Algebra – Kurzskript

Inhaltsverzeichnis

1 Gruppen

1.1 Gruppen und Untergruppen

Definition 1.1.1 *Eine **Gruppe** ist eine Paar $(G, \circ)$ bestehend aus einer Menge G und einer Verknüpfung $\circ\colon G \times G \to G$, die **assoziativ** ist (d. h. für alle $a, b, c \in G$ gilt $a \circ (b \circ c) = (a \circ b) \circ c$, so dass es ein **neutrales Element** $e \in G$ gibt (d. h. für alle $a \in G$ gilt $a \circ e = e \circ a = a$) und so dass jedes Element $a \in G$ ein **Inverses** $a^{-1} \in G$ besitzt (d. h. $a \circ a^{-1} = a^{-1} \circ a = e$).*

*Eine Gruppe heißt **abelsch** oder **kommutativ**, wenn außerdem für alle $a, b \in G$ gilt: $a \circ b = b \circ a$.*

Bemerkung 1.1.2 *Das neutrale Element einer Gruppe G und Inverse a^{-1} von Elementen $a \in G$ sind eindeutig.*

Notation 1.1.3

- *Wenn klar ist, welche Verknüpfung gemeint ist, sagen wir oft „G ist eine Gruppe“ (statt „$(G, \circ)$ ist eine Gruppe“). Insbesondere schreiben wir $\mathbb{Z}$ statt $(\mathbb{Z}, +)$, und wenn K ein Körper ist schreiben wir K statt $(K, +)$ und $K^\times$ statt $(K^\times, \cdot)$.*
- *Wenn wir nicht sagen, was die Verknüfung einer Gruppe ist, verwenden wir die **multiplikative Notation**: Die Verknüpfung schreiben wir als $a \cdot b$ (oder ab), das neutrale Element ist 1, und das Inverse von a ist a^{-1}.*
- *Bei abelschen Gruppen werden wir auch oft die **additive Notation** verwenden: Die Verknüpfung ist $a + b$, das neutrale Element ist 0, und das inverse von a ist $-a$.*

Beispiel 1.1.4 *Sei K ein Körper. Dann bildet die Menge $\mathrm{GL}_n(K)$ der invertierbaren $n \times n$-Matrizen eine Gruppe mit dem Matrixprodukt als Verknüpfung. (GL = general linear group = **allgemeine lineare Gruppe**.)*

Beispiel 1.1.5 *Ist M eine Menge, so definiert man die **symmetrische Gruppe** als $\mathrm{Sym}(M) := \{f\colon M \to M \mid f \text{ ist bijektiv}\}$, mit der Hintereinanderausführung von Abbildungen als Verknüpfung. Elemente von $\mathrm{Sym}(M)$ nennt man auch **Permutationen** von M.*
Wir setzen auch: $S_n := \mathrm{Sym}(\{1, \dots, n\})$.

Lemma 1.1.6 *Sei G eine Gruppe, und seien $a, b \in G$.*

- *Wenn es ein $c \in G$ gibt mit $ac = bc$ (oder $ca = cb$), so gilt $a = b$.*
- *Es gibt ein $d \in G$ mit $a = db$.*
- *Es gilt $(ab)^{-1} = b^{-1}a^{-1}$*

Notation 1.1.7 *Sei G eine Gruppe und $a \in G$. Wir setzen $a^0 := 1$ und, für $n \in \mathbb{N}$ positiv, $a^n := \underbrace{a \cdots a}_{n}$ und $a^{-n} := (a^n)^{-1} = (a^{-1})^n$.*

Wenn wir G mit additiver Notation schreiben, setzen wir entsprechend $0 \cdot a := 0$, $n \cdot a := \underbrace{a + \cdots + a}_{n}$ und $(-n) \cdot a := -(n \cdot a)$.

Bemerkung 1.1.8 *Für beliebige $m, n \in \mathbb{Z}$ gilt: $a^m \cdot a^n = a^{m+n}$.*

Definition 1.1.9 *Sei G eine Gruppe. Eine **Untergruppe** von G ist eine Teilmenge $H \subset G$, so dass H eine Gruppe ist (mit der auf H eingeschränkten Verknüpfung von G).*

*Ein **Normalteiler** von G ist eine Untergruppe $N \subset G$, so dass außerdem gilt: Für alle $a \in N$ und alle $b \in G$ gilt $bab^{-1} \in N$. Die Notation „$N \lhd G$“ bedeutet: N ist ein Normalteiler von G.*

Bemerkung 1.1.10 *Eine nicht-leere Teilmenge $H \subset G$ ist eine Untergruppe genau dann, wenn für alle $a, b \in H$ gilt: $a \cdot b \in H$ und $a^{-1} \in H$. Das neutrale Element von H ist dann das selbe wie das neutrale Element von G.*

Beispiel 1.1.11 $\mathrm{SL}_n(K) := \{A \in \mathrm{GL}_n(K) \mid \det A = 1\}$ *ist eine Untergruppe von $\mathrm{GL}_n(K)$ und sogar ein Normalteiler. ($SL = \underline{s}pecial\ \underline{l}inear\ group =$ **spezielle lineare Gruppe**.)*

Bemerkung 1.1.12 *Ist G eine abelsche Gruppe, so ist jede Untergruppe von G bereits ein Normalteiler.*

Beispiel 1.1.13 *Jede Untergruppe von $\mathbb{Z}$ hat die Form $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$, für ein $n \in \mathbb{N}$.*

Lemma 1.1.14 *Ist G eine Gruppe und sind $H_i \subset G$ Untergruppen für $i \in I$, wobei I eine beliebige, nicht-leere Indexmenge ist, so ist $\bigcap_{i \in I} H_i$ auch eine Untergruppe von G.*

Definition 1.1.15 *Sei G eine Gruppe und $A \subset G$ eine beliebige Teilmenge von G. Die von A **erzeugte** Untergruppe von G ist*

$$\langle A \rangle := \bigcap_{\substack{H \subset G \text{ Untergrp.} \\ \text{mit } A \subset H}} H.$$

*Man sagt auch, die Elemente von A sind **Erzeuger** von H.*

Beispiel 1.1.16 *Ist G eine Gruppe und $a \in G$, so ist $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$.*

Definition 1.1.17 *Seien G und H Gruppen. Das **(direkte) Produkt** von G und H ist die Gruppe $G \times H$ mit der komponentenweiser Verknüpfung:*

$$(a, b) \cdot (a', b') := (aa', bb')$$

für $a, a' \in G$, $b, b' \in H$.

Bemerkung 1.1.18 *G kann als Untergruppe von $G \times H$ aufgefasst werden, indem man $a \in G$ mit $(a, 1) \in G \times H$ identifiziert. Analog kann man H als Untergruppe von $G \times H$ auffassen.*

1.2 Gruppenhomomorphismen

Definition 1.2.1 *Seien G und H Gruppen. Ein **Gruppenhomomorphismus** ist eine Abbildung $f \colon G \to H$, für die gilt:*

$$\forall a, b \in G \colon f(ab) = f(a)f(b).$$

$\mathrm{Hom}(G, H)$ *bezeichnet die Menge aller Gruppenhomomorphimen von G nach H.*

*Das **Bild** von f ist* $\operatorname{im} f := \{f(a) \mid a \in G\}$*; der **Kern** von f ist* $\ker f := \{a \in G \mid f(a) = 1\}$.

*Ein **Isomorphismus von Gruppen** ist ein bijektiver Gruppenhomomorphismus.*

*Zwei Gruppen G und H heißen **isomorph** (Notation: $G \cong H$), wenn es einen Isomorphismus $G \to H$ gibt.*

*Ein **Endomorphismus** einer Gruppe G ist ein Homomorphismus von G nach G. Die Menge der Endomorphismen von G wird mit* $\operatorname{End}(G)$ *bezeichnet.*

*Ein **Automorphismus** einer Gruppe G ist ein Isomorphismus von G nach G. Die Menge der Automorphismen von G wird mit* $\operatorname{Aut}(G)$ *bezeichnet.*

Bemerkung 1.2.2 *Ist $f\colon G \to H$ ein Gruppenhomomorphismus, so gilt $f(1) = 1$ und, für $a \in G$, $f(a^{-1}) = f(a)^{-1}$.*

Bemerkung 1.2.3 *Die Verknüpfung von zwei Gruppenhomomorphismen ist wieder ein Gruppenhomomorphismus.*

Bemerkung 1.2.4 $\operatorname{Aut}(G)$ *ist eine Untergruppe von* $\operatorname{Sym}(G)$.

Beispiel 1.2.5 *Die Abbildung $S_n \to \mathbb{R}^\times, \sigma \mapsto \operatorname{sgn}(\sigma)$ ist ein Gruppenhomomorphismus. Den Kern $A_n := \{\sigma \in S_n \mid \operatorname{sgn}(\sigma) = 1\}$ nennt man die **alternierende Gruppe**.*

Lemma 1.2.6 *Sind G und H Gruppen und ist $f\colon G \to H$ ein Gruppenhomomorphismus, so ist* $\operatorname{im} f$ *eine Untergruppe von H und* $\ker f$ *ein Normalteiler von G.*

1.3 Nebenklassen, Quotienten und der Isomorphiesatz

Definition 1.3.1 *Sei G eine Gruppe und $H \subset G$ eine Untergruppe.*

- *Eine **Linksnebenklasse** von H ist eine Menge der Form $aH := \{ah \mid h \in H\}$ für $a \in G$. Die Menge aller Linksnebenklassen von H wird mit G/H bezeichnet.*
- *Eine **Rechtsnebenklasse** von H ist eine Menge der Form $Ha := \{ha \mid h \in H\}$ für $a \in G$. Die Menge aller Rechtsnebenklassen von H wird mit $H\backslash G$ bezeichnet.*

Lemma 1.3.2 *Ist G eine Gruppe und $N \lhd G$ ein Normalteiler und $a \in G$, so gilt $aN = Na$. Insbesondere sind Linksnebenklassen das gleiche wie Rechtsnebenklassen, und man spricht einfach von **Nebenklassen**.*

Bemerkung: Wenn wir additive Notation verwenden, schreiben wir Nebenklassen als $a + H = \{a + h \mid h \in H\}$.

