KURZSKRIPT ZUR VORLESUNG ALGEBRA IM WS 2019/20

1. Ganze Zahlen und Polynome

Notation:
$\mathbb{Z} := \{\text{ganze Zahlen}\} \supset \mathbb{N}_0 = \mathbb{Z}_{\geq 0} \supset \mathbb{N} = \mathbb{Z}_{>0}$
$\mathbb{Z}[x] := \{\text{Polynome mit ganzzahligen Koeffizienten}\}$
$= \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 : n \in \mathbb{N}_0, a_n, \ldots, a_1, a_0 \in \mathbb{Z}\}$

Theorem 1.1. *(Descartes): Sei $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ und $x_0 \in \mathbb{Q}$ eine Lösung von $f(x) = 0$. Dann ist $x_0 \in \mathbb{Z}$.*

Theorem 1.2. *(Descartes): Sei $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ und $x_0 = \frac{r}{s}$ (gekürzter Bruch) eine Lösung von $f(x) = 0$. Dann ist $r \in \mathbb{Z}$ ein Teiler von a_0 und $s \in \mathbb{Z}$ ein Teiler von a_n.*

Definition 1.3. Ein *Ring* ist eine Menge R mit zwei Abbildungen $+ : R \times R \to R$ und $\cdot : R \times R \to R$ sowie zwei ausgezeichneten Elementen $0 = 0_R$ und $1 = 1_R \neq 0_R$ so daß gilt:

- $(R, +)$ ist eine abelsche Gruppe mit neutralem Element 0, d.h.
  $+$ ist assoziativ: $(a + b) + c = a + (b + c) \quad \forall a, b, c \in R$,
  $\forall a : \exists - a : \; a + (-a) = 0 = -a + a$,
  abelsch: $a + b = b + a \quad \forall a, b \in R$
- die Multiplikation $\cdot$ ist assoziativ: $(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall a, b, c \in R$ mit Einselement 1: $a \cdot 1 = a = 1 \cdot a$
- es gilt das Distributivgesetz: $a \cdot (b+c) = a \cdot b + a \cdot c$ und $(a+b) \cdot c = a \cdot c + b \cdot c \quad \forall a, b, c \in R$.

R ist ein *kommutativer Ring*, falls zusätzlich $a \cdot b = b \cdot a \quad \forall a, b \in R$ gilt.

Definition 1.4. Seien R und S Ringe. Eine Abbildung $\varphi : R \to S$ heißt *Ringhomomorphismus*, wenn $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) \quad \forall a, b \in R$ und $\varphi(a + b) = \varphi(a) + \varphi(b) \quad \forall a, b \in R$. Wir verlangen auch $\varphi(1_R) = 1_S$.

Definition 1.5. Sei R ein kommutativer Ring.
Ein Element $a \in R$ heißt *Nullteiler* $\Leftrightarrow \exists b \in R \setminus \{0\} : ab = 0$.
R heißt *Integritätsbereich* $\Leftrightarrow 0$ ist der einzige Nullteiler in R.
Folgerung: Kürzungsregel: $r \neq 0$ mit $r \cdot s = r \cdot t \Rightarrow s = t$
Ein kommutativer Ring K heißt *Körper*, wenn $(K \setminus \{0\}, \cdot)$ eine Gruppe ist, d.h. jedes Element $\neq 0$ ist invertierbar.

Definition 1.6. Ein Integritätsbereich R heißt *euklidischer Ring*: $\Leftrightarrow \exists$ Abbildung
$\lambda : R \setminus \{0\} \to \mathbb{N}_0$, so daß $\forall a, b \in R, b \neq 0 : \exists q, r \in R : \underbrace{a = qb + r}_{\text{Division mit Rest}}$ und $r = 0$ oder $\lambda(r) < \lambda(b)$.
λ heißt *Gradfunktion*.

