenschaften.

(i) N/K ist normal.

(ii) Ist M ein Zwischenkörper mit $L \subset M \subset N$, so daß M/K normal ist, dann gilt $M = N$.

(b) Ist auch $L \subset N'$ eine endliche Erweiterung mit den obigen Eigenschaften, dann gibt es einen Isomorphismus $\sigma : N \to N'$ mit $\sigma\big|_L = \mathrm{id}_L$.

Definition 3.2.17. Ein Körper N wie im Satz heißt normaler Abschluß von L über K.

Beweis. **Zu (a):** Es gibt $x_1, \ldots, x_n \in L$ mit $L = K(x_1, \ldots, x_n)$. Sei $f_i \in K[X]$ das Minimalpolynom von x_i, $1 \leqslant i \leqslant n$. Sei N ein Zerfällungskörper von $f = f_1 \cdots f_n$, der L enthält. Dann ist N/K normal. Sei $L \subset M \subset N$ ein Zwischenkörper, so daß M/K normal is. Da M die Nullstellen x_i, $1 \leqslant i \leqslant n$ von f enthält, enthält M alle Nullstellen von f. Es folgt $M = N$.
Zu (b): N und N' sind Zerfällungskörper von f über K, also auch über L. Deshalb gibt es einen Isomorphismus wie behauptet. □

Definition 3.2.18. Ist $K \subset L$ eine Erweiterung, $x \in L$ algebraisch über K, $f \in K[X]$ das Minimalpolynom von x, dann heißen die Nullstellen von f in einem Zerfällungskörper die zu x konjugierten Elemente.

3.2.5 Die Anzahl der Einbettungen

Satz 3.2.19. *Sei $K \subset L$ eine endliche Erweiterung, $\varphi : K \to K'$ein Isomorphismus in einen Körper K', $K' \subset N'$ eine normale Erweiterung und $\psi : L \to N'$ ein Homomorphismus mit $\psi\big|_K = \varphi$.*

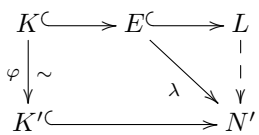
$$\begin{array}{ccc} K & \hookrightarrow & L \\ {\scriptstyle\varphi}\downarrow{\scriptstyle\sim} & & \downarrow{\scriptstyle\psi} \\ K' & \hookrightarrow & N' \end{array}$$

(a) Es gibt höchstens $[L:K]$ Ringhomomorphismen $\sigma : L \to N'$ mit $\sigma\big|_K = \varphi$.

(b) Der Unterkörper in N', der von den Bildern der σ in (a) erzeugt wird, ist der normale Abschluß von $\psi(L)$ über K'.

Zur Vorbereitung des Beweises werden wir folgendes Lemma zeigen.

Lemma. *Seien die Voraussetzungen wie im Satz. Ist $K \subset E \subset L$ eine Zwischenkörper, $\lambda : E \to N'$ ein Homomorphismus mit $\lambda\big|_K = \varphi$, so hat λ eine Fortsetzung $\lambda' : L \to N'$, dh. für λ' gilt $\lambda'\big|_E = \lambda$.*



Beweis. Nach dem Fortsetzungssatz 3.2.3 gibt es eine endliche Erweiterung $N' \subset M$ und einen Homomorphismus $\lambda' : L \to M$ mit $\lambda'\big|_E = \lambda$.

$$\begin{array}{ccc} E & \hookrightarrow & L \\ {\scriptstyle\lambda}\downarrow & & \downarrow{\scriptstyle\lambda'} \\ N' & \hookrightarrow & M \end{array}$$

Wir zeigen $\lambda'(L) \subset N'$. Sei $x \in L$, $f \in K[X]$ das Minimalpolynom von x. Da

$$^{\varphi}f(\lambda'(x)) = {}^{\lambda'}f(\lambda'(x)) = \lambda'(f(x)) = 0$$

folgt also $\lambda'(x) \in N'$. □

Beweis des Satzes. **Zu (a):** Sei ohne Einschränkung $K \subsetneq L$, sei $x \in L\backslash K$, $f \in K[X]$ das Minimalpolynom von x. Dann ist $\psi(x)$ Nullstelle von $^{\varphi}f$, also zerfällt $^{\varphi}f$ über N' in Linearfaktoren. Seien $y_1, \ldots, y_r$ die verschiedenen Nullstellen von $^{\varphi}f$ in N'. Es gilt $r = \deg(f)$. Zu jedem $1 \leqslant i \leqslant r$ gibt es einen Homomorphismus $\sigma_i : K(x) \to K'(y_i)$ mit $\sigma_i(x) = y_i$ und $\sigma_i\big|_K = \varphi$

$$\begin{array}{ccccc} K & \hookrightarrow & K(x) & \hookrightarrow & L \\ {\scriptstyle\varphi}\downarrow & & {\scriptstyle\sigma_i}\downarrow & & \\ K' & \hookrightarrow & K'(y_i) & \hookrightarrow & N' \end{array}$$

Nach dem Lemma kann σ_i zu einem Homomorphismus $L \to N'$ fortgesetzt werden. Da $[L : K(x)] < [L : K]$ ist, gibt es nach Induktionsannahme $k_i \leqslant [L : K(x)]$ solche Fortsetzungen σ_{ij}, $1 \leqslant j \leqslant k_i$. Die σ_{ij}, $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant k_i$, sind paarweise verschieden, ihre Anzahl ist

$$\sum_{i=1}^{r} k_i \leqslant [L : K(x)][K(x) : K] = [L : K].$$

Dies sind alle Homomorphismen $\sigma : L \to N'$ mit $\sigma\big|_K = \varphi$: Denn für ein solches σ ist $\sigma(x)$ Nullstelle von $^{\varphi}f$, also ist $\sigma(x) = y_i$ für ein $1 \leqslant i \leqslant r$. Somit gilt $\sigma\big|_{K(X)} = \sigma_i$, und deshalb ist $\sigma = \sigma_{ij}$ für ein $1 \leqslant j \leqslant k_i$.
Zu (b): Sei $\psi(K) \subset N \subset N'$ normaler Abschluß von $\psi(L)$. Sei $L = K(x_1, \ldots, x_n)$, und $f_k \in K[X]$ das Minimalpolynom von x_k, $1 \leqslant k \leqslant n$. Es gilt $\psi(L) = K'(\psi(x_1), \ldots, \psi(x_n))$ und $^{\varphi}f_k$ ist das Minimalpolynom von $\psi(x_k)$, $1 \leqslant k \leqslant n$. Also ist N Zerfällungskörper von $^{\varphi}f = {}^{\varphi}f_1 \cdots {}^{\varphi}f_n$. Für alle σ aus (a) gilt $^{\varphi}f_k(\sigma(x_k)) = \sigma(f_k(x_k)) = 0$, also ist $\sigma(x_k) \in N$, $1 \leqslant k \leqslant n$, und $\sigma(L) = K'(\sigma(x_1), \ldots, \sigma(x_n)) \in N$. Sei umgekehrt $z \in N$ Nullstelle von $^{\varphi}f_k$ für ein $1 \leqslant k \leqslant n$. Dann gibt es einen Isomorphismus $\tau : K(x_k) \to K'(z)$ mit $\tau(x_k) = z$ und $\tau\big|_K = \varphi$ und eine Fortsetzung $\tau' : L \to N'$ von τ.

$$\begin{array}{ccccc} K & \hookrightarrow & K(x_k) & \hookrightarrow & L \\ {\scriptstyle\varphi}\downarrow & & {\scriptstyle\tau}\downarrow & & {\scriptstyle\tau'}\downarrow \\ K' & \hookrightarrow & K'(z) & \hookrightarrow & N \end{array}$$

Es folgt $z = \tau(x_k) = \tau'(x_k) \in \mathrm{im}(\tau')$. Also ist N in dem von $\sigma(L)$ erzeugten Unterkörper von N' enthalten. □

Bemerkung 3.2.20. Seien die Bezeichnungen wie im Satz und dessen Beweis. Es gibt genau $[L : K]$ Homomorphismen $\sigma : L \to N'$ mit $\sigma\big|_K = \varphi$, genau dann, wenn $r = [K(x) : K]$ und $k_i = [L : K(x)]$ für $1 \leqslant i \leqslant r$.

Wir führen einige Bezeichnungen ein. Seien $\varphi : K \to L$, $\psi : K \to M$ Ringhomomorphismen zwischen Körpern. Dann sei $\mathrm{Alg}_K(L, M)$ die Menge aller K-Algebrenhomomorphimen $\sigma : L \to M$, dh. der Homomorphismen mit $\sigma \circ \varphi = \psi$. Ist L ein Körper, dann sei $\mathrm{Aut}(L)$ die Automorphismengruppe von L, dh. die Gruppe der bijektiven Ringhomomorphismen. Ist $K \subset L$ Körpererweiterung, dann sei

$$\mathrm{Gal}(L/K) = \left\{\sigma \in \mathrm{Aut}(L) \;\middle|\; \sigma\big|_K = \mathrm{id}_K\right\}.$$

Das ist eine Untergruppe von $\mathrm{Aut}(L)$. Sie heißt Galoisgruppe von L/K. Es gilt

$$\mathrm{Gal}(L/K) \subset \mathrm{Alg}_K(L, L).$$

Ist die Erweiterung $K \subset L$ endlich, dann gilt $\mathrm{Gal}(L/K) = \mathrm{Alg}_K(L, L)$, denn jeder K-Algebrenhomomorphismus $\sigma : L \to L$ ist injektiv, also bijektiv. Wenn L_0 der Primkörper von L ist, dann gilt $\mathrm{Aut}(L) = \mathrm{Gal}(L/L_0)$.

Folgerung 3.2.21. *Seien $K \subset L$, $K \subset M$ endliche Erweiterungen und es gebe $\psi : L \to M$ mit $\psi\big|_K = \mathrm{id}_K$.*

(a) Es gilt $|\mathrm{Alg}_K(L, M)| \leqslant [L : K]$.

(b) Weiterhin $|\mathrm{Gal}(L/K)| \leqslant [L : K]$.

Beweis. **Zu (a):** Sei $M \subset N$ eine Erweiterung, so daß N/K endlich und normal ist.

$$\begin{array}{ccccc} K & \hookrightarrow & L & & \\ \| & & \downarrow{\scriptstyle \psi} & & \\ K & \hookrightarrow & M & \hookrightarrow & N \end{array}$$

Nach dem Satz von vorher gilt $|\mathrm{Alg}_K(L, N)| \leqslant [L : K]$, also erst recht $|\mathrm{Alg}_K(L, M)| \leqslant [L : K]$.
Zu (b): Dies ist ein Spezialfall von (a): $|\mathrm{Gal}(L/K)| = |\mathrm{Alg}_K(L, L)| \leqslant [L : K]$. □

Folgerung 3.2.22. *Sei $K \subset L$ endlich und normal, $G = \mathrm{Gal}(L/K)$, $f \in K[X]$ ein irreduzibles Polynom, das über L in Linearfaktoren zerfällt. Sei Z die Menge der Nullstellen von f in L. Dann ist*

$$G \times Z \to Z, (\sigma, x) \mapsto \sigma(x)$$

eine transitive Operation. Für $x \in Z$ gilt $G_x = \mathrm{Gal}(L/K(x))$.

Beweis. Die Operation ist wohldefiniert. Wie im Beweis des Satzes zeigt man, daß es zu $x, y \in Z$ ein $\sigma \in G$ gibt, mit $y = \sigma(x)$.

$$\begin{array}{ccccc} K & \hookrightarrow & K(x) & \hookrightarrow & L \\ \| & & \downarrow & & \downarrow{\scriptstyle \sigma} \\ K & \hookrightarrow & K(y) & \hookrightarrow & L \end{array}$$

Für $\tau \in G$ gilt: $\tau \in G_x$ genau dann, wenn $\tau(x) = x$ genau dann, wenn $\tau\big|_{K(x)} = \mathrm{id}_{K(x)}$ genau dann, wenn $\tau \in \mathrm{Gal}(L/K(x))$. □

3.3 Separable Körpererweiterungen

3.3.1 Separable Erweiterungen

Zur Erinnerung: Sei K Körper, $f \in K[X]\backslash K$, $x \in K$ Nullstelle von f in K. Dann gibt es eindeutige $k \in \mathbb{N}$, $g \in K[X]$ mit $f = (X - x)^k g$ und $g(x) \neq 0$. Es heißt k die Vielfachheit der Nullstelle x von f. Das Element x heißt einfache Nullstelle von f, falls $k = 1$, mehrfache Nullstelle von f, falls $k > 1$.

Definition 3.3.1. Sei K ein Körper.

(a) Ein irreduzibles Polynom $f \in K[X]$ heißt separabel, wenn f in einem (und dann jedem) Zerfällungskörper nur einfache Nullstellen hat.

(b) Ein beliebiges Polynom $f \in K[X]\backslash K$ heißt separabel, wenn jeder irreduzible Faktor von f separabel ist.

(c) Der Körper K heißt perfekt oder vollkommen, wenn jedes irreduzible Polynom $f \in K[X]$ separabel ist.

(d) Sei $K \subset L$ Körpererweiterung. Ein Element $x \in L$ heißt separabel, wenn x algebraisch über K ist, und das Minimalpolynom von x über K separabel ist.

(e) Ein Oberkörper L heißt separabel über K, wenn jedes Element in L über K separabel ist.

Beispiele 3.3.2. (a) Das Polynom $f = X^3 - 2 \in \mathbb{Q}[X]$ ist separabel.

(b) Sei $K = \mathbb{Z}/(2)(X)$, $f = Y^2 + X \in K[Y]$. Dann ist f irreduzibel, denn f ist irreduzibel in $\mathbb{Z}/(2)[X][Y]$ nach Eisenstein. Es gibt eine Erweiterung $K \subset L = K(y)$ vom Grad 2 mit $0 = f(y) = y^2 + X$, also $y^2 = X$ über $\mathbb{Z}/(2)$ und es gilt

$$(Y + y)^2 = Y^2 + 2Yy + y^2 = Y^2 + y^2 = Y^2 + X = f.$$

Also ist f nicht separabel.

Proposition 3.3.3. *Seien $K \subset E \subset L$ Körpererweiterungen.*

(a) Ist $x \in L$ separabel über K, dann auch über E.

(b) Ist L/K separabel, dann auch E/K und L/E.

Beweis. **Zu (a):** Das Minimalpolynom von x über E ist Teiler in $E[X]$ des Minimalpolynoms von x über K.
Zu (b): Das ist klar für E/K, für L/E folgt das aus (a). □

Satz 3.3.4. *Für eine endliche Körpererweiterung $K \subset L$ sind folgende Aussagen äquivalent:*

(a) Die Erweiterung L/K ist separabel.

(b) Es gibt über K separabel Elemente $x_1, \ldots, x_n \in L$ mit $L = K(x_1, \ldots, x_n)$.

(c) Ist $\varphi : K \to K'$ ein Isomorphismus in einen Körper K', $K' \subset N'$ eine endliche normale Erweiterung und $\psi : L \to N'$ ein Homomorphismus mit $\psi\big|_K = \varphi$, so besitzt φ genau $[L : K]$ Forsetzungen $\sigma : L \to N'$.

Beweis. **[(a) ⇒ (b)]** Das ist klar.
[(b) ⇒ (c)] Induktion nach $[L : K]$. Sei ohne Einschränkung $K \subsetneq L$, $x_1 \in L \backslash K$, sei $f \in K[X]$ das Minimalpolynom von x_1. Dann ist $\varphi(x_1)$ Nullstelle von ${}^{\varphi}f$, also zerfällt ${}^{\varphi}f$ über N' in Linearfaktoren. Seien $y_1, \ldots, y_r \in N'$ die verschiedenen Nullstellen, hier gilt $r = \deg(f)$. Es gibt Isomorphismen $\sigma_i : K(x_1) \to K'(y_i)$ mit $\sigma_i(x_1) = y_i$ und $\sigma_i\big|_K = \varphi$, für $1 \leqslant i \leqslant r$. Wir sind fertig, falls $L = K(x_1)$. Falls $K(x_1) \subsetneq L$, dann gilt $L = K(x_1)(x_2, \ldots, x_n)$. Da die $x_2, \ldots, x_n$ über $K(x_1)$ separabel sind, und N' über $K'(y_i)$ normal, hat σ_i nach Induktion genau $[L : K(x_i)]$ Fortsetzungen $\sigma_{ij} : L \to N'$, $1 \leqslant j \leqslant [L : K(x_i)]$. Die σ_{ij} mit $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant [L : K(x_i)]$ sind alle Fortsetzungen $L \to N'$ von φ. Ihre Anzahl ist $r \cdot [L : K(x_1)] = [L : K]$.
[(c) ⇒ (a)] Sei $L \subset N$ eine endliche Erweiterung, so daß N/K normal ist. Wir wissen nach (c), daß es genau $[L : K]$ Fortsetzungen $\sigma : L \to N$ gibt.

$$\begin{array}{ccc} K & \hookrightarrow & L \\ \| & & \downarrow \sigma \\ K & \hookrightarrow & N \end{array}$$

Sei ohne Einschränkung $K \subsetneq L$, sei $x \in L \backslash K$ und $f \in K[X]$ das Minimalpolynom von x. Das Polynom f zerfällt über N in Linearfaktoren. Seien $y_1, \ldots, y_r$ die verschiedenen Nullstellen von f, $r \leqslant \deg f$. Nach der Bemerkung 3.2.20 ist $r = \deg(f)$, das heißt f ist separabel. Also ist L/K separabel. □

Folgerung 3.3.5. *Sei $K \subset L$ eine endliche Erweiterung.*

(a) Sei $L \subset N$ eine endliche Erweiterung, so daß N/K normal ist. L/K ist genau dann separabel, wenn $|\operatorname{Alg}_K(L, N)| = [L : K]$.

(b) Sei L/K normal. L/K ist genau dann separabel, wenn $|\operatorname{Gal}(L/K)| = [L : K]$ ist.

Beweis. Dies folgt aus dem Satz und dessen Beweis. □

Folgerung 3.3.6. *Sei $K \subset L$ endliche separabel Körpererweiterung, sei $L \subset N$ normaler Abschluß von L/K. Dann ist auch N/K separabel.*

Beweis. Sei $L = K(x_1, \dots, x_n)$, $f_i \in K[X]$ Minimalpolynom von x_i, $1 \leqslant i \leqslant n$. Der Körper N ist Zerfällungskörper von $f_1 \cdots f_n$. Da x_i separabel über K ist, ist f_i über K separabel, also sind alle Nullstellen von f_i separabel, $1 \leqslant i \leqslant n$. Folglich ist nach Satz die Erweiterung N/K separabel. □

Folgerung 3.3.7 (Transitivität der Separabilität)**.** *Sei $K \subset L$ endliche Erweiterung, $K \subset E \subset L$ ein Zwischenkörper. L/K ist genau dann separabel, wenn E/K und L/E separabel sind.*

Beweis. Wir haben betreits gesehen, daß E/K und L/E separabel sind, wenn L/K separabel ist. Seien nun E/K, L/E separabel, und $k = [E : K]$, $l = [L : E]$, sei $L \subset N$ endliche Erweiterung, so daß N/K normal ist. Da E/K separabel ist, gilt $|\operatorname{Alg}_K(E, N)| = k$. Sei $\sigma \in \operatorname{Alg}_K(E, N)$.

$$\begin{array}{ccccc} K & \hookrightarrow & E & \hookrightarrow & L \\ \| & & \sigma \downarrow & & \\ K & \hookrightarrow & \sigma(E) & \hookrightarrow & N \end{array}$$

Da L/E separabel ist und $N/\sigma(E)$ normal, besitzt σ genau l Fortsetzungen $L \to N$. Also gilt

$$|\operatorname{Alg}_K(L, N)| = k \cdot l = [E : K] \cdot [L : E] = [L : K]$$

und L/K ist separabel. □

Beispiel 3.3.8. Sei $K/\mathbb{Q}$ der Zerfällungskörper von $f = X^3 - 2 \in \mathbb{Q}[X]$. Wir wissen, daß

$$K = \mathbb{Q}(\sqrt[3]{2}, \omega) = \mathbb{Q}(\sqrt[3]{2})(\omega),$$

wobei $\omega = \frac{1}{2}(-1 + \sqrt{-3}) = e^{\frac{2\pi i}{3}} \in \mathbb{C}$. Das Minimalpolynom von ω über $\mathbb{Q}$ oder $\mathbb{Q}(\sqrt[3]{2})$ ist $\phi_3 = X^2 + X + 1$. $K/\mathbb{Q}$ ist normal und separabel, also gilt $|\operatorname{Gal}(K/\mathbb{Q})| = [K : \mathbb{Q}] = 6$. Die Gruppe $\operatorname{Gal}(K/\mathbb{Q})$ besteht genau aus folgenden Elementen

$$\begin{array}{rlll} \mathrm{id}_K: & \sqrt[3]{2} \mapsto \sqrt[3]{2}, & \omega \mapsto \omega \\ \alpha: & \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega, & \omega \mapsto \omega \\ \alpha^2: & \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega^2, & \omega \mapsto \omega \\ \beta: & \sqrt[3]{2} \mapsto \sqrt[3]{2}; & \omega \mapsto \omega^2, \\ \alpha\beta: & \sqrt[3]{2} \mapsto \omega\sqrt[3]{2}, & \omega \mapsto \omega^2 \\ \alpha^2\beta: & \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega^2, & \omega \mapsto \omega^2 \end{array}$$

Damit sieht man $\operatorname{ord}(\alpha) = 3$, $\operatorname{ord}(\beta) = 2$, $\beta\alpha\beta = \alpha^2$, dh. $\operatorname{Gal}(K/\mathbb{Q}) \cong \mathfrak{S}_3$.

Beispiel* 3.3.9. Es seien p eine Primzahl, $\mathbb{F}_p$ der Körper mit p Elementen, $\mathbb{F}_p(t)$ der Quotientenkörper des Polynomrings $\mathbb{F}_p[t]$, und $\mathbb{F}_p(t^p)$ der kleinste Unterkörper von $\mathbb{F}_p(t)$, der t^p enthält. Man zeige, daß das Polynom $X^p - t^p \in \mathbb{F}_p(t^p)[X]$ irreduzibel ist. Man zeige, daß die Körpererweiterung $\mathbb{F}_p(t) \supset \mathbb{F}_p(t^p)$ endlich und normal aber nicht separabel ist.

3.3.2 Der Satz vom primitiven Element

Satz 3.3.10. *Jede endliche separabel Erweiterung $K \subset L$ ist einfach, dh. es gibt $x \in L$ mit $L = K(x)$.*

Definition 3.3.11. Ein Element mit $x \in L$ mit $L = K(x)$ heißt primitives Element von L/K.

Beweis. Ist K endlich, dann ist auch L endlich also ist $(L^*, \cdot)$ zyklische Gruppe. Wenn $L^* = \langle x \rangle$, dann gilt $L = K(x)$. Wir können also annehmen, daß K unendlich ist. Es genügt zu zeigen, daß L/K einfach ist, wenn $L = K(x, y)$.

Sei $n = [L : K]$, ohne Einschränkung $n > 1$, und es sei $L \subset N$ eine endliche Erweiterung, so daß N/K normal ist. Es gilt

$$|\operatorname{Alg}_K(L, N)| = n.$$

Sei $\mathrm{Alg}_K(L,N) = \{\sigma_1, \ldots, \sigma_n\}$. Wir betrachten das Polynom

$$p = \prod_{i \neq j} [(\sigma_i(x) - \sigma_j(x)) + (\sigma_i(y) - \sigma_j(y))\, X] \in N[X].$$

Für $i \neq j$ gilt $\sigma_i \neq \sigma_j$, also gilt $\sigma_i(x) \neq \sigma_j(x)$ oder $\sigma_i(y) \neq \sigma_j(y)$ und es folgt $p \neq 0$. Da K unendlich ist, gibt es $\lambda \in K$ mit $p(\lambda) \neq 0$. Es folgt

$$\prod_{i \neq j} [\sigma_i(x + \lambda y) - \sigma_j(x + \lambda y)] \neq 0,$$

dh. für alle $i \neq j$: $\sigma_i(x + \lambda y) \neq \sigma_j(x + \lambda y)$.

Ist $f \in K[X]$ das Minimalpolynom von $x+\lambda y$, so sind $\sigma_i(x+\lambda y)$, $1 \leqslant i \leqslant n$, Nullstellen von f in N, also gilt $\deg(f) \geqslant n$. Trivialerweise gilt sogar Gleichheit. Also hat $x+\lambda y$ Grad n und es gilt $L = K(x+\lambda y)$. □

Aus dem Beweis folgt: Ist $K \subset L = K(x_1, \ldots, x_n)$ endliche separabel Erweiterung, so gibt es $\lambda_2, \ldots, \lambda_n \in K$, so daß $x_1 + \lambda_2 x_2 + \cdots + \lambda_n x_n$ primitives Element von L/K ist.

Beispiel* 3.3.12. Seien $p, q \in \mathbb{N}$ verschiedenen Primzahlen.

(a) Man zeige, daß die Körper $\mathbb{Q}(\sqrt{p})$ und $\mathbb{Q}(\sqrt{q})$ nicht isomorph sind (siehe Beispiel 3.1.17)

(b) Man zeige, daß die Körpererweiterung $\mathbb{Q}(\sqrt{p}, \sqrt{q})/\mathbb{Q}$ Grad 4 hat.

(c) Man bestimme das Minimalpolynom von $\sqrt{p} + \sqrt{q}$ und schließe daraus, daß $\sqrt{p} + \sqrt{q}$ ein primitives Element von $\mathbb{Q}(\sqrt{p}, \sqrt{q})/\mathbb{Q}$ ist.

3.3.3 Kriterien für die Separabilität von Polynomen

Sei K ein Körper.

Definition 3.3.13. Für $f = \sum_{i=0}^{n} \alpha_i X^i \in K[X]$ sei

$$f' = \sum_{i=1}^{n} \alpha_i i X^{i-1}.$$

Das Polynom $f' \in K[X]$ heißt (formale) Ableitung von f.

Die Abbildung

$$K[X] \to K[X], f \mapsto f'$$

ist K-linear und genügt der Produktregel, das heißt, für $f, g \in K[X]$ gilt $(fg)' = f'g + fg'$.

Proposition 3.3.14. *Für $f \in K[X] \backslash K$ sind äquivalent:*

(a) Das Polynom f hat in einem Oberkörper von K eine mehrfache Nullstelle.

(b) Die Polynome f und f' haben in einem Oberkörper von K eine gemeinsame Nullstelle.

(c) Es existiert ein nichtkonstantes Polynom $g \in K[X]$ mit $g \mid f$ und $g \mid f'$.

Beweis. **„(a) ⇒ (b)“** Es gibt $K \subset L$, $x \in L$, $1 < n \in \mathbb{N}$ und $f_1 \in L[X]$ mit $f = (X-x)^n f_1$ und $f_1(x) \neq 0$. Dann gilt:

$$f' = n(X-x)^{n-1} f_1 + (X-x)^n f_1'$$

also $f'(x) = 0$.
„(b) ⇒ (c) “] Sei $K \subset L$ eine Erweiterung, $x \in L$ eine gemeinsame Nullstelle von f und f'. Ist $g \in K[X]$ das Minimalpolynom von x, dann gilt $g \mid f$ und $g \mid f'$.
„(c) ⇒ (a) “ Sei g wie in (c), sei $K \subset L$ ein Oberkörper, in dem g eine Nullstelle x hat. Dann gilt $f(x) = 0 = f'(x)$. Sei $f = (X-x)^n f_1$ mit $n \in \mathbb{N}$, $f_1 \in L[X]$ und $f_1(x) \neq 0$. Wäre $n = 1$, so wäre $f' = f_1 + (X-x)f_1'$, also $f'(x) = f_1(x) \neq 0$. Also muß $n > 1$ sein. □

Satz 3.3.15. *Sei $f \in K[X]$ irreduzibel. Das Polynom f ist genau dann separabel, wenn $f' \neq 0$ ist.*

Beweis. Das Polynom f ist nicht separabel genau dann, wenn es in einem Oberkörper mehrere Nullstellen hat. Das gilt genau dann, wenn $g \in K[X]\backslash K$ existiert so daß $g \big| f$ und $g \big| f'$. Da f irreduzibel ist, gilt das genau dann, wenn $f \big| f'$, also $f' = 0$. □

Satz 3.3.16. *Sei* $\mathrm{char}(K) = 0$.

(a) Für $f \in K[X]$ gilt $f' = 0$ genau dann, wenn $f \in K$.

(b) Der Körper K ist vollkommen, dh. jedes irreduzible Polynom in $K[X]$ ist separabel.

Beweis. **Zu (a):** Sei $f = \sum_{i=0}^{n} \alpha_i X^i$, $f' = \sum_{i=1}^{n} \alpha_i i X^{i-1}$. Es gilt $f' = 0$ genau dann, wenn für alle $1 \leqslant i \leqslant n$: $i\alpha_i = 0$, genau dann, wenn $f = \alpha_0 \in K$.
Zu (b): Sei $f \in K[X]$ irreduzibel. Dann ist $f \in K[X]\backslash K$ und nach (a) ist $f' \neq 0$. Nach dem vorherigen Satz ist f dann separabel. □

Sei p eine Primzahl, R ein kommutativer Ring mit $p.R = 0$. Die Abbildung

$$\sigma : R \to R, x \mapsto x^p$$

ist ein Ringhomomorphismus, denn wegen $p \big| \binom{p}{i}$ für $1 \leqslant i \leqslant p-1$ gilt

$$(x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^{p-i} y^i = x^p + y^p;$$

Ferner gilt

$$(xy)^p = x^p y^p \text{ und } 1^p = 1.$$

Die Abbildung σ heißt Frobeniushomomorphismus. Man setzt $R^p = \mathrm{im}(\sigma)$.

Satz 3.3.17. *Sei* $\mathrm{char}(K) = p$, *wobei p eine Primzahl ist.*

(a) Für $f \in K[X]$ gilt $f' = 0$ genau dann, wenn $f \in K[X^p]$.

(b) Ein irreduzibles Polynom $f \in K[X]$ ist genau dann separabel, wenn $f \notin K[X^p]$.

(c) Der Körper K ist genau dann vollkommen, wenn $K = K^p$, dh. wenn σ surjektiv ist.