Lemma 1.3.3 *Sei G eine Gruppe und $H \subset G$ eine Untergruppe.*

(a) *Die Menge der Linksnebenklassen von H bildet eine Partition von G, d. h. jedes Element $a \in G$ liegt in genau einer Linksnebenklasse, nämlich $a \in aH$.*

(b) *Zwei Elemente $a, b \in G$ liegen in der gleichen Linksnebenklasse von H genau dann, wenn $a^{-1}b \in H$ gilt.*

(c) *Jede Linksnebenklasse von H hat die gleiche Kardinalität wie H (d. h. für beliebige $a \in G$ gilt: $\#(aH) = \#H$).*

Analoge Aussagen gelten für Rechtsnebenklassen.

Bemerkung 1.3.4 *Ist $f\colon G \to H$ ein Gruppenhomomorphismus, und sind $a, b \in G$, so gilt $f(a) = f(b)$ genau dann wenn $a \cdot (\ker f) = b \cdot (\ker f)$. Insbesondere ist f injektiv genau dann, wenn $\ker f = \{1\}$.*

Satz 1.3.5 *Ist G eine Gruppe und $N \lhd G$ ein Normalteiler, so wird durch $(aN) \cdot (bN) := (ab)N$ (für $a, b \in G$) eine Verknüpfgung auf G/N definiert; G/N ist mit dieser Verknüpfung eine Gruppe, und die Abbildung $G \to G/N, a \mapsto aN$ ist ein Gruppenhomomorphismus.*

Definition 1.3.6 *Die Gruppe G/N („G **modulo** N“) aus dem vorigen Satz wird **Quotientengruppe** (oder manchmal auch **Faktorgruppe**) genannt.*

Notation 1.3.7 *Ist G eine Gruppe, $N \lhd G$ und $a \in G$, so schreiben wir für die Nebenklasse $aN \in G/N$ manchmal auch $\bar{a}$.*

Satz 1.3.8 (Isomorphiesatz) *Seien G und H Gruppen und $f\colon G \to H$ ein Homomorphismus. Dann erhalten wir einen Isomorphismus $\tilde{f}\colon G/\ker f \to \operatorname{im} f$, so dass für alle $a \in G$ gilt: $\tilde{f}(\bar{a}) = f(a)$.*

Definition 1.3.9 *Sei G eine Gruppe.*

- *Statt „Kardinalität von G“ sagt man auch **Ordnung** von G. (Als Notation verwendet man trotzdem $\#G$.)*
- *Die **Ordnung** eines Elements a von G ist die kleinste positive natürliche Zahl n, so dass $a^n = 1$ gilt. Die Ordnung von a wird mit $\operatorname{ord}(a)$ bezeichnet. Gibt es kein $n \geqslant 1$ mit $a^n = 1$, so setzt man $\operatorname{ord}(a) := \infty$.*
- *Der **Index** einer Untergruppe $H \subset G$ ist definiert durch $[G : H] := \#(G/H)$. (Er kann auch unendlich sein.)*

Satz 1.3.10 *Sei G eine Gruppe, $H \subset G$ eine Untergruppe, $a \in G$ und $r \in \mathbb{Z}$. Dann gilt:*

(a) $\#G = \#H \cdot [G : H]$.

(b) *Falls* $\operatorname{ord}(a) = \infty$: $\langle a \rangle \cong \mathbb{Z}$, *und* $a^r = 1 \iff r = 0$.
Falls $\operatorname{ord}(a) = m < \infty$: $\langle a \rangle \cong \mathbb{Z}/m\mathbb{Z}$, *und* $a^r = 1 \iff m | r$.
Insbesondere ist $\operatorname{ord} a = \#\langle a \rangle$.

(c) *Ist G endlich, so ist $a^{\#G} = 1$.*

Definition 1.3.11 *Eine Gruppe G heißt **zyklisch**, wenn sie von einer einelementigen Menge erzeugt wird, d. h. wenn es ein $a \in G$ gibt mit $\langle a \rangle = G$. Solch ein a heißt **Erzeuger** von G.*

Bemerkung 1.3.12 *Satz 1.3.10 besagt insbesondere: Ist G zyklisch, so ist $G \cong \mathbb{Z}$ oder $G \cong \mathbb{Z}/m\mathbb{Z}$ für ein $m \in \mathbb{N}$, $m \geqslant 1$. Zyklische Gruppen sind also insbesondere abelsch.*

Satz 1.3.13 *Untergruppen zyklischer Gruppen sind zyklisch.*

Satz 1.3.14 (Chinesischer Restsatz, Gruppenversion) *Sind $a_1, \ldots, a_k \in \mathbb{N}_{\geqslant 1}$ paarweise teilerfremd und $m = a_1 \cdot a_2 \cdots a_k$, so ist*

$$\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_k\mathbb{Z}, n \mapsto (n + a_1\mathbb{Z}, \ldots, n + a_k\mathbb{Z})$$

ein Isomorphismus von Gruppen.

Notation 1.3.15 *Ist $q \geqslant 1$ eine natürliche Zahl und sind $a, b \in \mathbb{Z}$ beliebig, so sagt man, a ist **kongruent** zu b **modulo** q" (oder: „a und b sind kongruent modulo q"), wenn $a - b$ durch q teilbar ist. Notation dafür: $a \equiv b \mod q$.*

Korollar 1.3.16 (Chinesischer Restsatz mit Kongruenzen) *Seien $a_1, \ldots, a_k \in \mathbb{N}_{\geqslant 1}$ paarweise teilerfremd und $b_1, \ldots, b_k \in \mathbb{Z}$ beliebig. Dann gibt es genau ein $c \in \mathbb{N}$ mit $c < a_1 \cdot a_2 \cdots a_k$, das die Kongruenzgleichungen*

$$\begin{aligned} c &\equiv b_1 \mod a_1 \\ &\vdots \\ c &\equiv b_k \mod a_k \end{aligned}$$

erfüllt.

1.4 Endlich erzeugte abelsche Gruppen

Definition 1.4.1 *Eine Gruppe G heißt **endlich erzeugt**, wenn sie von einer endlichen Menge $A \subset G$ erzeugt wird (d. h. $\langle A \rangle = G$).*

Ab jetzt sind in diesem Abschnitt sind alle Gruppen abelsch, und wir verwenden die additive Notation.

Satz 1.4.2 *Sei G eine abelsche Gruppe und sei $m \in \mathbb{N}$.*

(a) *Sind $a_1, \ldots, a_m \in G$, so ist $f \colon \mathbb{Z}^m \to G, (r_1, \ldots, r_m) \mapsto r_1 a_1 + \cdots + r_m a_m$ ein Gruppenhomomorphismus mit Bild $\operatorname{im} f = \langle a_1, \ldots, a_m \rangle$.*

(b) *Jeder Gruppenhomomorphismus $f \colon \mathbb{Z}^m \to G$ hat die Form wie in (a), für gewisse $a_i \in G$, d. h. (a) definiert eine Bijektion $G^m \to \operatorname{Hom}(\mathbb{Z}^m, G)$.*

Bemerkung 1.4.3 *Wenn $G = \mathbb{Z}^n$ ist und wir Elemente von $\mathbb{Z}^m$ und $\mathbb{Z}^n$ als Spaltenvektoren auffassen, dann ist $f(v) = Av$, wobei $A := \big(a_1 \mid \cdots \mid a_m\big) \in \mathbb{Z}^{m \times n}$ die Matrix mit Spalten a_i ist.*

Satz 1.4.4 *Ist G eine abelsche Gruppe, die von einer n-elementigen Menge erzeugt wird, und ist $H \subset G$ eine Untergruppe, so wird H von einer m-elementigen Menge erzeugt für ein $m \leqslant n$*

Satz 1.4.5 (Elementarteilersatz) *Zu jeder Matrix $A \in \mathbb{Z}^{m \times n}$ gibt es invertierbare Matritzen $S \in \mathbb{Z}^{m \times m}$ und $T \in \mathbb{Z}^{n \times n}$ so dass S^{-1} und T^{-1} auch ganzzahlige Einträge haben und so dass SAT die Form*

$$SAT = \begin{pmatrix} d_1 & 0 & \cdots & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots & & \vdots \\ \vdots & \ddots & d_k & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix},$$

hat für gewisse $d_1, \ldots, d_k \in \mathbb{Z}$ mit $d_1 \mid d_2 \mid \cdots \mid d_k$ (d. h. d_i teilt d_{i+1}).

Die $d_1, \ldots, d_k$ durch A eindeutig bestimmt.