Sei R ein Integritätsbereich, $a, b \in R$. a teilt $b :\Leftrightarrow \exists c : ac = b$, Schreibweise $a \mid b$.
Zu $a, b \in R$ heißt $d \in R$ *größter gemeinsamer Teiler* von a und $b :\Leftrightarrow d \mid a$ und $d \mid b$ und $\forall e \in R : e \mid a$ und $e \mid b \Rightarrow e \mid d$. Schreibweise: $d = ggT(a, b)$.
Analog ist $v \in R$ das *kleinste gemeinsame Vielfache* von a und $b, kgV(a, b) :\Leftrightarrow a \mid v$ und $b \mid v$, und $\forall f \in R : a \mid f$ und $b \mid f \Rightarrow v \mid f$.
Ist R ein euklidischer Ring, dann liefert der *Euklidische Algorithmus* den $ggT(a, b)$ von $a, b \in R \setminus \{0\}$: Setze $a_1 := a, a_2 := b, \lambda(a_1) \geq \lambda(a_2) \Rightarrow \exists q_1, a_3 \in R$ mit $a_1 = q_1 a_2 + a_3$

und $a_3 = 0$ ($\Rightarrow a_2 \mid a_1$ und $a_2 = ggT(a_1, a_2)$) oder $\lambda(a_3) < \lambda(a_2)$. In diesem Fall $\exists q_2, a_4 \in R$ mit $a_2 = q_2 a_3 + a_4$, usw. mit $\lambda(a_2) > \lambda(a_2) \ldots \lambda(a_n)$ und $a_n = q_n a_{n+1}$. Dann ist $ggT(a, b) = a_n$ und $\exists s, t \in R : ggT(a, b) = sa + tb$, denn $a_1 = 1 \cdot a$, $a_2 = 1 \cdot b$, $a_3 = a_1 - q_1 a_2$, $a_4 = a_2 - q_2 a_3$, usw.

Definition 1.7. Sei R ein Integritätsbereich.

(a) Ein invertierbares Element $a \in R$ heißt *Einheit*.
(b) Zwei Elemente a und b in R heißen *assoziiert* $\Leftrightarrow a \mid b$ und $b \mid a$. Wir schreiben $a \sim b$.
(c) Ein Element $p \in R$ heißt *Primelement* (oder *prim*), falls $p \neq 0$, keine Einheit und $\forall a, b \in R : p \mid ab \Rightarrow p \mid a$ oder $p \mid b$.
(d) Ein Element $u \in R$ heißt *unzerlegbar* (oder *irreduzibel*), falls $u \neq 0$, keine Einheit und $\forall a, b \in R : u = ab \Rightarrow a$ Einheit oder b Einheit.

Allgemein gilt (in R Integritätsbereich): p prim $\Rightarrow p$ unzerlegbar.

Definition 1.8. Sei R ein Integritätsbereich. R heißt *faktorieller Ring* genau dann, wenn die folgenden beiden äquivalenten Aussagen erfüllt sind:

(1) Jedes Element $a \in R, a \neq 0, a$ keine Einheit, ist ein endliches Produkt $a = u_1 \ldots u_n$ von unzerlegbaren Elementen $u_1, \ldots, u_n$, die bis auf Reihenfolge und Einheiten eindeutig sind: Falls $a = u_1 \ldots u_n = v_1 \ldots v_l$ mit unzerlegbaren $v_1, \ldots, v_l \in R$, dann ist $n = l$ und $\exists \pi \in \Sigma_n : \; u_1 \sim v_{\pi(i)} \quad \forall i$.
(2) Jedes Element $a \in R, a \notin R^\times, a \neq 0$ läßt sich als (endliches) Produkt $a = u_1 \ldots u_n$ von unzerlegbaren Elementen schreiben, und jedes unzerlegbare Element u in A ist Primelement.

Definition 1.9. Sei R ein Ring, $I \subset R$. I heißt *Linksideal* falls $(I, +)$ eine Untergruppe von $(R, +)$ ist und $\forall a \in I, r \in R : r \cdot a \in I$.
Analog Rechtsideal: $a \cdot r \in I \quad \forall a \in I, r \in R$.
I ist ein zweiseitiges Ideal $\Leftrightarrow$ Links- und Rechtsideal.
R kommutativ, $a \in R$ fest, $Ra := \{xa : x \in R\} =< a >$ heißt *Hauptideal*.

Definition 1.10. Sei R ein Integritätsbereich. R heißt *Hauptidealring*: $\Leftrightarrow$ jedes Ideal $I \trianglelefteq R$ ist ein Hauptideal, d. h. von der Form Ra für ein $a \in R$.