Beweis. **Zu (a):** Sei $f = \sum_{i=0}^{n} \alpha_i X^i$, $f' = \sum_{i=1}^{n} \alpha_i i X^{i-1}$. Die Ableitung $f' = 0$ genau dann, wenn für alle $1 \leqslant i \leqslant n$ mit $p \nmid i$ gilt $\alpha_i = 0$. Man sieht leicht, das f dann genau die Form $f = \sum_{p|i} \alpha_i X^i$ hat, dh. $f \in K[X^p]$.
Zu (b): Wir wissen bereits, daß f genau dann separabel ist, wenn$f' \neq 0$. Und nach (a) ist dies genau dann der Fall, wenn f nicht in $K[X^p]$ enthalten ist.
Zu (c): Zum Beweis von (c) brauchen wir folgendes Lemma.

Lemma 3.3.18. *Sei* $\mathrm{char}(K) = p$ *und $\alpha \in K$. Das Polynom $f = X^p - \alpha$ ist genau dann irreduzibel in $K[X]$, wenn es in K keine Nullstellen hat.*

Beweis. Wir nehmen zunächst an, daß f in K eine Nullstelle x hat. Dann ist $\alpha = x^p$ und es gilt

$$f = X^p - \alpha = X^p - x^p = (X-x)^p.$$

Damit ist f reduzibel.

Habe andererseits f keine Nullstelle in K. Es gibt eine endliche Erweiterung $K \subset L$ und $x \in L\backslash K$ mit $f(x) = 0$. Dann ist $\alpha = x^p$ und $f = (X-x)^p$. Angenommen es gibt $g, h \in K[X]$, so daß $f = gh$. Ohne Einschränkung kann man annehmen, daß g und h normiert sind. Dann existieren $a, b \in \mathbb{N}$, mit $a + b = p$ und $g = (X-x)^a$ sowie $h = (X-x)^b$. Es folgt, dass $x^a, x^b \in K$. Wegen $1 \leqslant a < p$ sind a und p relativ prim und es gibt $u, v \in \mathbb{Z}$ mit $au + pv = 1$. Es folgt $x = x^{av} x^{pu} \in K$, was ein Widerspruch zur Annahme ist. □

Weiter im Beweis von Satz 3.3.17 (c): Sei zunächst K vollkommen, $\alpha \in K$ und $f = X^p - \alpha$. Da $f' = 0$ und K vollkommen ist, ist f reduzibel. Nach dem Lemma hat dann f in K eine Nullstelle x. Es folgt $\alpha = x^p \in K^p$, dh. α ist im Bild von σ enthalten, und $K = K^p$.

Sei andererseits $K = K^p$. Angenommen es gibt ein irreduzibles nicht separabels Polynom $f \in K[X]$. Dann ist $f \in K[X^p]$, etwa $f = \sum_{i=0}^{n} \alpha_i X^{pi}$. Für $0 \leqslant i \leqslant n$ gibt es nach Voraussetzung $\beta_i \in K$ mit $\beta_i^p = \alpha_i$. Es folgt

$$f = \sum_{i=0}^{n} \beta_i^p X^{pi} = \left(\sum_{i=0}^{n} \beta_i X^i \right)^p ,$$

unmöglich wegen der Irreduzibilität von f. Also ist jedes irreduzible Polynom in $K[X]$ separabel. □

Beispiele* 3.3.19. Welche der folgenden Körpererweiterungen sind normal, separabel, beides, keines davon?

(a) $\mathbb{C} / \mathbb{R}$.

(b) $\mathbb{C} / \mathbb{Q}$.

(c) Sei $f = X^3 - 1 \in \mathbb{Q}[X]$, α eine Nullstelle von f. $\mathbb{Q}(\alpha) / \mathbb{Q}$.

(d) Sei $f = X^4 - 3 \in \mathbb{Q}[X]$, α eine Nullstelle von f. $\mathbb{Q}(\alpha) / \mathbb{Q}$.

(e) Sei $f = X^3 - 1 \in \mathbb{F}_5[X]$, α eine Nullstelle von f. $\mathbb{F}_5(\alpha) / \mathbb{F}_5$.

(f) Sei $f = X^3 - t \in \mathbb{F}_2(t)[X]$, α eine Nullstelle von f. $\mathbb{F}_2(t)(\alpha) / \mathbb{F}_2(t)$.

(g) Sei $f = X^2 - t \in \mathbb{F}_2(t)[X]$, α eine Nullstelle von f. $\mathbb{F}_2(t)(\alpha) / \mathbb{F}_2(t)$.

(h) Sei $f = X^6 - t \in \mathbb{F}_2(t)[X]$, α eine Nullstelle von f. $\mathbb{F}_2(t)(\alpha) / \mathbb{F}_2(t)$.

3.4 Endliche Körper

Ist p eine Primzahl, dann setzt man $\mathbb{F}_p = \mathbb{Z} / p\mathbb{Z}$. Der Frobeniushomomorphismus $\sigma : \mathbb{F}_p \to \mathbb{F}_p$ ist injektiv, also bijektiv. Insbesondere ist $\mathbb{F}_p$ ein vollkommener Körper.

Satz 3.4.1 (Moore, 1893)**.** *(a) Seien $p \in \mathbb{N}$ eine Primzahl, $n \in \mathbb{N}$, und $\mathbb{F}_{p^n}$ ein Zerfällungskörper des Polynoms $f = X^{p^n} - X \in \mathbb{F}_p[X]$. Der Körper $\mathbb{F}_{p^n}$ besteht genau aus den Nullstellen des Polynoms f und hat p^n Elemente.*

(b) Ist K ein endlicher Körper, so gibt es $n \in \mathbb{N}$ und eine Primzahl $p \in \mathbb{N}$ mit $K = \mathbb{F}_{p^n}$.

Beweis. **Zu (a):** Es gilt $f' = p^n X^{p^n - 1} - 1 = -1$, also hat f in $\mathbb{F}_{p^n}$ nur einfache Nullstellen. Die Menge

$$L = \left\{ x \in \mathbb{F}_{p^n} \;\middle|\; x^{p^n} = x \right\} = \left\{ x \in \mathbb{F}_{p^n} \;\middle|\; \sigma^n(x) = x \right\}$$

ist ein Unterkörper von $\mathbb{F}_{p^n}$, der alle Nullstellen von f und $\mathbb{F}_p$ enthält. Also ist $L = \mathbb{F}_{p^n}$ und $|\, \mathbb{F}_{p^n} \,| = p^n$.
Sei K endlicher Körper. Dann ist $\mathrm{char}(K) = p$ eine Primzahl, der Primkörper K_0 von K ist isomorph zu $\mathbb{F}_p$, und mit $n = [K : K_0]$ gilt $|K| = p^n$. Wir zeigen $X^{p^n} - X = \prod_{x \in K} (X - x)$ in $K[X]$:
Wir wissen, daß K^* zyklisch von der Ordnung $p^n - 1$ ist. Es folgt $X^{p^n - 1} - 1 = \prod_{x \in K^*} (X - x)$, denn die $X - x$ sind paarweise teilerfremde Teiler von $X^{p^n - 1} - 1$. Es folgt $X^{p^n} - X = \prod_{x \in K} (X - x)$.
Diese Gleichung zeigt, daß K Zerfällungskörper des Polynoms $X^{p^n} - X$ über K_0 ist. Wegen der Eindeutigkeit von Zerfällungskörpern bis auf Isomorphie folgt $K \cong \mathbb{F}_{p^n}$. □

*Bemerkung** 3.4.2. Im obigen Satz wurde zwar gezeigt, daß jeder endliche Körper zu einem Körper $\mathbb{F}_{p^n}$ isomorph ist, jedoch gibt es auch andere Darstellungen eindlicher Körper und der Isomorphismus ist in der Regel nicht eindeutig.

Beispiel* 3.4.3. Hier betrachten wir verschiedene Darstellungen von Körpern der Ordnung 9. Man entscheide für die Beispiele

(a) $L = \mathbb{Z} / (9)$,

(b) $L = \mathbb{Z}[\sqrt{2}]/(3)$,

ob L ein Körper ist, und finde gegebenenfalls ein irreduzibles, normiertes Polynom $\pi(X) \in \mathbb{F}_3[X]$ und einen Isomorphismus

$$L \xrightarrow{\sim} \mathbb{F}_3[X]/(\pi(X)).$$

Folgerung 3.4.4. *Sei K endlicher Körper, $K \cong \mathbb{F}_{p^n}$.*

(a) Der Körper K ist perfekt.

(b) Es gilt $\mathrm{Aut}(K) = \mathrm{Gal}(K/K_0) = \langle\sigma\rangle$, und diese Gruppe hat Ordnung n. Dabei ist σ der Forbeniushomomorphismus von K.

Beweis. **Zu (a):** Der Frobeniushomomorphismus $\sigma : K \to K, x \mapsto x^p$ ist Ringhomomorphismus, also injektiv, und somit auch bijektiv.
Zu (b): Die Erweiterung K/K_0 ist nach dem Satz normal. Da K_0 perfekt ist, sind die Minimalpolynome aller Elemente von K separabel, also ist K/K_0 separabel. Es gilt dann

$$|\mathrm{Gal}(K/K_0)| = [K : K_0] = n.$$

Sicher ist σ in $\mathrm{Gal}(K/K_0)$ enthalten. Für alle $x \in K$ gilt $\sigma^n(x) = x^{p^n} = x$, also ist $\sigma^n = \mathrm{id}_K$. Gilt $\sigma^l = \mathrm{id}_K$ für $l \in \mathbb{N}$, dann gilt für alle $x \in K$: $x = \sigma^l(x) = x^{p^l}$. Es folgt $p^n \leqslant p^l$ und $n \leqslant l$. Also ist $\mathrm{ord}(\sigma) = n$ und $\mathrm{Gal}(K/K_0) = \langle\sigma\rangle$. □

Satz 3.4.5. *Sei $K \cong \mathbb{F}_{p^n}$ ein endlicher Körper, und $K \subset L$ eine endliche Körpererweiterung vom Grad m. Dann ist L isomorph zum endlichen Körper $\mathbb{F}_{p^{mn}}$, die Erweiterung L/K ist normal und separabel, die Galoisgruppe ist $\mathrm{Gal}(L/K) = \langle\sigma^n\rangle$ und diese Gruppe hat Ordnung m.*

Beweis. Da L endlicher Körper mit p^{nm} Elementen ist, ist L isomorph zu $\mathbb{F}_{p^{nm}}$. Da L Zerfällungskörper von $X^{p^{nm}} - X$ über K_0 ist, ist L auch Zerfällungskörper dieses Polynoms über K. Also ist L/K normal. Wie vorher sieht man, daß L/K separabel ist. Es folgt

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

Nach der Folgerung ist $\mathrm{Gal}(L/K_0) = \langle\sigma\rangle$ und diese Gruppe hat Ordnung nm. Für $1 \leqslant l \leqslant nm$ gilt $\sigma^l \in \mathrm{Gal}(L/K)$ genau dann, wenn $\sigma^l\big|_K = \mathrm{id}_K$. Dies gilt genau dann, wenn $n \big| l$, denn $\sigma\big|_K$ hat Ordnung n. Es folgt $\mathrm{Gal}(L/K) = \langle\sigma^n\rangle$. □

Beispiel 3.4.6 (Beispiel eines nichtperfekten Körpers)**.** Sei p ein Primzahl und $K = \mathbb{F}_p(X)$. Es gilt $K^p \subsetneq K$, denn $K^p = \mathbb{F}_p(X^p)$ und $X \in K \backslash K^p$. (Vergleiche 3.3.1.)

Beispiel* 3.4.7. Es seien p und q Primzahlen. Warum zerfällt das Polynom

$$f = X^{p^q} - X$$

über dem Körper $\mathbb{F}_p$ mit p Elementen in p verschiedene Faktoren vom Grad 1 und $\frac{p^q - p}{q}$ verschiedene irreduzible Faktoren vom Grad q?

Beispiel* 3.4.8. Sei F ein eindlicher Körper. Dann ist die multiplikative Gruppe F^* zyklisch.

3.5 Galoiserweiterungen

3.5.1 Definition

Definition 3.5.1. Eine Körpererweiterung $K \subset L$ heißt Galois'sch oder Galoiserweiterung, wenn L/K normal und separabel ist.

Satz 3.5.2. *Für eine endliche Erweiterung $K \subset L$ sind äquivalent:*

(a) Die Erweiterung L/K ist Galois'sch.

(b) Der Körper L ist Zerfällungskörper eines separabeln Polynoms in $K[X]$.

(c) Der Körper L ist Zerfällungskörper eines irreduziblen, separabeln Polynoms in $K[X]$.

Beweis. **[(a) ⇒ (c)]** Es gibt $x \in L$ mit $L = K(x)$. Sei $f \in K[X]$ das Minimalpolynom von x. Dann ist f irreduzibel und separabel und L ist Zerfällungskörper von f.
[(c) ⇒ (b)] Das ist klar.
[(b) ⇒ (a)] Gilt (b), so ist L/K normal. Da L durch Adjunktion endlich vieler separabelr Elemente aus K entsteht, ist L/K separabel. □

3.5.2 Der Zugang nach Dedekind und Artin

Für einen Körper L und eine Untergruppe $G \subset \mathrm{Aut}(L)$ sei

$$\mathrm{Fix}_L(G) = \mathrm{Fix}(G) = \left\{ x \in L \;\middle|\; \forall \sigma \in G : \sigma(x) = x \right\}.$$

Dies ist ein Unterkörper von L, er heißt Fixkörper von G in L. Für einen Unterkörper $K \subset L$ gilt $K \subset \mathrm{Fix}(G)$ genau dann, wenn $G \subset \mathrm{Gal}(L/K)$. Ein Hauptergebnis des Abschnitts ist folgender Satz.

Satz 3.5.3 (Artin)**.** *Sei L ein Körper, $G \subset \mathrm{Aut}(L)$ eine Untergruppe und $K = \mathrm{Fix}_L(G)$. Die Erweiterung L/K ist genau dann endlich, wenn G endlich ist. Gelten diese Aussagen, dann ist $G = \mathrm{Gal}(L/K)$ und $|G| = [L : K]$.*

Es folgen einige Vorbemerkungen zum Beweis.

Definition 3.5.4. Seien Γ eine Gruppe und L ein Körper. Ein Gruppenhomomorphismus $\xi : \Gamma \to L^*$ heißt Charakter von Γ in L. Die Menge aller Charaktere von Γ in L bezeichnen wir mit $\mathrm{Gr}(\Gamma, L^*)$. Sie ist Teilmenge des L-Vektorraums L^Γ aller Abbildungen $f : \Gamma \to L$; dabei sei $(l.f)(x) = lf(x)$ für $l \in L$ und $x \in \Gamma$.

Lemma 3.5.5 (Dedekind)**.** *Die Menge $\mathrm{Gr}(\Gamma, L^*)$ ist linear unabhängige Teilmenge des L-Vektorraums L^Γ, dh. jede endliche Teilmenge von $\mathrm{Gr}(\Gamma; L^*)$ ist linear unabhängig.*

Beweis. Wir nehmen an, das sei falsch. Dann gibt es eine kleinste Zahl, $n \in \mathbb{N}$ mit folgenden Eigenschaften: Es gibt paarweise verschiedene $\xi_1, \ldots, \xi_n \in \mathrm{Gr}(\Gamma, L^*)$ und $l_1, \ldots, l_n \in L^*$ mit $\sum_{i=1}^n l_i \xi_i = 0$. Dann ist $n > 1$, denn aus $l_1 \xi_1 = 0$ folgt

$$0 = l_1 \xi_1(1) = l_1 . 1 = l_1,$$

unmöglich. Da $\xi_1 \neq \xi_n$, gibt es $x \in \Gamma$ mit $\xi_1(x) \neq \xi_n(x)$. Für $y \in \Gamma$ gilt damit: ist $\sum_{i=1}^n l_i \xi_i(y) = 0$, dann ist

$$\begin{aligned} \sum_{i=1}^n l_i \xi_1(x) \xi_i(y) &= 0 \\ \sum_{i=1}^n l_i \xi_i(x) \xi_i(y) &= \sum_{i=1}^n l_i \xi_i(x \cdot y) = 0, \end{aligned}$$

also $\sum_{i=1}^n l_i (\xi_1(x) - \xi_i(x)) \xi_i(y) = 0$. Es folgt

$$\sum_{i=2}^n l_i (\xi_1(x) - \xi_i(x)) \xi_i(y) = 0$$

mit $l_1(\xi_1(x) - \xi_n(x)) \neq 0$. Widerspruch zur Minimalität von n. □

Folgerung 3.5.6. *Seien $K \subset L \subset M$ Körpererweiterungen.*

(a) Die Menge $\mathrm{Alg}_K(L, M)$ ist linear unabhängige Teilmenge des M-Vektorraums $\mathrm{Hom}_K(L, M)$. Dabei sei $(\mu.f)(l) = \mu f(l)$ für $\mu \in M$, $f \in \mathrm{Hom}_K(L, M)$, $l \in L$.

(b) Ist L/K endlich, so gilt

$$|\mathrm{Alg}_K(L, M)| \leqslant [L : K].$$

Insbesondere gilt

$$|\mathrm{Gal}(L/K)| \leqslant [L : K].$$

Beweis. **Zu (a):** Seien $\sigma_1, \dots, \sigma_n \in \mathrm{Alg}_K(L, M)$ paarweise verschieden, $\mu_1, \dots, \mu_n \in M$ mit $\sum_{i=1}^n \mu_i \sigma_i = 0$. Da die σ_i injektiv sind, gilt $\sigma_i\big|_{L^*} \in \mathrm{Gr}(L^*, M^*)$ für alle $1 \leqslant i \leqslant n$, und die Charaktere sind paarweise verschieden. Da $\sum_{i=1}^n \mu_i \sigma_i\big|_{L^*} = 0$ folgt $\mu_1 = \dots = \mu_n = 0$ aus Lemma 3.5.5.
Zu (b): Sei L/K endlich. Nach (a) genügt es zu zeigen, daß $\dim_M \mathrm{Hom}_K(L, M) = [L : K]$ ist. Sei $l_1, \dots, l_n$ eine K-Basis von L, sei $\lambda_1, \dots, \lambda_n \in \mathrm{Hom}_K(L, K)$ die dazu duale Basis, dh. $\lambda_i(l_j) = \delta_{ij}$ für alle $1 \leqslant i, j \leqslant n$. Dann ist $\lambda_1, \dots, \lambda_n$ auch M-Basis von $\mathrm{Hom}_K(L, M)$: Wenn $\sum_{i=1}^n \mu_i \lambda_i = 0$ mit $\mu_1, \dots, \mu_n \in M$, dann gilt für alle j,

$$0 = \sum_{i=1}^n \mu_i \lambda_i(l_j) = \mu_j,$$

dh. die λ_i sind linear unabhängig. Ferner gilt

$$\sigma = \sum_{i=1}^n \sigma(l_i)\lambda_i$$

für alle $\sigma \in \mathrm{Hom}_K(L, M)$, dh. die λ_i sind eine Basis. □

Proposition 3.5.7. *Sei L ein Körper, G eine endliche Untergruppe von $\mathrm{Aut}(L)$ und $K = \mathrm{Fix}(G)$. Dann ist die Abbildung*

$$T = T_G : L \to K, x \mapsto \sum_{\sigma \in G} \sigma(x)$$

surjektiv und K-linear. Sie heißt Spur von L/K zu G.

Beweis. Für $x \in L$ und $\tau \in G$ gilt

$$\tau T(x) = \sum_{\sigma \in G} \tau\sigma(x) = \sum_{\sigma \in G} \sigma(x) = T(x).$$

Also gilt $T(x) \in \mathrm{Fix}(G) = K$ für alle $x \in L$, dh. T ist wohldefiniert. Da alle $\sigma \in G$ K-linear sind, ist T K-linear. Da G nach Folgerung 3.5.6 linear unabhängige Teilmenge von $\mathrm{Hom}_K(L, L)$ ist, ist $T = \sum_{\sigma \in G} \sigma \neq 0$, also ist T surjektiv. □

Lemma 3.5.8. *Es seien L ein Körper, G eine endliche Untergruppe von $\mathrm{Aut}(L)$ und $K = \mathrm{Fix}(G)$. Dann gilt $[L : K] = |G|$ und $G = \mathrm{Gal}(L/K)$.*

Beweis. Sei $G = \{\sigma_1, \dots, \sigma_n\}$ mit $\sigma_i \neq \sigma_j$ für $i \neq j$. Wir zeigen zunächst $[L : K] \leqslant n$. Dazu zeigen wir, daß jede Familie $l_1, \dots, l_m$ in L mit $m > n$ in K linear abhängig ist. Wir betrachten die Matrix

$$A = (\sigma_i^{-1}(l_j))_{1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m} \in L^{n,m}.$$

Wegen $m > n$ gibt es $0 \neq (x_i) \in L^{m,1}$ mit

$$A \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = 0.$$

Man kann annehmen, daß $x_r = 1$ ist für ein $1 \leqslant r \leqslant m$. Nach Proposition gibt es $l \in L$ mit $T(l) \neq 0$. Sei $(y_i) = l\,(x_i)$. Es folgt

$$A \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix} = 0,$$

dh. für alle $1 \leqslant i \leqslant n$, $\sum_{j=1}^m \sigma_i^{-1}(l_j) y_j = 0$, oder nach Anwendung von σ_i: $\sum_{j=1}^m l_j \sigma_i(y_j) = 0$. Wir erhalten eine Linearkombination $\sum_{i=1}^n \sum_{j=1}^m l_j \sigma_i(y_j) = \sum_{j=1}^m l_j T(y_j) = 0$, mit $t(y_r) = t(l) \neq 0$. Also ist die Familie $l_1, \dots, l_m$ linear abhängig.
Es gilt $G \subset \mathrm{Gal}(L/K)$, also haben wir

$$[L : K] \leqslant n = |G| \leqslant |\,\mathrm{Gal}(L/K)| \leqslant [L : K],$$

wobei die letzte Ungleichung nach Folgerung 3.5.6 gilt. Es folgt $|G| = [L : K]$ und $G = \mathrm{Gal}(L/K)$. □

Folgerung 3.5.9. *Sei L ein Körper, G eine endliche Untergruppe von $\mathrm{Aut}(L)$ und $K = \mathrm{Fix}(G)$.*

(a) Für jede Körpererweiterung $j : L \hookrightarrow L'$ ist die Abbildung

$$G \to \mathrm{Alg}_K(L, L'), \sigma \mapsto j \circ \sigma$$

bijektiv.

(b) Die Erweiterung L/K ist Galois'sch und endlich.

Beweis. **Zu (a):** Die Injektivität der Abbildung ist klar. Nach Lemma 3.5.8 ist L/K endlich. Nach Folgerung 3.5.6 gilt dann $|\mathrm{Alg}_K(L, L')| \leqslant [L : K]$. Es folgt mit Lemma 3.5.8

$$|G| \leqslant |\mathrm{Alg}_K(L, L')| \leqslant [L : K] = |G|.$$

Also ist die Abbildung auch surjektiv.
Zu (b): Nach Lemma 3.5.8 ist $[L : K]$ endlich. Für jeden Oberkörper $L \subset L'$ und alle $\tau \in \mathrm{Alg}_K(L, L')$ gilt $\tau(L) = L$. Also ist L/K normal. Da

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

ist, ist L/K separabel. □

Beweis des Satzes von Artin. Sei L/K endlich. Es gilt $G \subset \mathrm{Gal}(L/K)$, also $|G| \leqslant |\mathrm{Gal}(L/K)| \leqslant [L : K]$ nach Folgerung 3.5.6. Also ist G endlich. Sei umgekehrt G endlich. Nach Lemma 3.5.8 ist dann $[L : K]$ endlich und es gilt $G = \mathrm{Gal}(L/K)$ und $|G| = [L : K]$. □

Satz 3.5.10. *Für eine Körpererweiterung $K \subset L$ sind äquivalent:*

(a) Die Erweiterung L/K ist endlich und Galois'sch.

(b) Es gibt eine endliche Untergruppe G von $\mathrm{Aut}(L)$ mit $K = \mathrm{Fix}(G)$.

(c) Die Erweiterung L/K ist endlich und $K = \mathrm{Fix}(\mathrm{Gal}(L/K))$.

(d) Die Erweiterung L/K ist endlich und $|\mathrm{Gal}(L/K)| = [L : K]$.

Beweis. **[(a) ⇒ (d)]** Ist L/K endlich, normal und separabel, dann ist nach Abschnitt 3.3.1 $|\mathrm{Gal}(L/K)| = [L : K]$.
[(d) ⇒ (c)] Sei $E = \mathrm{Fix}(\mathrm{Gal}(L/K))$. Es gilt $K \subset E$. Nach dem Satz 3.5.3 von Artin ist $[L : E] = |\mathrm{Gal}(L/K)|$. Aus (d) folgt $[L : E] = [L : K] = [L : E] \cdot [E : K]$, also $[E : K] = 1$ und $E = K$.
[(c) ⇒ (b)] Nach Folgerung 3.5.6 ist $|\mathrm{Gal}(L/K)| \leqslant [L : K]$. Also ist $G = \mathrm{Gal}(L/K)$ endlich und $K = \mathrm{Fix}(G)$.
[(b) ⇒ (a)] Nach dem Satz 3.5.3 von Artin ist $G = \mathrm{Gal}(L/K)$ und $|G| = [L : K]$. Ebenfalls nach Folgerung 3.5.9 ist L/K Galois'sch. □

3.5.3 Erste Beispiele

Beispiel 3.5.11. Endliche Erweiterungen von endlichen Körpern sind Galois'sch.

Beispiel 3.5.12. Sei $d \in \mathbb{Z} \setminus \{0, 1\}$ quadratfrei. Der Körper $\mathbb{Q}(\sqrt{d}) \subset \mathbb{C}$ ist Zerfällungskörper des irreduziblen, separabeln Polynoms $X^2 - d \in \mathbb{Q}[X]$, also ist $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ Galoiserweiterung vom Grad 2. Eine $\mathbb{Q}$-Basis von $\mathbb{Q}(\sqrt{d})/$ ist $\{1, \sqrt{d}\}$. Die Abbildung

$$\sigma : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}(\sqrt{d}), \alpha + \beta\sqrt{d} \mapsto \alpha - \beta\sqrt{d}$$

ist Automorphismus der Ordnung 2 mit $\sigma\big|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$. Es folgt

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) = \langle\sigma\rangle.$$

Ist $K \subset \mathbb{C}$ eine quadratische Erweiterung von $\mathbb{Q}$, dh. mit $[K : \mathbb{Q}] = 2$, so gibt es genau eine quadratfreie Zahl $d \in \mathbb{Z} \setminus \{0, 1\}$ mit $K = \mathbb{Q}(\sqrt{d})$.

Beweis dazu. Sei $x \in K \setminus \mathbb{Q}$, sei $f = X^2 + \alpha X + \beta \in \mathbb{Q}[X]$ das Minimalpolynom von x. Es gilt $f = (X + \frac{\alpha}{2})^2 + \beta - \frac{\alpha^2}{4}$. Für $y = x + \frac{\alpha}{2}$ gilt $K = \mathbb{Q}(y)$ und das Minimalpolynom von y ist $g = X^2 - \gamma$ mit $\gamma = \frac{\alpha^2}{4} - \beta$. Es folgt $y = \pm\sqrt{\gamma}$. Es gibt $u, v \in \mathbb{N}$ und eine quadratfreie Zahl $d \in \mathbb{Z} \setminus \{0, 1\}$ mit $\gamma = \frac{u^2 d}{v^2}$. Es folgt $K = \mathbb{Q}(\sqrt{d})$. Die Eindeutigkeit ist leicht zu sehen. □

Beispiel 3.5.13. Jede quadratische Erweiterung $K \subset L$ ist normal. Denn für $x \in L \setminus K$ gilt $L = K(x)$. Ist $f = X^2 + \alpha X + \beta \in K[X]$ das Minimalpolynom von x, dann $f = X^2 + \alpha X + \beta - x^2 - \alpha x - \beta = (X - x)(X + x + \alpha)$. Also ist L/K Zerfällungskörper von f. Insbesondere ist jede separabel quadratische Erweiterung $K \subset L$ Galoiserweiterung.

Beispiel 3.5.14. Das Polynom $f = X^3 - 2 \in \mathbb{Q}[X]$ ist irreduzibel und separabel. Der Körper $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$ mit $\omega = \frac{1}{2}(-1 + \sqrt{-3})$ ist Zerfällungskörper von f. Also ist $K/\mathbb{Q}$ Galois'sch. Wir wissen, daß $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathfrak{S}_3$ ist.

3.5.4 Der Hauptsatz der Galoistheorie

Hauptsatz der Galoistheorie 3.5.15. *Sei $K \subset L$ eine endliche Galoiserweiterung mit $G = \mathrm{Gal}(L/K)$, sei $\mathscr{K}$ die Menge aller Zwischenkörper zwischen K und L, $\mathscr{G}$ die Menge aller Untergruppen von G. Dann gilt:*

(a) Die Abbildungen

$$\begin{aligned} \mathscr{K} \to \mathscr{G}, &\quad E \mapsto \mathrm{Gal}(L/E) \\ \mathscr{G} \to \mathscr{K} &\quad H \mapsto \mathrm{Fix}_L(H) \end{aligned}$$

sind zueinander invers und antiton. Das heißt, sie sind antiton (monoton und ordnungsumkehrend), und für alle $E \in \mathscr{K}$ gilt $E = \mathrm{Fix}_L(\mathrm{Gal}(L/E))$, und für alle $H \in \mathscr{G}$ gilt $H = \mathrm{Gal}(L/\mathrm{Fix}_L(H))$.

(b) Für $E \in \mathscr{K}$ ist L/E Galois'sch und es gilt

$$\begin{aligned} [L : E] &= |\mathrm{Gal}(L/E)| \\ [E : K] &= [G : \mathrm{Gal}(L/E)]\,. \end{aligned}$$

Für $E \in \mathscr{K}$, $H = \mathrm{Gal}(L/E)$ sind äquivalent:

(i) Die Erweiterung E/K ist Galois'sch.

(ii) Für alle $\sigma \in G$ ist $\sigma(E) = E$.

(iii) Die Gruppe H ist ein Normalteiler von G.

Gilt eine der Aussagen (i)-(iii), dann ist die Abbildung

$$G \to \mathrm{Gal}(E/K), \sigma \mapsto \sigma\big|_E$$

ein surjektiver Gruppenhomomorphismus mit Kern H. Dann ist

$$G/H \to \mathrm{Gal}(E/K), \sigma H \mapsto \sigma\big|_E,$$

Isomorphismus.