Satz 1.4.6 (Beschreibung der Untergruppen von $\mathbb{Z}^m$) *Ist $H \subset \mathbb{Z}^m$ eine Untergruppe, so gibt es einen Automorphismus $f \colon \mathbb{Z}^m \to \mathbb{Z}^m$ so dass $f(H) = d_1\mathbb{Z} \times \cdots \times d_m\mathbb{Z}$ ist.*

Lemma 1.4.7 *Sei G eine abelsche Gruppe und $n \in \mathbb{N}$.*
(a) *$nG := \{na \mid a \in G\}$ ist eine Untergruppe von G.*
(b) *Ist $G \cong H_1 \times \cdots \times H_k$, so ist $nG \cong nH_1 \times \cdots \times nH_k$.*
(c) *Ist $G \cong \mathbb{Z}/m\mathbb{Z}$ und m ist ein Vielfaches von n, so ist $nG \cong \mathbb{Z}/\frac{m}{n}\mathbb{Z}$.*
(d) *Ist $G \cong \mathbb{Z}/m\mathbb{Z}$ und m ist teilerfremd zu n, so ist $nG \cong \mathbb{Z}/m\mathbb{Z}$.*
(e) *Ist $G \cong \mathbb{Z}/m\mathbb{Z}$ und n ist ein Vielfaches von m, so ist $nG \cong \{0\}$.*

Satz 1.4.8 (Klassifikation der endlich erzeugten abelschen Gruppen) *Jede endlich erzeugte abelsche Gruppe G ist isomorph zu einer Gruppe der Form $\mathbb{Z}^s \times \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}$, wobei jedes m_i eine Primpotenz ist, d. h. $m_i = p_i^{r_i}$ für Primzahlen p_i und natürliche Zahlen $r_i \geqslant 1$. Außerdem sind s und die m_i eindeutig durch G bestimmt, bis auf Reihenfolge der m_i.*

1.5 Operationen von Gruppen auf Mengen

Definition 1.5.1 *Sei G eine Gruppe und X eine Menge. Eine **Operation** λ von G auf X ist eine Abbildung $G \times X \to X, (a, x) \mapsto \lambda_a(x)$, so dass für alle $a, b \in G$ und alle $x \in X$ gilt:*
(a) *$\lambda_1(x) = x$.*
(b) *$\lambda_a(\lambda_b(x)) = \lambda_{ab}(x)$.*
*Hat man eine solche Operation gewählt, sagt man auch „G **operiert** auf X“. Operationen schreibt man manchmal auch als Verküpfung: Statt „$\lambda_a(x)$“ schreibt man „$a \cdot x$“ oder „ax“.*

Bemerkung 1.5.2 *Sei λ eine Operation von G auf X. Für $a \in G$ ist dann $\lambda_a \in \mathrm{Sym}(X)$; auf diese Weise ist eine Operation von G auf X das selbe wie ein Gruppenhomomorphismus $G \to \mathrm{Sym}(X), a \mapsto \lambda_a$. (Formaler ausgedrückt hat man eine Bijektion zwischen Operationen und solchen Gruppenhomomorphismen.)*

Bemerkung 1.5.3 *Ist λ eine Operation einer Gruppe G auf einer Menge X und ist H eine Untergruppe von G, so definiert λ auch eine Operation von H auf X.*

Definition 1.5.4 *Sei G eine Gruppe, die auf einer Menge X operiert und sei $x \in X$.*
(a) *Die **Bahn** von x ist die Menge $Gx := \{ax \mid a \in G\} \subset X$.*
(b) *Man sagt, x wird von $A \subset G$ **festgehalten** (oder **stabilisiert**), wenn für alle $a \in A$ gilt: $ax = x$. Der **Stabilisator** von x ist $\mathrm{Sta}_G(x) := \{a \in G \mid ax = x\}$.*
*Man sagt „G operiert **transitiv** auf X“, wenn es für alle $x, x' \in X$ ein $a \in G$ gibt mit $ax = x'$.*

Satz 1.5.5 *Sei G eine Gruppe, die auf einer Menge X operiert. Dann gilt:*
(a) *Für jedes $x \in X$ ist $\mathrm{Sta}_G(x)$ eine Untergruppe von G.*
(b) *Die Menge $\{Gx \mid x \in X\}$ aller Bahnen bilden eine Partition von X.*
(c) *Für alle $x \in X$ gilt: $\#(Gx) = [G : \mathrm{Sta}_G(x)]$.*

Korollar 1.5.6 *Ist G eine endliche Gruppe, die auf einer endlichen Menge X operiert, und sind $Gx_1, \ldots, Gx_k$ die Bahnen dieser Operation (mit $Gx_i \neq Gx_j$*

für $i \neq j$), so gilt

$$\#X = \sum_{i=1}^{k} \#(Gx_i) = \sum_{i=1}^{k} [G : \operatorname{Sta}_G x_i] = \sum_{i=1}^{k} \frac{\#G}{\#\operatorname{Sta}_G x_i}$$

1.6 Konjugation und Zentrum

Satz 1.6.1 *Sei G eine Gruppe.*

(a) *Für jedes $a \in G$ ist die Abbildung $G \to G, x \mapsto axa^{-1}$ ein Automorphismus von G.*

(b) *G operiert auf sich selbst durch $(a, x) \mapsto axa^{-1}$ (für $a, x \in G$).*

(c) *G operiert auf der Menge aller Untergruppen von G durch $(a, H) \mapsto aHa^{-1} = \{aha^{-1} \mid h \in H\}$ (für $a \in G$ und $H \subset G$ eine Untergruppe).*

Definition 1.6.2 *Die Abbildung $x \mapsto axa^{-1}$ aus Satz 1.6.1 (a) heißt **Konjugation** mit a, und die Operationen aus (b) und (c) heißen **Konjugationsoperation**. Die Bahnen der Konjugationsoperationen nennt man **Konjugationsklassen** (von Elementen bzw. von Untergruppen). Zwei Elemente $a, a' \in G$ bzw. Untergruppen $H, H' \subset G$ heißen **konjugiert** (man sagt auch: „a ist konjugiert zu a'“), wenn sie in der gleichen Konjugationsklasse liegen.*

Satz 1.6.3 *Sei G eine Gruppe und $H \subset G$ eine Untergruppe. Dann sind die folgenden Aussagen äquivalent:*

(a) *H ist ein Normalteiler.*

(b) *H ist eine Vereinigung von Konjugationsklassen von Elementen von G.*

(c) *H wird unter der Konjugationsoperation von ganz G festgehalten.*

Definition 1.6.4 *Sei G eine Gruppe.*

(a) *Man sagt, dass zwei Elemente $a, b \in G$ **kommutieren**, wenn $ab = ba$ gilt.*

(b) *Das **Zentrum** von G ist $Z(G) := \{a \in G \mid \forall b \in G\colon ab = ba\}$.*

Satz 1.6.5 *Sei G eine Gruppe.*

(a) *$Z(G)$ ist genau die Vereinigung aller einelementigen Konjugationsklassen von Elementen von G.*

(b) *$Z(G)$ ein Normalteiler von G.*

Definition 1.6.6 *Sei p eine Primzahl. Eine p-Gruppe ist eine endliche Gruppe, deren Ordnung eine Potenz von p ist.*

Satz 1.6.7 *Ist G eine nicht-triviale p-Gruppe (für eine Primzahl p), so hat G nicht-triviales Zentrum, d. h. $Z(G) \supsetneq \{1\}$.*

1.7 Kompositionsreihen

Definition 1.7.1 *Sei G eine Gruppe.*

(a) *G heißt **einfach**, wenn sie nicht trivial ist und ihre einzigen Normalteiler $\{1\}$ und G sind.*

(b) *Eine **Kompositionsreihe** von G ist eine Folge von Untergruppen $\{1\} = G_0 \subset G_1 \subset \cdots \subset G_r = G$ so dass G_{i-1} ist ein Normalteiler in G_i ist und G_i/G_{i-1} einfach ist für $i = 1, \ldots, r$. Die G_i/G_{i-1} nennt man **Kompositionsfaktoren** von G.*

Satz 1.7.2 (Jordan-Hölder) *Jede endliche Gruppe G besitzt eine Normalreihe, und die Kompositionsfaktoren sind bis auf Reihenfolge und bis auf Isomorphie eindeutig durch G bestimmt, d h.: Sind $\{1\} = G_0 \subset G_1 \subset \cdots \subset G_r = G$ und $\{1\} = G'_0 \subset G'_1 \subset \cdots \subset G'_{r'} = G$ Kompositionsreihen, so ist $r = r'$ und es gibt eine Permutation $\sigma \in S_r$ so dass $G_i/G_{i-1} \cong G'_{\sigma(i)}/G'_{\sigma(i)-1}$ für $i = 1, \ldots, r$.*

Definition 1.7.3 *Eine Gruppe heißt **auflösbar**, wenn alle Kompositionsfaktoren abelsch sind.*

Satz 1.7.4 *Jede p-Gruppe ist auflösbar.*

1.8 Die symmetrischen und alternierenden Gruppen

Definition 1.8.1 *Der **Träger** eines Elements $\sigma \in S_n$ ist $\{x \in \{1, \ldots, n\} \mid \sigma(x) \neq x\}$.*

Bemerkung 1.8.2 *Sind $\sigma_1, \sigma_2 \in S_n$ Elemente, deren Träger X_1, X_2 disjunkt sind, so gilt für $\sigma := \sigma_1 \circ \sigma_2$:*

$$\sigma(x) = \begin{cases} \sigma_1(x) & \text{falls } x \in X_1 \\ \sigma_2(x) & \text{falls } x \in X_2 \\ x & \text{sonst.} \end{cases}$$

Insbesondere ist der Träger von σ genau $X_1 \cup X_2$, und es gilt $\sigma = \sigma_2 \circ \sigma_1$.

Definition 1.8.3 *Ein Element $\sigma \in S_n$ heißt **Zykel** (der Länge $k \geqslant 1$), wenn es paarweise verschiedene $x_1, \ldots, x_k \in X$ gibt, so dass gilt:*
(a) *Der Träger von σ ist in $\{x_1, \ldots, x_k\}$ enthalten;*
(b) *$\sigma\colon x_1 \mapsto x_2, x_2 \mapsto x_3, \ldots, x_{k-1} \mapsto x_k, x_k \mapsto x_1$.*
(Falls $k \geqslant 2$ ist der Träger von σ genau $\{x_1, \ldots, x_k\}$.) Wir verwenden die Notation „$(x_1\, x_2\, \ldots\, x_k)$“ für diesen Zykel σ.