Theorem 1.11. *Ein euklidischer Ring R ist ein Hauptidealring.*

Korollar 1.12. *Die Ideale in $\mathbb{Z}$ sind genau die Mengen $\mathbb{Z}n$ für $n \in \mathbb{N}_0$.*

Teilbarkeit kann man über Ideale formulieren:
$a \mid b \Leftrightarrow < b > \subset < a >$
$a \sim b \Leftrightarrow < a > = < b >$
Ein Ideal I ist ein *Primideal* $:\Leftrightarrow [I \neq R$ und $a \cdot b \in I \Rightarrow a \in I$ oder $b \in I]$
p prim $\Leftrightarrow < p > \neq 0$ ist ein Primideal
u unzerlegbar $\Leftrightarrow [\forall a \in R : < u > \subset < a > \Rightarrow (< u > = < a >$ oder $< a > = R)]$
Sei R ein beliebiger Ring und $I \triangleleft R$, $I \neq R$ ein zweiseitiges Ideal. R/I ist der *Quotientenring* (oder *Restklassenring*), d.h. $R/I = \{\bar{r} : r \in R\}$ wobei $\bar{r} = r + I = \{r + x : x \in I\}$, d.h. $\bar{r} = \bar{s} \Leftrightarrow r - s \in I$, $\bar{r} + \bar{s} = \overline{r + s}$, $\bar{r} \cdot \bar{s} = \overline{rs}$, $\bar{1}$ ist das Einselement, $\bar{0}$ ist das Nullelement.

Lemma 1.13. *Sei R ein kommutativer Ring und $I \triangleleft R$, $I \neq R$.*
Dann ist I ein Primideal $\Leftrightarrow R/I$ ist ein Integritätsbereich.

Ein Ideal $m \triangleleft R$, $m \neq R$ (kommutativ) ist *maximal*: $\Leftrightarrow \forall I \leq R$ mit $m \leq I \leq R$ gilt : $I = m$ oder $I = R$.

Korollar 1.14. *Sei R ein Hauptidealring und $p \in R$. Dann ist p prim $\Leftrightarrow p$ ist unzerlegbar. Ein Primideal $\neq < 0 >$ ist ein maximales Ideal.*

Korollar 1.15. *Sei R ein faktorieller Ring und $a \in R \setminus \{0\}$. Dann gibt es nur endlich viele verschiedene Hauptideale $< b > \supset < a >$.*

Theorem 1.16. *Sei R ein Integritätsbereich. R ist faktoriell $\Leftrightarrow$ jedes unzerlegbare Element in R ist prim und jede aufsteigende Kette von Hauptidealen $I_1 \subset I_2 \subset \cdots \subset I_n \subset I_{n+1} \subset \ldots (n \in \mathbb{N})$ wird stationär, d.h. $\exists N_0 \in \mathbb{N}$ so daß $I_{N_0} = I_{N_0+1} = \cdots = I_l \quad \forall l \geq N_0$.*

Proposition 1.17. *Sei R ein kommutativer Ring. Dann sind die folgenden Aussagen äquivalent:*

(a) *Jede aufsteigende Kette $I_1 \subset I_2 \subset I_3 \ldots$ von Idealen in R wird stationär.*
(b) *In jeder nichtleeren Menge von Idealen in R gibt es ein bezüglich Inklusion maximales Element.*
(c) *Jedes Ideal I in R ist endlich erzeugbar, d.h. von der Form $< a_1, \ldots, a_n >:= Ra_1 + \cdots + Ra_n$ mit $a_1, \ldots, a_n \in R$.*

Wenn die Aussagen erfüllt sind, heißt R ein *noetherscher Ring.* (Emmy Noether, 1882-1935)

Korollar 1.18. *Sei R ein Hauptidealring. Dann ist R faktoriell und noethersch.*

Beispiel eines Integritätsbereichs, in dem unzerlegbar $\neq$ prim gilt (also auch nicht faktoriell), bzw. Produktdarstellung aus Unzerlegbaren nicht eindeutig ist: $R = \{a+b\sqrt{-5} \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$.