Beweis. **Zu (b):** Sei $E \in \mathscr{K}$. Die Erweiterung L/E ist endlich, normal und separabel, also ist L/E endliche Galoiserweiterung. Dann gilt $[L : E] = |\mathrm{Gal}(L/E)|$. Aus

$$[G : \mathrm{Gal}(L/E)] \cdot |\mathrm{Gal}(L/E)| = |G| = [L : K] = [L : E] \cdot [E : K]$$

folgt $[G : \mathrm{Gal}(L/E)] = [E : K]$.
Zu (a): Beide Abbildungen sind wohldefiniert. Sie sind antiton, denn aus $E_1 \subset E_2$ folgt $\mathrm{Gal}(L/E_2) \subset \mathrm{Gal}(L/E_1)$ und aus $H_1 \subset H_2$ folgt $\mathrm{Fix}_L(H_2) \subset \mathrm{Fix}_L(H_1)$. Weiterhin gilt für $H \in \mathscr{G}$ und $E = \mathrm{Fix}_L(H)$ nach dem Satz 3.5.3 von Artin, daß $\mathrm{Gal}(L/E) = H$. Andererseits ist für $E \in \mathscr{K}$ die Erweiterung L/E nach (b) Galois'sch und nach dem Charakterisierungssatz 3.5.2 gilt $E = \mathrm{Fix}_L(\mathrm{Gal}(L/E))$.

Zu (c): [(i) ⇒ (ii)] Sei E/K Galois'sch. Da E/K normal ist, gilt $\sigma(E) = E$ für alle $\sigma \in G$.
[(ii) ⇒ (iii)] Nach (ii) ist die Abbildung $G \to \mathrm{Gal}(E/K)$, $\sigma \mapsto \sigma\big|_E$ wohldefiniert. Sie ist offenbar ein Homomorphismus. Für $\sigma \in G$ gilt $\sigma\big|_E = \mathrm{id}_E$ genau dann, wenn $\sigma \in \mathrm{Gal}(L/E) = H$. Also ist H der Kern dieses Homomorphismus und damit ein Normalteiler.
[(iii) ⇒ (ii)] Für $\sigma \in G$, $\tau \in H$, $x \in E$ gilt:

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

da $\sigma^{-1}\tau\sigma \in H$. Also $\sigma(x) \in \mathrm{Fix}_L(H) = E$. Es folgt $\sigma(E) = E$ für alle $\sigma \in G$.
[(ii) ⇒ (i)] Nach (ii) ist $G\big|_E \subset \mathrm{Gal}(E/K)$. Wegen $\mathrm{Fix}_L(G) = K$ gilt $\mathrm{Fix}_E(G\big|_E) = K$. Nach dem Charakterisierungssatz 3.5.2 ist also E/K Galois'sch.
Beweis des Zusatzes Die Abbildung $G \to \mathrm{Gal}(E/K)$, $\sigma \mapsto \sigma\big|_E$ ist Gruppenhomomorphismus mit Kern H. Also

$$[G : H] \leqslant |\mathrm{Gal}(E/K)| = [E : K] = [G : H].$$

Somit ist die Abbildung surjektiv. □

Folgerung 3.5.16. *Sei $K \subset L$ endliche Galoiserweiterung, sei $E \in \mathscr{K}$. Die Abbildung*

$$\mathrm{Gal}(L/K) \to \mathrm{Alg}_K(E, L), \sigma \mapsto \sigma\big|_E$$

ist surjektiv.

Beweis. Für $\sigma, \tau \in \mathrm{Gal}(L/K)$ ist $\sigma\big|_E = \tau\big|_E$ genau dann, wenn $\tau^{-1}\sigma\big|_E = \mathrm{id}_E$. Dies gilt genau dann, wenn $\tau^{-1}\sigma \in \mathrm{Gal}(L/E) = H$, das heißt $\sigma H = \tau H$. Es folgt

$$[G : H] = |G\big|_E| \leqslant |\mathrm{Alg}_K(E, L)| = [E : K] = [G : H],$$

also ist die Abbildung surjektiv. (Anders mit dem Fortsetzungssatz 3.2.3.) □

Folgerung 3.5.17. *Sei $K \subset L$ endliche Galoiserweiterung Für $E, E' \in \mathscr{K}$ und $\sigma \in \mathrm{Gal}(L/K)$ sind äquivalent:*

(a) $E' = \sigma(E)$,

(b) $\mathrm{Gal}(L/E') = \sigma\,\mathrm{Gal}(L/E)\sigma^{-1}$.

Beweis. **[(a) ⇒ (b)]** Sei $E' = \sigma(E)$. Für $\tau \in \mathrm{Gal}(L/K)$ ist $\tau \in \mathrm{Gal}(L/E')$ genau dann, wenn für alle $x \in E$ gilt $\tau\sigma(x) = \sigma(x)$. Dies ist genau dann richtig, wenn für alle $x \in E$ $\sigma^{-1}\tau\sigma(x) = x$, dh. genau dann, wenn $\sigma^{-1}\tau\sigma \in \mathrm{Gal}(L/E)$, in anderen Worten, wenn $\tau \in \sigma\,\mathrm{Gal}(L/E)\sigma^{-1}$.
[(b) ⇒ (a)] Wie oben gilt $\mathrm{Gal}(L/\sigma(E)) = \sigma\,\mathrm{Gal}(L/E)\sigma^{-1}$. Nach Voraussetzung (b) gilt $\mathrm{Gal}(L/\sigma(E)) = \mathrm{Gal}(L/E')$. Hieraus folgt $E' = \sigma(E)$. □

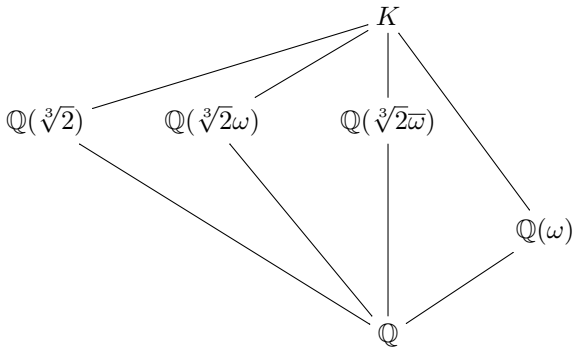
Beispiel 3.5.18 (Endliche Körper)**.** Sei $K \cong \mathbb{F}_{p^n}$ und $K \subset L$ endliche Erweiterung vom Grad m. Die Körper zwischen K und L sind genau die $\mathbb{F}_{p^{nd}}$ mit $d \in \mathbb{N}$, $d\big|m$.

Beweis. Die Erweiterung L/K ist Galois'sch mit Galoisgruppe $\mathrm{Gal}(L/K) = \langle\sigma^n\rangle$, wobei σ der Frobeniushomomorphismus von L ist. Die Körper zwischen K und L sind genau die Fixkörper $\mathrm{Fix}_L(\langle\sigma^{nd}\rangle)$ mit $d \in \mathbb{N}$, $d\big|m$. Ist $m = dd'$, $E = \mathrm{Fix}_L(\langle\sigma^{nd}\rangle)$, dann gilt

$$[E : K] = [\langle\sigma^n\rangle : \langle\sigma^{nd}\rangle] = \frac{m}{d'} = d.$$

Es folgt $E \cong \mathbb{F}_{p^{nd}}$. □

Beispiel 3.5.19. Sei $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$ der Zerfällungskörper von $X^3 - 2 \in \mathbb{Q}[X]$ mit $\omega = \frac{1}{2}(-1 + \sqrt{-3})$. Es gilt $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathfrak{S}_3$. Die Körper zwischen $\mathbb{Q}$ und K sind



Die Unterkörper vom Grad 3 sind die Fixkörper der drei Untergruppen der Ordnung 2 von $\mathrm{Gal}(K/\mathbb{Q})$, der Unterkörper vom Grad 2 ist der Fixkörper von A_3. Die Körper vom Grad 3 sind zueinander konjugiert. Nur K und $\mathbb{Q}(\omega)$ sind Galois'sch über $\mathbb{Q}$.

Satz 3.5.20. *Sei $K \subset L$ endliche Galoiserweiterung mit $G = \mathrm{Gal}(L/K)$. Wie im Hauptsatz seien $\mathscr{K}$ und $\mathscr{G}$ definiert.*

(a) Sei $E \in \mathscr{K}$ und $x \in E$ ein primitives Element über K. Ist $H = \mathrm{Gal}(L/E)$ und $\sigma_1, \ldots, \sigma_m$ eine Linkstransversale von H in G. Dann ist $\prod_{i=1}^m (X - \sigma_i(x))$ das Minimalpolynom von x über K. Ist insbesondere x ein primitives Element von L über K, dann ist $\prod_{\sigma \in G}(X - \sigma(x))$ das Minimalpolynom von x über K.

(b) Sei $L = K(x)$, $H \in \mathscr{G}$, $E = \mathrm{Fix}_L(H)$ und $g = \prod_{\sigma \in H}(X - \sigma(x)) = \sum_{i=0}^t \alpha_i X^i$. Dann gilt $E = K(\alpha_0, \ldots, \alpha_{t-1})$.

Beweis. **Zu (a):** Da E/K separabel ist, gibt es $x \in E$ mit $E = K(x)$. Sei $G = \bigcup_{i=1}^m \sigma_i H$, wobei $m = [G : H] = [E : K]$; sei $f = \prod_{i=1}^m (X - \sigma_i(x))$. Das Polynom f liegt in $K[X]$: Für $\sigma \in G$ ist $\sigma\sigma_1, \ldots, \sigma\sigma_m$ ebenfalls eine Linkstransversale von H in G. Also gibt es $\pi \in \mathfrak{S}_m$ mit $\sigma\sigma_i H = \sigma_{\pi(i)} H$, für $1 \leqslant i \leqslant m$. Es folgt $\sigma\sigma_i(x) = \sigma_{\pi(i)}(x)$, $1 \leqslant i \leqslant m$, also

$$^\sigma f = \prod_{i=1}^m (X - \sigma\sigma_i(x)) = \prod_{i=1}^m (X - \sigma_i(x)) = f.$$

Da dies für alle $\sigma \in G$ gilt, folgt $f \in K[X]$. Offenbar ist f das Minimalpolynom von x über K.

Zu (b): Die Erweiterung L/E ist Galois'sch mit $H = \mathrm{Gal}(L/E)$. Nach (a) ist $g = \prod_{\sigma \in H}(X - \sigma(x))$ das Minimalpolynom von x über E. Die Behauptung folgt nur aus dem nachfolgenden Lemma. □

Lemma 3.5.21. *Sei $K \subset L = K(x)$ eine endliche und einfache Erweiterung, sei $K \subset E \subset L$ ein Zwischenkörper und $g = \sum_{i=0}^t \alpha_i X^i$ das Minimalpolynom von x über E. Dann gilt $E = K(\alpha_0, \ldots, \alpha_{t-1})$.*

Beweis. Sei $E' = K(\alpha_0, \ldots, \alpha_{t-1})$. Dann gilt $E' \subset E$ und $g \in E'[X]$. Das Polynom g ist normiert und irreduzibel auch über E', also ist g das Minimalpolynom von x auch über E'. Da $L = E(x) = E'(x)$ ist, gilt

$$[L : E] = \deg(g) = [L : E'] = [L : E][E : E'].$$

Es folgt $[E : E'] = 1$ und $E = E'$. □

Beispiel* 3.5.22. Man zeige, daß das Polynom $f = X^4 - X^2 - 1 \in \mathbb{Q}[X]$ irreduzibel ist und bestimme einen Zerfällungskörper L, sowie alle Zwischenkörper $\mathbb{Q} \subset E \subset L$.

Beispiel* 3.5.23. Sei L/K eine endliche Galoiserweiterung. Man zeige, daß für $\alpha \in L$ folgende Aussagen äquivalent sind:

(a) Es gilt $L = K(\alpha)$.

(b) Für alle $g \in \mathrm{Gal}(L/K)$ mit $g \neq \mathrm{id}$ gilt $g(\alpha) \neq \alpha$.

3.5.5 Kompositа als Galoiserweiterungen

Sei $K \subset L$ Körpererweiterung, seien E, F Zwischenkörper zwischen K und L. Man setzt

$$EF = E(F) = F(E) = K(E \cup F)$$

und nennt EF das Kompositum von E und F.

Satz 3.5.24. *Sei $K \subset L$ Körpererweiterung, seien E, E', F Körper zwischen K und L mit $E \subset E'$. Wenn E'/E eine endliche Galoiserweiterung ist, dann ist auch $E'F/EF$ eine endliche Galoiserweiterung und die Abbildung*

$$\varphi : \mathrm{Gal}(E'F/EF) \to \mathrm{Gal}(E'/E), \sigma \mapsto \sigma\big|_{E'}$$

ist ein injektiver Gruppenhomorphismus.

Beweis. Ist E' Zerfällungskörper eines separabeln Polynoms f über E, dann ist $E'F$ Zerfällungskörper von f über EF, also ist$E'F/EF$ endlich und Galois'sch. Die Abbildung $\varphi : \mathrm{Gal}(E'F/EF) \to \mathrm{Gal}(E'/E), \sigma \mapsto \sigma\big|_{E'}$ ist wohldefiniert, da E'/E normal ist, und offenbar ist φ Homomorphismus. Ist $\varphi(\sigma) = \mathrm{id}_{E'}$, so gilt $\sigma\big|_{E'} = \mathrm{id}_{E'}$, außerdem $\sigma\big|_F = \mathrm{id}_F$. Es folgt $\sigma = \mathrm{id}_{EF}$. Damit ist φ injektiv. □

Satz 3.5.25. *Sei $K \subset L$ Körpererweiterung, seien E, F Körper zwischen K und L, so daß E/K und F/K endliche Galoiserweiterungen sind.*

(a) Die Erweiterung EF/K ist endliche Galoiserweiterung und die Abbildung

$$\varphi : \mathrm{Gal}(EF/E) \to \mathrm{Gal}(F/E \cap F), \sigma \mapsto \sigma\big|_F,$$

ist ein Gruppenisomorphismus.

(b) Die Abbildung

$$\psi : \mathrm{Gal}(EF/K) \to \mathrm{Gal}(E/K) \times \mathrm{Gal}(F/K), \sigma \mapsto (\sigma\big|_E, \sigma\big|_F),$$

ist injektiver Homomorphismus. Wenn $E \cap F = K$ ist, dann ist ψ auch surjektiv.

Beweis. **Zu (a):** Ist E beziehungsweise F Zerfällungskörper des separabeln Polynoms $f \in K[X]$, beziehungsweise $g \in K[X]$, dann ist EF Zerfällungskörper des separabeln Polynoms fg. Also ist EF/K endliche Galoiserweiterung. Offenbar ist EF/F und $F/E \cap F$ endliche Galoiserweiterung. Die Abbildung $\varphi : \mathrm{Gal}(EF/E) \to \mathrm{Gal}(F/E \cap F), \sigma \mapsto \sigma\big|_F$ ist wohldefiniert, da $\sigma(F) = F$ und $\sigma\big|_{E\cap F} = \mathrm{id}_{E\cap F}$. Offenbar ist φ Homomorphismus. Ist $\varphi(\sigma) = \mathrm{id}_F$, so gilt $\sigma\big|_F = \mathrm{id}_F$. Nach Voraussetzung gilt $\sigma\big|_E = \mathrm{id}_E$, also ist $\sigma = \mathrm{id}_{EF}$. Somit ist φ injektiv. Um zu zeigen, daß φ surjektiv ist, sei $H = \mathrm{im}(\varphi)$. Es gilt $\mathrm{Fix}_F(H) = E \cap F$, denn für $x \in F$ ist $x \in \mathrm{Fix}_F(H)$ genau dann, wenn für alle $\sigma \in \mathrm{Gal}(E/F)$ gilt $\sigma(x) = x$. Dies ist genau dann, wenn $x \in E \cap F$. Da $F/E \cap F$ Galois'sch ist, folgt $\mathrm{Gal}(F/E \cap F) = \mathrm{Gal}(F/\mathrm{Fix}_F(H)) = H$. Damit ist φ auch surjektiv.
Zu (b): Offenbar ist ψ ein Homomorphismus und injektiv. Sei nun $E \cap F = K$, und seien $\sigma \in \mathrm{Gal}(E/K)$, $\tau \in \mathrm{Gal}(F/K)$. Nach (a) gibt es $\widetilde{\sigma} \in \mathrm{Gal}(EF/F)$ mit $\widetilde{\sigma}\big|_E = \sigma$. Ebenso $\widetilde{\tau} \in \mathrm{Gal}(EF/E)$ mit $\widetilde{\tau}\big|_F = \tau$. Dann gilt $\widetilde{\sigma}, \widetilde{\tau} \in \mathrm{Gal}(EF/K)$ und damit $\widetilde{\sigma}\widetilde{\tau} \in \mathrm{Gal}(EF/K)$. Es gilt $\widetilde{\sigma}\widetilde{\tau}\big|_E = \widetilde{\sigma}\big|_E$ und $\widetilde{\sigma}\widetilde{\tau}\big|_F = \widetilde{\tau}\big|_F = \tau$. Also gilt $\psi(\widetilde{\sigma}\widetilde{\tau}) = (\sigma, \tau)$. Folglich ist ψ surjektiv. □

Beispiel* 3.5.26. Sei $K = \mathbb{Q}$ und $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Man bestimme ein primitives Element der Erweiterung L/K, dh. $\alpha \in L$ mit $L = K(\alpha)$. Anschließend berechne man die Minimalpolynome von α über allen Zwischenkörpern $K \subset M \subset L$.

3.6 Zerfällungskörper von $X^n - a$

3.6.1 Einheitswurzeln

Definition 3.6.1. Sei K ein Körper, $n \in \mathbb{N}$. Das Element $\xi \in K$ heißt n-te Einheitswurzel, wenn $\xi^n = 1$. Die Menge aller n-ten Einheitswurzeln in K bezeichnet man mit $\mu_n(K)$.

Proposition 3.6.2. *Sei K ein Körper, $n \in \mathbb{N}$.*

(a) Die Menge $\mu_n(K)$ ist eine zyklische Untergruppe von K^*, deren Ordnung n teilt.

(b) Sei L Zerfällungskörper von $X^n - 1 \in K[X]$.

(i) Ist $\mu_n(L) = \langle\zeta\rangle$, dann ist $L = K(\zeta)$.

(ii) Teilt die Charakteristik von K nicht n, so hat $\mu_n(L)$ Ordnung n. Ist $\mathrm{char}(K) = p$ eine Primzahl mit $p \mid n$, und ist $n = p^k m$ mit $k \in \mathbb{N}$ und $p \nmid m$, dann gilt $\mu_n(L) = \mu_m(L)$. Insbesondere hat $\mu_n(L)$ Ordnung m. Insbesondere hat $\mu_n(L)$ genau dann Ordnung n, wenn $\mathrm{char}(L) \nmid n$.

Beweis. **Zu (a):** Es ist klar, daß $\mu_n(K)$ Untergruppe von K^* ist, und höchstens n Elemente hat. Also ist $\mu_n(K)$ zyklisch, etwa $\mu_n(K) = \langle\zeta\rangle$. Da $\zeta^n = 1$ ist, gilt also $\mathrm{ord}(\zeta) \mid n$.
Zu (b i): Das ist klar.
Zu (b ii): Es gelte $\mathrm{char}(K) \nmid n$. Dann ist die Ableitung von $(X^n - 1)$ gleich $(X^n - 1)' = nX^{n-1}$, also ungleich null und $X^n - 1$ und nX^{n-1} sind teilerfremd. Also hat $X^n - 1$ in L n verschiedene Nullstellen. Also hat $\mu_n(L)$ Ordnung n. Sei $\mathrm{char}(K) = p$ prim und k bzw. m wie angegeben. Dann gilt für $\zeta \in L$: $\zeta^n = 1$ genau dann, wenn $(\zeta^m - 1)^{p^k} = 0$ genau dann, wenn $\zeta^m = 1$. Also gilt $\mu_n(L) = \mu_m(L)$ und $\mu_m(L)$ hat Ordnung m. □

Definition 3.6.3. Eine n-te Einheitswurzel $\zeta \in K$ heißt primitiv, wenn $\mathrm{ord}(\zeta) = n$ ist, das heißt, wenn $\mu_n(K) = \langle\zeta\rangle$ und $\mu_n(K)$ Ordnung n hat. Dann gibt es $\varphi(n)$ primitive n^{te} Einheitswurzeln.

Beispiele 3.6.4. (a) Die n^{ten} Einheitswurzeln in $\mathbb{C}$ sind $e^{\frac{2\pi ik}{n}}$, $1 \leqslant k \leqslant n$. Die primitiven sind dabei diejenigen, für die n und k teilerfremd sind.

(b) Sei p Primzahl, $n \in \mathbb{N}$. Alle Elemente in $\mathbb{F}_{p^n}^*$ sind $(p^n - 1)^{\text{te}}$ Einheitswurzeln.

Beispiel* 3.6.5. Sei ζ_3 primitive dritte Einheitswurzel, ζ_4 primitive vierte Einheitswurzel. Sei $K = \mathbb{Q}(\sqrt{3})$. Man betrachte die Erweiterungen $K(\zeta_4)/K$ und $K(\zeta_3)/K$ und zeige, daß der Schnitt $K(\zeta_3) \cap K(\zeta_4)$ den Grundkörper K echt enthält.
Hinweis: $\zeta_3 = \frac{-1+\sqrt{-3}}{2}$.

3.6.2 Zerfällungskörper von $X^n - a$

Satz 3.6.6. *Seien K ein Körper, $0 \neq a \in K$, $n \in \mathbb{N}$ mit $\mathrm{char}(K) \nmid n$ und L ein Zerfällungskörper von $X^n - a \in K[X]$. Dann gilt:*

(a) Die Erweiterung L/K ist endlich und Galois'sch.

(b) Die Gruppe $\mathrm{Gal}(L/K)$ ist isomorph zu einer Untergruppe des semidirekten Produktes $\mathbb{Z}/n\mathbb{Z} \times_j (\mathbb{Z}/n\mathbb{Z})^*$, wobei $j : (\mathbb{Z}/n\mathbb{Z})^* \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ der bekannte Isomorphismus $j(\overline{x})(\overline{y}) = \overline{xy}$ für $x \in (\mathbb{Z}/n\mathbb{Z})^*$, $y \in \mathbb{Z}/n\mathbb{Z}$ ist.

Beweis. **Zu (a):** Das Polynom $X^n - a$ und seine formelle Ableitung $(X^n - a)' = nX^{n-1} \neq 0$ sind teilerfremd, also hat $X^n - a$ lauter verschiedene Nullstellen in L, also ist es separabel.
Zu (b): Sei $b \in L$ mit $b^n = a$. Wir zeigen, daß L eine primitive n-te Einheitswurzel ε enthält. Seien $x_1, \ldots, x_n$ die Nullstellen von $X^n - a$ in L. Dann ist $\left(\frac{x_i}{b}\right)^n = 1$ für $1 \leqslant i \leqslant n$. Also sind die $\frac{x_i}{b}$, $1 \leqslant i \leqslant n$ lauter verschiedene Einheitswurzeln. Dann gibt es in L eine primitive n^{te} Einheitswurzel ε. Die $b, \varepsilon b, \ldots, \varepsilon^{n-1} b$ sind alle Nullstellen von $X^n - a$ und es gilt $L = K(b\varepsilon)$.
Sei $\sigma \in \mathrm{Gal}(L/K)$. Dann gilt

$$\sigma(b)^n = \sigma(b^n) = \sigma(a) = a.$$

Also existiert $k \in \mathbb{Z}$ mit $\sigma(b) = \varepsilon^k b$. Außerdem gilt

$$\sigma(\varepsilon)^n = \sigma(\varepsilon^n) = \sigma(1) = 1.$$

Da $\sigma(\varepsilon)$ ebenfalls primitive n^{te} Einheitswurzel ist, existiert $l \in \mathbb{Z}$, l, n teilerfremd mit $\sigma(\varepsilon) = \varepsilon^l$. Wir definieren:

$$\rho : \mathrm{Gal}(L/K) \to \mathbb{Z}/n\mathbb{Z} \times_j (\mathbb{Z}/n\mathbb{Z})^*, \rho(\sigma) = (\overline{k}, \overline{l}).$$

Beachte, daß k und l modulo n eindeutig bestimmt sind, also ρ wohldefiniert ist. Die Abbildung ρ ist darüberhinaus ein Gruppenhomomorphismus: Sei $\tau \in \mathrm{Gal}(L/K)$, $\tau(b) = \varepsilon^s b$ und $\tau(\varepsilon) = \epsilon^t$ mit $s, t \in \mathbb{Z}$, so daß t, n teilerfremd sind. Dann

$$\begin{aligned} \sigma\tau(b) &= \sigma(\varepsilon)^s \sigma(b) = \varepsilon^{ls}\varepsilon^k b = \varepsilon^{ls+k} b \\ \sigma\tau(\varepsilon) &= \sigma(\varepsilon)^t = \varepsilon^{lt} \end{aligned}$$

Also

$$\rho(\sigma\tau) = (\overline{ls+k}, \overline{lt}) = (\overline{k} + j(\overline{l})(\overline{s}), \overline{lt}) = (\overline{k}, \overline{l})(\overline{s}, \overline{t}) = \rho(\sigma)\rho(\tau).$$

Die Abbildung ρ ist injektiv, denn aus $\rho(\sigma) = (\overline{k}, \overline{l}) = (\overline{0}, \overline{1})$ folgt $\overline{k} = \overline{0}$ und $\overline{l} = \overline{1}$, also $\sigma(b) = b$ und $\sigma(\varepsilon) = \varepsilon$, dh. $\sigma = \mathrm{id}_L$. □

Sei proj_1 beziehungsweise proj_2 die Projektion von $\mathbb{Z}/n\mathbb{Z} \times_j (\mathbb{Z}/n\mathbb{Z})^*$ auf den ersten beziehungsweise zweiten Faktor.

Folgerung 3.6.7. *Sei K Körper, $n \in \mathbb{N}$ mit $\mathrm{char}(K) \nmid n$ und $K^{(n)}$ ein Zerfällungskörper von $X^n - 1 \in K[X]$.*

(a) Die Erweiterung $K^{(n)}/K$ ist Galois'sch.

(b) Die Gruppe $\mathrm{Gal}(K^{(n)}/K)$ ist isomorph zu einer Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^*$. Sie ist also abelsch und ihre Ordnung teilt $\varphi(n)$.

Beweis. Im Satz sei $a = 1$. Für $\sigma \in \mathrm{Gal}(K^{(n)}/K)$ gilt $1 = \sigma(b) = \varepsilon^k \cdot 1$, also $\overline{k} = \overline{0}$. Dann ist der Homomorphismus

$$\mathsf{proj}_2 \circ \rho : \mathrm{Gal}(K^{(n)}/K) \to (\mathbb{Z}/n\mathbb{Z})^*$$

injektiv, denn aus $(\mathsf{proj}_2 \circ \rho)(\sigma) = \overline{l} = \overline{1}$ folgt $\overline{l} = \overline{1}$, und damit $\rho(\sigma) = (\overline{0}, \overline{1})$ also $\sigma = \mathrm{id}_{K^{(n)}}$. □

Folgerung 3.6.8. *Sei K ein Körper, $0 \neq a \in K$, $n \in \mathbb{N}$ mit $\mathrm{char}(K) \nmid n$ und L Zerfällungskörper von $X^n - a$. Wenn K eine primitive n^{te} Einheitswurzel ε enthält, dann gilt:*

(a) Die Erweiterung L/K ist Galois'sch.

(b) Die Gruppe $\mathrm{Gal}(L/K)$ ist isomorph zu einer Untergruppe von $\mathbb{Z}/n\mathbb{Z}$. Also ist $\mathrm{Gal}(L/K)$ zyklisch und ihre Ordnung teilt n.

Beweis. Für $\sigma \in \mathrm{Gal}(L/K)$ folgt aus $\varepsilon = \sigma(\varepsilon) = \varepsilon^l$, daß $\overline{l} = \overline{1}$. Der Homomorphismus $\mathsf{proj}_1 \circ \rho : \mathrm{Gal}(L/K) \to \mathbb{Z}/n\mathbb{Z}$ ist injektiv, denn ist $(\mathsf{proj}_1 \circ \rho)(\sigma) = \overline{l} = \overline{0}$, dann $\overline{l} = \overline{0}$, also $\sigma(b) = b$, also $\sigma = \mathrm{id}_L$. □

Wir werden später eine wichtige Umkehrung der Folgerung beweisen.

Beispiel* 3.6.9. Es sei ζ_5 eine primitive fünfte Einheitswurzel des Körpers $\mathbb{Q}$.

(a) Man zeige, daß $\zeta_5 + \zeta_5^{-1} \in \mathbb{Q}(\zeta_5)$ eine Nullstelle des Polynoms $X^2 + X - 1$ ist.

(b) Man zeige $\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \cong \mathbb{Z}/(4)$ und folgere daraus, daß es genau einen Zwischenkörper $\mathbb{Q} \subsetneq K \subsetneq \mathbb{Q}(\zeta_5)$ gibt.

(c) Man bestimme $\alpha \in \mathbb{Z}$ so, daß $K = \mathbb{Q}(\sqrt{\alpha})$ gilt. Hinweis: Man zeige dazu, daß $\zeta_5 + \zeta_5^{-1} \in K$.

3.6.3 Kreisteilungspolynome

Proposition 3.6.10. *Sei K ein Körper, $n \in \mathbb{N}$ mit $\mathrm{char}(K) \nmid n$ und $K^{(n)}$ ein Zerfällungskörper von $X^n - 1 \in K[X]$. Ferner sei P_n die Menge aller primitiven n^{ten} Einheitswurzeln in $K^{(n)}$ und $\phi_{K,n} = \phi_n = \prod_{\zeta \in P_n}(X - \zeta)$.*

(a) Das Polynom ϕ_n ist in $K[X]$ enthalten, und $\deg(\phi_n) = \varphi(n)$.

(b) Das Polynom $X^n - 1$ zerfällt über K als $X^n - 1 = \prod_{\mathbb{N} \ni d \mid n} \phi_d$.