*Zykel der Länge 2 nennt man auch **Transpositionen**.*

Satz 1.8.4 *Jedes Element $\sigma \in S_n$ lässt sich als Produkt $\sigma_1 \circ \cdots \circ \sigma_m$ von Zykeln σ_j schreiben, die paarweise disjunkte Träger haben. Verwendet man keine Zykel der Länge 1, so ist diese Schreibweise eindeutig bis auf Reihenfolge. (Man nennt dies die **Zykelzerlegung** von σ.)*

Satz 1.8.5 *Ist $\sigma = (x_1 \ldots x_k)$ ein Zykel und $\tau \in S_n$ beliebig, so ist $\tau\sigma\tau^{-1} = (\tau(x_1) \ldots \tau(x_k))$.*

Bemerkung 1.8.6 *Zwei Elemente $\sigma, \sigma' \in S_n$ sind konjugiert genau dann, wenn sie in der Zykelzerlegung die gleichen Zykellängen haben (also wenn für jedes $k \geqslant 2$ gilt: In der Zykelzerlegung von σ kommen genauso viele Zykel der Länge k vor wie in der Zykelzerlegung von σ').*

Satz 1.8.7 *Ist $\sigma \in S_n$ ein Zykel der Länge k, so ist $\operatorname{sgn}(\sigma) = (-1)^{k+1}$.*

Satz 1.8.8 (a) *Die alternierende Gruppe A_n ist einfach genau dann wenn $n \geqslant 5$ ist.*
(b) *Die symmetrische Gruppe S_n ist auflösbar genau dann, wenn $n \leqslant 4$ ist.*

1.9 Die Sylow-Sätze

Definition 1.9.1 *Sei p eine Primzahl und G eine endliche Gruppe. Wir schreiben die Ordnung von G als $\#G = m \cdot p^\ell$ für $\ell, m \in \mathbb{N}$ mit $p \nmid m$.*

(a) *Eine **p-Untergruppe** von G ist eine Untergruppe, die eine p-Gruppe ist (also der Ordnung p^k für ein $k \leqslant \ell$).*

(b) *Eine **Sylow-p-Untergruppe** von G ist eine Untergruppe der Ordnung genau p^ℓ.*

Satz 1.9.2 (Sylow-Sätze) *Sei G endlich und sei p eine Primzahl. Wir schreiben $\#G = m \cdot p^\ell$ für $\ell, m \in \mathbb{N}$ mit $p \nmid m$. Dann gilt:*

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

(b) *Ist s die Anzahl der Sylow-p-Untergruppen von G, so gilt $s \equiv 1 \mod p$ und $s \mid m$.*

(c) *Alle Sylow-p-Untergruppen von G sind konjugiert, d. h. sind $H, H' \subset G$ Sylow-p-Untergruppen, so gibt es ein $a \in G$ mit $aHa^{-1} = H'$.*

2 Ringe

Es gibt verschieden allgemeine Definitionen von Ringen. In dieser Vorlesung werden, wenn nicht anders angegeben, alle Ring kommutativ und mit 1 sein.

2.1 Ringe und Unterringe

Definition 2.1.1 *Ein **kommutativer Ring mit eins** ist eine Tripel $(R, +, \cdot)$ bestehend aus einer Menge R mit zwei Verknüpfungen $+, \cdot \colon R \times R \to R$ mit folgenden Eigenschaften:*

(a) *$(R, +)$ ist eine abelsche Gruppe;*

(b) *$\cdot$ ist assoziativ und kommutativ;*

(c) *es gibt ein bezüglich $\cdot$ neutrales Element (das mit 1 bezeichnet wird);*

(d) *Distributivität gilt (d. h. für alle $a, b, c \in R$ gilt: $a \cdot (b + c) = a \cdot c + b \cdot c$).*

Bemerkung 2.1.2 *Das neutrale Element bezüglich $\cdot$ ist eindeutig.*

Notation 2.1.3 (a) *Wenn bei einem Ring $(R, +, \cdot)$ klar ist, was die Verknüpfungen sein sollen, sagen wir oft einfach nur „R ist ein Ring“.*

(b) *Für $a \in R$ und $n \in \mathbb{N}$ setzen wir:*
$n \cdot a := \underbrace{a + a + \cdots + a}_{n}$, $(-n) \cdot a := -(n \cdot a)$,
$a^0 = 1$, $a^n := \underbrace{a \cdot a \cdots a}_{n}$

Beispiel 2.1.4 *Ist R ein Ring, so ist auch $R[X] = \{\sum_{i=0}^{n} a_i X^i \mid n \in \mathbb{N}, a_i \in R\}$ ein Ring (der **Polynomring** über R). Die Elemente von $R[X]$ heißen **Polynome**; Elemente von $R[X]$ der Form aX^k (für $a \in R$, $k \in \mathbb{N}$) nennt man **Monome**.*

Beispiel 2.1.5 *Ist R ein Ring und sind $X_1, \ldots, X_k$ verschiedene Variablen, so setzen wir $R[X_1, \ldots, X_k] := R[X_1][X_2] \ldots [X_k]$. In diesem Fall ist ein **Monom** ein Element der Form $a \cdot X_1^{n_1} \cdots X_k^{n_k}$, mit $a \in R$ und $n_1, \ldots, n_k \in \mathbb{N}$. Jedes Element von $R[X_1, \ldots, X_k]$ ist eine endliche Summen von Monomen.*

Definition 2.1.6 *Sei R ein Ring. Ein* ***Unterring*** *(genauer: Unterring mit 1) von R ist eine Teilmenge $S \subset R$, so dass S ein Ring ist (mit der auf S eingeschränkten Addition von Multiplikation von R) und $1 \in S$ gilt.*

Definition 2.1.7 *Seien R und S Ringe. Das* ***(direkte) Produkt*** *von R und S ist die Menge $R \times S$ mit der komponentenweiser Verknüpfung:*

$$(a,b) + (a',b') := (a+a', b+b') \qquad \textit{und} \qquad (a,b) \cdot (a',b') := (a \cdot a', b \cdot b')$$

für $a, a' \in R$, $b, b' \in S$.

2.2 Ideale und Quotienten

Definition 2.2.1 *Sei R ein Ring. Ein* ***Ideal*** *von R ist eine additive Untergruppe $\mathfrak{a} \subset R$, so dass außerdem für alle $r \in R$ und $a \in \mathfrak{a}$ gilt: $ra \in \mathfrak{a}$.*

Bemerkung: Eine nicht-leere Teilmenge $\mathfrak{a} \subset R$ ist ein Ideal, wenn für alle $a, b \in \mathfrak{a}$ und alle $r \in R$ gilt: $a + b \in \mathfrak{a}$ und $ra \in \mathfrak{a}$.

Bemerkung 2.2.2 *Die einzigen Ideale eines Körpers K sind $\{0\}$ und K.*

Satz 2.2.3 *Ist R ein Ring und sind $\mathfrak{a}_i \subset R$ Ideale für $i \in I$, wobei I eine beliebige, nicht-leere Indexmenge ist, so ist $\bigcap_{i \in I} \mathfrak{a}_i$ auch ein Ideal.*

Definition 2.2.4 *Sei R ein Ring und $A \subset R$ eine beliebige Teilmenge. Das von A* ***erzeugte*** *Ideal ist*

$$(A) := \bigcap_{\substack{\mathfrak{a} \subset R \text{ Ideal} \\ \text{mit } A \subset \mathfrak{a}}} \mathfrak{a}.$$

Satz 2.2.5 *Ist R ein Ring und $A \subset R$, so ist*

$$(A) = \{ \sum_{i=1}^{n} r_i a_i \mid n \in \mathbb{N}, r_i \in R, a_i \in A \}.$$

Satz 2.2.6 *Ist R ein Ring und $\mathfrak{a} \subset R$ ein Ideal, so wird durch $(a+\mathfrak{a}) \cdot (b+\mathfrak{a}) := (ab) + \mathfrak{a}$ (für $a, b \in R$) eine Verknüpfgung auf der additiven Gruppe $R/\mathfrak{a}$ definiert; $R/\mathfrak{a}$ ist mit dieser Verknüpfung ein Ring.*

Definition 2.2.7 *Der Ring $R/\mathfrak{a}$ („R* ***modulo*** *$\mathfrak{a}$“) aus dem vorigen Satz wird* ***Quotientenring*** *(oder manchmal auch* ***Faktorring*** *oder* ***Restklassenring****) genannt. Ist klar, welches Ideal $\mathfrak{a}$ gemeint ist, so schreiben wir statt $a + \mathfrak{a}$ oft $\bar{a}$ (für $a \in R$).*

Beispiel 2.2.8 *Ist K ein Körper und $f \in K[X]$ ein Polynom vom Grad $n \geqslant 1$, so lässt sich jedes Element von $K[X]/(f)$ eindeutig schreiben in der Form $a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} + (f)$, für $a_0, \ldots, a_{n-1} \in K$.*

2.3 Ringhomomorphismen und der Isomorphiesatz

Definition 2.3.1 *Seien R und S Ringe. Ein **Ringhomomorphismus** (genauer: Homomorphismus von Ringen mit 1) ist eine Abbildung $f\colon R \to S$, so dass für alle $a, b \in R$ gilt: $f(a+b) = f(a) + f(b)$; $f(a \cdot b) = f(a) \cdot f(b)$; $f(1) = 1$.* $\mathrm{Hom}(R, S)$ *bezeichnet die Menge aller Ringhomomorphismen von R nach S.*

*Das **Bild** von f ist* $\operatorname{im} f := \{f(a) \mid a \in R\}$*; der **Kern** von f ist* $\ker f := \{a \in R \mid f(a) = 0\}$.