2. Gruppen

Definition 2.1. Eine *Gruppe* ist eine Menge G mit einer Abbildung
$*\colon\ G \times G \to G,\ (g_1, g_2) \mapsto g_1 * g_2$ (oder $g_1 g_2$) so daß gilt:

- die Multiplikation ist assoziativ: $g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3 \quad \forall g_1, g_2, g_3 \in G$
- es existiert ein neutrales Element $e : \exists e : \forall g \in G : e * g = g = g * e$
- jedes Element hat ein inverses Element: $\forall g \in G :\ \exists h \in G :\ g * h = h * g = e$
  Bezeichnung: $h =: g^{-1}$

G ist eine *endliche Gruppe*, wenn die Menge G endlich ist.
G ist eine *abelsche* (oder: *kommutative*) Gruppe, wenn $g_1 * g_2 = g_2 * g_1 \quad \forall g_1, g_2 \in G$

Beispiele:
$\mathrm{Bij}(X) = \{f : X \to X \text{ bijektiv}\}$ für X Menge, $* =$ Komposition
$\Sigma_n = \mathrm{Bij}(\{1, \ldots, n\})$, die *symmetrische Gruppe*, die Elemente heißen *Permutationen*

Definition 2.2. Seien G und H Gruppen. Ein *Gruppenhomomorphismus* $\varphi\colon\ G \to H$ ist eine Abbildung, für die gilt: $\varphi(g_1 *_G g_2) = \varphi(g_1) *_H \varphi(g_2) \quad \forall g_1, g_2 \in G$.
Daraus folgt $\varphi(e_G) = e_H$.
Ist φ bijektiv, nennt man es einen *Isomorphismus.*
Wenn die Gruppe H eine Teilmenge von G ist, ist H eine *Untergruppe* von G, wenn die Inklusion $i\colon\ H \hookrightarrow G$ ein Gruppenhomomorphismus ist. Ist $\phi\colon\ H \to G$ ein injektiver Gruppenhomomorphismus und $\phi(H)$ eine Untergruppe von G, so nennen wir H ebenfalls eine Untergruppe.
Schreibweise: $H < G$.

Theorem 2.3. *(Satz von Cayley): Jede (endliche) Gruppe ist Untergruppe einer symmetrischen Gruppe (bzw. einer Gruppe von Bijektionen).*

Definition 2.4. Eine Gruppe G heißt *zyklisch*: $\Leftrightarrow \exists g \in G : G = \{g^n : n \in \mathbb{Z}\}$.

Die Ordnung $ord(G) = |G|$ einer Gruppe ist ihre Elementezahl $\in \mathbb{N} \cup \{\infty\}$.

Proposition 2.5. *Zwei zyklische Gruppen G_1 und G_2 sind isomorph $\Leftrightarrow |G_1| = |G_2|$. Bis auf Isomorphie gibt es zu jeder Ordnung $\in \mathbb{N} \cup \{\infty\}$ genau eine zyklische Gruppe dieser Ordnung.*

Proposition 2.6. *Sei G eine zyklische Gruppe. G ist durch $|G|$ bis auf Isomorphie bestimmt.*

(a) *Wenn $|G| = \infty$, dann ist $G \simeq \mathbb{Z}$ (mit Addition). Die Untergruppen von $\mathbb{Z}$ sind genau die $n\mathbb{Z}$ mit $n \in \mathbb{N}_0$.*

(b) *Wenn $|G| = n$ für $n \in \mathbb{N}$, dann ist $G \cong \mathbb{Z}/n\mathbb{Z}$ (mit Addition). Die Untergruppen von $\mathbb{Z}/n\mathbb{Z}$ sind zyklisch. Ihre Ordnungen sind genau die Teiler $d \mid n$. Zu jedem $d \mid n$ gibt es genau eine Untergruppe H_d der Ordnung d. H_d ist erzeugt von $\frac{n}{d}$.*

Definition 2.7. Sei G eine Gruppe, $H < G$ eine Untergruppe und $g \in G$. Die Menge $gH = \{gh : h \in H\}$ heißt *Linksnebenklasse* von g, die Menge $Hg = \{hg : h \in H\}$ heißt *Rechtsnebenklasse* von g.