Beweis. **Zu (a):** Es gilt $|P_n| = \varphi(n)$, also $\deg \phi_n = \varphi(n)$. Für alle $\sigma \in \mathrm{Gal}(K^{(n)}/K)$ gilt

$$^{\sigma}\phi_n = \prod_{\zeta \in P_n} (X - \sigma(\zeta)) = \prod_{\zeta \in P_n} (X - \zeta) = \phi_n,$$

denn $\sigma(P_n) = P_n$. Also liegen die Koeffizienten von ϕ_n in $\mathrm{Fix}_{K^{(n)}}(\mathrm{Gal}(K^{(n)}/K)) = K$.
Zu (b): Es gilt $\mu_n(K^{(n)}) = \bigcup_{d|n} \mu_d(K^{(n)})$, also

$$X^n - 1 = \prod_{\zeta \in \mu_n(K^{(n)})} (X - \zeta) = \prod_{d|n} \prod_{\zeta \in P_d} (X - \zeta) = \prod_{\mathbb{N} \ni d|n} \phi_d.$$

□

Definition 3.6.11. Voraussetzungen und Bezeichnungen wie in der Proposition.

(a) Der Körper $K^{(n)}$ heißt Körper der n^{ten} Einheitswurzeln oder n^{ter} Kreisteilungskörper über K.

(b) Das Polynom ϕ_n heißt n^{tes} Kreisteilungspolynom.

Für $m \neq n \in \mathbb{N}$ mit $\mathrm{char}(K) \nmid n, m$ sind ϕ_n und ϕ_m teilerfremd.

Beispiele 3.6.12. Sei $\mathrm{char}(K) = 0$. Es ist $\phi_1 = X - 1$. Ist p Primzahl, so ist $X^p - 1 = \phi_1\phi_p$. Also ist

$$\phi_p = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + X + 1.$$

Ist außerdem $k \in \mathbb{N}$, dann $X^{p^k} - 1 = \phi_1\phi_p \cdots \phi_{p^{k-1}}\phi_{p^k} = (X^{p^{k-1}} - 1)\phi_{p^k}$. Also

$$\phi_{p^k} = \frac{X^{p^k} - 1}{X^{p^{k-1}} - 1} = X^{p^{k-1}(p-1)} + \cdots + X^{p^k - 1} + 1 = \phi_p(X^{p^{k-1}}).$$

Die ersten zehn Kreisteilungspolynome sind:

$$\begin{aligned}
\phi_1 &= X - 1 \\
\phi_2 &= X + 1 \\
\phi_3 &= X^2 + X + 1 \\
\phi_4 &= X^2 + 1 \\
\phi_5 &= X^4 + X^3 + X^2 + X + 1 \\
\phi_6 &= X^2 - X + 1 \\
\phi_7 &= X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 \\
\phi_8 &= X^4 + 1 \\
\phi_9 &= X^6 + X^3 + 1 \\
\phi_{10} &= X^4 + X^3 + X^2 - X + 1
\end{aligned}$$

Satz 3.6.13 (Gauß)**.** *Sei $n \in \mathbb{N}$.*

(a) Das n^{te} Kreisteilungspolynom ϕ_n über $\mathbb{Q}$ liegt in $\mathbb{Z}[X]$ und ist irreduzibel in $\mathbb{Z}[X]$ und $\mathbb{Q}[X]$.

(b) Der Körper $\mathbb{Q}^{(n)}$ der n^{ten} Einheitswurzeln ist Galoiserweiterung von $\mathbb{Q}$ vom Grad $\varphi(n)$. Ist $\varepsilon \in \mathbb{Q}^{(n)}$ eine primitive n^{te} Einheitswurzel, dann gilt $\mathbb{Q}^{(n)} = \mathbb{Q}(\varepsilon)$ und das Minimalpolynom von ε über $\mathbb{Q}$ ist ϕ_n.

(c) Die Abbildung $\rho : \mathrm{Gal}(\mathbb{Q}^{(n)} / \mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^*$ mit $\rho(\sigma) = \bar{l}$, wenn $\sigma(\varepsilon) = \varepsilon^l$, ist Gruppenisomorphismus.

Beweis. **Zu (a):** Wir zeigen, daß $\phi_n \in \mathbb{Z}[X]$ ist. Wir wissen, daß $\phi_n \in \mathbb{Q}[X]$. Da $X^n - 1 = \prod_{d|n} \phi_d$ und die ϕ_d normiert sind, gilt $\phi_d \in \mathbb{Z}[X]$ für alle $d \big| n$ nach Folgerung 2.6.32(a).

Nun zeigen wir, daß ϕ_n irreduzibel ist. Sei $\zeta \in P_n$ und $f \in \mathbb{Q}[X]$ das Minimalpolynom von ζ. Dann gilt $f \big| \phi_n$. Dann gibt es $g \in \mathbb{Q}[X]$ mit $X^n - 1 = f \cdot g$, wobei auch g normiert ist, und $f, g \in \mathbb{Z}[X]$. Wir zeigen, daß für jede Zahl $m \in \mathbb{N}$, so daß m und n teilerfremd sind, gilt $f(\zeta^m) = 0$. Dann haben f und ϕ_n die gleichen Nullstellen, also gilt $f = \phi_n$. Zuerst zeigen wir: Ist $\xi \in P_n$ mit $f(\xi) = 0$, dann gilt auch $f(\xi^p) = 0$ für jede Primzahl p mit $p \nmid n$. Wir schließen indirekt und nehmen an, es gebe p prim mit $p \nmid n$, $\xi \in P_n$ mit $f(\xi) = 0$ und $f(\xi^p) \neq 0$. Dann gilt $0 = (\xi^p)^n - 1 = f(\xi^p)g(\xi^p)$ also $g(\xi^p) = 0$, dh. ξ ist Nullstelle von $g(X^p)$. Da f Minimalpolynom von ξ ist, gibt es $h \in \mathbb{Q}[X]$ mit $g(X^p) = f \cdot h$. Weiter ist h normiert und $h \in \mathbb{Z}[X]$. Wir betrachten den kanonischen Homomorphismus $\mathbb{Z}[X] \to \mathbb{F}_p[X], q \mapsto \overline{q}$. Sei $g = \sum_{i=0}^t z_i X^i \in \mathbb{Z}[X]$, $\overline{g}^p = \sum_{i=0}^t \overline{z}_i^p X^{pi} = \overline{g}(X^p) = \overline{fh}$. Da f und h normiert sind, und $\overline{f}$ nicht konstant ist, ist auch $\overline{g}$ nicht konstant. Also haben $\overline{f}$ und $\overline{g}$ einen gemeinsamen nichtkonstanten Faktor. Damit hat $X^n - \overline{1} = \overline{f}\overline{g}$ in einem Zerfällungskörper eine mehrfache Nullstelle. Da $X^n - \overline{1}$ und die formale Ableitung $(X^n - \overline{1})' = nX^{n-1} \neq 0$ teilerfremd sind, hat man einen Widerspruch.
Um den Beweis abzuschließen, sei $\zeta \in P_n$ mit $f(\zeta) = 0$ und $m \in \mathbb{N} \setminus \{1\}$, so daß m und n teilerfremd sind. Sei $m = p_1 \cdots p_r$ mit p_i prim. Dann folgt $f(\zeta^{p_1}) = 0$, also $f(\zeta^{p_1 p_2}) = 0$, etc. also $f(\zeta^m) = 0$.
Zu (b): Wir wissen, daß $\mathbb{Q}^{(m)} / \mathbb{Q}$ Galois'sch ist mit $\mathbb{Q}^{(m)} = \mathbb{Q}(\varepsilon)$. Es ist $\phi_n(\varepsilon) = 0$, außerdem ist ϕ_n normiert und irreduzibel. Also ist es das Minimalpolynom von ε. Es folgt $[\mathbb{Q}^{(n)} : \mathbb{Q}] = \deg(\phi_n) = \varphi(n)$.
Zu (c): Wir wissen auch, daß $\rho : \mathrm{Gal}(\mathbb{Q}^{(n)} / \mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^*$ injektiv ist. Nach (b) gilt $|\mathrm{Gal}(\mathbb{Q}^{(n)} / \mathbb{Q})| = [\mathbb{Q}^{(n)} : \mathbb{Q}] = \varphi(n) = |\mathbb{Z}/n\mathbb{Z}^*|$. Also ist ρ Isomorphismus. □

3.6.4 Verhalten der Kreisteilungspolynome über endlichen Körpern

Lemma 3.6.14. *Sei K ein Körper, $n \in \mathbb{N}$ mit $\mathrm{char}(K) \nmid n$ und $\gamma : \mathbb{Z} \to K$, $z \mapsto z \cdot 1$ der kanonische Homomorphismus. Dann ist ϕ_n das n^{te} Kreisteilungspolynom über K, dh. ${}^\gamma\phi_n = \phi_{K,n}$.*

Beweis. Durch Induktion nach n. Ist $n = 1$, so ist $\phi_1 = X - 1$, also ${}^\gamma\phi_1 = X - 1_K = \phi_{K,1}$. Sei $n > 1$. In $\mathbb{Z}[X]$ gilt $X^n - 1 = \prod_{d|n} \phi_d$; in $K[X]$ gilt

$$\prod_{d|n} \phi_{K,d} = X^n - 1_K = {}^\gamma(X^n - 1) = \prod_{d|n} {}^\gamma\phi_n = \Big(\prod_{n>d|n} \phi_{K,d}\Big) {}^\gamma\phi_n.$$

Nach Kürzen folgt ${}^\gamma\phi_n = \phi_{K,n}$. □

Sei p eine Primzahl, $k \in \mathbb{N}$, $q = p^k$, $K = \mathbb{F}_q$ der Körper mit q Elementen. Ferner sei $n \in \mathbb{N}$ mit $p \nmid n$, $K^{(n)}$ der Zerfällungskörper von $X^n - 1 \in K[X]$ und $\varepsilon \in K^{(n)}$ eine primitive n^{te} Einheitswurzel. Dann ist $K^{(n)} = K(\varepsilon)$. Wir wissen, daß $\rho : \mathrm{Gal}(K^{(n)}/K) \to \mathbb{Z}/n\mathbb{Z}^*$ mit $\rho(\tau) = \bar{l}$, wenn $\tau(\varepsilon) = \varepsilon^l$, ein injektiver Homomorphismus ist. Der Körper $K^{(n)}$ ist ebenfalls endlich, es gilt $\mathrm{Gal}(K^{(n)}/K) = \langle \sigma^k \rangle$, wobei σ der Frobeniushomomorphismus ist.

Satz 3.6.15. *Wir behalten die Bezeichnungen von oben bei.*

(a) Es gilt $\rho(\sigma^k) = \overline{q}$, und $\mathrm{im}(\rho) = \langle \overline{q} \rangle$. Damit folgt $[K^{(n)} : K] = \mathrm{ord}(\overline{q}) = \mathrm{ord}_n(q)$.

(b) Das Bild $\overline{\phi}_n \in \mathbb{F}_p[X]$ des n^{ten} Kreisteilungspolynoms $\phi_n \in \mathbb{Z}[X]$ ist genau dann irreduzibel über K, wenn $\mathbb{Z}/n\mathbb{Z}^* = \langle \overline{q} \rangle$, dh. wenn $\mathrm{ord}_n(q) = \varphi(n)$.

Beweis. **Zu (a):** Es gilt $\sigma^k(\varepsilon) = \varepsilon^{p^k} = \varepsilon^q$. Also $\rho(\sigma^l) = \overline{q}$. Da σ^k die Gruppe $\mathrm{Gal}(K^{(n)}/K)$ erzeugt, ist $\mathrm{im}(\rho)) = \langle \overline{q} \rangle$.
Zu (b): Nach dem Lemma ist $\overline{\phi}_n$ das n^{te} Kreisteilungspolynom über $K = \mathbb{F}_p$. Es folgt $\overline{\phi}_n(\varepsilon) = 0$. Damit gilt: $\overline{\phi}_n$ ist irreduzibel über K genau dann, wenn $\overline{\phi}_n$ Minimalpolynom von ε ist genau dann, wenn $[K^{(n)} : K] = \deg(\overline{\phi}_n) = \varphi(n)$, genau dann, wenn $\mathrm{ord}_n(q) = \varphi(n)$. Es folgt, daß $\overline{\phi}_n$ höchstens dann irreduzibel über K ist, wenn $(\mathbb{Z}/n\mathbb{Z})^*$ zyklisch ist. Ein Satz von Gauß charakterisiert diese n. □

Beispiele 3.6.16. (a) Sei $p = 2$, $n \in \mathbb{N}$ ungerade. Das Polynom ϕ_n ist genau dann irreduzibel über $\mathbb{F}_2$, wenn $\mathrm{ord}_n(2) = \varphi(n)$. Dies ist z. B. der Fall für ϕ_1, ϕ_3, ϕ_5, ϕ_9, ϕ_{11}, $\phi_{13}, \ldots$ Andererseits ist $\phi_7 = (X^3 + X + 1)(X^3 + X^2 + 1)$ reduzibel über $\mathbb{F}_2$.

(b) Das Polynom $\phi_8 = X^4 + 1$ ist irreduzibel über $\mathbb{Z}$ und $\mathbb{Q}$, aber reduzibel über $\mathbb{F}_p$, für eine Primzahl p, denn $\mathbb{Z}/8\mathbb{Z}^* = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$ ist nicht zyklisch.

Beispiel* 3.6.17. Man berechne für $K = \mathbb{Q}, \mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_{13}, \mathbb{F}_{29}$ den Grad der Körpererweiterung $[K^{(n)} : K]$.

3.7 Weitere Resultate über Galoiserweiterungen

3.7.1 Die Galoisgruppe von Polynomen vom Grad 3 und 4

Sei K ein Körper, $f = f_1 \cdots f_r \in K[X]$ mit paarweise nicht assoziierten, irreduziblen $f_1, \ldots, f_r$. Sei L ein Zerfällungskörper von f über K, $M = \{x \in L \mid f(x) = 0\}$, $M_i = \{x \in L \mid f_i(x) = 0\}$ für $i = 1, \ldots, r$. Es gilt $M = \bigcup_{i=1}^r M_i$. Man nennt $G(f) = \mathrm{Gal}(L/K)$ die Galoisgruppe von f. Man hat die Operation

$$G(f) \times M \to M, (\sigma, x) \mapsto \sigma(x).$$

Proposition 3.7.1. *Unter diesen Voraussetzungen gilt:*

(a) Die Bahnen dieser Operationen sind $M_1, \ldots, M_r$.

(b) Die Abbildung $G(f) \to \mathfrak{S}_M, \sigma \mapsto (x \mapsto \sigma(x))$ ist injektiver Gruppenhomomorphismus.

Beweis. **Zu (a):** In Folgerung 3.2.22 wurde gezeigt, daß $G(f)$ auf M_i transitiv operiert.
Zu (b): Ist $\sigma(x) = \tau(x)$ für alle $x \in M$, dann gilt $\sigma = \tau$. □

Insbesondere ist f genau dann irreduzibel, wenn $G(f)$ auf M transitiv operiert. Sei nun f zusätzlich separabel, $M = \{x_1, \ldots, x_n\}$ mit $x_i \neq x_j$ falls $i \neq j$. Dann ist L/K Galois'sch, $|\mathrm{Gal}(L/K)| = |G(f)| = [L : K]$. Wegen $\mathfrak{S}_M \cong \mathfrak{S}_n$hat man die Einbettung $\varphi : G(f) \to \mathfrak{S}_n$ mit $\varphi(\sigma)(i) = j$ falls $\sigma(x_i) = x_j$.

Folgerung 3.7.2. *Mit diesen Voraussetzungen gilt:*

(a) Die Ordnung von $G(f)$ teilt $n!$.

(b) Ist f irreduzibel, dann teilt n die Ordnung von $G(f)$.

Beweis. Das ist klar. □

Sei $G = G(f)$, $G_+ = \varphi^{-1}(A_n)$. Dann ist $G_+ \triangleleft G$, $[G : G_+] \leqslant [S_n : A_n] = 2$. Man setzt

$$\begin{aligned} \delta = \delta(f) &= \prod_{i<j}(x_i - x_j) \in L\backslash\{0\} \\ D = D(f) &= \delta^2 = \prod_{i<j}(x_i - x_j)^2. \end{aligned}$$

Für $\sigma \in G$ gilt

$$\sigma(\delta) = \prod_{i<j}(\sigma(x_i) - \sigma(x_j)) = \prod_{i<j}(x_{\varphi(\sigma)(i)} - x_{\varphi(\sigma)(j)}) = (-1)^m\delta,$$

wobei m die Anzahl der Transversionen von $\varphi(\sigma)$ ist. Es folgt $\sigma(D) = D$ für alle $\sigma \in G$. Also ist $D \in \mathrm{Fix}(G) = K$. Man nennt D die Diskriminante von f.

Proposition 3.7.3. *Sei $\mathrm{char}(K) \neq 2$, $f = f_1 \cdots f_r \in K[X]$ separabel wie oben. Dann gilt:*

(a) Der Fixkörper von G_+ ist $\mathrm{Fix}(G_+) = K(\delta)$, die Erweiterung $K(\delta)/K$ ist Galois'sch mit Galoisgruppe $\mathrm{Gal}(K(\delta)/K) \cong G/G_+$ vom Grad $[K(\delta) : K] \leqslant 2$.

(b) Genau dann gilt $G = G_+$, wenn D Quadrat eines Elementes von K ist.

Beweis. **Zu (a):** Für $\sigma \in G_+$ ist $\varphi(\sigma) \in A_n$, also ist $\sigma(\delta) = \delta$. Es folgt $K(\delta) \subset \mathrm{Fix}(G_+)$. Wenn $G_+ = G$ ist, dann ist $\mathrm{Fix}(G_+) = K$, also $K(\delta) = K$. Ist $G_+ \neq G$, $\sigma \in G\backslash G_+$, dann ist $\varphi(\sigma)$ ungerade, also $\sigma(\delta) = -\delta \neq \delta$. Also gilt $K \subsetneq K(\delta)$. Da

$$[\mathrm{Fix}(G_+) : K] = [G : G_+] = 2$$

ist, folgt $K(\delta) = \mathrm{Fix}(G_+)$. Da G_+ Normalteiler von G ist, ist $K(\delta) = \mathrm{Fix}(G_+)$ Galoiserweiterung von K mit $\mathrm{Gal}(K(\delta)/K) \cong G/G_+$.
Zu (b): Es gilt $G = G_+$ genau dann, wenn $K(\delta) = K$. Dies gilt genau dann, wenn $\delta \in K$, das heißt, es gibt $\alpha \in K$ mit $D = \alpha^2$. □

Beispiele 3.7.4. (a) Ist $f = X^2 + bX + c \in K[X]$, $f = (X - x_1)(X - x_2) = X^2 - (x_1 + x_2)X + x_1x_2$, dann $D = (x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1x_2 = b^2 - 4ac$.

(b) Sei $f = X^3 + bX^2 + cX + d \in K[X]$. Wir werden sehen: $D = b^2c^2 + 18bcd - 4b^3d - 4c^3 - 27d^2$.

Satz 3.7.5. *Sei* $\mathrm{char}(K) \neq 2$, $f \in K[X]$ *normiert irreduzibel, separabel vom Grad* 3 *und* $G = G(f)$.

(a) Es gilt $G \cong A_3$ *oder* $G \cong \mathfrak{S}_3$.

(b) Genau dann gilt $G \cong A_3$, *wenn* D *Quadrat in* K *ist.*

Beweis. **Zu (a):** Die Gruppe G ist isomorph zu einer Untergruppe von $\mathfrak{S}_3$ und es gilt $3\big||G|$, also gilt $G \cong A_3$ oder $G \cong \mathfrak{S}_3$.
Zu (b): Die Gruppe G ist isomorph zu A_3 genau dann, wenn $\varphi(G) = A_3$, das heißt $G = G_+$. Wie oben gesehen ist dies genau dann der Fall, wenn D Quadrat in K ist. □

Beispiel* 3.7.6. Für $k \in \mathbb{Z}$ sei $a = k^2 + k + 7$. Man zeige: Das Polynom $X^3 - aX + a$ ist irreduzibel über $\mathbb{Q}$ und hat Galoisgruppe isomorph zu A_3.

Folgerung 3.7.7. *Sei* K *Unterkörper von* $\mathbb{R}$, $f \in K[X]$ *normiert und irreduzibel vom Grad* 3, *und sei* $G = G(f)$. *Dann gilt:*

(a) Hat f *nur eine reelle Nullstelle, dann ist* $D < 0$ *und* $G \cong \mathfrak{S}_3$.

(b) Hat f *lauter reelle Nullstellen, dann ist* $D > 0$. *Genau dann ist* $G \cong A_3$, *wenn* D *Quadrat in* K *ist.*

Beweis. Das Polynom hat mindestens eine reelle Nullstelle α.
Zu (a): Ist $z \in \mathbb{C} \setminus \mathbb{R}$ Nullstelle von f, so ist auch $\overline{z}$ Nullstelle von f. Dann gilt

$$D = ((\alpha - z)(\alpha - \overline{z})(z - \overline{z}))^2 = \big(|\alpha - z|^2 2i\Im(z)\big)^2 = -4|\alpha - z|^4\Im(z)^2 < 0.$$

Also kann D kein Quadrat in K sein, es folgt $G \cong \mathfrak{S}_3$.
Zu (b): Hat F lauter reelle Nullstellen, so ist $D > 0$. Die Behauptung folgt nun aus dem Satz von vorher. □

Beispiele 3.7.8. (a) Das Polynom $f = X^3 - 2 \in \mathbb{Q}[X]$ ist irreduzibel, seine Diskriminante ist $D = -27(-2)^2 = -27 \cdot 4 < 0$. Also hat f genau eine reelle Nullstelle und es gilt $G(f) \cong \mathfrak{S}_3$.

(b) Das Polynom $f = X^3 - 3X - 1 \in \mathbb{Q}[X]$ ist irreduzibel, seine Diskriminante ist $D = -4(-3)^3 - 27(-1)^2 = 4 \cdot 27 - 27 = 9^2 > 0$. Also hat f drei reelle Nullstellen und es gilt $G(f) \cong A_3$.

(c) Das Polynom $f = X^3 - 4X - 1 \in \mathbb{Q}[X]$ ist irreduzibel, seine Diskriminante ist $D = -4(-4)^3 - 27(-1)^2 = 256 - 27 = 229 > 0$, kein Quadrat. Also hat f drei reelle Nullstellen, aber $G(f) \cong \mathfrak{S}_3$.

Sei $f = X^4 + bX^3 + cX^2 + dX + e \in K[X]$ irreduzibel, separabel sei $M = \{x_1, \ldots, x_4\}$ die Menge der Nullstellen im Zerfällungskörper L und $G = G(f)$. Es gilt $4\big||G|$ und man hat die Einbettung $\varphi : G \to \mathfrak{S}_4$. Sei $V = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$ die Klein'sche Vierergruppe, $N = \varphi^{-1}(V)$. Dann ist $N \lhd G$ ein Normalteiler und $[G : N] \leqslant [\mathfrak{S}_4 : V] = 6$. Seien

$$\alpha = x_1x_2 + x_3x_4, \beta = x_1x_3 + x_2x_4, \gamma = x_1x_4 + x_2x_3 \in L.$$

Diese Elemente sind paarweise verschieden, denn $0 \neq (x_1 - x_2)(x_3 - x_4) = (x_1x_3 + x_2x_4) - (x_2x_3 + x_1x_4) = \beta - \gamma$ und $0 \neq (x_1 - x_3)(x_2 - x_4) = (x_1x_2 + x_3x_4) - (x_2x_3 + x_1x_4) = \alpha - \gamma$ und $0 \neq (x_1 - x_4)(x_2 - x_3) = (x_1x_2 + x_3x_4) - (x_1x_3 + x_2x_4) = \alpha - \beta$. Sei $E = K(\alpha, \beta, \gamma)$.

Proposition 3.7.9. *Es gilt* $\mathrm{Fix}(N) = E$, $\mathrm{Gal}(L/E) = N$, *und* E/K *ist Galois'sch mit* $\mathrm{Gal}(E/K) \cong G/N$.

Beweis. Für $\sigma \in N$ gilt $\sigma(\alpha) = \alpha$, $\sigma(\beta) = \beta$ und $\sigma(\gamma) = \gamma$. Also ist $N \subset \mathrm{Gal}(L/E)$. Sei $\sigma \in G \setminus N$, dann ist $\varphi(\sigma) \in \mathfrak{S}_4 \setminus V$. Also ist $\varphi(\sigma)$ ein Zwei-, Drei-, oder Vierzykel. Für jeden Fall sieht man, daß $\sigma \notin \mathrm{Gal}(L/E)$ ist. [Ist zum Beispiel $\varphi(\sigma) = (12)$, so ist $\sigma(\alpha) = \alpha$, $\sigma(\beta) = \gamma$, $\sigma(\gamma) = \beta$, etc.] Es folgt $N = \mathrm{Gal}(L/E)$ und $\mathrm{Fix}(N) = E$. Da $N \lhd G$ ist, ist E/K Galois'sch mit $\mathrm{Gal}(E/K) \cong G/N$. Sei

$$g = (X - \alpha)(X - \beta)(X - \gamma) = X^3 - (\alpha + \beta + \gamma)X^2 + (\alpha\beta + \alpha\gamma + \beta\gamma)X - \alpha\beta\gamma \in E[X].$$

Da alle Koeffizienten von g unter allen $\sigma \in G$ unverändert bleiben, ist sogar $g \in K[X]$. Man kann nachrechnen, daß $g = X^3 - cX^2 + (ba - 4e)X - b^2e + 4ce - d^2$ ist. Das Polynom g heißt die kubische Resolvente von f. Offenbar ist E Zerfällungskörper von g. □

Satz 3.7.10. *Sei $f \in K[X]$ normiert, irreduzibel und separabel vom Grad 4, $G = G(f)$ und $m = [E : K] = [G : N]$. Dann gilt:*

(a) Ist $m = 6$, dann ist $G \cong \mathfrak{S}_4$.

(b) Ist $m = 3$, dann ist $G \cong A_4$.

(c) Ist $m = 1$, dann ist $G \cong V$.

(d) Im Fall $m = 2$ ist entweder $G \cong D_4$ oder $G \cong \mathbb{Z}/(4)$. Der erste Fall tritt genau dann ein, wenn f über E irreduzibel bleibt.

Beweis. Die Gruppe G ist zu einer Untergruppe von $\mathfrak{S}_4$ isomorph und es gilt $4 \big| |G|$. Da jede Untergruppe von $\mathfrak{S}_4$ zu einer der Untergruppen $\{e\}$, $\mathbb{Z}/(2)$, $\mathbb{Z}/(4)$, V, D_4, A_4 oder $\mathfrak{S}_4$ selbst isomorph ist, ist G zu einer der Gruppen $\mathbb{Z}/(4)$, V, D_4, A_4 oder $\mathfrak{S}_4$ isomorph. Ist $G = \langle\sigma\rangle \cong \mathbb{Z}/(4)$, dann gilt $\varphi(\sigma^2) \in V$, also ist $N = \langle\sigma^2\rangle$ und $|N| = [G : N] = 2$. In den anderen Fällen ist $V \subset \mathrm{im}(\varphi)$, also $N \cong V$, $|N| = 4$ und $[G : N] \in \{1, 2, 3, 6\}$.

Ist $m = 6$, dann $|G| = 6 \cdot |N| = 24$, also $G \cong \mathfrak{S}_4$. Ist $m = 3$, dann $|G| = 3 \cdot |N| = 12$, also $G \cong A_4$. Ist $m = 1$, dann ist $|G| = 1 \cdot |N| = 4$, also $G \cong V$. Ist $m = 2$ so gibt es folgende Möglichkeiten $|G| = 2 \cdot |N| = 4$, also $|N| = 2$ und $G \cong \mathbb{Z}/(4)$, oder $|G| = 2 \cdot |N| = 8$, also $|N| = 4$ und $G \cong D_4$. Im ersten Fall, also $|N| = 2$, kann $N = \mathrm{Gal}(L/E)$ nicht transitiv auf M operieren, also ist f über E reduzibel. Im zweiten Fall, also $|N| = 4$, operiert $N = \mathrm{Gal}(L/E)$ transitiv auf M, also bleibt f über E irreduzibel. □

Beispiele 3.7.11. (a) Das Polynom $f = X^4 - 2 \in \mathbb{Q}[X]$ hat die kubische Resolvente $g = X^3 + 8X = X(X^2 + 8)$. Ein Zerfällungskörper von g ist $E = \mathbb{Q}(\sqrt{-8})$, also ist $m = [E : \mathbb{Q}] = 2$. Das Polynom f ist irreduzibel über E, denn $f = (X - \sqrt[4]{2})(X + \sqrt[4]{2})(X - i\sqrt[4]{2})(X + i\sqrt[4]{2})$. Es folgt also $G \cong D_4$.

(b) Das Polynom $f = X^4 + 3X^3 - 3X + 2 \in \mathbb{Q}[X]$ ist irreduzibel. Seine kubische Resolvente $g = X^3 - X + 14$ ist ebenfalls irreduzibel mit Diskriminante $D(g) = -4(-1)^3 - 27 \cdot 14 < 0$. Also ist $G(g) \cong \mathfrak{S}_3$. Damit ist der Grad des Zerfällungskörpers $E/\mathbb{Q}$ gleich 6. Es folgt $G = G(f) \cong \mathfrak{S}_4$.

Beispiel* 3.7.12. Man bestimme die Galoisgruppe von $X^4 + 8X + 12$ über $\mathbb{Q}$.

Beispiel* 3.7.13. Gegeben sei das Element $z = X^2 + X^{-2}$ des rationalen Funktionenkörpers $\mathbb{Q}(X)$.

(a) Man zeige, daß $\mathbb{Q}(X)$ über $\mathbb{Q}(z)$ endlich vom Grad $\leqslant 4$ ist.

(b) Man bestimme die Gruppe aller Automorphismen von $\mathbb{Q}(X)$, die z festlassen.

(c) Man zeige, daß $\mathbb{Q}(X)$ über $\mathbb{Q}(z)$ Galois'sch ist und gebe alle Körper zwischen $\mathbb{Q}(X)$ und $\mathbb{Q}(z)$ an.

3.7.2 Endliche abelsche Gruppen als Galoisgruppen über $\mathbb{Q}$

Für $n \in \mathbb{N}$ gilt:

$$X^n - 1 = \prod_{d|n} \phi_d \text{ in } \mathbb{Z}[X].$$

Es folgt $-1 = \prod_{d|n} \phi_d(0)$, also $\phi_d(0) \in \{\pm 1\}$ für alle $d \in \mathbb{N}$. Für eine Primzahl p mit $p \nmid n$ ist das Bild $\overline{\phi}_n$ von ϕ_n in $\mathbb{F}_p[X]$ das n^{te} Kreisteilungspolynom.