*Ein **Isomorphismus von Ringen** ist ein bijektiver Ringhomomorphismus.*

*Zwei Ringe R und S heißen **isomorph** (Notation: $R \cong S$), wenn es einen Isomorphismus $R \to S$ gibt.*

*Ein **Endomorphismus** eines Rings R ist ein Homomorphismus von R nach R. Die Menge der Endomorphismen von R wird mit* $\mathrm{End}(R)$ *bezeichnet.*

*Ein **Automorphismus** eines Rings R ist ein Isomorphismus von R nach R. Die Menge der Automorphismen von R wird mit* $\mathrm{Aut}(R)$ *bezeichnet.*

Bemerkung 2.3.2 *Ist $f\colon R \to S$ ein Ringhomomorphismus, so gilt $f(0) = 0$ und, für $a \in R$, $f(-a) = -f(a)$.*

Bemerkung 2.3.3 *Die Verknüpfung von zwei Ringomomorphismen ist wieder ein Ringhomomorphismus. Das Inverse eines Ring-Isomorphismus ist wieder ein Ring-Isomorphismus.*

Beispiel 2.3.4 *Ist R ein Ring und $a \in R$, so ist die Abbildung $R[X] \to R, f \mapsto f(a)$ ein Ringhomomorphismus.*

Beispiel 2.3.5 *Ist R ein Ring und $\mathfrak{a} \subset R$ ein Ideal, so ist die Abbildung $R \to R/\mathfrak{a}, a \mapsto a + \mathfrak{a}$ ist ein Ringhomomorphismus.*

Beispiel 2.3.6 $\mathbb{R}[X]/(X^2+1) \cong \mathbb{C}$.

Beispiel 2.3.7 *Ist R ein beliebiger Ring, so gibt es genau einen Ringhomomorphismus $\mathbb{Z} \to R$. Er bildet $n \geqslant 1$ auf $\underbrace{1 + \cdots + 1}_{n \text{ mal}}$ ab.*

Satz 2.3.8 *Sind R und S Ringe und ist $f\colon R \to S$ ein Ringhomomorphismus, so ist* $\operatorname{im} f$ *ein Unterring von S und* $\ker f$ *ein Ideal von R.*

Satz 2.3.9 (Isomorphiesatz) *Seien R und S Ringe und $f\colon R \to S$ ein Homomorphismus. Dann erhalten wir einen Isomorphismus $\tilde{f}\colon R/\ker f \to \operatorname{im} f$, so dass für alle $a \in R$ gilt: $\tilde{f}(\bar{a}) = f(a)$.*

2.4 Integritätsbereiche

Definition 2.4.1 *Ein Ring R heißt **Integritätsbereich** (oder **nullteilerfrei**) wenn für alle $a, b \in R\backslash\{0\}$ gilt: $a \cdot b \neq 0$.*

Satz 2.4.2 *Ist R ein Integritätsbereich und sind $a, b \in R$ und $c \in R\backslash\{0\}$ mit $ac = bc$, so gilt $a = b$.*

Satz 2.4.3 *Sei R ein Integritätsbereich. Dann existiert ein Körper K und ein injektiver Ringhomomorphismus $f\colon R \to K$ so dass jedes Element von K sich schreiben lässt als $\frac{f(a)}{f(b)}$ für geeignete $a \in R, b \in R\backslash\{0\}$.*

Definition 2.4.4 *Der Körper K aus Satz 2.4.3 wird* ***Quotientenkörper*** *von R genannt und mit $\mathrm{Quot}(R)$ bezeichnet.*

Notation 2.4.5 *Jeden Integritätsbereich R fassen wir in Zukunft als Teilmenge von $\mathrm{Quot}(R)$ auf; insbesondere ist, für $a, b \in R$ mit $b \neq 0$, „$\frac{a}{b}$“ als Element von $\mathrm{Quot}(R)$ wohldefiniert.*

Satz 2.4.6 *Der Quotientenkörper eines Integritätsbereichs R hat die folgende universelle Eigenschaft: Ist $f' \colon R \to K'$ ein injektiver Ringhomomorphismus in einen Körper K', so gibt es genau eine Fortsetzung von f' zu einem Ringhomomorphismus $g \colon \mathrm{Quot}(R) \to K'$.*

Satz 2.4.7 *Ist R ein Integritätsbereich, so gilt für Polynome $f, g \in R[X]\backslash\{0\}$: $\deg(fg) = \deg f + \deg g$. Insbesondere ist auch $R[X]$ ein Integritätsbereich.*

Definition 2.4.8 *Ist K ein Körper, so schreibt man den Quotientenkörper des Polynomrings mit runden Klammern: $K(X_1, \ldots, X_n) := \mathrm{Quot}(K[X_1, \ldots, X_n])$.*

2.5 Faktorielle Ringe

Definition 2.5.1 *Sei R ein Ring.*

(a) *Eine* ***Einheit*** *von R ist ein Element $a \in R$, so dass es ein $b \in R$ gibt mit $ab = 1$. Die Menge der Einheiten von R wird mit $R^\times$ bezeichnet.*

(b) *Für $a, b \in R$ sagt man „a* ***teilt*** *b“, wenn es ein $c \in R$ gibt mit $a \cdot c = b$. Notation dafür: $a \mid b$. Man sagt auch a ist ein* ***Teiler*** *von b oder b ist ein* ***Vielfaches*** *von a.*

(c) *Ein Element $a \in R$ heißt* ***irreduzibel*** *(in R) wenn a keine Einheit ist und aus $b \cdot c = a$ (für $b, c \in R$) folgt, dass b oder c eine Einheit ist.*

(d) *Zwei Elemente $a, b \in R$ heißen* ***teilerfremd****, wenn aus $c \mid a$ und $c \mid b$ folgt, dass c eine Einheit ist (für $c \in R$).*

Satz 2.5.2 *Die Menge $R^\times$ der Einheiten eines Rings R bildet eine Gruppe bezüglich der Multiplikation.*

Bemerkung 2.5.3 *Sei R ein Integritätsbereich und seien $a, b, c \in R\backslash\{0\}$. Dann gilt:*

(a) $a \mid b \iff b \in (a) \iff (b) \subset (a) \iff \frac{b}{a} \in R$

(b) $a \mid b \wedge b \mid c \Rightarrow a \mid c$

(c) $a \mid b \Rightarrow ac \mid bc$

(d) $a \mid b \wedge a \mid c \Rightarrow a \mid (b + c)$

(e) $a \mid 1 \iff a \in R^\times \iff (a) = R \iff a^{-1} \in R$

(f) $(a \mid b \wedge b \mid a) \iff \frac{a}{b} \in R^\times \iff (a) = (b)$

(g) *Sind a und b irreduzibel, so ist $\frac{a}{b} \in R^\times$ oder a und b sind teilerfremd.*

Beispiel 2.5.4 *Für beliebige Ringe R gilt: $(R[X])^\times = R^\times$.*

Definition 2.5.5 *Ein Ring R heißt* ***faktoriell*** *wenn er ein Integritätsbereich ist und „eindeutige Primfaktorzerlegungen“ existieren, d. h. wenn folgendes gilt:*

(a) *Zu jedem $a \in R\backslash\{0\}$ gibt es irreduzible Elemente $p_1, \ldots, p_k \in R$ und eine Einheit $e \in R^\times$ mit $a = e \cdot p_1 \cdot p_2 \cdots p_k$. (Dies nennt man eine* ***Primfaktorzerlegung*** *von a.)*

(b) *Ist* $a = e' \cdot p'_1 \cdot p'_2 \cdots p'_{k'}$ *eine weitere Primfaktorzerlegung von* a*, so ist* $k' = k$*, und nach Umnummerierung gilt* $\frac{p'_i}{p_i} \in R^\times$*.*

Definition 2.5.6 (a) *Ein Ideal* $\mathfrak{a}$ *in einem Ring* R *heißt* ***Hauptideal****, wenn es ein* $a \in R$ *gibt mit* $\mathfrak{a} = (a)$*.*
(b) *Ein Integritätsbereich* R *heißt* ***Hauptidealring****, wenn jedes Ideal ein Hauptideal ist.*

Definition 2.5.7 *Ein Integritätsbereich* R *heißt* ***euklidisch****, wenn es eine Abbildung* $\sigma\colon R\backslash\{0\} \to \mathbb{N}$ *gibt, so dass folgendes gilt: Sind* $a, b \in R\backslash\{0\}$*, so gibt es* $c, r \in R$ *mit* $a = bc + r$ *und entweder* $r = 0$ *oder* $\sigma(r) < \sigma(b)$*.*

Beispiel 2.5.8 $\mathbb{Z}$ *ist euklidisch mit* $\sigma(a) := |a|$*.*

Beispiel 2.5.9 *Ist* K *ein Körper, so ist* $K[X]$ *euklidisch mit* $\sigma(f) := \deg f$*.*

Satz 2.5.10 *Ist* R *euklidisch, so ist* R *ein Hauptidealring.*

Lemma 2.5.11 *Sei* R *ein Hauptidealring und seien* $a, b, b' \in R\backslash\{0\}$*.*
(a) a *und* b *sind teilerfremd genau dann, wenn* $(a, b) = R$ *ist.*
(b) *Ist* a *teilerfremd zu* b *und zu* b'*, so ist* a *auch teilerfremd zu* bb'*.*

Satz 2.5.12 *Hauptidealringe sind faktoriell.*

Bemerkung 2.5.13 *Ist* R *ein faktorieller Ring und sind* $a, b, b' \in R\backslash\{0\}$ *so dass* a *teilerfremd zu* b *und auch zu* b' *ist, so ist* a *auch teilerfremd zu* bb'*.*

2.6 p-Bewertungen

In diesem gesamten Abschnitt sei R ein faktorieller Ring und $K = \mathrm{Quot}(R)$.