Theorem 2.8. *(Satz von Lagrange): Sei G eine Gruppe, H eine Untergruppe und $[G : H]$ die Anzahl der Linksnebenklassen. Dann gilt: $|G| = |H| \cdot [G : H]$. Insbesondere ist $|H|$ ein Teiler von $|G|$.*
$[G : H]$ heißt der Index *von H in G.*

Definition 2.9. Sei G eine Gruppe und H eine Untergruppe. H heißt *normale Untergruppe* (oder *Normalteiler*): $\Leftrightarrow \forall g \in G : gH = Hg$, das heißt für jedes g stimmen die Links- und die Rechtsnebenklasse bezüglich H überein.
Schreibweise: $H \triangleleft G$ (oder $H \trianglelefteq G$ oder $H \trianglelefteqslant G$)

Theorem 2.10. *Sei G eine Gruppe.*

(a) *$H < G$ ist normal $\Leftrightarrow gHg^{-1} = H \quad \forall g \in G$*
$\Leftrightarrow ghg^{-1} \in H \quad \forall g \in G, h \in H$.

(b) *Sei $N \trianglelefteq G$ und $G/N := \{gN : g \in G\}$ die Menge der Linksnebenklassen.*
G/N ist eine Gruppe mit Multiplikation $g_1N * g_2N := (g_1g_2)N$
G/N heißt Faktorgruppe *(oder* Quotientengruppe*).*

(c) *Sei G' eine Gruppe und $\varphi : G \to G'$ ein Gruppenhomomorphismus.*
Dann ist $H := Kern(\varphi) = \{g \in G : \varphi(g) = e = e_{G'}\}$ normal in G.
Es gilt $Im(\varphi) = \{\varphi(g) : g \in G\} \cong G/H$.

Eine Gruppe G, die nur $\{e\}$ und G als Normalteiler hat, heißt einfache Gruppe.

Korollar 2.11. *(Kleiner Satz von Fermat)*
Sei $p \in \mathbb{N}$ eine Primzahl und $x \in \mathbb{Z} \setminus p\mathbb{Z}$, d.h. $p \nmid x$. Dann gilt $p \mid (x^{p-1} - 1)$, d.h. $x^{p-1} \equiv 1 \mod p$.

Proposition 2.12. *Sei p prim und $|G| = 2p$. Dann ist entweder $G \cong \mathbb{Z}/2p\mathbb{Z}$ oder $G \cong D_{2p}$.*

3. Operationen von Gruppen auf Mengen

Definition 3.1. Sei G eine Gruppe und $X \neq \emptyset$ eine Menge. X heißt *G-Menge*, wenn es eine *(Links-)Operation* von G auf X gibt, d.h. eine Abbildung $G \times X \to X, (g, m) \mapsto gm$ mit den Eigenschaften

(O1) $(g_1g_2)m = g_1(g_2m) \quad \forall m \in X, g_1, g_2 \in G$
(O2) $em = m \quad \forall m \in M$.

Man sagt dann: G *operiert* auf der Menge X.

Definition 3.2. Sei G eine Gruppe, die auf einer Menge X operiert. Für $m \in X$ ist die *Bahn* $G \cdot m$ von m (unter der Operation von G) definiert als $\{gm : g \in G\}$
Die Operation von G auf X heißt *transitiv*: $\Leftrightarrow \exists m \in X : X = G \cdot m$
$\Leftrightarrow \quad \forall m_1, m_2 \in X : \exists g \in G : gm_1 = m_2$
Ein $m \in X$ heißt *Fixpunkt*: $\Leftrightarrow G \cdot m = \{m\} \Leftrightarrow gm = m \quad \forall g \in G$
Für $m \in X$ ist der *Stabilisator* definiert als $Stab_G(m) := \{g \in G : gm = m\}$;

$\text{Stab}_G(m)$ wird auch *Isotropiegruppe* genannt.
Die Operation G auf X heißt *treu*, wenn die Abbildung $G \to Abb(X,X)$ injektiv ist, äquivalent dazu ist: $gm = m \quad \forall m \in X \Rightarrow g = e$.
Das *Zentrum* $Z(G)$ einer Gruppe G ist definiert als $Z(G) = \{m \in G : gm = mg \quad \forall g \in G\}$.
$C_G(m) := \{g \in G : gm = mg\}$ heißt der *Zentralisator* von $m \in M$.