Proposition 3.7.14. *Es sein $n, p, k \in \mathbb{N}$, p eine Primzahl mit $p \nmid n$ und $q = p^k$. Folgende Aussagen sind äquivalent:*

(a) Der Körper $\mathbb{F}_q$ enthält eine primitive n^{te} Einheitswurzel.

(b) Das Polynom $\overline{\phi}_n \in \mathbb{F}_p[X]$ hat eine Nullstelle in $\mathbb{F}_q$.

(c) Es gilt die Kongruenz $q \equiv 1 \mod n$.

Beweis. Die Äquivalenz **[(a) ⇔ (b)]** ist klar. Für die Äquivalenz **[(a) ⇔ (c)]** stellen wir fest, daß $\mathbb{F}_q$ eine primitive n^{te} Einheitswurzel enthält, genau dann, wenn $\mathbb{F}_q^*$ eine (zyklische) Untergruppe der Ordnung n enthält. Dies ist genau dann der Fall, wenn $n \big| q - 1$, in andern Worten, wenn $q \equiv 1 \mod n$. □

Es folgt: Ist $n \in \mathbb{N}$, $n > 1$, $q \equiv 1 \mod n$, dann ist $\overline{\phi}_n$ in $\mathbb{F}_q$ reduzibel.

Satz 3.7.15. *Sei $n \in \mathbb{N}$. Dann gibt es unendlich viele Primzahlen p mit $p \equiv 1 \mod n$.*

Beweis. Seien $p_1 < \ldots < p_r$ Primzahlen mit $p_i \equiv 1 \mod n$. Wir zeigen, daß es eine weiter Primzahl p_{r+1} mit $p_{r+1} \equiv 1 \mod n$ gibt. Sei $x = n \cdot p_1 \cdots p_r$. Für alle $t \in \mathbb{Z}$ gilt $\phi_n(xt) \equiv \phi_n(0) = \pm 1 \mod x$, also $x \big| \phi_n(xt) \pm 1$. Da ϕ_n normiert ist und vom Grad $\varphi(n)$, ist die Menge $\{\phi_n(xt) \mid t \in \mathbb{N}\}$ nicht nach oben beschränkt. Also gibt es $t_0 \in \mathbb{N}$ mit $\phi_n(xt_0) > 1$. Sei p_{r+1} Primzahl mit $p_{r+1} \big| \phi_n(xt_0)$. Da $x \big| \phi_n(xt_0) \pm 1$, gilt $p_{r+1} \nmid x$, also auch $p_{r+1} \nmid n$. Es gilt $\phi_n(xt_0) \equiv 0 \mod p_{r+1}$, also ist die Restklasse $xt_0 + (p_{r+1})$ primitive n^{te} Einheitswurzel in $\mathbb{F}_{p_{r+1}}$. Nach Proposition gilt $p_{r+1} \equiv 1 \mod n$. Wegen $p_{r+1} \nmid x$ gilt auch $p_{r+1} \notin \{p_1, \ldots, p_r\}$. □

Dieser Satz ist ein Spezialfall des Primzahlsatzes von Dirichlet: Sind $a \in \mathbb{Z} \setminus \{0\}$ und $n \in \mathbb{N}$ teilerfremd, dann gibt es unendlich viele Primzahlen p mit $p \equiv a \mod n$. Dies kann man mit analytische Hilfsmitteln beweisen.

Satz 3.7.16. *Sei G eine endliche abelsche Gruppe. Dann gibt es eine endliche Galoiserweiterung $\mathbb{Q} \subset K$ mit $\mathrm{Gal}(K/\mathbb{Q}) \cong G$.*

Beweis. Es gibt Primzahlpotenzen $q_1, \ldots, q_r$ mit $G \cong \prod_{i=1}^r \mathbb{Z}/(q_i)$. Nach dem vorhergehenden Satz enthält jede Restklasse $1 + (q_i)$, $1 \leqslant i \leqslant r$, unendlich viele Primzahlen. Also gibt es paarweise verschiedene Primzahlen $p_1, \ldots, p_r$ mit $p_i \equiv 1 \mod q_i$, $1 \leqslant i \leqslant r$. Die Abbildung

$$\gamma : \prod_{i=1}^r \mathbb{Z}/(p_i - 1) \to \prod_{i=1}^r \mathbb{Z}/(q_i), z_i + (p_i - 1) \mapsto z_i + (q_i)$$

ist surjektiver Gruppenhomomorphismus. Sei $n = p_1 \cdots p_r$ und sei $\mathbb{Q}^{(n)}$ der n^{te} Kreisteilungskörper über $\mathbb{Q}$. Man hat die Gruppenhomomorphismen

$$\mathrm{Gal}(\mathbb{Q}^{(n)}/\mathbb{Q}) \cong (\mathbb{Z}/n)^* \cong \prod_{i=1}^r (\mathbb{Z}/p_i)^* \cong \prod_{i=1}^r \mathbb{Z}/(p_i - 1) \xrightarrow{\gamma} \prod_{i=1}^r \mathbb{Z}/(q_i) \cong G.$$

Die Komposition dieser Homomorphismen ist surjektiv. Sei N der Kern dieser Komposition, $K = \mathrm{Fix}_{\mathbb{Q}^{(n)}}(N)$. Da N Normalteiler ist, ist $K/\mathbb{Q}$ Galois'sch mit $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}^{(n)}/\mathbb{Q})/N \cong G$. □

3.7.3 Das allgemeine Polynom n-ten Grades

Sei K ein Körper, $K[X_1, \ldots, X_n]$ der Polynomring in den Unbestimmten $X_1, \ldots, X_n$ und $L = K(X_1, \ldots, X_n)$ sein Quotientenkörper. Für $\sigma \in \mathfrak{S}_n$ sei der K-Algebrenhomomorphismus

$$\varphi_\sigma : K[X_1, \ldots, X_n] \to K[X_1, \ldots, X_n] \text{ definiert durch } \varphi_\sigma(f) = f(X_{\sigma(1)}, \ldots, X_{\sigma(n)}).$$

Man erhält so den injektiven Gruppenhomomorphismus

$$\mathfrak{S}_n \to \mathrm{Aut}(K[X_1, \ldots, X_n]), \sigma \mapsto \varphi_\sigma,$$

beziehungsweise die Operation

$$\mathfrak{S}_n \times K[X_1, \ldots, X_n] \to K[X_1, \ldots, X_n], (\sigma, f) \mapsto \varphi_\sigma(f).$$

Man setzt $\sigma f = \varphi_\sigma(f)$. Für $\sigma \in \mathfrak{S}_n$ hat φ_σ die eindeutige Fortsetzung

$$\varphi_\sigma : L \to L, \frac{f}{g} \mapsto \frac{\varphi_\sigma(f)}{\varphi_\sigma(g)} = \frac{\sigma f}{\sigma g}.$$

Wieder setzt man $\sigma \cdot \frac{f}{g}$ statt $\varphi_\sigma\left(\frac{f}{g}\right) = \frac{\sigma f}{\sigma g}$ und erhält den injektiven Gruppenhomomorphismus

$$\mathfrak{S}_n \to \mathrm{Gal}(L/K), \sigma \mapsto \varphi_\sigma,$$

beziehungsweise die Operation

$$\mathfrak{S}_n \times L \to L, \left(\sigma, \frac{f}{g}\right) \mapsto \sigma \cdot \frac{f}{g}.$$

Wir fassen auf diese Weise die $\mathfrak{S}_n$ als Untergruppen von $\mathrm{Gal}(L/K)$ auf.

Definition 3.7.17. Ein Polynom $f \in K[X_1, \ldots, X_n]$ heißt symmetrisch, wenn $\sigma f = f$ für alle $\sigma \in \mathfrak{S}_n$. Allgemein heißt eine rationale Funktion $\frac{f}{g} \in L$ symmetrisch, wenn $\sigma \cdot \frac{f}{g} = \frac{f}{g}$ für alle $\sigma \in \mathfrak{S}_n$. Die Menge der symmetrischen Polynome in $K[X_1, \ldots, X_n]$ beziehungsweise der symmetrischen rationalen Funktionen in L ist ein Unterring beziehungsweise Unterkörper der K enthält.

Beispiel 3.7.18. Sei Y eine weitere Unbestimmte. Dann gilt $\prod_{i=1}^{n}(Y - X_i) = \sum_{k=0}^{n}(-1)^k s_k Y^{n-k} \in K[X_1, \ldots, X_n][Y]$, wobei

$$\begin{aligned}
s_0 &= 1 \\
s_1 &= X_1 + \ldots + X_n \\
s_2 &= X_1X_2 + X_1X_3 + \ldots + X_{n-1}X_n = \sum_{i<j} X_iX_j \\
&\vdots \\
s_k &= \sum_{1 \leqslant i_1 < \ldots < i_k \leqslant n} X_{i_1} \cdots X_{i_k} \\
&\vdots \\
s_n &= X_1 \cdots X_n
\end{aligned}$$

Die $s_0, s_1, \ldots, s_n$ heißen elementarsymmetrische Polynome in den Unbestimmten $X_1, \ldots, X_n$. Die Symmetrie ist klar, denn

$$\sum_{k=0}^{n}(-1)^k \sigma s_k Y^{n-k} = \prod_{i=1}^{n}(Y - \sigma X_i) = \prod_{i=1}^{n}(Y - X_i) = \sum_{k=0}^{n}(-1)^k s_k Y^{n-k},$$

also $\sigma s_k = s_k$ für alle $1 \leqslant k \leqslant n$. Alle Elemente in $K[s_1, \ldots, s_n]$, allgemeiner $E = K(s_1, \ldots, s_n)$ sind symmetrisch. Also gilt

$$E \subset \mathrm{Fix}_L(\mathfrak{S}_n) \text{ und } \mathfrak{S}_n \subset \mathrm{Gal}(L/E).$$

Weiterhin ist $f = \prod_{i=1}^{n}(Y - X_i) = \sum_{k=0}^{n}(-1)^k s_k Y^{n-k} \in E[Y]$, L ist Zerfällungskörper von f und f ist separabel.

Satz 3.7.19. *Die Erweiterung L/E ist endliche Galoiserweiterung und* $\mathrm{Gal}(L/E) = \mathfrak{S}_n$.

Beweis. Wir haben gesehen, daß L/E endliche Galoiserweiterung ist. Da L Zerfällungskörper von f ist, gilt $[L : E] \leqslant \deg(f)! = n!$. Insgesamt haben wir

$$n! \leqslant |\mathrm{Gal}(L/E)| = [L : E] \leqslant n!,$$

also $\mathfrak{S}_n = \mathrm{Gal}(L/E)$. □

Folgerung 3.7.20. *Es gilt $E = K(s_1, \ldots, s_n) = \mathrm{Fix}_L(\mathfrak{S}_n)$, das heißt zu jeder symmetrischen rationalen Funktion $z \in K(X_1, \ldots, X_n)$ gibt es $u, v \in K[Y_1 \ldots, Y_n]$ mit $v(s_1, \ldots, s_n) \neq 0$ und $z = \frac{u(s_1,\ldots,s_n)}{v(s_1,\ldots,s_n)}$. Der Körper E heißt Körper der symmetrischen rationalen Funktionen.*

Allgemein gilt der Hauptsatz für elementarsymmetrische Polynome in $R[X_1, \ldots, X_n]$, den wir später beweisen.

Folgerung 3.7.21. *Jede endliche Gruppe ist isomorph zur Galoisgruppe einer endlichen Galoiserweiterung.*

Beweis. Sei G endliche Gruppe der Ordnung n. Nach dem Satz von Cayley 1.3.8 ist G isomorph zu einer Untergruppe H von $\mathfrak{S}_n$. Nach dem Satz gibt es eine endliche Galoiserweiterung L/E mit $\mathrm{Gal}(L/E) = \mathfrak{S}_n$. Ist $\widetilde{E} = \mathrm{Fix}_L(H)$, so ist $L/\widetilde{E}$ endliche Galoiserweiterung mit $\mathrm{Gal}(L/\widetilde{E}) = H \cong G$. □

Sei $M = K(U_1, \ldots, U_n)$ der rationale Funktionenkörper in den Unbestimmten $U_1, \ldots, U_n$ über K, sei Y eine weitere Unbestimmte. Sei

$$F = Y^n + U_1Y^{n-1} + \cdots + U_{n-1}Y + U_n \in M[Y].$$

Dieses Polynom F heißt allgemeines Polynom n^{ten} Grades. Wir wollen seine Galoisgruppe bestimmen.

Satz 3.7.22. *Die Galoisgruppe des allgemeinen Polynoms* $F = Y^n + U_1 Y^{n-1} + \cdots + U_{n-1}Y + U_n \in M[Y]$ *ist isomorph zu* $\mathfrak{S}_n$.

Beweis. Sei N ein Zerfällungskörper von F und seien $x_1, \ldots, x_n \in N$ die Nullstellen von F. Es gilt

$$F = \prod_{i=1}^{n}(Y - x_i) = \sum_{k=0}^{n}(-1)^k s_k(x_1, \ldots, x_n)Y^{n-k},$$

also $U_k = (-1)^k s_k(x_1, \ldots, x_n)$, für $1 \leqslant k \leqslant n$. Es folgt

$$N = M(x_1, \ldots, x_n) = K(U_1, \ldots, U_n, x_1, \ldots, x_n) = K(x_1, \ldots, x_n).$$

Wir haben folgendes kommutative Diagramm

$$\begin{array}{ccc} K[X_1, \ldots, X_n] & \xrightarrow{\alpha} & K[x_1, \ldots, x_n] \\ \uparrow & & \uparrow \\ K[s_1, \ldots, s_n] & \xrightarrow[\sim]{\alpha'} & K[U_1, \ldots, U_n] \end{array}$$

wobei α definiert ist durch $\alpha(g) = g(x_1, \ldots, x_n)$, und α' die Einschränkung von α ist. Wegen obiger Formeln ist α' sinnvoll und surjektiv. Außerdem ist α' injektiv: Sei nämlich $g \in K[Y_1, \ldots, Y_n]$ mit $\alpha'(g(s_1, \ldots, s_n)) = 0$. Dann gilt $0 = g(s_1(x_1, \ldots, x_n), \ldots, s_n(x_1, \ldots, x_n)) = g(-U_1, U_2, \ldots, (-1)^n U_n)$. Also ist $g = 0$, und somit $g(s_1, \ldots, s_n) = 0$. Es folgt, daß auch α injektiv ist: Sei $0 \neq f \in K[X_1, \ldots, X_n]$, dann ist $g = \prod_{\sigma \in \mathfrak{S}_n} \sigma f \neq 0$ und symmetrisch. Also gibt es $u, v \in K[Y_1, \ldots, Y_n]$ mit $v(s_1, \ldots, s_n) \neq 0$ und $g = \frac{u(s_1, \ldots, s_n)}{v(s_1, \ldots, s_n)}$. Es folgt

$$0 \neq \alpha'(u(s_1, \ldots, s_n)) = \alpha(u(s_1, \ldots, s_n)) = \alpha(g)\alpha(v(s_1, \ldots, s_n)).$$

Also ist $\alpha(g) \neq 0$ und damit $\alpha(f) \neq 0$. Die Abbildungen α und α' induzieren Isomorphismen, die wir ebenfalls mit α, und α' bezeichnen, zwischen den Quotientenkörpern.

$$\begin{array}{ccc} K(X_1, \ldots, X_n) & \xrightarrow{\alpha} & K(x_1, \ldots, x_n) = N \\ \uparrow & & \uparrow \\ K(s_1, \ldots, s_n) & \xrightarrow[\sim]{\alpha'} & K(U_1, \ldots, U_n) = M \end{array}$$

Wieder ist α' die Restriktion von α. Da die Erweiterung $K(X_1, \ldots, X_n)/K(s_1, \ldots, s_n)$ Galois'sch ist, mit Galoisgruppe $\mathfrak{S}_n$, hat auch N/M diese Eigenschaft. □

3.7.4 Beweis des Fundamentalsatzes der Algebra nach Artin

Proposition 3.7.23. *Jedes quadratische Polynom* $f \in \mathbb{C}[X]$ *hat in* $\mathbb{C}$ *eine Nullstelle.*

Beweis. Für alle $w \in \mathbb{C}$ existiert $z \in \mathbb{C}$ mit $w = z^2$. Denn ist $w = re^{i\varphi}$ mit $r \in \mathbb{R}_0^+$, $0 \leqslant \varphi < 2\pi$, $z = \sqrt{r}e^{i\frac{\varphi}{2}}$. Dann gilt $z^2 = w$.

Sei ohne Einschränkung f normiert, $f = X^2 + \beta X + \gamma$. Dann $f = (X + \frac{\beta}{2})^2 + \gamma - \frac{\beta^2}{4}$. Es gibt $\delta \in \mathbb{C}$ mit $\delta^2 = \frac{\beta^2}{4} - \gamma$. Damit ist $f = (X + \frac{\beta}{2} + \delta)(X + \frac{\beta}{2} - \delta)$. □

Fundamentalsatz der Algebra 3.7.24. *Jedes Polynom* $f \in \mathbb{C}[X] \setminus \mathbb{C}$ *hat in* $\mathbb{C}$ *eine Nullstelle.*

Beweis. Sei $f \in \mathbb{C}[X] \setminus \mathbb{C}$ und L Zerfällungskörper von f. Dann ist $\mathbb{R} \subset L$ eine endliche und separabel Erweiterung. Sei $L \subset N$ normaler Abschluß von L/R. Wenn wir $N = \mathbb{C}$ zeigen können, dann folgt $L = \mathbb{C}$ und wir sind fertig. Es genügt also zu zeigen: Ist $\mathbb{C} \subset N$ endliche Erweiterung , so daß $N/\mathbb{R}$ Galois'sch ist, so folgt $N = \mathbb{C}$. Sei $G = \mathrm{Gal}(N/\mathbb{R})$.

Wir zeigen als erstes, daß G eine 2-Gruppe ist: Wegen $\mathbb{R} \subset \mathbb{C} \subset N$ ist die Ordnung von G gerade und besitzt eine nicht-triviale 2-Sylowuntergruppe P. Sei $F = \mathrm{Fix}_N(P)$. Dann ist $[F : \mathbb{R}] = [G : P]$ ungerade. Sei $x \in F$ ein primitives Element über $\mathbb{R}$, $g \in \mathbb{R}[X]$ sein Minimalpolynom. Da $\deg(g) = [F : \mathbb{R}]$ ungerade

ist, hat g in $\mathbb{R}$ eine Nullstelle, also gilt $\deg(g) = 1$, $F = \mathbb{R}$. Es folgt $G = P$.

Sei weiter $H = \mathrm{Gal}(N/\mathbb{C}) \subset G$. Wir zeigen, daß $H = \{e\}$ ist. Angenommen dies ist nicht der Fall. Als nicht-triviale 2-Gruppe hat H einen Normalteiler H' vom Index 2. Sei $F' = \mathrm{Fix}_N(H')$. Dann ist $\mathbb{C} = \mathrm{Fix}(H) \subset F' = \mathrm{Fix}(H')$ eine Körpererweiterung vom Grad 2. Dies widerspricht der Proposition. Es folgt $H = \{e\}$ und damit $N = \mathbb{C}$. □

Beispiel* **3.7.25.** In eine ähnliche Richtung geht folgende Aufgabe: Sei $p \in \mathbb{N}$ prim. Ist K ein Körper von Charakteristik 0, so daß $p \big| [L : K]$ für jede endliche nicht-triviale Erweiterung L von K, dann ist der Grad jeder endlichen Erweiterung von K eine p-Potenz, d.h $[L : K] = p^n$.

3.8 Auflösbarkeit von Gleichungen durch Radikale

3.8.1 Auflösbare Gruppen

Für eine Gruppe G ist $[G, G]$ die Kommutatoruntergruppe von G. Man setzt

$$\begin{aligned} D^0(G) &= G \\ D^1(G) &= [G, G] \\ D^{n+1}(G) &= D^1(D^n(G)) = [D^n(G), D^n(G)] \quad \text{für } n \geqslant 1 \end{aligned}$$

Für jeden Gruppenhomomorphismus $\varphi : G \to G'$ und alle $n \geqslant 0$ gilt $\varphi(D^n(G)) \subset D^n(G')$ (Induktion). Indbesondere sind die $D^n(G)$, $n \geqslant 0$, Normalteiler von G. Die Faktorgruppe $D^n(G)/D^{n+1}(G)$ ist abelsch aber im Allgemeinen nicht zentrale Untergruppe von $G/D^{n+1}(G)$, $n \geqslant 0$. Die Folge

$$G = D^0(G) \supset D^1(G) \supset D^2(G) \supset \ldots$$

heißt abgeleitete Reihe von G.

Proposition und Definition 3.8.1. *Eine Gruppe G heißt auflösbar, wenn folgende äquivalente Bedingungen erfüllt sind:*

(a) Es gibt $n \in \mathbb{N}_0$ mit $D^n(G) = \{e\}$.

(b) Es gibt eine Folge von Normalteilern $G = H_0 \supset H_1 \supset \ldots \supset H_m = \{e\}$, $m \geqslant 0$, so daß H_i/H_{i+1} abelsch ist für $0 \leqslant i < m$.

(c) Es gibt eine Folge von Untergruppen $G = H_0 \supset H_1 \supset \ldots \supset H_m = \{e\}$, $m \geqslant 0$, so daß $H_{i+1} \triangleleft H_i$ und H_i/H_{i+1} abelsch ist für $0 \leqslant i < m$.

In (b) und (c) gilt $D^i(g) \subset H_i$, $0 \leqslant i \leqslant m$. Eine Folge von Untergruppen wie in (c) heißt Normalreihe mit abelschen Faktoren.

Beweis. **(a) ⇒ (b):** Gilt (a), so hat die Folge $(D^i(G))_{0 \leqslant i \leqslant m}$ die in (b) gewünschte Eigenschaft.
(b) ⇒ (c): Das ist klar.
(c) ⇒ (a): Gilt (c), so ist $D^i(G) \subset H_i$, $0 \leqslant i \leqslant m$: Das ist klar für $i = 0$. Sei $D^i(G) \subset H_i$ für ein $0 \leqslant i < m$, dann ist $D^{i+1}(G) = [D^i(G), D^i(G)] \subset [H_i, H_i] \subset H_{i+1}$. Da $H_m = \{e\}$, folgt $D^m(G) = \{e\}$. □

Proposition 3.8.2. *Sei G eine Gruppe.*

(a) Ist G auflösbar, so auch jede Untergruppe und jedes epimorphe Bild von G.

(b) Ist $N \triangleleft G$, so daß N und G/N auflösbar sind, dann ist G auflösbar.

(c) Endliche direkte Produkte auflösbarer Gruppen sind auflösbar.

Beweis. **Zu (a):** Sei $G = H_0 \supset H_1 \supset \ldots \supset H_m = \{e\}$ eine Normalreihe mit abelschen Faktoren. Sei $U \subset G$ Untergruppe von G. Man hat die Folge

$$U = U \cap H_0 \supset U \cap H_1 \supset \ldots \supset U \cap H_m = \{e\}.$$

Es gilt $U \cap H_{i+1} \triangleleft U \cap H_i$ und da die Abbildung

$$U \cap H_i/U \cap H_{i+1} \to H_i/H_{i+1}, xU \cap H_{i+1} \mapsto xH_{i+1}$$

injektiver Homomorphismus ist, ist mit H_i/H_{i+1} auch $U \cap H_i/U \cap H_{i+1}$ abelsch.
Ist $f : G \to G'$ surjektiver Homomorphismus, dann hat man die Folge

$$G' = f(G) = f(H_0) \supset f(H_1) \supset \dots f(H_m) = \{e\}.$$

Es gilt $f(H_{i+1}) \triangleleft f(H_i)$ und da die Abbildung

$$H_i/H_{i+1} \to f(H_i)/f(H_{i+1}), xH_{i+1} \mapsto f(x)f(H_{i+1})$$

Monoider Homomorphismus ist, ist auch $f(H_i)/f(H_{i+1})$ abelsch.
Zu (b): Sind $N = N_0 \supset N_1 \supset \dots \supset N_l = \{e\}$ und $G/N = H_0/N \supset H_1/N \supset \dots \supset H_m/N = \{e\}$ Normalreihen mit abelschen Faktoren, so findet man eine Normalreihe mit abelschen Faktoren für G.
Zu (c): Dies folgt aus (b). □

Proposition 3.8.3. *Sei G eine endliche auflösbare Gruppe und $N \triangleleft G$. Es gibt eine Normalreihe mit abelschen Faktoren*

$$G = H_0 \supset H_1 \supset \dots \supset H_m = \{e\},$$

so daß die $[H_i : H_{i+1}]$, $0 \leqslant i \leqslant m$ Primzahlen sind und $N \in \{H_0, \dots, H_m\}$ ist.

Beweis. Sei zuerst G abelsch, $G \neq \{e\}$ und $N = \{e\}$. Sei $G = H_0$. Da es zu jedem Teiler d von $|G|$ eine Untergruppe der Ordnung d in G gibt, gibt es eine Untergruppe $H_1 \subset H_0$, so daß $[H_0 : H_1]$ prim ist. Induktiv findet man nun eine Folge wie behauptet.
Sei nun G auflösbar, $N = \{e\}$. Sei $G = H_0 \supset H_1 \supset \dots \supset H_m = \{e\}$ Normalreihe mit abelschen Faktoren. Nach dem eben gezeigten, kann diese zu einer Normalreihe

$$G = H_0 = H_{01} \supset H_{02} \supset \dots H_{0k_0} = H_1 = H_{11} \supset H_{12} \supset \dots \supset H_{1k_1} = H_2 \supset \dots \supset \{e\}$$

wie gewünscht verfeinert werden.
Allgemein: Sei G auflösbar, $\{e\} \neq N \triangleleft G$. Man argumentiert wie beim Beweis der Aussage (b) der vorhergehenden Proposition. □

Beispiele 3.8.4. (a) Abelsche Gruppen, endliche p-Gruppen und endliche nilpotente Gruppen sind auflösbar.

(b) $\mathfrak{S}_3$ und $\mathfrak{S}_4$ sind auflösbar mit den Normalreihen mit abelschen Faktoren

$$\mathfrak{S}_3 \supset A_3 \supset \{e\} \quad \text{und} \quad \mathfrak{S}_4 \supset A_4 \supset V \supset \{e\}$$

aber nicht nilpotent.

(c) D_n, $n \geqslant 2$, ist auflösbar, denn jede solche Gruppe hat einen zyklischen Normalteiler vom Index 2.

(d) Endliche, einfache nicht-abelsche Gruppen sind nicht auflösbar. Insbesondere sind die Gruppen A_n für $n \geqslant 5$ nicht auflösbar. Damit sind auch die $\mathfrak{S}_n$ für $n \geqslant 5$ nicht auflösbar.

(e) Sind $p \neq q$ Primzahlen, $a, b \in \mathbb{N}$. Dann ist jede Gruppe der Ordnung $p^a q^b$ auflösbar (Burnside).

(f) Jede Gruppe ungerader Ordnung ist auflösbar (Feit, Thompson).

Beispiel* 3.8.5. Sei G eine Gruppe der Ordnung $|G| = 105$. Wir zeigen "von Hand", daß G auflösbar ist. Aus Beispiel 1.6.19 wissen wir bereits, daß G einen Normalteiler N der Ordnung $|N| = 7$ oder $|N| = 5$ hat. Wir benutzen, daß G auflösbar ist, wenn es einen Normalteiler $N \triangleleft G$ gibt, so daß G/N und N auflösbar sind.

Wir betrachten zunächst den Fall, daß $|N| = 5$. Da N Primzahlordnung hat, also zyklisch ist, ist N abelsch, und damit auflösbar (sogar nilpotent). Wir müssen zeigen, daß G/N auflösbar ist. Nach Lagrange gilt

$$|G/N| = [G : N] = \frac{|G|}{|N|} = \frac{105}{5} = 21.$$

Wir zeigen, daß jede Gruppe H der Ordnung 21 auflösbar ist. Mit $21 = 3 \cdot 7$ sei s_3, bzw. s_7, die Anzahl der 3- bzw. 7-Sylowuntergruppen von H. Dann gilt $s_7 | 3$, also $s_7 \in \{1, 3\}$. Wegen $s_7 \equiv 1 \mod 7$ also $s_7 = 1$. Da es also nur eine einzige 7-Sylowuntergruppe M gibt, ist diese Normalteiler. Außerdem ist sie zyklisch von Primzahlordnung, also abelsch und damit auflösbar (sogar nilpotent). Weiter ist analog zu oben

$$|H/M| = [H : M] = \frac{|H|}{|M|} = \frac{21}{7} = 3$$

zyklisch, also abelsch, also auflösbar. Es folgt, daß bereits H auflösbar ist.

Betrachte nun den Fall, daß $|N| = 7$. Wieder ist N von Primzahlordnung, also zyklisch, also abelsch, und damit auflösbar. Wir müssen wieder zeigen, daß G/N auflösbar ist. Wie oben gilt nach Lagrange

$$|G/N| = [G : N] = \frac{|G|}{|N|} = \frac{105}{7} = 15.$$

Es ist zu zeigen, daß jede Gruppe H der Ordnung 15 auflösbar ist. Dies ist genau analog zum obigen Fall. Mit $15 = 3 \cdot 5$ sei s_3, bzw. s_5 die Anzahl der 3- bzw. 5-Sylowuntergruppen von H. Dann gilt $s_5 | 3$, also $s_5 \in \{1, 3\}$. Wegen $s_5 \equiv 1 \mod 5$ ist $s_5 = 1$. Da es also nur eine einzige 5-Sylowuntergruppe M gibt, ist diese Normalteiler. Außerdem ist sie zyklisch von Primzahlordnung, also abelsch und damit auflösbar (sogar nilpotent). Weiter ist analog zu oben

$$|H/M| = [H : M] = \frac{|H|}{|M|} = \frac{15}{5} = 3$$

zyklisch, also abelsch, also auflösbar. Es folgt, daß bereits H auflösbar ist.

3.8.2 Norm und Spur einer endlichen Galoiserweiterung

Definition 3.8.6. Sei $K \subset L$ eine endliche Galoiserweiterung mit $G = \mathrm{Gal}(L/K)$. Für $x \in L$ sei

$$\begin{aligned} T_{L/K}(x) &= \sum_{\sigma \in G} \sigma(x) \\ N_{L/K}(x) &= \prod_{\sigma \in G} \sigma(x) \end{aligned}$$

Offenbar liegen diese Elemente in K. Die Abbildungen $T_{L/K} : L \to K$ und $N_{L/K} : L \to K$ heißen Spur beziehungsweise Norm von L/K.