Satz 2.6.1 *Ist* $p \in R$ *irreduzibel, so lässt sich jedes Element* $c \in K^\times$ *schreiben als* $c = p^n \frac{a}{b}$ *für* $a, b \in R$*, die zu* p *teilerfremd sind und für ein* $n \in \mathbb{Z}$*. Hierbei ist* n *durch* p *und* c *eindeutig festgelegt.*

Definition 2.6.2 *Die Zahl* n *aus Satz 2.6.1 heißt „*p***-Bewertung** *von* c*“ und wird mit* $v_p(c)$ *bezeichnet. Man setzt* $v_p(0) := \infty$*.*

Satz 2.6.3 *Jedes Element* $c \in \mathrm{Quot}(R)$ *lässt sich schreiben als*

$$c = e \cdot \prod_{i=1}^{k} p_i^{v_{p_i}(a)},$$

wobei die $p_i \in R$ *irreduzibel sind,* $e \in R^\times$*, und für* $i \neq j$ *ist* p_i/p_j *keine Einheit.*
Insbesondere ist $c \in R$ *genau dann, wenn* $v_p(c) \geqslant 0$ *für alle irreduziblen* p*.*

Bemerkung 2.6.4 *Sei* $p \in R$ *irreduzibel.*
(a) *Für* $a, b \in K\backslash\{0\}$ *gilt:* $v_p(ab) = v_p(a) + v_p(b)$*.*
(b) *Für* $a \in R$ *und* $m \in \mathbb{Z}$ *gilt:* $p^m \mid a \iff v_p(a) \geqslant m$*.*

2.7 Polynomringe

Sei weiterhin R ein faktorieller Ring und $K = \mathrm{Quot}(R)$.

Lemma 2.7.1 *Ist $p \in R$ irreduzuibel, so ist $R/(p)$ ein Integritätsbereich.*

Definition 2.7.2 *Sei $p \in R$ irreduzibel und sei $f = \sum_{i=0}^{n} a_i X^i \in K[X]$. Dann setzen wir $v_p^*(f) := \min_i v_p(a_i)$.*

Satz 2.7.3 *Für $f, g \in K[X]$ gilt: $v_p^*(fg) = v_p^*(f) + v_p^*(g)$.*

Satz 2.7.4 *Ist $f \in R[X] \backslash R$ irreduzibel in $R[X]$, so ist f auch irreduzibel in $K[X]$. Genauer gilt: ist $f = g \cdot h$ für $g, h \in K[X]$, so gibt es ein $c \in K^\times$, so dass $c^{-1} \cdot g$ und $c \cdot h$ in $R[X]$ liegen.*

Satz 2.7.5 (Satz von Gauß) *Ist R faktoriell, so auch $R[X]$.*

Korollar 2.7.6 (a) *Ist K ein Körper, so ist $K[X_1, \ldots, X_n]$ faktoriell.*
(b) *$\mathbb{Z}[X_1, \ldots, X_n]$ ist faktoriell.*

Satz 2.7.7 (Eisensteinsches Irreduzibilitätskriterium) *Ist $f = \sum a_i X^i \in R[X]$ ein Polynom vom Grad $n \geqslant 1$, und gibt es ein irreduzibles Element $p \in R$ mit $p \mid a_i$ für $i < n$, $p^2 \nmid a_0$ und $p \nmid a_n$, so ist f irreduzibel in $K[X]$.*

Beispiel 2.7.8 *Ist p prim, so ist $f(X) := X^{p-1} + X^{p-2} + \cdots + X + 1$ irreduzibel in $\mathbb{Q}[X]$.*

2.8 Maximale Ideale

Definition 2.8.1 *Sei R ein Ring. Ein Ideal $\mathfrak{a} \subsetneq R$ heißt **maximal**, wenn es kein Ideal $\mathfrak{b} \subsetneq R$ gibt mit $\mathfrak{a} \subsetneq \mathfrak{b}$.*

Satz 2.8.2 *Sei R ein Hauptidealring und $a \in R$. Das Hauptideal (a) ist maximal genau dann, wenn a irreduzibel ist.*

Satz 2.8.3 *Ein Ideal $\mathfrak{a}$ in einem Ring R ist maximal genau dann, wenn $R/\mathfrak{a}$ ein Körper ist.*

Satz 2.8.4 *Sei R ein Ring und $\mathfrak{a} \subsetneq R$ ein beliebiges Ideal. Dann existiert ein maximales Ideal $\mathfrak{a}_0 \supset \mathfrak{a}$.*

2.9 Der chinesische Restsatz für Ringe

Satz 2.9.1 (Chinesischer Restsatz, Ringversion) *Ist R ein Ring und sind $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ Ideale, so dass für alle $i \neq j$ das von $\mathfrak{a}_i \cup \mathfrak{a}_j$ erzeugte Ideal bereits ganz R ist, so ist der Ringhomomorphismus*

$$R \to (R/\mathfrak{a}_1 \times \cdots \times R/\mathfrak{a}_n), a \mapsto (a + \mathfrak{a}_1, \ldots, a + \mathfrak{a}_n)$$

surjektiv, und der Kern ist $\mathfrak{a}_1 \cap \mathfrak{a}_2 \cap \cdots \cap \mathfrak{a}_n$.

3 Körper

3.1 Körpererweiterungen

Definition 3.1.1 *Sei R ein Ring. Der Kern des Ringhomomorphismus $\mathbb{Z} \to R$ (aus Beispiel 2.3.7) hat die Form $n\mathbb{Z}$, für ein $n \in \mathbb{N}$. Dieses n nennt man die* ***Charakteristik*** *von R, und man schreibt* $\operatorname{char} R$ *dafür.*

Satz 3.1.2 *Ist K ein Körper, so ist* $\operatorname{char} K$ *entweder* 0 *oder eine Primzahl.*

Definition 3.1.3 *Sei L ein Körper. Ein* ***Unterkörper*** *ist eine Teilmenge $K \subset L$, so dass K auch wieder ein Körper ist. Man nennt L dann einen* ***Oberkörper*** *von K, und man schreibt auch „L/K ist eine* ***Körpererweiterung***“ *um zu sagen, dass L ein Körper ist und K ein Unterkörper von L.*

Bemerkung 3.1.4 *Ist L/K eine Körpererweiterung, so ist L ein K-Vektorraum.*

Definition 3.1.5 *Der* ***Grad*** *einer Körpererweiterung L/K ist $[L : K] := \dim_K L$, d. h. die Dimension von L als K-Vektorraum aufgefasst. ($[L : K]$ kann auch ∞ sein.) Eine* ***endliche Körpererweiterung*** *ist eine Körpererweiterung von endlichem Grad.*

Satz 3.1.6 *Sind $K \subset L \subset M$ Körper, so gilt $[M : K] = [M : L] \cdot [L : K]$. Insbesondere ist $[M : K]$ endlich genau dann, wenn sowohl $[M : L]$ als auch $[L : K]$ endlich sind.*

Satz 3.1.7 *Ist K ein beliebiger Körper, und sind $K_i \subset K$ Unterkörper für $i \in I$, so ist der Schnitt $\bigcap_{i \in I} K_i$ auch ein Unterkörper von K. Insbesondere enthält jeder Körper K einen kleinsten Unterkörper.*

Definition 3.1.8 *Den kleinsten Unterkörper eines Körpers K nennt man den* ***Primkörper*** *von K.*

Satz 3.1.9 *Der Primkörper eines Körpers K ist isomorph zu $\mathbb{Q}$ falls* $\operatorname{char} K = 0$ *ist und isomorph zu $\mathbb{F}_p$ falls* $\operatorname{char} K = p$ *ist für eine Primzahl p.*

3.2 Adjunktion von Elementen

Definition 3.2.1 *Sind $K \subset L$ Körper und sind $a_i \in L$ für $i \in I$, so schreibt man $K((a_i)_{i \in I})$ für den kleinsten Unterkörper von L, der K und alle a_i enthält. Man nennt dies den von den a_i* ***erzeugten Körper*** *(über K). Man sagt auch, $K((a_i)_{i \in I})$ ist der Körper, den man aus K durch* ***Adjunktion*** *der Elemente a_i erhält.*

Satz 3.2.2 *Sei L/K eine Körpererweiterung und sei $a \in L$. Wenn es überhaupt ein Polynom $f \in K[X] \backslash \{0\}$ gibt mit $f(a) = 0$, dann gibt es genau ein normiertes Polynom $f_0 \in K[X] \backslash \{0\}$ minimalen Grades, für das $f_0(a) = 0$ gilt. Dieses f_0 ist auch das einzige normierte irreduzible Polynom mit $f_0(a) = 0$, und für beliebige Polynome $f \in K[X]$ gilt: $f(a) = 0 \iff f_0 \mid f$.*

Definition 3.2.3 *Sei L/K eine Körpererweiterung und sei $a \in L$.*

(a) *a heißt* ***algebraisch*** *über K, wenn es ein Polynom $f \in K[X] \backslash \{0\}$ gibt mit $f(a) = 0$. Sonst nennt man a* ***transzendent*** *über K.*

(b) *Ist a algebraisch über K, so nennt man das Polynom f_0 aus Satz 3.2.2 das Minimalpolynom von a (über K). Notation dafür:* $\mathrm{MiPo}_{a/K}$. *Den Grad* $\deg \mathrm{MiPo}_{a/K}$ *nennt man auch den* ***Grad*** *von a über K.*

Man nennt eine komplexe Zahl algebraisch bzw. transzendent, wenn sie algebraisch über $\mathbb{Q}$ ist bzw. transzendent über $\mathbb{Q}$.