Proposition 3.3. *(Bahnensatz): Sei X eine G-Menge und $m \in X$ mit Stabilisator G_m. Dann $\exists$ Bijektion (von Mengen) $\phi : G/G_m \to G \cdot m$ zwischen der Menge der Linksnebenklassen und der Bahn. Insbesondere gilt $|G \cdot m| = [G : G_m]$, d.h. die Elementezahl der Bahn ist genau die Anzahl der Linksnebenklassen bezüglich G_m.*

Korollar 3.4. *(Klassengleichung): Sei $X = G$ mit Konjugationsoperation. Dann gilt:*

$$|G| = |Z(G)| + \sum_{\substack{g \in G, g \notin Z(G) \\ g \text{ Repräsentanten der Bahnen mit Länge } >1}} [G : C_G(g)]$$

Proposition 3.5. *Sei $|G| \in \{p, p^2\}$, p prim. Dann ist G abelsch.*

Theorem 3.6. *(Satz von Cauchy): Sei G eine endliche Gruppe und p eine Primzahl, die $|G|$ teilt. Dann gibt es ein Element $g \in G$ mit $ord(g) = p$.*

Sei p eine Primzahl. Eine endliche Gruppe heißt *p-Gruppe*, wenn es ein $n \in \mathbb{N}$ gibt, sodass $|G| = p^n$ gilt.

Korollar 3.7. *Sei G eine endliche Gruppe und p eine Primzahl. Dann ist G eine p-Gruppe $\Leftrightarrow \quad \forall \in G : \exists n \in \mathbb{N}_0 : ord(g) = p^n$.*

Korollar 3.8. *Sei p eine Primzahl und G eine p-Gruppe.*

(a) *Sei X eine endliche Menge, auf der G operiert, und $X^G := \{x_0 \in X : gx_0 = x_0 \; \forall g \in G\}$ die Menge der Fixpunkte. Dann gilt $|X^G| \equiv |X| \mod p$.*
(b) *Für $G \neq \{e\}$ ist $Z(G) \neq \{e\}$, d.h. das Zentrum einer nichttrivialen p-Gruppe ist nichttrivial.*

Korollar 3.9. *(Burnsides Zähllemma: Burnside 1900, Frobenius 1887, Cauchy 1835): Sei G eine endliche Gruppe, die auf der endlichen Menge X operiert, und sei X/G die Menge der Bahnen. Dann gilt: $|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|$, wobei $X^g := \{x_0 \in X : gx_0 = x_0\}$.*

Theorem 3.10. *(Sylow-Sätze) [Peter Ludwig Sylow, 1872]*
Sei G eine endliche Gruppe und p eine Primzahl, die $|G|$ teilt. Sei $|G| = p^m q$ mit $ggT(p,q) = 1$. Dann gilt:

(a) *Für alle k mit $1 \leq k \leq m$ gibt es Untergruppen H mit $|H| = p^k$.*
(b) *Eine Untergruppe S mit $|S| = p^m$ heißt* p-Sylowuntergruppe. Sei S eine p-Sylowuntergruppe und $H < G$ eine p-Gruppe. Dann $\exists g \in G : H < gSg^{-1}$. gSg^{-1} ist auch eine Sylowuntergruppe, also ist jede p-Gruppe $H < G$ in einer p-Sylowuntergruppe enthalten.
(c) Sei s_0 die Anzahl aller p-Sylowuntergruppen von G. Dann gilt:
$s_0 \mid q$ und $s_0 \equiv 1 \mod p$.

$G_S = Stab_G(S) = \{g \in G : gSg^{-1} = S\} =: N_G(S)$, heißt der *Normalisator* von S.