Proposition 3.8.7. *Sei $K \subset L$ endliche Galoiserweiterung vom Grad n.*

(a) Die Abbildung $T_{L/K}$ ist K-linear.

(b) Für alle $x, y \in L$ gilt $N_{L/K}(xy) = N_{L/K}(x)N_{L/K}(y)$. Man sagt $N_{L/K}$ ist multiplikativ.

(c) Für $x \in K$ gilt $T_{L/K}(x) = nx$ und $N_{L/K}(x) = x^n$.

Beweis. Das ist klar. □

Beispiel* 3.8.8. Als Anwendung von Norm und Spur zeige man:

(a) Es gilt $\sqrt[3]{3} \notin \mathbb{Q}(\sqrt[3]{2})$.

(b) Das Element $1 - \zeta_3 \in \mathbb{Q}(\zeta_3)$ ist kein perfektes Quadrat.

3.8.3 Zyklische Galoiserweiterungen

Definition 3.8.9. Eine endliche Galoiserweiterung L/K heißt zyklisch/abelsch/auflösbar, wenn $\mathrm{Gal}(L/K)$ zyklisch/abelsch/auflösbar ist.

Hilberts "Satz 90" 3.8.10. *Sei $K \subset L$ eine endliche zyklische Galoiserweiterung mit $\mathrm{Gal}(L/K) = \langle\sigma\rangle$. Für $y \in L$ gilt $N_{L/K}(y) = 1$ genau dann, wenn es $x \in L^*$ gibt mit $y = \frac{x}{\sigma(x)}$.*

Beweis. Sei $n = [L : K] = \mathrm{ord}(\sigma)$. Für $x \in L^*$, $y = \frac{x}{\sigma(x)}$ gilt

$$N_{L/K}(y) = \frac{x}{\sigma(x)} \frac{\sigma(x)}{\sigma^2(x)} \cdots \frac{\sigma^{n-1}(x)}{\sigma^n(x)} = 1.$$

Sei umgekehrt $y \in L$ mit $N_{L/K}(y) = 1$. Nach dem Lemma von Dedeking 3.5.5 ist die Abbildung

$$\sigma^0 + y\sigma + y\sigma(y)\sigma^2 + \cdots + y\sigma(y)\sigma^2(y)\cdots\sigma^{n-2}(y)\sigma^{n-1} : L^* \to L$$

nicht null, also gibt es $z \in L^*$ mit

$$x := z + y\sigma(z) + y\sigma(y)\sigma^2(z) + \cdots + y\sigma(y)\cdots\sigma^{n-2}(y)\sigma^{n-1}(z) \neq 0.$$

Es folgt

$$y\sigma(x) = y\sigma(z) + y\sigma(y)\sigma^2(z) + \cdots + y\sigma(y)\cdots\sigma^{n-1}(y)\sigma^n(z) = x,$$

denn im letzten Summand ist $y\sigma(y)\cdots\sigma^{n-1}(y) = N_{L/K}(y) = 1$ und $\sigma^n(z) = z$. Es folgt $y = \frac{x}{\sigma(x)}$. □

Satz 3.8.11. *Sei K ein Körper und $n \in \mathbb{N}$ mit $\mathrm{char}(K) \nmid n$. Wir nehmen an, daß K eine primitive n^{te} Einheitswurzel enthält.*

(a) Ist $f = X^n - a \in K[X]$, L ein Zerfällungskörper von f und $x \in L$ eine Nullstelle von f, dann gilt $L = K(x)$ und L/K ist eine zyklische Galoiserweiterung. Ferner ist $d = [L : K]$ Teiler von n, es gilt $x^d \in K$ und $X^d - x^d$ ist das Minimalpolynom von x über K. Ist f irreduzibel, dann ist L/K zyklische Galoiserweiterung vom Grad n.

(b) Wenn umgekehrt $K \subset L$ eine zyklische Galoiserweiterung vom Grad n ist, dann gibt es $x \in L$ mit $x^n \in K$ und $L = K(x)$. Also ist $X^n - x^n$ das Minimalpolynom von x und L ist sein Zerfällungskörper.

Beweis. **Zu (a):** Sei ohne Einschränkung $a \neq 0$. Wir wissen: Es gilt $L = K(x)$, die Erweiterung L/K ist Galois'sch und es gibt einen injektiven Homomorphismus

$$\mathrm{Gal}(L/K) \to \mathbb{Z}/n\mathbb{Z}.$$

Insbesondere ist $\mathrm{Gal}(L/K)$ zyklisch. Ist $\mathrm{Gal}(L/K) = \langle\sigma\rangle$ von der Ordnung $d = [L : K]$, so gilt $d \mid n$ und es gibt $1 \leqslant i \leqslant n$ mit $\sigma(x) = \varepsilon^i x$. Offenbar ist ε^i eine primitive d^{te} Einheitswurzel. Es folgt

$$\sigma(x^d) = \sigma(x)^d = \varepsilon^{id} x^d = x^d,$$

also $x^d \in K$. Also ist $X^d - x^d \in K[X]$ das Minimalpolynom von x und L ist ein Zerfällungskörper. Ist f irreduzibel, dann ist $[L : K] = n$.
Zu (b): Sei umgekehrt $K \subset L$ endliche zyklische Galoiserweiterung vom Grad n mit $\mathrm{Gal}(L/K) = \langle\sigma\rangle$. Da $\varepsilon \in K$ ist, gilt

$$N_{L/K}(\varepsilon^{-1}) = \varepsilon^{-n} = 1.$$

Nach Hilberts Satz 90 gibt es also $x \in L^*$ mit $\varepsilon^{-1} = \frac{x}{\sigma(x)}$. Es folgt $\sigma(x) = x\varepsilon$, allgemeiner $\sigma^i(x) = \varepsilon^i x$ für alle $1 \leqslant i \leqslant n$. Also sind die $\sigma^i(x)$, $1 \leqslant i \leqslant n$, paarweise verschieden. Es folgt

$$n = [L : K] \geqslant [K(x) : K] \geqslant n,$$

also ist $L = K(x)$. Wie oben gilt

$$\sigma(x^n) = \sigma(x)^n = \varepsilon^n x^n = x^n,$$

also ist $x^n \in K$. Dann ist $X^n - x^n \in K[X]$ das Minimalpolynom von x und L ist sein Zerfällungskörper. □

Hilberts "Satz 90" 3.8.12 (additive Form)**.** *Sei $K \subset L$ eine endliche zyklische Galoiserweiterung mit $\mathrm{Gal}(L/K) = \langle\sigma\rangle$. Für $y \in L$ gilt $T_{L/K}(y) = 0$ genau dann, wenn es $x \in L$ gibt mit $y = x - \sigma(y)$.*

Beweis. Sei $n = [L : K] = \mathrm{ord}(\sigma)$. Für $y = x - \sigma(x)$ mit $x \in L$ gilt

$$T_{L/K}(y) = (x - \sigma(x)) + \big(\sigma(x) - \sigma^2(x)\big) + \cdots + \big(\sigma^{n-1}(x) - \sigma^n(x)\big) = x - x = 0.$$

Sei umgekehrt $y \in L$ mit $T_{L/K}(y) = 0$. Da die Spur $T_{L/K} : L \to K$ nicht null ist, gibt es $z \in L$ mit $T_{L/K}(z) \neq 0$. Also gibt es $x \in L$ mit

$$xT_{L/K}(z) = y\sigma(x) + (y + \sigma(y))\,\sigma^2(z) + \cdots + \big(y + \sigma(y) + \cdots + \sigma^{n-2}(y)\big)\,\sigma^{n-1}(z).$$

Es folgt

$$\begin{aligned}\sigma(x)T_{L/K}(z) = \sigma(xT_{L/K}(z)) &= \sigma(y)\sigma^2(x) + \big(\sigma(y) + \sigma^2(y)\big)\,\sigma^3(z) + \cdots + \big(\sigma(y) + \sigma^2(y) + \cdots + \sigma^{n-1}(y)\big)\,\sigma^n(z)\\ &= \sigma(y)\sigma^2(z) + \big(\sigma(y) + \sigma^2(y)\big)\,\sigma^3(z) + \cdots + \big(T_{L/K}(y) - y\big)\,z\\ &= \sigma(y)\sigma^2(z) + \big(\sigma(y) + \sigma^2(y)\big)\,\sigma^3(z) + \cdots - yz\end{aligned}$$

Zusammen ergibt das

$$\begin{aligned}(x - \sigma(x))\,T_{L/K}(z) &= y\sigma(z) + (y + \sigma(y))\,\sigma^2(z) + \cdots + \big(y + \sigma(y) + \cdots + \sigma^{n-2}(y)\big)\,\sigma^{n-1}(z)\\ &\quad - \big[\sigma(y)\sigma^2(z) + \cdots + \big(\sigma(y) + \cdots + \sigma^{n-2}(y)\big)\,\sigma^{n-1}\big] + yz\\ &= y\big(z + \sigma(z) + \cdots + \sigma^{n-1}(z)\big) = yT_{L/K}(z)\end{aligned}$$

Also $y = x - \sigma(x)$. □

Proposition 3.8.13. *Sei K ein Körper mit Primzahlcharakteristik p, $f = X^p - X - a \in K[X]$ und L ein Zerfällungskörper von f.*

(a) Ist $x \in L$ eine Nullstelle von f, dann sind $x + i$, $0 \leqslant i < p$ alle Nullstellen. Also ist f separabel, $L = K(x)$, insbesondere L/K Galois'sch.

(b) Das Polynom f ist genau dann irreduzibel, wenn f in K keine Nullstelle hat.

(c) Ist f reduzibel, so zerfällt f über K vollständig in Linearfaktoren.

Beweis. **Zu (a):** Sei $x \in L$ eine Nullstelle von f. Dann gilt

$$f(x + i) = (x + i)^p - (x + i) - a = x^p + i^p - x - i - a = 0.$$

Also sind die $x + i$, $0 \leqslant i < p$, alle Nullstellen von f. Alles andere ist klar.
Zu (b) und (c): Is f irreduzibel, so hat f in K keine Nullstelle. Sei f reduzibel, dann gibt es irreduzible Polynome $g_1, \ldots, g_r \in K[X]$ mit $r > 1$ und $f = g_1 \cdots g_r$. Sei $x_i \in L$ Nullstelle von g_i. Nach (a) gilt $K(x_1) = \ldots = K(x_r)$, also ist

$$p = \deg(f) = \sum_{i=1}^{r} \deg(g_i) = r\deg(g_1).$$

Es folgt $r = p$ und $\deg(g_1) = \ldots = \deg(g_r) = 1$. Also liegen die Nullstellen von f alle in K. □

Satz 3.8.14 (Artin, Schreier)**.** *Sei K ein Körper mit Primzahlcharakteristik p.*

(a) Ist $f = X^p - X - a \in K[X]$, L ein Zerfällungskörper von f und $x \in L$ eine Nullstelle von f, so ist $L = K(x)$ und L/K ist zyklische Galoiserweiterung vom Grad 1 oder p. Genau dann ist $[L : K] = p$, wenn f irreduzibel ist.

(b) Ist L/K zyklische Galoiserweiterung vom Grad p, so gibt es $a \in K$ und eine Nullstelle des irreduziblen Polynoms $f = X^p - X - a \in K[X]$ mit $L = K(x)$.

Beweis. **Zu (a):** Ist $x \in L$ Nullstelle von f, dann sind $x+i$, $0 \leqslant i < p$, alle Nullstellen von f, und es gilt $L = K(x)$. Da f irreduzibel ist, ist L/K Galoiserweiterung mit $|\operatorname{Gal}(L/K)| = [L:K] \in \{1, p\}$. Insbesondere ist $\operatorname{Gal}(L/K)$ zyklisch. Die letzte Aussage ist klar.
Zu (b): Sei $\operatorname{Gal}(L/K) = \langle\sigma\rangle$ von der Ordnung p. Es gilt $T_{L/K}(-1) = p(-1) = 0$, also gibt es nach der additiven Form von Hilberts Satz 90 ein $x \in L$ mit $x - \sigma(x) = -1$. Es folgt $\sigma(x) = x+1$, allgemeiner $\sigma^i(x) = x+i$, $0 \leqslant i < p$. Es gilt

$$\sigma(x^p - x) = \sigma(x)^p - \sigma(x) = (x+1)^p - (x+1) = x^p + 1 - x - 1 = x^p - x,$$

also $a = x^p - x \in K$. Da $\sigma^i(x)$, $0 \leqslant i < p$, paarweise verschieden sind, folgt $p = [L:K] \geqslant [K(x):K] \geqslant p$, also $L = K(x)$. Das Element x ist Nullstelle des irreduzibeln Polynoms $X^p - X - a$. □

3.8.4 Durch Radikale auflösbare Erweiterungen

Eine endliche Erweiterung $K \subset L$ heiße vom Typ I (Typ II, Typ III respektive), wenn L aus K durch Adjunktion einer Einheitswurzel (einer Nullstelle des Polynoms $X^n - a \in K[X]$ mit $\operatorname{char}(K) \nmid n$, einer Nullstelle eines Polynoms $X^p - X - a \in K[X]$ mit $\operatorname{char}(K) = p > 0$, respektive) entsteht. Die adjungierten Elemente heißen auch Radikale.

Definition 3.8.15. (a) Eine endliche Erweiterung $K \subset M$ heißt Radikalerweiterung, wenn es eine Folge von Zwischenkörpern $K = M_0 \subset M_1 \subset \ldots \subset M_r = M$ gibt, so daß die Erweiterungen $M_i \subset M_{i+1}$ von einem der Typen I,II oder III sind. Offenbar ist dann M/K separabel.

(b) Eine endliche Erweiterung $K \subset L$ heißt durch Radikale auflösbar, wenn es eine Radikalerweiterung $K \subset M$ gibt, mit $L \subset M$.

(c) Eine endliche Erweiterung $K \subset L$ heißt auflösbar, wenn es eine Erweiterung $L \subset M$ gibt, so daß M/K endliche auflösbare Galoiserweiterung ist.

Bemerkung 3.8.16. (a) Eine endliche Galoiserweiterung ist genau dann auflösbar im Sinne dieser Definition, wenn sie auflösbar ist im Sinne von Definition 3.8.9, das heißt, wenn $\operatorname{Gal}(L/K)$ auflösbar ist.

(b) Sei $K \subset L$ endliche separabel Erweiterung und $L \subset L'$ normaler Abschluß von L/K. Die Erweiterung L/K ist genau dann auflösbar, wenn L'/K auflösbare Galoiserweiterung ist.

Beweis. **Zu (a):** Ist $K \subset L$ endliche Galoiserweiterung und gibt es $L \subset M$, so daß M/K endliche auflösbare Galoiserweiterung ist, dann ist $\operatorname{Gal}(L/K)$ isomorph zu einer Faktorgruppe von $\operatorname{Gal}(M/K)$, somit auflösbar. Die umgekehrte Implikation ist klar.
Zu (b): Es ist klar, daß L/K auflösbar ist, wenn L'/K auflösbare Galoiserweiterung ist. Sei umgekehrt L/K auflösbar. Dann gibt es eine Erweiterung $L \subset M$, so daß M/K endliche auflösbare Galoiserweiterung ist. Sei $L \subset L'' \subset M$ der normale Abschluß von L in M. Dann ist L''/K auflösbare Galoiserweiterung nach (a). Da es einen K-Algebrenisomorphismus $L' \to L''$ gibt, ist dann auch L'/K auflösbare Galoiserweiterung. □

Beispiel 3.8.17. Sei $K = \mathbb{Q}(\sqrt[3]{2})(\omega) = \mathbb{Q}(\sqrt[3]{2}, \omega)$ der Zerfällungskörper von $X^3 - 2 \in \mathbb{Q}[X]$, wobei $\omega = e^{\frac{2\pi i}{3}}$. Dann ist $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ Erweiterung vom Typ II und $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\sqrt[3]{2}, \omega)$ vom Typ I. Also ist $K/\mathbb{Q}$ Galois'sche Radikalerweiterung.

Seien $K \subset L$ und $K \subset F$ endliche Körpererweiterungen. Nach dem Fortsetzungssatz 3.2.3 gibt es einen Oberkörper $F \subset N$ und einen Homomorphismus $\psi : L \to N$, so daß das Diagramm

$$\begin{array}{ccc} K & \hookrightarrow & L \\ \downarrow & & \downarrow{\scriptstyle \psi} \\ F & \hookrightarrow & N \end{array}$$

kommutativ ist. Man erhält daraus das Diagramm

$$\begin{array}{ccc} K & \hookrightarrow & \psi(L) \\ \downarrow & & \downarrow \\ F & \hookrightarrow & N \end{array}$$

von Inklusionen. In N kann man das Kompositum $F\psi(L)$ bilden. Dabei wurde also L durch den isomorphen Körper $\psi(L)$ ersetzt.

Lemma 3.8.18. *Seien*

$$\begin{array}{ccc} K & \hookrightarrow & L \\ \downarrow & & \downarrow \\ F & \hookrightarrow & N \end{array}$$

endliche Erweiterungen. Ist L/K Radikalerweiterung (beziehungsweise durch Radikale auflösbar, auflösbare Galoiserweiterung, auflösbare Erweiterung, respektive), dann gilt dies jeweils auch für FL/F.

$$\begin{array}{ccccc} K & \hookrightarrow & L & & \\ \downarrow & & \downarrow & & \\ F & \hookrightarrow & FL & \hookrightarrow & N. \end{array}$$

Beweis. Wir betrachten jeden Erweiterungstyp separat.

(a) Ist $K = L_0 \subset L_1 \subset \ldots \subset L_r = L$ Radikalerweiterung wie in der Definition 3.8.15, dann ist auch $F = FL_0 \subset FL_1 \subset \ldots FL_r = FL$ eine solche.

(b) Sei L/K durch Radikale auflösbar. Dann gibt es eine Erweiterung $L \subset M$, so daß M/K endliche Radikalerweiterung ist. Mithilfe der Vorbemerkung erhält man ein Diagramm

$$\begin{array}{ccccc} K & \hookrightarrow & L & \hookrightarrow & M \\ \downarrow & & \downarrow & & \downarrow \\ F & \hookrightarrow & FL & \hookrightarrow & FM \\ & & \downarrow & & \\ & & N & & \end{array}$$

Nach (a) ist FM/F Radikalerweiterung, also ist FL/F durch Radikale auflösbar.

(c) Sei L/K auflösbare Galoiserweiterung. Nach Satz 3.5.25 ist FL/F endliche Galoiserweiterung und man hat einen Isomorphismus

$$\mathrm{Gal}(FL/F) \to \mathrm{Gal}(L/L \cap F).$$

Als Untergruppe von $\mathrm{Gal}(L/K)$ ist $\mathrm{Gal}(L/L \cap F)$ auflösbar, somit ist auch $\mathrm{Gal}(LF/F)$ auflösbar.

(d) Sei L/K auflösbare Erweiterung. Dann gibt es einen Oberkörper $L \subset M$, so daß M/K endliche Galoiserweiterung ist. Wie in (b) haben wir

$$\begin{array}{ccccc} K & \hookrightarrow & L & \hookrightarrow & M \\ \downarrow & & \downarrow & & \downarrow \\ F & \hookrightarrow & FL & \hookrightarrow & FM \end{array}$$

Nach (c) ist FM/F auflösbare Galoiserweiterung, somit ist FL/F auflösbare Erweiterung.

□

Lemma 3.8.19. *Seien $K \subset E \subset L$ endliche Erweiterungen. Die Erweiterung L/K ist genau dann auflösbar, beziehungsweise durch Radikale auflösbar, wenn E/K und L/E die jeweiligen Eigenschaften haben.*

Beweis. Wir geben zunächst den Beweis für „auflösbar“. Sei L/K auflösbar, $L \subset M$ eine Erweiterung, so daß M/K auflösbare Galoiserweiterung ist, also $K \subset E \subset L \subset M$. Dann ist E/K ebenfalls auflösbar. Als Untergruppe der auflösbaren Gruppe $\mathrm{Gal}(M/K)$ ist $\mathrm{Gal}(M/E)$ auflösbar, also ist M/E auflösbare Galoiserweiterung, somit ist L/E auflösbar.

Umgekehrt nehmen wir nun an, daß E/K und L/E auflösbar sind. Wir haben zu zeigen, daß L/K auflösbar ist.

Wir zeigen zuerst, daß es genügt, dies für auflösbare Galoiserweiterungen E/K und L/E zu tun. Es gibt einen Oberkörper $E \subset E'$, so daß E'/K endliche auflösbare Galoiserweiterung ist. Nach Lemma 3.8.18 ist dann auch $E'L/E'$ auflösbar. Also gibt es einen Oberkörper $E'L \subset L'$, so daß L'/E' endliche auflösbare Galoiserweiterung ist.

$$\begin{array}{ccccc} K & \hookrightarrow & E & \hookrightarrow & L \\ & & \downarrow & & \downarrow \\ & & E' & \hookrightarrow & E'L & \hookrightarrow & L' \end{array}$$

Wenn wir zeigen können, daß L'/K auflösbare Galoiserweiterung ist, dann folgt, daß L/K aufösbar ist.

Seien also jetzt E/K und L/E endliche, auflösbare Galoiserweiterungen Da E/K und L/E separabel sind, ist dann auch L/K separabel. Sei $L \subset M$ normaler Abschluß von L/K. Dann ist M/K endliche Galoiserweiterung. Wir werden zeigen, daß $\mathrm{Gal}(M/K)$ auflösbar ist. Wie wissen aus Satz 3.2.19, daß M von allen $\sigma(M)$, $\sigma \in \mathrm{Alg}_K(L, M)$ erzeugt wird, das heißt, daß M das Kompositum aller $\sigma(L)$, $\sigma \in \mathrm{Alg}_K(L, M)$ ist. Da E/K Galois'sch ist, gilt $\sigma(E) = E$ für alle $\sigma \in \mathrm{Alg}_K(L, M)$.

$$\begin{array}{ccccccc} K & \hookrightarrow & E & \hookrightarrow & L & \hookrightarrow & M \\ \| & & \downarrow{\scriptstyle\sigma} & & \downarrow{\scriptstyle\sigma} & & \\ K & \hookrightarrow & E & \hookrightarrow & \sigma(L) & \hookrightarrow & M \end{array}$$

Jedes σ induziert einen Gruppenisomorphismus von Galoisgruppen

$$\mathrm{Gal}(L/E) \to \mathrm{Gal}(\sigma(L)/\sigma(E)) = \mathrm{Gal}(\sigma(L)/E).$$

Nach Satz 3.5.25 hat man einen injektiven Homomorphismus

$$\mathrm{Gal}(M/E) \to \prod_{\sigma \in \mathrm{Alg}_K(L,M)} \mathrm{Gal}(\sigma(L)/E).$$

Da alle Faktoren des Produkts auflösbar sind, ist das Produkt aufösbar, damit auch $\mathrm{Gal}(M/E)$. Nun ist der Homomorphismus

$$\mathrm{Gal}(M/K) \to \mathrm{Gal}(E/K), \tau \mapsto \tau\big|_E$$

surjektiv mit Kern $\mathrm{Gal}(M/E)$. Da $\mathrm{Gal}(E/K) \cong \mathrm{Gal}(M/K)/\mathrm{Gal}(M/E)$ und $\mathrm{Gal}(M/E)$ auflösbar sind, ist $\mathrm{Gal}(M/K)$ auflösbar.

Nun kommen wir zum Beweis von „durch Radikale auflösbar“. Sei L/K durch Radikale auflösbar. Dann ist offensichtlich auch E/K durch Radikale auflösbar. Ist $L \subset M$ ein Oberkörper, so daß M/K Radikalerweiterung ist, dann ist nach Lemma 3.8.18 auch $E \subset EM = M$ Radikalerweiterung, also ist L/E durch Radikale auflösbar. Seien umgekehrt E/K und L/E durch Radikale auflösbar. Dann gibt es einen Oberkörper $E \subset E'$, so daß E'/K Radikalerweiterung ist.

$$\begin{array}{ccccc} K & \hookrightarrow & E & \hookrightarrow & L \\ & & \downarrow & & \downarrow \\ & & E' & \hookrightarrow & E'L \end{array}$$

Da L/E durch Radikale auflösbar ist, ist nach Lemma 3.8.18 auch $E'L/E'$ durch Radikale auflösbar. Also gibt es einen Oberkörper $E'L \subset L'$, so daß L'/E' Radikalerweiterung ist. Dann ist auch L'/K Radikalerweiterung, somit ist L/K durch Radikale auflösbar. □

Lemma 3.8.20. *Ist $K \subset L$ Erweiterung vom Typ I,II oder III, so ist L/K auflösbar.*

Beweis. **Typ I:** Sei $L = K(\varepsilon)$ mit einer Einheitswurzel ε. Man kann annehmen, daß ε primitive n^{te} Einheitswurzel ist mit $\mathrm{char}(K) \nmid n$. Wir wissen, daß L/K Galoiserweiterung ist und daß $\mathrm{Gal}(L/K)$ isomorph zu einer Untergruppe von $(\mathbb{Z}/(n))^*$ ist. Also ist $\mathrm{Gal}(L/K)$ abelsch, somit auflösbar.

Typ II: Sei $L = K(x)$, wobei x Nullstelle eines Polynoms $X^n - a \in K[X]$ ist mit $\text{char}(K) \nmid n$. Sei $K \subset F$ Zerfällungskörper von $X^n - 1 \in K[X]$. Dann ist FL Zerfällungskörper von $X^n - a$ über F. Da F eine primitive n^{te} Einheitswurzel enthält, ist FL/F zyklische Galoiserweiterung, also auflösbare Galoiserweiterung.

$$\begin{array}{ccc} K & \hookrightarrow & L \\ \downarrow & & \downarrow \\ F & \hookrightarrow & FL \end{array}$$

Da F/K vom Typ I ist, ist FL/K auflösbar, somit mit Lemma 3.8.19 auch L/K.

Typ III: Ist $\text{char}(K) = p > 0$ und $L = K(x)$, wobei x Nullstelle eines Polynoms $X^p - X - a \in K[X]$ ist, dann ist L/K zyklische Galoiserweiterung, also auflösbar. □

Satz 3.8.21 (Abel, Ruffini)**.** *Eine endliche Körpererweiterung $K \subset L$ ist genau dann durch Radikale auflösbar, wenn sie auflösbar ist.*

Beweis. Sei L/K durch Radikale auflösbar. Es gibt also eine Folge von Erweiterungen,

$$K = M_0 \subset M_1 \subset \ldots \subset M_r = M,$$

so daß jede Erweiterung $M_i \subset M_{i+1}$vom Typ I,II oder III ist, $0 \leqslant i < r$, mit $L \subset M$. Nach Lemma 3.8.20 sind alle $M_i \subset M_{i+1}$, $0 \leqslant i < r$ auflösbar. Nach Lemma 3.8.19 sind dann M/K und L/K auflösbar.

Sei umgekehrt L/K auflösbar. Da L in einer endlichen auflösbaren Galoiserweiterung enthalten ist und es genügt die Auflösbarkeit durch Radikale für diese zu beweisen, können wir von vornherein annehmen, daß L/K Galois'sch ist. Sei m das Produkt aller Primteiler q von $[L : K]$ mit $q \nmid \text{char}(K)$ und sei F der Zerfällungskörper von $X^m - 1 \in K[X]$.

$$\begin{array}{ccc} K & \hookrightarrow & L \\ \downarrow & & \downarrow \\ F & \hookrightarrow & FL \end{array}$$

Wir werden zeigen, daß FL/F Radikalerweierung ist. Da $K \subset F$ vom Typ I ist, ist dann auch FL/K Radikalerweiterung, somit ist L/K durch Radikale auflösbar. Da L/K auflösbare Galoiserweiterung ist, gilt dies nach Lemma 3.8.18 auch für FL/F. Wegen

$$\text{Gal}(FL/F) \cong \text{Gal}(L/L \cap F) \subset \text{Gal}(L/K)$$

gilt $[FL : F] \big| [L : K]$. Da $\text{Gal}(FL/F)$ auflösbar ist, gibt es eine Normalreihe

$$\text{Gal}(FL/F) = H_0 \supset H_1 \supset \ldots \supset H_r = \{e\}$$

so daß $[H_i : H_{i+1}] = p_i$ Primzahl ist, $0 \leqslant i < r$. Sei $N_i = \text{Fix}_{FL}(H_i)$, $0 \leqslant i \leqslant r$. Wir erhalten die Folge

$$F = N_0 \subset N_1 \subset \ldots \subset N_r = FL.$$

Für $0 \leqslant i < r$ ist $H_{i+1} \triangleleft H_i$, also ist $N_i \subset N_{i+1}$ Galoiserweiterung mit

$$[N_{i+1} : N_i] = [H_i : H_{i+1}] = p_i.$$

Wenn $p_i \nmid \text{char}(K)$, dann gilt $p_i \big| [FL : F] \big| [L : K]$, also $p_i \big| m$. Wegen $F \subset N_i$ enthält N_i eine primitive $p_i{}^{\text{te}}$ Einheitswurzel. Nach Satz 3.8.11 gibt es also $a \in N_i$ und eine Nullstelle $x \in N_{i+1}$ des Polynoms $X^{p_i} - a$ mit $N_{i+1} = N_i(x)$. Also ist $N_i \subset N_{i+1}$ vom Typ II. Wenn $p_i = \text{char}(K)$ ist, dann gibt es $a \in N_i$ und eine Nullstelle des Polynoms $X^{p_i} - X - a$ mit $N_{i+1} = N_i(x)$. Also ist $N_i \subset N_{i+1}$ von Typ III. Damit ist gezeigt, daß FL/F Radikalerweiterung ist. Es folgt L/K ist durch Radikale auflösbar. □

Folgerung 3.8.22. *Jede separabel Erweiterung $K \subset L$ vom Grad $\leqslant 4$ ist durch Radikale auflösbar.*

Beweis. Nach dem Satz 3.3.10 vom primitiven Element gibt es $x \in L$ mit $L = K(x)$. Sei $f \in K[X]$ das Minimalpolynom von x und $L \subset L'$ein Zerfällungskörper von f. Dann ist L'/K Galoiserweiterung und $\text{Gal}(L'/K)$ ist isomorph zu einer Untergruppe von $\mathfrak{S}_4$, also auflösbar. Also ist L/K (durch Radikale) auflösbar. □

Folgerung 3.8.23. *Sei $K \subset L$ eine endliche und separabel Erweiterung, $L \subset L'$ ein normaler Abschluß von L/K. Wenn $\mathrm{Gal}(L'/K)$ eine einfache nicht-abelsche Untergruppe enthält, dann ist L/K nicht durch Radikale auflösbar.*

Beweis. Wenn $\mathrm{Gal}(L'/K)$ eine einfache, nicht-abelsche Untergruppe enthält, dann ist $\mathrm{Gal}(L'/K)$ nicht auflösbar, also L'/K nicht auflösbar. Nach Bemerkung 3.8.16 am Anfang dieses Abschnitts ist dann L/K nicht (durch Radikale) auflösbar. □

Definition 3.8.24. Sei $f \in K[X]$ und $K \subset L$ Zerfällungskörper von f. Die Gleichung $f = 0$ ist durch Radikale auflösbar, wenn L/K diese Eigenschaft hat.