Beispiel 3.2.4 *Ist $n \in \mathbb{N}$ keine Quadratzahl, so hat $\sqrt{n}$ das Minimalpolynom* $\mathrm{MiPo}_{\sqrt{n}/\mathbb{Q}} = X^2 - n$. *Insbesondere ist $\sqrt{n} \notin \mathbb{Q}$.*

Satz 3.2.5 *Ist L/K eine Körpererweiterung und ist $a \in L$, so gilt:*

(a) *Ist a algebraisch über K, so ist $[K(a) : K]$ gleich dem Grad von a über K, und es gibt (genau) einen Isomorphismus $K[X]/(\mathrm{MiPo}_{a/K}) \to K(a)$, der auf K die Identität ist und $\bar{X}$ auf a abbildet.*

(b) *Ist a transzendent über K, so ist $[K(a) : K] = \infty$, und es gibt (genau) einen Isomorphismus* $\mathrm{Quot}\, K[X] \to K(a)$, *der auf K die Identität ist und X auf a abbildet.*

Definition 3.2.6 *Sei $n \in \mathbb{N}$, $n \geqslant 1$. Eine* ***n-te Einheitswurzel*** *ist eine komplexe Zahl z, so dass $z^n = 1$ ist. Eine* ***primitive n-te Einheitswurzel*** *ist eine n-te Einheitswurzel, die keine k-te Einheitswurzel für $k < n$ ist.*

Bemerkung 3.2.7 $\zeta_n := e^{2\pi i/n}$ *ist eine primitive n-te Einheitswurzel.*

Beispiel 3.2.8 *Sei p prim und sei $\zeta_p := e^{2\pi i/n}$. Dann ist $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$.*

Satz 3.2.9 *Sind $M/L/K$ Körpererweiterungen und ist $a \in M$, so ist $[L(a) : L] \leqslant [K(a) : K]$.*

Bemerkung: In der Situation aus Satz 3.2.9 muss $[L(a) : L]$ kein Teiler von $[K(a) : K]$ sein.

Satz 3.2.10 *Sei L die Menge der komplexen Zahlen, die sich als Ausdruck schreiben lassen, in dem nur rationale Zahlen, plus, minus, mal, durch und Quadratwurzeln vorkommen. Formaler: Sei L der kleinste Körper, der $\mathbb{Q}$ enthält und für den gilt: $\forall a \in \mathbb{C} : a^2 \in L \Rightarrow a \in L$. Ein $a \in \mathbb{C}$ liegt genau dann in L, wenn es $a_1, \ldots, a_n = a \in \mathbb{C}$ gibt, so dass $a_i^2 \in \mathbb{Q}(a_1, \ldots, a_{i-1})$ gilt für $i = 1, \ldots, n$. Insbesondere gilt, für alle $a \in L$: $[\mathbb{Q}(a) : \mathbb{Q}]$ ist eine Zweierpotenz.*

Beispiel 3.2.11 $\sqrt[3]{2} \notin L$.

3.3 Anwendung: Konstruktion mit Zirkel und Lineal

Definition 3.3.1 *Sei $E \subset \mathbb{C}$.*

(a) *Eine Gerade $G = \{a + rb \mid r \in \mathbb{R}\}$ (für $a \in \mathbb{C}, b \in \mathbb{C}^\times$) ist aus E* ***1-Schritt-konstruierbar****, wenn sie mindestens zwei verschiedene Elemente von E enthält.*

(b) *Ein Kreis $K = \{z \in \mathbb{C} \mid |z - m| = r\}$ (für $m \in \mathbb{C}, r \in \mathbb{R}_{>0}$) ist aus E* ***1-Schritt-konstruierbar****, wenn sein Mittelpunkt m in E liegt und es $z_1, z_2 \in E$ gibt mit $|z_1 - z_2| = r$.*

(c) *Ein Punkt $z \in \mathbb{C}$ ist aus E* ***1-Schritt-konstruierbar****, wenn $z \in F_1 \cap F_2$ ist, wobei F_1 und F_2 zwei verschiedene Geraden, zwei verschiedene Kreise oder eine Gerade und ein Kreis sind, die beide aus E 1-Schritt-konstruierbar sind.*

(d) *Ein Punkt $z \in \mathbb{C}$ heißt aus E **konstruierbar**, wenn es $z_1, \dots, z_n = z \in \mathbb{C}$ gibt, so dass z_i aus $E \cup \{z_1, \dots, z_{i-1}\}$ 1-Schritt-konstruierbar ist, für $i = 1, \dots, n$.*

Satz 3.3.2 *Die Menge der aus $\{0,1\}$ konstruierbaren Punkte ist genau der Körper L aus Satz 3.2.10.*

Korollar 3.3.3 *„Würfelverdopplung ist nicht mit Zirkel und Lineal möglich“: Aus $\{0,1\}$ lassen sich keine Punkte $a, b \in \mathbb{C}$ konstruieren, deren Abstand die Kantenlänge eines Würfels mit Volumen 2 ist.*

Korollar 3.3.4 *Ist $p \geqslant 3$ prim und $p-1$ keine Zweierpotenz, so lässt sich das regelmäße p-Eck nicht mit Zirkel und Lineal konstruieren.*

Korollar 3.3.5 *Ist $p \geqslant 3$ prim, so lässt sich das regelmäße p^2-Eck nicht mit Zirkel und Lineal konstruieren.*

Korollar 3.3.6 *Das regelmäßige n-Eck lässt sich genau dann konstruieren, wenn $n = 2^\ell \cdot p_1 \cdots p_k$ ist für $\ell \in \mathbb{N}$ und paarweise verschiedene Primzahlen $p_i \geqslant 3$, für die $p_i - 1$ eine Zweierpotenz ist.*

(Der Beweis der Konstruierbarkeit des p-Ecks, falls $p-1$ eine Zweierpotenz ist, kommt später.)

Korollar 3.3.7 *Es gibt keine Konstruktion mit Zirkel und Lineal, mit der beliebige Winkel gedrittelt werden können.*

3.4 Algebraische Körpererweiterungen

Definition 3.4.1 *Eine Körpererweiterung L/K heißt **algebraisch**, wenn alle $a \in L$ algebraisch über K sind.*

Satz 3.4.2 *Ist L/K eine beliebige Körpererweiterung, so ist die Menge $\{a \in L \mid a \text{ ist algebraisch über } K\}$ ein Unterkörper von L.*

Satz 3.4.3 *Ist L/K algebraisch und M/L algebraisch, so ist auch M/K algebraisch.*

Satz 3.4.4 *Für einen Körper K sind äquivalent:*
(a) *Jedes Polynom in $K[X]$ zerfällt in Linearfaktoren.*
(b) *Jedes irreduzible Polynom in $K[X]$ hat Grad 1.*
(c) *Die einzige algebraische Körpererweiterung von K ist K selbst.*
(d) *Jedes Polynom in $K[X]$ hat (mindestens) eine Nullstelle in K.*

Definition 3.4.5 *Ein Körper K, der die Bedingungen aus Satz 3.4.4 erfüllt, heißt **algebraisch abgeschlossen**.*

Bemerkung 3.4.6 *Sind K und L Körper und ist $f\colon K \to L$ ein Ringhomomorphismus, so ist f automatisch injektiv.*

Definition 3.4.7 *Einen Ringhomomorphismus $f\colon K \to L$ zwischen Körpern K und L nennt man auch **Körperhomomorphismus**; entsprechend sagt man auch **Körperisomorphismus** und **Körperautomorphismus**. Wegen der vorigen Bemerkung nennt man einen Körperhomomorphismus $f\colon K \to L$ auch oft eine „**Einbettung** von K in L“.*

Satz 3.4.8 *Ist K ein Körper, $L \supset K$ eine algebraische Erweiterung von K und $M \supset K$ algebraisch abgeschlossen, so gibt es eine Einbettung $L \to M$, die die Identität auf K ist.*

Bemerkung: Bessere Formulierung von Satz 3.4.8: Sind K, L, M Körper und $\phi_1 \colon K \to L$ und $\phi_2 \colon K \to M$ Einbettungen, so dass $L/\phi_1(K)$ algebraisch ist und M algebraisch abgeschlossen, so gibt es eine Einbettung $\psi \colon L \to M$ mit $\phi_2 = \psi \circ \phi_1$.

Satz 3.4.9 *Zu jedem Körper K gibt es eine algebraische Erweiterung $L \supset K$, die algebraisch abgeschlossen ist. Diese algebraische Erweiterung ist eindeutig bis auf Isomorphismus über K.*

Definition 3.4.10 *Den Körper L aus Satz 3.4.9 nennt man den **algebraischen Abschluss** von K; Notation für den algebraischen Abschluss: K^{alg}.*

Bemerkung 3.4.11 *Ist K ein Körper und ist $\phi \in \mathrm{End}(K^{\mathrm{alg}})$ ein Endomorphismus, der auf K die Identität ist, so ist ϕ schon ein Autormophismus von K^{alg}.*

Bemerkung 3.4.12 *Ist L/K eine algebraische Körpererweiterung, so können (und werden) wir L nach Satz 3.4.8 als Unterkörper von K^{alg} auffassen.*

Definition 3.4.13 *Sei L/K eine Körpererweiterung. Ein „**Autormorphismus von L über K**“ ist ein Automorphismus von L, der die Identität auf K ist. Man schreibt $\mathrm{Aut}(L/K)$ für die Menge der Automorphismen von L über K. Sei $L' \supset K$ ein weiterer Oberkörper. Eine „**Einbettung von L in L' über K**“ ist eine Einbettung von L in L', die auf K die Identität ist.*

Bemerkung 3.4.14 *Ist $K \subset L \subset M$, so ist $\mathrm{Aut}(M/L)$ eine Untergruppe von $\mathrm{Aut}(M/K)$.*