Lemma 3.11. *Sei S eine p-Sylowuntergruppe von G und H eine p-Gruppe mit $H \subset N_G(S)$. Dann ist $H \subset S$.*

Korollar 3.12. *Seien p und q Primzahlen, $p < q, p \nmid (q-1)$ und sei G eine Gruppe der Ordnung $p \cdot q$. Dann gilt: $G \simeq \mathbb{Z}/pq\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.*

Korollar 3.13. *(Satz von Wilson): Sei $n \in \mathbb{N}, n > 1$. Dann gilt: n ist eine Primzahl $\Leftrightarrow$ $(n-1)! \equiv -1 \mod n$.*

4. Körperweiterungen

Definition 4.1. Seien K und L Körper mit $K \subset L$, so daß K ein Teilring von L ist, d.h. ein Ring mit derselben Struktur, also denselben $+, \cdot, 0, 1$. Die Inklusion $K \subset L$ heißt *Körpererweiterung*, K heißt *Teilkörper* von L und L heißt *Erweiterungskörper* von K.
Ein Körper K' mit $K \subset K' \subset L$ so, daß K' ein Teilkörper von L ist, heißt *Zwischenkörper*.
Falls $L = K(a_1, \ldots, a_n)$ für $a_1, \ldots, a_n \in L$ ist, dann heißt L *endlich erzeugt* über K.
Die Körpererweiterung $K \subset L$ wird auch mit L/K bezeichnet.
L/K heißt *einfach* (oder *einfache Erweiterung*) $:\Leftrightarrow \exists a \in L : L = K(a)$.

Definition 4.2. Sei L/K eine Körpererweiterung. Die Vektorraum-Dimension $[L : K] := dim_K L$ heißt der *Grad* der Körpererweiterung. Die Erweiterung L/K heißt *endlich* $:\Leftrightarrow [L : K] < \infty$.

Lemma 4.3. *(Gradformel): Seien M/L und L/K Körpererweiterungen, also $K < L < M$. Dann gilt $[M : K] = [M : L] \cdot [L : K]$.*

Proposition 4.4. *Seien R, S kommutative Ringe, $R[x]$ der Ring der Polynome mit Koeffizienten in R, $\alpha : R \to S$ ein Ringhomomorphismus und $s_0 \in S$. Dann gibt es genau einen Ringhomomorphismus $\varphi : R[x] \longrightarrow S$ mit $\varphi|_R = \alpha$ und $\varphi(x) = s_0$. φ heißt* Auswertungshomomorphismus.

Definition 4.5. Sei L/K eine Körpererweiterung, $\alpha : K \to L$ die Inklusion und $\varphi : K[x] \to L$ ein Auswertungshomomorphismus mit $\varphi(x) = a \in L$.
Wenn φ injektiv ist, heißt a *transzendent* (über K). Sonst heißt a *algebraisch* (oder *algebraisch abhängig*) über K.

Definition 4.6. Sei L/K eine Körpererweiterung und L/K algebraisch, $a \in L, \varphi : K[x] \to L$ der Auswertungshomomorphismus mit $x \mapsto a$.
Das normierte Polynom $m(x)$ mit $Kern(\varphi) =< m(x) >$ heißt das *Minimalpolynom* von a über K. Bezeichnung: $m_a = m_{a,K} = m_a(x)$.

Theorem 4.7. *(Satz von Kronecker): Sei K ein Körper und $f(x) \in K[x]$ ein irreduzibles Polynom. Dann existiert eine einfache und endliche Körpererweiterung $L = K(a)$, so daß $f(x)$ in L mindestens die Nullstelle a hat. Es gilt $[L : K] = \deg f$.*
Also ist jede polynomiale Gleichung mit Koeffizienten in einem Körper lösbar.

Proposition 4.8. *Sei L/K eine Körpererweiterung und $a \in L$. Dann sind äquivalent:*

(a) $K[a] = K(a)$
(b) *a ist algebraisch abhängig über K*
(c) $dim_K K(a) < \infty$

Dann gilt $\deg m_a = [K(a) : K]$. *Bezeichnung:* Grad *von a ist* $[K(a) : K]$.

Definition 4.9. Eine Körpererweiterung L/K heißt *algebraisch*:$\Leftrightarrow$ alle $a \in L$ sind algebraisch abhängig über K.