Folgerung 3.8.25. *Sei $f \in K[X]$ ein separabels Polynom vom Grad $\leqslant 4$, dann ist die Gleichung $f = 0$ durch Radikale auflösbar.*

Beweis. Die Galoisgruppe $G(f)$ ist isomorph zu einer Untergruppe von $\mathfrak{S}_4$, damit auflösbar. □

Folgerung 3.8.26. *Sei K ein Körper und $f \in K[X]$ ein separabels Polynom. Wenn die Galoisgruppe $G(f)$ eine zu einer der Gruppen A_n, $n \geqslant 5$, isomorphen Untergruppe enthält, dann ist die Gleichung $f = 0$ nicht durch Radikale auflösbar. Ist insbesondere $F = X^n + U_1X^{n-1} + \ldots + U_{n-1}X + U_n \in K(U_1, \ldots, U_n)[X]$ das allgemeine Polynom n^{ten} Grades, dann ist die Gleichung $F = 0$ für $n \geqslant 5$ nicht durch Radikale auflösbar.*

Beweis. Da die A_n, $n \geqslant 5$, nicht auflösbar sind, kann im ersten Fall $G(f)$ nicht auflösbar sein. Im zweiten Fall ist $G(F) \cong \mathfrak{S}_n$. □

Beispiel* 3.8.27. Sei L/K eine nichttriviale endliche Galoiserweiterung mit auflösbarer Galoisgruppe. Zeigen Sie, daß es einen Zwischenkörper $K \subset E \subset L$ gibt, so daß E/K Galois'sch mit abelscher Galoisgruppe ist.

Beispiel* 3.8.28. Sei L/K eine endliche Galoiserweiterung vom Grad 105. Ist L/K auflösbar? Man gebe ein Beipiel einer solchen Erweiterung an.

3.8.5 Beispiele

Das erste Beispiel betrachtet quadratische Erweiterungen. Sei k ein Körper mit Charakteristik $\mathrm{char}(k) \neq 2$, sei $K = k(U_1, U_2)$ der rationale Funktionenkörper in den Unbestimmten U_1, U_2 über k. Sei $F = X^2 + U_1X + U_2 \in K[X]$ das allgemeine quadratische Polynom, $K \subset L$ Zerfällungskörper von F, $x_1, x_2 \in L$ die Nullstellen von F. Dann ist $F = (X - x_1)(X - x_2)$, also $-U_1 = x_1 + x_2$ und $U_2 = x_1x_2$. Sei $\delta = x_1 - x_2$, $D = \delta^2 = (x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1x_2 = U_1^2 - 4U_2$. Die Galoisgruppe von F ist $\mathfrak{S}_2$, also ist $\delta \notin K$, also gilt $L = K(\delta)$. Es gilt $\delta - U_1 = 2x_1$, also

$$\begin{aligned} x_1 &= \frac{1}{2}(-U_1 + \delta) \\ x_2 &= x_1 - \delta = \frac{1}{2}(-U_1 - \delta) \end{aligned}$$

Schreibt man noch $\delta = \sqrt{D}$, dann erhält man

$$\begin{aligned} x_1 &= \frac{1}{2}(-U_1 + \sqrt{D}) \\ x_2 &= \frac{1}{2}(-U_1 - \sqrt{D}) \end{aligned}$$

Das zweite Beispiel betrachtet kubische Erweiterungen. Seien k ein Körper mit Charakteristik $\mathrm{char}(k) \neq 2, 3$, und $K = k(U_1, U_2, U_3)$ der rationale Funktionenkörper in den Unbestimmten U_1, U_2, U_3 über k, $F = X^3 + U_1X^2 + U_2X + U_3 \in K[X]$ das allgemeine kubische Polynom, $K \subset L$ Zerfällungkörper von$F$ und $x_1, x_2, x_3 \in L$ die Nullstellen. Sei $Y = X + \frac{1}{3}U_1$ (genannt Tschrinhaustransformation), dann ist

$$\begin{aligned} F(X) &= (Y - \frac{1}{3}U_1)^3 + U_1(Y - \frac{1}{3}U_1)^2 + U_2(Y - \frac{1}{3}U_1) + U_3 \\ &= Y^3 - 3Y^2\frac{1}{3}U_1 + 3Y\frac{1}{9}U_1^2 - \frac{1}{27}U_1^3 + Y^2U_1 - \frac{2}{3}YU_1^2 + \frac{1}{9}U_1^3 + YU_2 - \frac{1}{3}U_1U_2 + U_3 \\ &= Y^3 + (-\frac{1}{3}U_1^2 + U_2)Y + (\frac{2}{27}U_1^3 - \frac{1}{3}U_1U_2 + U_3) \\ &=: Y^3 + pY + q =: g(Y) \end{aligned}$$

Die Nullstellen von g sind $y_i = x_i + \frac{1}{3}U_1$, $1 \leqslant i \leqslant 3$. Es gilt $y_1 + y_2 + y_3 = 0$, und F und g haben dieselbe Diskriminante $D = -4p^3 - 27q^2$, denn

$$D = \prod_{i<j}(x_i - x_j)^2 = \prod_{i<j}(y_i - y_j)^2.$$

Es gilt $L = K(x_1, x_2, x_3) = K(y_1, y_2, y_3)$, das heißt F und g haben denselben Zerfällungskörper. Also haben sie auch dieselbe Galoisgruppe, nämlich $\mathfrak{S}_3$. Wir wissen, daß der Fixkörper von A_3 gleich $K(\delta)$ ist, wobei $\delta = \prod_{i<j}(x_i - x_j) = \prod_{i<j}(y_i - y_j)$.

Sei $L \subset L'$ der Zerfällungskörper des Polynoms $X^3 - 1 \in L[X]$, sei $\varepsilon = \frac{1}{2}(-1+\sqrt{-3}) \in L'$ eine primitive dritte Einheitswurzel. Es gilt

$$\begin{aligned} \varepsilon^2 &= \varepsilon^{-1} \\ \varepsilon + \varepsilon^2 &= -1 \\ \varepsilon - \varepsilon^2 &= \sqrt{-3} \end{aligned}$$

Wir betrachten folgende sogenannte Lagrange'sche Resolventen:

$$z_1 = y_1 + \varepsilon y_2 + \varepsilon^2 y_3 \quad \text{und} \quad z_2 = y_1 + \varepsilon^2 y_2 + \varepsilon y_3,$$

wofür gilt

$$z_1 z_2 = \sum_{i=1}^{3} y_i^2 - \sum_{i<j} y_i y_j = (\sum_{i=1}^{3} y_i)^2 - 3\sum_{i<j} y_i y_j = -3p.$$

Ferner gilt:

$$z_1^3 = \sum_{i=1}^{3} y_i^3 + 3\varepsilon(y_1^2 y_2 + y_2^2 y_3 + y_3^2 y_1) + 3\varepsilon^2(y_1 y_2^2 + y_2 y_3^2 + y_3 y_1^2) + 6y_1 y_2 y_3 = \sum_{i=1}^{3} y_i^3 + 3\varepsilon s + 3\varepsilon^2 t + 6(-q).$$

Die entsprechende Formel für z_2^3 erhält man durch Vertauschen von ε und ε^2. Es gilt

$$\delta = (y_1 - y_2)(y_2 - y_3)(y_1 - y_3) = y_1^2 y_2 + y_2^2 y_3 + y_3^2 y_1 - (y_1 y_2^2 + y_2 y_3^2 + y_3 y_1^2) = s - t = u - 2t,$$

wobei $s + t = u$ ist. Damit berechnen wir

$$\varepsilon s + \varepsilon^2 t = \varepsilon(s + t) + (\varepsilon^2 - \varepsilon)t = \frac{1}{2}(-1 + \sqrt{-3})u - \sqrt{-3}t = \frac{-u}{2} + \frac{\sqrt{-3}}{2}(u - 2t) = -\frac{u}{2} + \frac{\sqrt{-3}}{2}\delta$$

Und weiter

$$0 = (y_1 + y_2 + y_3)(y_1 y_2 + y_2 y_3 + y_3 y_1) = u - 3q$$

also $u = 3q$, damit

$$0 = (y_1 + y_2 + y_3)^3 = \sum_{i=1}^{3} y_i^3 + 3u - 6q = \sum_{i=1}^{3} y_i^3 + 3q$$

also $\sum_{i=1}^{3} y_i^3 = -3q$. Es folgt

$$\begin{aligned} z_1^3 &= -3q + 3(\varepsilon s + \varepsilon^2 t) - 6q = -9q + 3(-\frac{3q}{2} + \frac{\sqrt{-3}}{2}\delta) = -\frac{27}{2}q + \frac{3\sqrt{-3}}{2}\delta \\ z_2^3 &= -\frac{27}{2}q - \frac{3\sqrt{-3}}{2}\delta \end{aligned}$$

also

$$\begin{aligned} z_1 &= \sqrt[3]{-\frac{27}{2}q + \frac{3\sqrt{-3}}{2}\delta} \\ z_2 &= \sqrt[3]{-\frac{27}{2}q - \frac{3\sqrt{-3}}{2}\delta}, \end{aligned}$$

wobei die dritten Wurzeln geeignet zu wählen sind, insbesondere muß $z_1 z_2 = -3p$ gelten. Schreibt man noch $\delta = \sqrt{D}$, so hat man

$$\begin{aligned} z_1 &= \sqrt[3]{-\frac{27}{2}q + \frac{3}{2}\sqrt{-3D}} \\ z_2 &= \sqrt[3]{-\frac{27}{2}q - \frac{3}{2}\sqrt{-3D}}. \end{aligned}$$

Wegen $\varepsilon + \varepsilon^2 = -1$ folgt

$$\begin{aligned} y_1 &= \frac{1}{3}(z_1 + z_2) \\ y_2 &= \frac{1}{3}(\varepsilon^2 z_1 + \varepsilon z_2) \\ y_3 &= \frac{1}{3}(\varepsilon z_1 + \varepsilon^2 z_2) \end{aligned}$$

(Formeln von Cardano)

3.8.6 Konstruktionen mit Zirkel und Lineal

Sei $M \subset \mathbb{R}^2$ eine Menge mit mindestens zwei Punkten, $g(M)$ die Menge aller Geraden durch zwei verschiedenen Punkte in M, $k(M)$ die Menge aller Kreise, deren Mittelpunkte in M liegen und deren Radius jeweils die Abstände zweier Punkte in M sind. Mit folgenden Operationen werden aus Punkten in M Punkte in $\mathbb{R}^2$ konstruiert:

(S1) Schnitt zweier verschiedener Geraden in $g(M)$.

(S2) Schnitt einer Geraden in $g(M)$ mit einem Kreis in $k(M)$.

(S3) Schnitt zweier verschiedener Kreise.

Die Menge der aus M konstruierten Punkte sei M'. Offenbar gilt $M \subset M'$. Wir setzen induktiv

$$\begin{aligned} M_0 &= M \\ M_1 &= M' \\ &\vdots \\ M_{n+1} &= (M_n)' \\ \hat{M} &= \bigcup_{n \geqslant 0} M_n \end{aligned}$$

Die Punkte aus $\hat{M}$ heißen (mit Zirkel und Lineal) konstruiert. Jeder Punkt aus $\hat{M}$ kann durch endlich viele Operationen (S1), (S2), (S3) aus M erhalten werden. Es gilt $(\hat{M})' = \hat{M}$, denn ist $p \in (\hat{M})'$, so kann P aus endlich vielen Punkten in $\hat{M}$ konstituiert werden, diese liegen in M_n für $n \geqslant 0$ groß genug, also gilt $P \in M_n' = M_{n+1} \subset \hat{M}$.

Wir sehen jetzt $\mathbb{R}^2$ als $\mathbb{C}$ an. Für $M \subset \mathbb{C}$ sei $\overline{M} = \{\overline{z} \in \mathbb{C} \mid z \in M\}$.

Satz 3.8.29. *Sei $M \subset \mathbb{C}$ mit $0, 1 \in M$.*

(a) Die Menge $\hat{M}$ ist der kleinste Unterkörper von $\mathbb{C}$ mit folgenden Eigenschaften:

$$M \subset \hat{M}, \qquad \overline{\hat{M}} = \hat{M}, \qquad \forall z \in \mathbb{C} : z^2 \in \hat{M} \Rightarrow z \in \hat{M}.$$

(b) Der Körper $K = \mathbb{Q}(M \cup \overline{M})$ ist Unterkörper von $\hat{M}$ und $K = \overline{K}$.

Beweis. Wir zeigen zunächst, daß $\hat{M}$ Unterkörper von $\mathbb{C}$ ist. Seien $z_1, z_2 \in \hat{M}$. Wir zeigen, daß $z_1 \pm z_2$, $z_1 \cdot z_2$ und z_1^{-1}, falls $z_1 \neq 0$, konstruierbar sind; dann gilt $z_1 \pm z_2, z_1 \cdot z_2, z_1^{-1} \in \hat{M}$, falls $z_1 \neq 0$. Das Element $z_1 + z_2$ ist allein mit dem Zirkel konstruierbar. Zu z_2 ist offenbar $-z_2$ konstruierbar. Also ist $z_1 - z_2$ konstruierbar.

Um zu zeigen, daß $z_1 \cdot z_2$ konstruierbar ist, bemerken wir zunächst, daß für $g \in g(\hat{M})$ und $z \in g \cap \hat{M}$ die zu g orthogonale Gerade g' durch z in $g(\hat{M})$ liegt. Für positive $r_1, r_2 \in \hat{M} \cap \mathbb{R}$ ist $r_1 \cdot r_2$ konstruierbar. Seien nun $z_k = r_k(\cos\varphi_k + i\sin\varphi_k)$, $k = 1, 2$, mit $0 \leqslant \varphi_1, \varphi_2 < 2\pi$, $r_1, r_2 > 0$. Dann ist

$$z_1 z_2 = r_1 r_2(\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2)).$$

Die Punkte r_1 und r_2 sind konstruierbar, also ist $r_1 \cdot r_2$ konstruierbar. Der Winkel $\varphi_1 + \varphi_2$ ist konstruierbar. Also ist $z_1 \cdot z_2$ konstruierbar.

Zeigen wir nun, daß z_1^{-1} für $z_1 \neq 0$ konstruierbar ist. Es gilt $z_1^{-1} = r_1^{-1}(\cos(-\varphi_1)) + i\sin(-\varphi_1)$. Da r_1^{-1} und $-\varphi_1$ konstruierbar sind, ist z_1^{-1} konstruierbar.

Die ersten beiden charakterisierenden Eigenschaften sieht man leicht wie folgt: Wir wissen, daß $M \subset \hat{M}$ ist. Zu $z \in \hat{M}$ ist $\overline{z}$ konstruierbar. Es folgt $\overline{\hat{M}} \subset \hat{M}$, also $\hat{M} \subset \overline{\hat{M}}$, und damit Gleichheit. Offenbar gilt $K = \mathbb{Q}(M \cup \overline{M}) \subset \hat{M}$. Wegen $M \cup \overline{M} \subset K$, gilt $M \cup \overline{M} \subset \overline{K}$. Da $\overline{K}$ ebenfalls Unterkörper von $\mathbb{C}$ ist, folgt $K = \mathbb{Q}(M \cup \overline{M}) \subset \overline{K}$ und $K = \overline{K}$. Dies ist die Aussage (b).

Für die dritte charakterisierende Eigenschaft, sei nun $0 \neq z = r(\cos\varphi + i\sin\varphi)$ mit $r > 0$, $0 \leqslant \varphi < 2\pi$ und $z^2 = r^2(\cos(2\varphi) + i\sin(2\varphi)) \in \overline{M}$. Zu zeigen ist, daß z konstruierbar ist. Der Winkel φ ist konstruierbar. Um zu zeigen, daß r konstruierbar ist, können wir annehmen, daß $r^2 > 1$, andernfalls ersetze man r durch nr mit geeignetem n. Der Punkt $1 + iy$ auf dem Kreis $|z - \frac{r^2}{2}| = \frac{r^2}{2}$ mit Radius $\frac{r^2}{2}$ um den Punkt $\frac{r^2}{2}$ ist offensichtlich konstruierbar. Man erhält also ein rechtwinkliges Dreieck mit Katheten der Längen 1 und y und Hypotenuse $x = \sqrt{1 + y^2}$. Es gilt $|1 + iy - \frac{r^2}{2}| = \frac{r^2}{2}$ genau dann, wenn $(1 - \frac{r^2}{2})^2 + y^2 = \frac{r^4}{4}$. Und dies gilt, genau dann, wenn $(1 - r^2 + y^2) = 0$, genau dann, wenn $x = r$.

Es bleibt die Minimalität von $\hat{M}$ in (a) zu zeigen. Zur Vorbereitung beweisen wir folgendes

Lemma. *Ist $L \subset \mathbb{C}$ ein Unterkörper mit $i \in L$ und $\overline{L} = L$, so gilt*

(i) Ist $z \in \mathbb{C}$ Schnittpunkt zweier verschiedener Geraden in $g(L)$, dann liegt z in L.

(ii) Ist $z \in \mathbb{C}$ Schnittpunkt einer Geraden in $g(L)$ und eines Kreises in $k(L)$, oder zweier verschiedener Kreise in $k(L)$, so existiert $w \in \mathbb{C}$ mit $w^2 \in L$ und $z \in L(w)$.

Beweis hierzu. Wir bemerken zuerst: Ist $z = x + iy \in L$ mit $x, y \in \mathbb{R}$, dann gilt $x, y \in L$, denn $x = \frac{1}{2}(z + \overline{z})$ und $y = \frac{1}{2i}(z - \overline{z})$. Sei nun z Schnittpunkt zweier verschiedener Geraden $g = \{z_0 + \lambda z_1 \mid \lambda \in \mathbb{R}\}$ und $g' = \{z_0' + \mu z_1' \mid \mu \in \mathbb{R}\}$, mit $z_0, z_0', z_1, z_1' \in L$ und $z_k = x_k + iy_k$, $z_k' = x_k' + iy_k'$, $k = 0, 1$. Dann ist z bestimmt durch die Gleichung $z_0 + \lambda z_1 = z_0' + \mu z_1'$, das heißt durch die Gleichungen

$$\begin{aligned} x_0 + \lambda x_1 &= x_0' + \mu x_1' \\ y_0 + \lambda y_1 &= y_0' + \mu y_1' \end{aligned}$$

Als Matrixgleichung

$$\begin{pmatrix} x_1 & x_1' \\ y_1 & y_1' \end{pmatrix} \begin{pmatrix} \lambda \\ \mu \end{pmatrix} = \begin{pmatrix} x_0' - x_0 \\ y_0' - y_0 \end{pmatrix}.$$

Die Koeffizienten dieses Systems liegen alle in L und es gilt $\det \begin{pmatrix} x_1 & x_1' \\ y_1 & y_1' \end{pmatrix} \neq 0$: Also liegen λ und μ in L, somit auch z.

Sei jetzt z Schnittpunkt von $\{z_0 + \lambda z_1 \mid \lambda \in \mathbb{R}\}$ mit $z_1 \neq 0$ und dem Kreis um z_2 mit Radius $r > 0$, wobei $z_0, z_1, z_2, r \in L$.

Es gibt $\lambda \in \mathbb{R}$ mit $z = z_0 + \lambda z_1$ und $|z_2 - z|^2 = r^2$, das heißt $|z_0 + \lambda z_1 - z_2|^2 = r^2$, äquivalent zu $|\lambda + \frac{-z_2 + z_0}{z_1}|^2 = \left(\frac{r}{|z_1|}\right)^2$, das heißt $(\lambda + x)^2 + y = \left(\frac{r}{|z_1|}\right)^2$, wobei $\frac{z_0 - z_2}{z_1} = x + iy$ ist mit $x, y \in \mathbb{R}$. Es gibt $w \in \mathbb{C}$ mit $w^2 = \left(\frac{r}{|z_1|}\right)^2 - y^2$. Dafür gilt $\lambda + x = \pm w$. Es folgt $\lambda \in L(w)$, also $z = z_0 + \lambda z_1 \in L(w)$.

Sei schließlich z Schnittpunkt von zwei verschiedenen Kreisen, das heißt, es genügt den Gleichungen $|z - z_0|^2 = r_0^2$, $|z - z_1|^2 = r_1^2$ mit $z_0, z_1, r_0, r_1 \in L$ und $z_1 \neq z_0$. Seien $z = x + iy$, $z_k = x_k + iy_k$, $k \in \{0, 1\}$. Dann haben wir

$$\begin{aligned} (x - x_0)^2 + (y - y_0)^2 &= r_0^2 \\ (x - x_1)^2 + (y - y_1)^2 &= r_1^2. \end{aligned}$$

Subtraktion ergibt die Geradengleichung

$$x\lambda(x_1 - x_0) + y\lambda(y_1 - y_0) = r_0^2 - r_1^2 + x_1^2 - x_0^2 + y_1^2 - y_0^2,$$

wobei $(x_1 - x_0, y_1 - y_0) \neq (0, 0)$ ist und alle Koeffizienten in L liegen. Die Behauptung folgt nun aus dem vorhergehenden Fall. □

Nun zur Minimalität von $\hat{M}$. Sei L ein Unterkörper von $\mathbb{C}$ mit $M \subset L$, $\overline{L} = L$ und für alle $z \in \mathbb{C}$ mit $z^2 \in L$ folge $z \in L$. Wir zeigen $\hat{M} \subset L$: Es gilt $M_0 = M \subset L$ nach Voraussetzung, wegen $i^2 = -1 \in L$ folgt $i \in L$. Also gelten die Aussagen (i) und (ii) aus dem Lemma für L. Wir nehmen an $M_n \subset L$ für ein $n \geqslant 0$ und zeigen $M_{n+1} \subset L$. Damit wird $\hat{M} \subset L$ gezeigt sein. Sei $z \in M_{n+1}$. Dann entsteht z durch eine der Operationen (S1), (S2), (S3) aus M_n. Ist z Schnittpunkt zweier verschiedener Geraden in $g(M_n) \subset g(L)$, dann gilt $z \in L$ nach dem Lemma. Ist z Schnittpunkt einer Geraden in $g(M_n) \subset g(L)$ mit einem Kreis in $k(M_n) \subset k(L)$, oder zweier verschiedener Kreise in $k(M_n) \subset k(L)$, so gibt es nach dem Lemma ein $w \in \mathbb{C}$ mit $w^2 \in L$ und $z \in L(w)$. Aus der Voraussetzung für L folgt $w \in L$, also $z \in L$. □

Im nächsten Satz seien alle Körper Unterkörper von $\mathbb{C}$.

Satz 3.8.30. *Sei $M \subset \mathbb{C}$ mit $0, 1 \in M$ und $K = \mathbb{Q}(M, \overline{M})$. Für einen Punkt $z \in \mathbb{C}$ sind folgende Aussagen äquivalent:*

(a) Es ist $z \in \hat{M}$, das heißt z ist aus M (mit Zirkel und Lineal) konstruierbar.

(b) Es gibt eine Folge von Erweiterungen $K = L_0 \subset L_1 \subset \ldots \subset L_r = L$, $r \in \mathbb{N}_0$, und $w_i \in L_i$ mit $w_i^2 \in L_{i-1}$ und $L_i = L_{i-1}(w_i)$ für $1 \leqslant i \leqslant r$, so daß $z \in L$ ist.

(c) Das Element z ist algebraisch über K und die Galoisgruppe des Minimalpolynoms $f \in K[X]$ von z ist eine 2-Gruppe.

Eine Erweiterung wie in (b) heißt der Kürze halber spezielle Radikalerweiterung.

Beweis. **[(a) ⇒ (b)]** Sei E die Menge aller $z \in \mathbb{C}$, die der Bedingung (b) genügen. Wir werden $\hat{M} \subset E$ zeigen, indem wir zeigen, daß E Unterkörper von $\mathbb{C}$ ist mit $M \subset E$, $E = \overline{E}$, und so daß für alle $z \in \mathbb{C}$ mit $z^2 \in E$ bereits $z \in E$ gilt.
Offenbar ist $K \subset E$, insbesondere also $M \subset E$. Nun zeigen wir, daß E Unterkörper von $\mathbb{C}$ ist: Seien $z_1, z_2 \in E$, seien $K \subset L_i$, $i = 1, 2$, spezielle Radikalerweiterungen mit $z_i \in L_i$. Dann ist L_1L_2 spezielle Radikalerweiterung (siehe Lemma 3.8.18), und es gilt $z_1 \pm z_2 \in L_1L_2$. Offenbar gilt $z_1^{-1} \in L_1$ falls $z_1 \neq 0$. Nun zeigen wir $E = \overline{E}$: Sei $z \in E$, $K \subset L$ spezielle Radikalerweiterung mit $z \in L$. Dann ist $K = \overline{K} \subset \overline{L}$ ebenfalls spezielle Radikalerweiterung und es gilt $\overline{z} \subset \overline{L}$. Es folgt $\overline{z} \in E$. Also haben wir $\overline{E} \subset E$, damit $E = \overline{E}$. Sei schließlich $z \in \mathbb{C}$ mit $z^2 \in E$. Dann gibt es eine spezielle Radikalerweiterung $K \subset L$ mit $z^2 \in L$. Dann ist $K \subset L \subset L(z)$ spezielle Radikalerweiterung mit $z \in L(z)$, folglich gilt $z \in E$:

[(b) ⇒ (c)] Sei $K \subset L$ spezielle Radikalerweiterung mit $z \in L$. Sei $L \subset L'$ normaler Abschluß von L/K. Die Erweiterung L'/K ist dann Galois'sch. Da L' Kompositum der $\sigma(L)$, $\sigma \in \mathrm{Alg}_K(L, L')$ ist, ist auch L'/K spezielle Radikalerweiterung. Es folgt, daß $\mathrm{Gal}(L'/K)$ eine 2-Gruppe ist. Offenbar ist das Element z algebraisch über K. Sei $f \in K[X]$ sein Minimalpolynom und F Zerfällungskörper von f mit $F \subset L'$.

Da $G(f) = \mathrm{Gal}(F/K)$ zu einer Faktorgruppe von $\mathrm{Gal}(L'/K)$ isomorph ist, ist $G(f)$ ebenfalls eine 2-Gruppe.

[(c) ⇒ (a)] Sei f Minimalpolynom von z, F ein Zerfällungskörper von f und $G = G(f) = \mathrm{Gal}(F/K)$ sei 2-Gruppe. Es gibt eine Normalreihe $G = H_0 \supset H_1 \supset \ldots \supset H_r = \{e\}$ mit $[H_i : H_{i+1}] = 2$ für $0 \leqslant i < r$. Sei $F_i = \mathrm{Fix}_F(H_i)$, $0 \leqslant i \leqslant r$. Man erhält so eine Folge $K = F_0 \subset F_1 \subset \ldots \subset F_r = F$ in der $F_{i-1} \subset F_i$ Galois'sch vom Grad 2 ist. Es gibt $w_i \in F_i$ mit $w_i^2 \in F_{i-1}$ und $F_i = F_{i-1}(w_i)$, $1 \leqslant i \leqslant r$. Wegen $w_1^2 \in K = F_0 \subset \hat{M}$ folgt $w_1 \in \hat{M}$, also $F_1 = F_0(w_1) \subset \hat{M}$. Induktiv folgt $F_r = F \subset \hat{M}$, somit $z \in \hat{M}$. □

Einige Beispiele

Würfelverdopplung 3.8.31. *Gegeben sei ein Würfel der Kantenlänge $a > 0$. Ist ein Würfel doppelten Inhalts, nämlich $2a^3$, aus a mit Zirkel und Lineal konstruierbar?*

Sei speziell $a = 1$, ist $\sqrt[3]{2}$ aus $M = \{0, 1\}$ konstruierbar? Es gilt $K = \mathbb{Q}(M \cup \overline{M}) = \mathbb{Q}$. Das Minimalpolynom von $\sqrt[3]{2}$ über $\mathbb{Q}$ ist $f = X^3 - 2$, es gilt $G(f) \cong \mathfrak{S}_3$. Da $\mathfrak{S}_3$ keine Zweigruppe ist, ist $\sqrt[3]{2}$ nicht aus M konstruierbar. □

Winkeldreiteilung 3.8.32. *Gegeben ist ein Winkel φ. Ist $\frac{\varphi}{3}$ mit Zirkel und Lineal konstruierbar? Genauer: Ist $z = e^{i\frac{\varphi}{3}}$ aus $\{0, 1, w = e^{i\varphi}\}$ konstruierbar?*

Wir betrachten speziell $\varphi = \frac{\pi}{3}$, das heißt $w = e^{i\frac{\pi}{3}} = e^{2\pi i\frac{1}{6}} = \frac{1}{2}(1 + i\sqrt{-3})$. Sei $z = e^{i\frac{\pi}{9}} = x + iy$ mit $x = \cos\frac{\pi}{9}$ und $y = \sin\frac{\pi}{9}$. Der Punkt z ist genau dann konstruierbar, wenn x, y kontruierbar sind. Es gilt

$$w = z^3 = x^3 - 3xy^2 + (3x^2y - y^3)i = x^3 - 3x(1 - x^2) + (3(1 - y^2)y - y^3)i = 4x^3 - 3x + (3y - 4y^3)i.$$

Es folgt $4x^3 - 3x - \frac{1}{2} = 0$, also $(2x)^3 - 3(2x) - 1 = 0$. Das Polynom $X^3 - 3X - 1 \in \mathbb{Q}[X]$ ist irreduzibel, also hat $2x$ den Grad 3 über $\mathbb{Q}$. Damit sind $2x$, x und z nicht konstruierbar. □

Quadratur des Kreises 3.8.33. *Sei $a > 0$. Kann man ein Quadrat konstruieren, dessen Fläche gleich der Kreisfläche $a^2\pi$ ist?*

Sei speziell $a = 1$. Die Frage ist dann, ob $\sqrt{\pi}$ konstruierbar ist. Wäre das der Fall, so wäre auch π konstruierbar, insbesondere algebraisch über $K = \mathbb{Q}$. Aber π ist transzendent. □

Reguläres n-Eck 3.8.34. *Sei $M = \{0, 1\}$. Ist $z_n = e^{\frac{2\pi i}{n}}$, $n \in \mathbb{N}$, aus M konstruierbar?*

In diesem Fall ist $K = \mathbb{Q}$, das Minimalpolynom von z_n ist ϕ_n, die Galoisgruppe von ϕ_n ist isomorph zu $(\mathbb{Z}/(n))^*$. Also ist z_n genau dann konstruierbar, wenn $\varphi(n)$ Potenz von 2 ist. Ist p Primzahl, so gilt $\varphi(n) = p - 1$. Also ist z_p genau dann konstruierbar, wenn $p - 1$ Potenz von 2 ist.