Satz 3.4.15 *Sei K ein Körper und seien $a_1, a_2 \in K^{\mathrm{alg}}$. Dann liegen a_1 und a_2 genau dann in der gleichen Bahn unter der Operation von $\mathrm{Aut}(K^{\mathrm{alg}}/K)$ auf K^{alg}, wenn sie das selbe Minimalpolynom über K haben.*

3.5 Normale Körpererweiterungen

Definition 3.5.1 *Sei K ein Körper. Der **Zerfällungskörper** (über K) eines Polynoms $f \in K[X] \backslash \{0\}$ ist der kleinste Unterkörper $L \subset K^{\mathrm{alg}}$, der K enthält und so dass f in $L[X]$ in Linearfaktoren zerfällt.*

Satz 3.5.2 *Ist $f \in K[X]$ und sind $a_1, \ldots, a_n \in K^{\mathrm{alg}}$ die Nullstellen von f, so ist $L := K(a_1, \ldots, a_n)$ der Zerfällungskörper von f. Es gilt $[L : K] \leqslant n!$.*

Satz 3.5.3 *Die folgenden Bedingungen an eine endliche Körpererweiterung L/K sind äquivalent:*

(a) *L ist Zerfällungskörper eines Polynoms $f \in K[X] \backslash \{0\}$.*
(b) *Für alle $a \in L$ zerfällt $\mathrm{MiPo}_{a/K}$ in $L[X]$ in Linearfaktoren.*
(c) *Jeder Automorphismus $\sigma \in \mathrm{Aut}(K^{\mathrm{alg}}/K)$ bildet L auf sich selbst ab. (Insbesondere ist $\sigma|_L \in \mathrm{Aut}(L/K)$.)*

Definition 3.5.4 *Wenn die Bedingungen aus Satz 3.5.3 gelten, nennt man die Körpererweiterung L/K* ***normal****. Man sagt auch: „L ist* ***normal*** *über K“. (Ist L/K unendlich, so sind nur noch (b) und (c) äquivalent, und man verwendet dies als Definition von normal.)*

Bemerkung 3.5.5 *Sind $K \subset L \subset M$ Körper und ist M/K normal, so ist auch M/L normal.*

3.6 Separable Körpererweiterungen

Satz 3.6.1 *Ist K ein Körper der Charakteristik 0 und $f \in K[X]$ irreduzibel, so hat f in K^{alg} keine mehrfachen Nullstellen (d. h. alle Linearfaktoren von f in $K^{\mathrm{alg}}[X]$ sind verschieden).*

Definition 3.6.2 *Sei L/K eine algebraische Körpererweiterung.*

(a) *Ein Element $a \in L$ heißt* ***separabel*** *über K wenn sein Minimalpolynom $\mathrm{MiPo}_{a/K}$ keine mehrfachen Nullstellen in K^{alg} hat.*

(b) *Die Körpererweiterung L/K heißt* ***separabel****, wenn alle Elemente von L separabel über K sind.*

Bemerkung 3.6.3 *Nach Satz 3.6.1 ist eine algebraische Körpererweiterung L/K immer separabel, wenn $\operatorname{char} K = 0$ ist.*

Bemerkung 3.6.4 *Sind $K \subset L \subset M$ Körper und ist M/K separabel, so sind auch L/K und M/L separabel.*

Satz 3.6.5 *Sei L/K eine endliche separable Körpererweiterung. Dann gibt es genau $[L : K]$ viele Einbettungen von L nach K^{alg}, die auf K die Identität sind.*

3.7 Galois-Theorie

Definition 3.7.1 *Eine Körpererweiterung L/K heißt* ***galoissch****, wenn sie normal und separabel ist. (Man sagt auch: „L/K ist eine* ***Galois-Erweiterung****.“) Ist L/K galoissch, so nennt man $\mathrm{Aut}(L/K)$ auch die* ***Galois-Gruppe*** *von L/K (und oft schreibt man $\mathrm{Gal}(L/K)$ dafür).*

Satz 3.7.2 *Ist L/K eine endliche galoissche Körpererweiterung, so ist $\#\,\mathrm{Aut}(L/K) = [L : K]$.*

Definition 3.7.3 *Ein* ***Zwischenkörper*** *einer Körpererweiterung L/K ist ein Körper F mit $K \subset F \subset L$.*

Satz 3.7.4 *Ist L/K eine Körpererweiterung und $H \subset \mathrm{Aut}(L/K)$ eine Untergruppe, so ist die Menge $F := \{a \in L \mid \forall \sigma \in H : \sigma(a) = a\}$ ein Zwischenkörper von L/K.*

Definition 3.7.5 *Den Körper F aus Satz 3.7.4 nennt man den* ***Fixkörper*** *von H; Notation dafür: $\mathrm{Fix}(H)$.*

Satz 3.7.6 (Hauptsatz der Galois-Theorie) *Sei L/K eine endliche galoissche Körpererweiterung mit Galoisgruppe $G = \mathrm{Aut}(L/K)$. Dann hat man eine Bijektion zwischen der Menge der Untergruppen von G und der Menge der Zwischenkörper von L/K, die gegeben ist durch $H \mapsto \mathrm{Fix}(H)$. Die Umkehrabbildung ist $F \mapsto \mathrm{Aut}(L/F)$.*

Definition 3.7.7 *Die Bijektion aus Satz 3.7.6 heißt* ***Galois-Korrespondenz****.*

Satz 3.7.8 *Sei L/K eine endliche Galoiserweiterung mit Galois-Gruppe $G = \mathrm{Aut}(L/K)$, seien $H, H' \subset G$ Untergruppen und seien $F = \mathrm{Fix}(H)$, $F' = \mathrm{Fix}(H')$. Dann gilt:*

(a) *Die Galois-Korrespondenz ist „inklusionsumkehrend“, d. h. $H \subset H' \iff F \supset F'$.*
(b) *$[L : F] = \#H$ und $[F : K] = [G : H]$*
(c) *Die Körpererweiterung F/K ist normal genau dann, wenn H ein Normalteiler von G ist. Ist dies der Fall, so hat man eine surjektive Einschränkungsabbildung $\mathrm{Aut}(L/K) \to \mathrm{Aut}(F/K)$, deren Kern H ist. Insbesondere ist dann also $\mathrm{Aut}(F/K) \cong G/H$.*

Beispiel 3.7.9 *Sei p prim, $\zeta_p := e^{2\pi i/p}$ und $L := \mathbb{Q}(\zeta_p)$. Dann ist $[L : \mathbb{Q}]$ galoissch, und wir haben einen Isomorphismus $\mathbb{F}_p^\times \to \mathrm{Aut}(L/\mathbb{Q})$, der gegeben ist durch $k \mapsto (\zeta_p \mapsto \zeta_p^k)$.*

Beispiel 3.7.10 *Sei p prim, sei K ein Körper mit $\zeta_p \in K$, sei $b \in K$ so, dass $f(X) := X^p - b$ keine Nullstelle in K hat, und sei L der Zerfällungskörper von f. Dann ist $\mathrm{Aut}(L/K)$ isomorph zu $\mathbb{Z}/p\mathbb{Z}$.*

Satz 3.7.11 *Sei K ein Körper, seien $L, K' \subset K^{\mathrm{alg}}$ Körpererweiterungen von K und sei $L' \subset K^{\mathrm{alg}}$ der kleinste Körper, der L und K' enthält. Wir nehmen an, dass L/K endlich und galoissch ist. Dann ist auch L'/K' endlich und galoissch und wir haben einen injektiven Gruppenhomomorphismus $\mathrm{Aut}(L'/K') \to \mathrm{Aut}(L/K), \sigma \mapsto \sigma|_L$. Insbesondere ist $[L' : K']$ ein Teiler von $[L : K]$.*

Beispiel 3.7.12 *Sei $K \subset \mathbb{Q}^{\mathrm{alg}}$ ein Körper und sei p prim. Dann ist $K(\zeta_p)/K$ galoissch, und die Galois-Gruppe $\mathrm{Aut}(K(\zeta_p)/K)$ ist isomorph zu einer Untergruppe von $\mathbb{F}_p^\times$.*

3.8 Anwendung: Radikalerweiterungen

Satz 3.8.1 *Ist p eine Primzahl, so dass $p - 1$ eine Zweierpotenz ist, so ist das regelmäßige p-Eck mit Zirkel und Lineal konstruierbar.*

Definition 3.8.2 *Ein Element $a \in \mathbb{Q}^{\mathrm{alg}}$ heißt* ***durch Radikale auflösbar****, wenn es $a_1, \ldots, a_\ell \in \mathbb{C}$ und $r_1, \ldots, r_\ell \geqslant 1$ gibt, so dass für $K_i := \mathbb{Q}(a_1, \ldots, a_i)$ gilt: $a_i^{r_i} \in K_{i-1}$ und $a \in K_\ell$.*

Satz 3.8.3 *Sei $f \in \mathbb{Q}[X]$ und sei $L \supset \mathbb{Q}$ der Zerfällungskörper von f. Dann sind die Nullstellen von f durch Radikale auflösbar genau dann, wenn die Gruppe $\mathrm{Aut}(L/\mathbb{Q})$ auflösbar ist.*

Satz 3.8.4 *Ist $f \in \mathbb{Q}[X]$ ein Polynom vom Grad höchstens 4, so sind die Nullstellen von f durch Radikale auflösbar.*

Satz 3.8.5 *Ist $f \in \mathbb{Q}[X]$ ein irreduzibles Polynom fünften Grades mit genau drei reellen Nullstellen und ist L der Zerfällungskörper von f, so ist $\mathrm{Aut}(L/\mathbb{Q}) \cong S_5$. Insbesondere sind die Nullstellen von f nicht durch Radikale auflösbar.*

Index