Proposition. *Ist $2^m + 1$ Primzahl, wobei $m \in \mathbb{N}$ ist, dann gibt es $k \in \mathbb{N}$ mit $m = 2^k$.*

Beweis. Ist $m = ql$ mit $q = 2^k$, $k \in \mathbb{N}_0$, und $l > 2$ ungerade. Dann gilt

$$2^m + 1 = 2^{ql} + 1 = (2^q + 1)(2^{q(l-1)} - 2^{q(l-2)} + \ldots - 2^q + 1)$$

und es gilt $1 < 2^q + 1 < 2^m + 1$. Also ist $2^m + 1$ nicht prim. □

Für $k \in \mathbb{N}_0$ heißt $F_k = 2^{2^k} + 1$ die k-te Fermat'sche Zahl. Fermat'sche Primzahlen sind

$$\begin{aligned} F_0 &= 3 \\ F_1 &= 5 \\ F_2 &= 17 \\ F_3 &= 257 \\ F_4 &= 65537 \end{aligned}$$

Man kennt keine weiteren.

Es folgt, daß z_p konstruierbar ist, wenn p Fermat'sche Primzahl ist. Allgemeiner gilt:

Satz 3.8.35 (Gauß)**.** *Sei $n \in \mathbb{N}$, $n > 2$. Folgende Aussagen sind äquivalent:*

(a) Der Punkt z_n ist konstruierbar.

(b) Die Euler'sche Zahl $\varphi(n)$ ist Potenz von 2.

(c) Es gibt $m \in \mathbb{N}_0$ und Fermat'sche Primzahlen $p_1 < \ldots < p_r$, $r \in \mathbb{N}_0$, mit $n = 2^m p_1 \cdots p_r$.

Beweis. Die Äquivalenz **„(a) ⇔ (b)“** hatten wir bereits oben gesehen. Für die Äquivalenz **„(b) ⇔ (c)“** sei $n = 2^m p_1^{\nu_1} \cdots p_r^{\nu_r}$ mit $m, r \in \mathbb{N}_0$, Primzahlen $p_1, \ldots, p_r$ und $\nu_1, \ldots, \nu_r \in \mathbb{N}$. Dann ist

$$\varphi(n) = e(p_1 - 1)p_1^{\nu_1 - 1} \cdots (p_r - 1)p_r^{\nu_r - 1} \quad \text{mit } e = \begin{cases} 1 & \text{falls } m = 0 \\ 2^{m-1} & \text{falls } m \geqslant 1 \end{cases}$$

Das heißt $\varphi(n)$ ist Potenz von 2 genau dann, wenn $\nu_1 = \ldots = \nu_r = 1$ und $p_1 - 1, \ldots, p_r - 1$ Potenzen von 2 sind, das heißt, wenn $\nu_1, \ldots, \nu_r = 1$ und $p_1, \ldots, p_r$ Fermat'sche Primzahlen sind. □

Beispiel* 3.8.36. Ist $z_{2017} = e^{\frac{2\pi i}{2017}}$ mit Zirkel und Lineal konstruierbar?

3.9 Der Hauptsatz über elementarsymmetrische Polynome

3.9.1 Basen in Algebren

Sei $\varphi : R \to T$ ein Homomorphismus zwischen kommutativen Ringen. Dann ist T eine R-Algebra und man hat auf T eine Skalarmultiplikation

$$r.t = \varphi(r)t \quad \text{für } r \in R, t \in T.$$

Eine Familie $(t_i)_{i\in I}$ von Elementen in T heißt Erzeugendensystem von T über R, wenn es zu jedem $t \in T$ eine Familie $(r_i)_{i\in I}$ von Elementen in R, $r_i = 0$ für fast alle $i \in I$ gibt mit $t = \sum_{i\in I} r_i t_i$. Die Familie $(t_i)_{i\in I}$ heißt frei oder linear unabhängig über R, wenn für jede Familie $(r_i)_{i\in I}$ von Elementen in R, $r_i = 0$ für fast alle $i \in I$, mit $\sum_{i\in I} r_i t_i = 0$ gilt $r_i = 0$ für alle $i \in I$. Die Familie $(t_i)_{i\in I}$ heißt Basis von T über R, wenn sie freies Erzeugendensystem ist.

Beispiel 3.9.1. Sei $T = R[X_1, \ldots, X_n]$ der Polynomring in n Unbestimmten. Dann ist die Familie der Monome $X_1^{a_1} \cdots X_n^{a_n}$, $(a_1, \ldots, a_n) \in \mathbb{N}_0^n$ eine Basis von T über R.

Eine Familie $t_1, \ldots, t_n \in T$ heißt linear unabhängig über R, wenn der Homomorphismus

$$R[X_1, \ldots, X_n] \to T, f \mapsto f(t_1, \ldots, t_n)$$

injektiv ist.

3.9.2 Der Hauptsatz über elementarsymmetrische Polynome

Sei $R \neq 0$ ein kommutativer Ring, $n \in \mathbb{N}$ und $R[X_1, \ldots, X_n]$ der Polynomring in n Unbestimmten über R. Für $\sigma \in \mathfrak{S}_n$ ist

$$\varphi_\sigma : R[X_1, \ldots, X_n] \to R[X_1, \ldots, X_n], f \mapsto f(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$$

ein R-Algebrenautomorphismus. Man setzt $\sigma f = \varphi_\sigma(f)$.

Definition 3.9.2. Ein Polynom $f \in R[X_1, \ldots, X_n]$ heißt symmetrisch, wenn $\sigma f = f$ für alle $\sigma \in \mathfrak{S}_n$.

Beispiele 3.9.3. (a) Für $k \in \mathbb{N}_0$ ist die k^{te} Potenzsumme $p_k = \sum_{i=1}^n X_i^k$ symmetrisch. Dabei ist $p_0 = n.1$.

(b) Die Diskriminante $D(X_1, \ldots, X_n) = \prod_{i<j}(X_i - X_j)^2$ ist symmetrisch.

(c) Sei Y eine weitere Unbestimmte. Dann ist $\prod_{i=1}^n (Y - X_i) = \sum_{k=0}^n (-1)^k s_k Y^{n-k} \in R[X_1, \ldots, X_n][Y]$, wobei

$$\begin{aligned} s_0 &= 1 \\ s_1 &= X_1 + \ldots X_n \\ &\vdots \\ s_k &= \sum_{1\leqslant i_1<\ldots<i_k\leqslant n} X_{i_1} \cdots X_{i_k} \\ &\vdots \\ s_n &= X_1 \cdots X_n. \end{aligned}$$

Die $s_1, \ldots, s_n$ sind symmetrisch, sie heißen elementarsymmetrische Polynome als Funktionen in $X_1, \ldots, X_n$. Die symmetrischen Polynome in $R[X_1, \ldots, X_n]$ bilden eine Unteralgebra von $R[X_1, \ldots, X_n]$, die $R[s_1, \ldots, s_n]$ enthält.

Hauptsatz über elementarsymmetrische Polynome 3.9.4. *Seien R, $R[X_1, \ldots, X_n]$ und $R[s_1, \ldots, s_n]$ wie oben.*

(a) Die Unteralgebra der symmetrischen Polynome in $R[X_1, \ldots, X_n]$ stimmt mit $R[s_1, \ldots, s_n]$ überein.

(b) *Die $s_1, \dots, s_n$ sind algebraisch unabhängig über R.*

(c) *Die Familie $X_1^{\alpha_1} \cdots X_n^{\alpha_n}$, mit $0 \leqslant \alpha_i < i$ für $1 \leqslant i \leqslant n$, ist eine Basis von $R[X_1, \dots, X_n]$ über $R[s_1, \dots, s_n]$.*

Beweis. Induktion nach n. Sei $n = 1$, dann ist $s_1 = X_1$ und alle Polynome in $R[X_1]$ sind symmetrisch, alle drei Behauptungen sind trivial.

Sei nun $n > 1$. Wir sehen $R[X_1, \dots, X_n]$ als Polynomring in $X_1, \dots, X_{n-1}$ über $R[X_n]$ an. Die Induktionsannahme lautet:

(a') Die $R[X_n]$-Unteralgebra der in $X_1, \dots, X_{n-1}$ symmetrischen Polynome in $R[X_1, \dots, X_n]$ ist $R[s'_1, \dots, s'_{n-1}, X_n]$, wobei $s'_1, \dots, s'_{n-1}$ die elementarsymmetrischen Polynome in $R[X_1, \dots, X_{n-1}]$ sind.

(b') Die $s'_1, \dots, s'_{n-1}$ sind algebraisch unabhängig über $R[X_n]$.

(c') Die Familie $X_1^{\alpha_1} \cdots X_{n-1}^{\alpha_{n-1}}$, mit $0 \leqslant \alpha_i < i$ für $1 \leqslant i \leqslant n-1$, ist Basis von $R[X_1, \dots, X_n]$ über $R[s'_1, \dots, s'_{n-1}, X_n]$.

Aus

$$\sum_{k=0}^{n} (-1)^k s_k Y^{n-k} = \prod_{i=1}^{n} (Y - X_i) = (Y - X_n) \cdot \sum_{k=0}^{n-1} (-1)^k s'_k Y^{n-1-k}$$

folgt

$$\begin{aligned} s_0 &= s'_0 = 1 \\ s_k &= s'_k + s'_{k+1} X_n \quad \text{für } 1 \leqslant k \leqslant n-1 \\ s_n &= s'_n X_n \end{aligned}$$

Induktiv setzt man

$$s'_k = (-1)^k X_n^k + \sum_{j=1}^{k} (-1)^{k-j} s_j X_n^{k-j} \quad \text{für } 1 \leqslant k \leqslant n-1.$$

Aus diesen Formeln folgt, daß $R[s'_1, \dots, s'_{n-1}, X_n] = R[s_1, \dots, s_{n-1}, X_n]$ ist.

Lemma. *Die Tupel $s'_1, \dots, s'_{n-1}, X_n$ und $s_1, \dots, s_{n-1}, X_n$ sind algebraisch unabhängig über R*

Beweis hierzu. Nach (b') sind $s'_1, \dots, s'_{n-1}$ algebraisch unabhängig über $R[X_n]$. Dann sind $s'_1, \dots, s'_{n-1}, X_n$ algebraisch unabhängig über R: Sei

$$\begin{aligned} h = \textstyle\sum_{\alpha_1, \dots, \alpha_{n-1}} h_{\alpha_1, \dots, \alpha_{n-1}}(Y_n) Y_1^{\alpha_1} \cdots Y_{n-1}^{\alpha_{n-1}} \in R[Y_1, \dots, Y_n] \qquad &\text{mit} \\ 0 = h(s'_1, \dots, s'_{n-1}, X_n) = \textstyle\sum_{\alpha_1, \dots, \alpha_{n-1}} h_{\alpha_1, \dots, \alpha_{n-1}}(X_n) (s'_1)^{\alpha_1} \cdots (s'_{n-1})^{\alpha_{n-1}}. \end{aligned}$$

Dann gilt für alle $\alpha_1, \dots, \alpha_{n-1}$, da die $s'_1, \dots, s'_{n-1}$ algebraisch unabhängig über $R[X_n]$ sind, $h_{\alpha_1, \dots, \alpha_{n-1}}(X_n) = 0$, das heißt $h_{\alpha_1, \dots, \alpha_{n-1}} = 0$, und damit $h = 0$. Also ist das erste Tupel algebraisch unabhängig über R.

Es gibt einen $R[X_n]$-Algebrenhomomorphismus

$$\begin{aligned} \varphi : R[s'_1, \dots, s'_{n-1}, X_n] \to R[s'_1, \dots, s'_{n-1}, X_n] \quad &\text{mit} \\ \varphi(s'_k) = (-1)^k X_n^k + \textstyle\sum_{i=1}^{k} (-1)^{k-i} s'_i X_n^{k-i} \quad &\text{für } 1 \leqslant k \leqslant n-1. \end{aligned}$$

Es gilt für $1 \leqslant k \leqslant n$

$$\varphi(s_k) = \varphi(s'_k) + \varphi(s'_{k-1}) X_n = (-1)^k X_n^k + \sum_{i=1}^{k} (-1)^{k-i} s'_i X_n^{k-i} + (-1)^{k-1} X_n^k + \sum_{i=1}^{k-1} (-1)^{k-1-i} s'_i X_n^{k-i} = s'_k.$$

Ist nun $f \in R[Y_1, \dots, Y_n]$ mit $f(s_1, \dots, s_{n-1}, X_n) = 0$, so gilt

$$0 = \varphi(f(s_1, \dots, s_{n-1}, X_n)) = f(\varphi(s_1), \dots, \varphi(s_{n-1}), X_n) = f(s'_1, \dots, s'_{n-1}, X_n).$$

Also ist $f = 0$, und damit ist auch das zweite Tupel über R algebraisch unabhängig. □

Nun zum Beweis von (a), (b) und (c).
Zu (a): Wir müssen zeigen, daß jedes symmetrische Polynom $f \in R[X_1, \ldots, X_n]$ in $R[s_1, \ldots, s_n]$ liegt. Wir argumentieren mit Induktion über $\deg(f)$. Da die homogenen Komponenten von f ebenfalls symmetrisch sind, können wir annehmen, daß f symmetrisch und homogen ist. Sei außerdem $f \notin R$, mit $\deg(f) = m > 0$. Da f in $X_1, \ldots, X_{n-1}$ symmetrisch ist, gilt $f \in R[s'_1, \ldots, s'_{n-1}, X_n]$ nach (a'), also $f \in R[s_1, \ldots, s_{n-1}, X_n]$. Es gibt eindeutig bestimmte $f_1, \ldots, f_i \in R[s_1, \ldots, s_{n-1}]$ mit $f = \sum_{j=1}^{i} f_j X_n^j$. Dabei ist $f_0 = 0$ oder $f_0 \neq 0$ und homogen vom Grad m. Ist $f = f_0$, so ist man fertig. Ist $f \neq f_0$, so gibt es genau ein $g \in R[X_1, \ldots, X_n]$ mit

$$f - f_0 = g \cdot X_n.$$

Da $f - f_0$ symmetrisch ist, ist dann $f - f_0$ durch $X_1, \ldots, X_n$ teilbar, also ist $f - f_0$ durch $X_1 \cdots X_n = s_n$ teilbar. Somit gibt es $h \in R[X_1, \ldots, X_n]$ mit

$$f - f_0 = h s_n.$$

Dann ist h ebenfalls symmetrisch und homogen. Da $\deg(h) < \deg(f)$ gilt nach Induktionsannahme über $\deg(f) = m$, daß $h \in R[s_1, \ldots, s_n]$ ist. Es folgt $f \in R[s_1, \ldots, s_n]$.
Bemerkung. Man mache sich die Konstruktion am Beispiel $f = X_1^2 X_2 + X_1 X_2^2$ klar.
Zu (b): Aus $0 = \prod_{i=1}^{n}(X_n - X_i) = \sum_{k=0}^{n}(-1)^k s_k Y_n^{n-k}$ folgt

$$(-1)^{n+1} s_n = \sum_{k=0}^{n-1}(-1)^k s_k X_n^{n-k} = X_n^n - s_1 X_n^{n-1} + \ldots + (-1)^{n-1} s_{n-1} X_n.$$

Wir beweisen zunächst folgendes allgemeinere Lemma.

Lemma. *Sei A ein kommutativer Ring, $A[X]$ der Polynomring in einer Unbestimmten über A. Sei $h = c_n X^n + \ldots + c_1 X + c_0 \in A[X]$ mit $n \geqslant 1$ und $a_n \in A^*$. Dann gilt:*

(a) Das Element h ist algebraisch unabhängig über A .

(b) Die Familie $1, X, \ldots, X^{n-1}$ ist eine Basis von $A[X]$ über $A[h]$.

Beweis hierzu. **Zu (a):** Für $p = a_0 + \ldots + a_m Y^m \in A[Y]$ mit $m \geqslant 0$, $a_m \neq 0$ gilt $p(h) \neq 0$. Also ist h algebraisch unabhängig über A.
Zu (b): Sei $f \in A[X]$. Wir zeigen, daß es eine eindeutig bestimmte Familie $r_j \in A[X]$, $i \in \mathbb{N}_0$, fast alle Null gibt mit $\deg(r_j) < n$ und $f = \sum_{j \geqslant 0} r_j h^j$. Dies ist klar, wenn $\deg(f) < n$ ist. Andernfalls gibt es eindeutig bestimmte $r_0, q_0 \in A[X]$ mit $f = q_0 h + r_0$ und $\deg(r_0) < n$. Da $\deg(q_0) < \deg(f)$ ist, gibt es nach Induktion eine eindeutige Darstellung $q_0 = \sum_{j \geqslant 0} r_{j+1} h^j$ wie behauptet. Es folgt

$$f = \sum_{j \geqslant 0} r_{j+1} h^{j+1} + r_0 = \sum_{j \geqslant 0} r_j h^j.$$

Die Eindeutigkeit ist klar. Jedes r_j hat eine eindeutige Darstellung

$$r_j = \sum_{i=0}^{n-1} a_{ij} X^i \quad \text{mit } a_{ij} \in A.$$

Man erhält

$$f = \sum_{i=0}^{n-1}\Big(\sum_{j \geqslant 0} a_{ij} h^j\Big) X^i \quad \text{mit } \sum_{i=0}^{n-1} a_{ij} h^j \in A[h] \text{ für } 0 \leqslant i \leqslant n-1.$$

Die Eindeutigkeit ist ebenfalls klar. □

Wenn wir das Lemma auf $A = R[s_1, \ldots, s_{n-1}]$, $X = X_n$ und $h = (-1)^{n+1} s_n$ anwenden, dann erhalten wir, daß s_n algebraisch unabhängig über $R[s_1, \ldots, s_{n-1}]$ ist. Da $s_1, \ldots, s_{n-1}$ algebraisch unabhängig über R sind, ist dann $s_1, \ldots, s_n$ algebraisch unabhängig über R.
Zu (c): Nach (c') ist $X_1^{\alpha_1} \cdots X_{n-1}^{\alpha_{n-1}}$, mit $0 \leqslant \alpha_i < i$ für $1 \leqslant i \leqslant n-1$, eine Basis von $R[X_1, \ldots, X_n]$ über $R[s_1, \ldots, s_{n-1}, X_n]$. Nach dem Lemma ist $1, X_n, \ldots, X_n^{n-1}$ eine Basis von $R[s_1, \ldots, s_{n-1}, X_n]$ über $R[s_1, \ldots, s_{n-1}]$. Dann ist die Familie $X_1^{\alpha_1} \cdots X_n^{\alpha_n}$, mit $0 \leqslant \alpha_i < i$ für $1 \leqslant i \leqslant n$, Basis von $R[X_1, \ldots, X_n]$ über $R[s_1, \ldots, s_n]$. Damit ist der Satz bewiesen. □

Bemerkung 3.9.5. Der Beweis des Satzes ist konstruktiv. Betrachten wir die Gleichung $f = f_0(s_1, \ldots, s_{n-1}) + hs_n$. Bei $X_n \mapsto 0$ erhält man

$$f(X_1, \ldots, X_{n-1}, 0) = f_0(s'_1, \ldots, s'_{n-1}).$$

Also konstruiert man eine Darstellung von f als Polynom in $s_1, \ldots, s_n$ wie folgt:

(i) Man stellt $f(X_1, \ldots, X_{n-1}, 0) = f_0(s'_1, \ldots, s'_{n-1})$ als Polynom in $s'_1, \ldots, s'_{n-1}$ dar.

(ii) Man ersetzt in f_0 die $s'_1, \ldots, s'_{n-1}$ durch $s_1, \ldots, s_{n-1}$. Dann gibt es ein homogenes, symmetrisches Polynom h mit $f - f_0 = hs_n$. Nun stellt man h als Polynom in $s_1, \ldots, s_n$ dar.

In (i) wird die Anzahl der Unbestimmten, in (ii) wird der Grad von f gesenkt.

3.9.3 Beispiele

Beispiel 3.9.6. Die Diskriminante

$$D(X_1, \ldots, X_n) = \prod_{i<j} (X_i - X_j)^2$$

ist symmetrisch. Es gilt

$$\prod_{i<j} (X_i - X_j) = \det \begin{pmatrix} 1 & \ldots & 1 \\ X_1 & \ldots & X_n \\ \vdots & & \vdots \\ X_1^{n-1} & \ldots & X_n^{n-1} \end{pmatrix},$$

also

$$D = \det \left(\begin{pmatrix} 1 & \ldots & 1 \\ X_1 & \ldots & X_n \\ \vdots & & \vdots \\ X_1^{n-1} & \ldots & X_n^{n-1} \end{pmatrix} \begin{pmatrix} 1 & \ldots & 1 \\ X_1 & \ldots & X_n \\ \vdots & & \vdots \\ X_1^{n-1} & \ldots & X_n^{n-1} \end{pmatrix} \right) = \det \begin{pmatrix} n & p_1 & \ldots & p_{n-1} \\ p_1 & p_2 & \ldots & p_n \\ \vdots & & & \vdots \\ p_{n-1} & p_n & \ldots & p_{2(n-1)} \end{pmatrix}.$$

Mit Hilfe der Newton'schen Formeln kann man die p_i durch die s_k ausdrücken.

Beispiel 3.9.7. Sei K ein Körper, $f = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 \in K[X]$, L ein Zerfällungskörper von f und $x_1, \ldots, x_n \in L$ die Nullstellen von f. Dann ist

$$f = \prod_{i=1}^{n} (X - x_i) = \sum_{k=0}^{n} (-1)^k s_k(x_1, \ldots, x_n) X^{n-k},$$

also $a_{n-k} = (-1)^k s_k(x_1, \ldots, x_n)$ für $1 \leqslant k \leqslant n$. Da $D(X_1, \ldots, X_n)$ symmetrisch ist, gibt es $g \in K[X_1, \ldots, X_n]$ mit $D(X_1, \ldots, X_n) = g(s_1, \ldots, s_n)$. Es folgt

$$D(x_1, \ldots, x_n) = g(s_1(x_1, \ldots, x_n), \ldots, s_n(x_1, \ldots, x_n)) = g(-a_{n-1}, \ldots, (-1)^n a_0).$$

Speziell: sei $f = X^3 + bX^2 + cX + d \in K[X]$, $f = (X - x_1)(X - x_2)(X - x_3)$, dann gilt:

$$\begin{aligned} -b &= s_1(x_1, x_2, x_3) \\ c &= s_2(x_1, x_2, x_3) \\ -d &= s_3(x_1, x_2, x_3) \end{aligned}$$

Weiter ist

$$D(x_1, x_2, x_3) = \det \begin{pmatrix} 3 & p_1 & p_2 \\ p_1 & p_2 & p_3 \\ p_2 & p_3 & p_4 \end{pmatrix}.$$

Wir berechnen $p_1, \ldots, p_4$ unter Berücksichtigung der Gleichheit $x_i^3 = -bx_i^2 - cx_i - d$ für $1 \leqslant i \leqslant 3$:

$$\begin{aligned} p_1 &= s_1(x_1,x_2,x_3) = -b \\ p_2 &= s_1^2(x_1,x_2,x_3) - 2s_2(x_1,x_2,x_3) = b^2 - 2c \\ p_3 &= -bp_2 - cp_1 - 3d = -b(b^2-2c) - c(-b) - 3d = -b^3 + 3bc - 3d \\ p_4 &= -bp_3 - cp_2 - dp_1 = -b(-b^3+3bc-3d) - c(b^2-2c) - d(-b) = b^4 - 4b^2c + 4bd + 2c^2. \end{aligned}$$

Schließlich

$$D(x_1,x_2,x_3) = 3(p_2p_1 - p_3^2) - p_1(p_1p_4 - p_2p_3) + p_2(p_1p_3 - p_2^2) = b^2c^2 + 18bcd - 4b^3d - 4c^3 - 17d^2.$$

Beispiel 3.9.8. Seien

$$\begin{aligned} \alpha &= X_1X_2 + X_3X_4 \\ \beta &= X_1X_3 + X_2X_4 \\ \gamma &= X_1X_4 + X_2X_3 \end{aligned}$$

in $R[X_1, \ldots, X_4]$

$$g = (Y-\alpha)(Y-\beta)(Y-\gamma) = Y^3 + b_2Y^2 + b_1Y + b_0 \in R[X_1,\ldots,X_4][Y].$$

Dabei gilt

$$\begin{aligned} -b_2 &= \alpha+\beta+\gamma = \sum_{i<j} X_iX_j = s_2 \\ b_1 &= \alpha\beta + \alpha\gamma + \beta\gamma = \sum_{\substack{j<k \\ i\notin\{j,k\}}} X_i^2X_jX_k \\ -b_0 &= \alpha\beta\gamma = \sum_{i<j<k} X_i^2X_j^2X_k^2 + \sum_{\substack{j<k<l \\ i\notin\{j,k,l\}}} X_i^3X_jX_kX_l = u + v \end{aligned}$$

Damit sind u, v, b_1, b_2 symmetrisch. Wir berechnen zuerst b_1:

$b_1 = X_1^2(X_2X_3+X_2X_4+X_3X_4)+X_2^2(X_1X_3+X_1X_4+X_3X_4)+X_3^2(X_1X_2+X_1X_4+X_2X_4)+X_4^2(X_1X_2+X_1X_3+X_2X_3)$

Also mit $X_4 = 0$: $b_1(X_1,X_2,X_3,0) = X_1X_2X_3(X_1+X_2+X_3) = s_1's_3'$. Nun ist

$$b_1 - s_1s_3 = b_1 - (X_1+X_2+X_3+X_4)(X_1X_2X_3 + X_1X_2X_4 + X_1X_3X_4 + X_2X_3X_4) = -4s_4,$$

also

$$b_1 = s_1s_3 - 4s_4.$$

Nun zu u:

$$u = X_1^2X_2^2X_3^2 + X_1^2X_2^2X_4^2 + X_1^2X_3^2X_4^2 + X_2^2X_3^2X_4^2,$$

Wieder mit $X_4 = 0$: $u(X_1,X_2,X_3,0) = (s_3')^2$. Nun ist

$$\begin{aligned} u - s_3^2 &= u - (X_1X_2X_3 + X_1X_2X_4 + X_1X_3X_4 + X_2X_3X_4)^2 \\ &= -2(X_1^2X_2^2X_3X_4 + X_1^2X_2X_3^2X_4 + X_1^2X_2X_3X_4^2 + X_1X_2^2X_3^2X_4 + X_1X_2^2X_3X_4^2 + X_1X_2X_3^2X_4^2) \\ &= -2s_2s_4 \end{aligned}$$

also

$$u = s_3^2 - 2s_2s_4.$$

Zuletzt v: es gilt

$$v = \sum_{\substack{j<k<l \\ i\notin\{j,k,l\}}} X_i^3X_jX_kX_l = s_4(X_1^2+X_2^2+X_3^2+X_4^2) = s_4p_2$$

und

$$p_2 = s_1^2 - 2(X_1X_2 + X_1X_3 + X_1X_4 + X_2X_3 + X_2X_4 + X_3X_4) = s_1^2 + 2s_2.$$

Also

$$v = s_1^2s_4 - 2s_2s_4.$$

Es folgt:

$$b_0 = u + v = s_1^2s_4 - 4s_2s_4 + s_3^2.$$

Beispiel 3.9.9. Sei $f = X^4 + bX^3 + cX^2 + dX + e \in K[X]$, sei L ein Zerfällungskörper von f und $x_1, \ldots, x_4 \in L$ die Nullstellen von f. Es gilt:

$$\begin{aligned} -b &= s_1(x_1, x_2, x_3, x_4) \\ c &= s_2(x_1, x_2, x_3, x_4) \\ -d &= s_3(x_1, x_2, x_3, x_4) \\ e &= s_4(x_1, x_2, x_3, x_4) \end{aligned}$$

Die kubische Resolvente von f erhält man, indem man in Beispiel 3.9.8 die X_i durch x_i ersetzt für $1 \leqslant i \leqslant 4$:

$$\begin{aligned} b_2(x_1, \ldots, x_4) &= -s_2(x_1, \ldots, x_4) = -c \\ b_1(x_1, \ldots, x_4) &= s_1(x_1, \ldots, x_4)s_3(x_1, \ldots, x_4) - 4s_4(x_1, \ldots, x_4) = bd + 4e \\ b_0(x_1, \ldots, x_4) &= -s_1^2(x_1, \ldots, x_4)s_4(x_1, \ldots, x_4) + 4s_2(x_1, \ldots, x_4)s_4(x_1, \ldots, x_4) - s_3^2(x_1, \ldots, x_4) = -b^2e + 4ce - d^2 \end{aligned}$$

also

$$g = Y^3 - cY^2 + (bd - 4e)Y + b^2e + 4ce - d^2.$$

Literaturverzeichnis

[1] Artin Michael: *Algebra*. Birkhäuser Verlag, (1993).

[2] Bosch Siegfried: *Algebra*. Springer-Lehrbuch, 6. Auflage, Springer-Verlag Berline Heidelberg, (2006).

[3] Bourbaki Nicolas: *Algèbre 1-10*. In Éléments de Mathématiques.

[4] Hungerford Thomas W.: *Algebra*. Graduate Texts in Mathematics, Springer-Verlag New York, (1974).

[5] Lange Serge: *Algebra*. Graduate Texts in Mathematics, Springer-Verlag New York, (2002).

[6] Perrin Daniel: *Cours d'algèbre (Agrégation)*. CAPES, Ellipses, (1996).

[7] Serre Jean-Pierre: *Cours d'arithmétique*. 4e édition, PUF, Paris, (1995).

Universität Regensburg
Fakultät für Mathematik
Universitätsstraße 31
93053 Regensburg
Germany
(+ 49) 941-943-2664
veronika.ertl@mathematik.uni-regensburg.de
http://www.mathematik.uni-regensburg.de/ertl/