Proposition 4.10. *Seien M/L und L/K Körpererweiterungen. Dann gilt:*

(a) *L/K endlich $\Rightarrow$ L/K algebraisch*
(b) *L/K endlich erzeugt und algebraisch $\Leftrightarrow$ L/K endlich*
(c) *M/L und L/K algebraisch $\Rightarrow$ M/K algebraisch*

Sei R ein Integritätsbereich, $Q(R) = Quot(R) := \{[\frac{r}{s}] : r, s \in R, s \neq 0\}$, wobei $[\frac{r}{s}]$ die Äquivalenzklasse von Brüchen ist, mit $[\frac{r}{s}] = [\frac{p}{q}] \Leftrightarrow rq = ps$ (in R gilt die Kürzungsregel).
Dann ist R ein Körper: der *Quotientenkörper* von R, mit

- Addition $\frac{r}{s} + \frac{r'}{s'} = \frac{rs'+r's}{ss'}$,
- Multiplikation $\frac{r}{s} \cdot \frac{p}{q} = \frac{rp}{sq}$,
- $0 = \frac{0}{1}, 1 = \frac{1}{1}$ und $\frac{r}{s} \cdot \frac{s}{r} = 1$, falls $r \neq 0$,
- $r = \frac{r}{1}$ und damit $Q(R) \supset R$.

Definition und Proposition 4.11. *Sei K ein Körper. K heißt* algebraisch abgeschlossen *wenn eine der folgenden äquivalenten Bedingungen erfüllt ist:*

(a) *Jedes nichtkonstante Polynom $f(x) \in K[x] \setminus K$ hat eine Nullstelle in K.*
(b) *Jedes nichtkonstante Polynom $f(x) \in K[x] \setminus K$ ist ein Produkt von Linearfaktoren: $\exists f_1, \ldots, f_n \in K[x]$ mit $\deg f_j = 1$ für alle $j = 1, \ldots, n$ so, daß $f = f_1 \cdot f_2 \cdot \ldots \cdot f_n$.*
(c) *Jedes irreduzible Polynom hat Grad 1. Die irreduziblen normierten Polynome sind also genau die $x - a$ für $a \in K$.*
(d) *Für jede algebraische Körpererweiterung L/K gilt $L = K$.*

Notation für K algebraisch abgeschlossen: $K = \bar{K}$.

Definition 4.12. Sei K ein Körper und $\bar{K} \supset K$ eine algebraische Körpererweiterung, so daß $\overline{K}$ algebraisch abgeschlossen ist. Dann heißt $\overline{K}$ (ein) *algebraischer Abschluß* von K.

Theorem 4.13. *Jeder Körper K hat einen algebraischen Abschluß $\bar{K}$.*

Auswahlaxiom 4.14. *(AC) Sei $I \neq \emptyset$ eine Menge und $\{M_i : i \in I\}$ eine Familie nichtleerer Mengen: $M_i \neq \emptyset \quad \forall i \in I$. Dann existiert eine Funktion (Auswahlfunktion) $f : I \to \bigcup_{i \in I} M_i$ mit $f(i) \in M_i \quad \forall i \in I$. Es existiert also ein $(x_i)_{i \in I} \in \bigtimes_{i \in I} M_i$ (kartesisches Produkt).*

Sei M eine Menge. Eine *partielle Ordnung* $\leq$ auf M ist eine Relation mit:
$\forall x \in M : x \leq x$ (Reflexivität)
$\forall x, y, z \in M : x \leq y$ und $y \leq z \Rightarrow x \leq z$ (Transitivität)
$\forall x, y \in M : x \leq y$ und $y \leq x \Rightarrow x = y$ (Antisymmetrie)

- Eine partielle Ordnung $\leq$ heißt *Totalordnung*: $\Leftrightarrow \forall x, y \in M : x \leq y$ oder $y \leq x$.
- Sei $N \subset M$. $a \in M$ ist eine *obere Schranke* für $N :\Leftrightarrow \forall x \in N : x \leq a$.
- $a \in M$ ist ein *maximales Element*: $\Leftrightarrow \forall x \in M : x \geq a \Rightarrow x = a$.

Zorns Lemma 4.15. *Sei $M \neq \emptyset$ partiell geordnet durch $\leq$, so daß für jede total geordnete Teilmenge (auch* Kette *genannt) $N \leq M$ eine obere Schranke (in M, nicht notwendigerweise in N) existiert. Dann gibt es (mindestens) ein maximales Element in M.*

Theorem 4.16. *Sei R ein kommutativer Ring (mit $0 \neq 1$). Dann existiert ein maximales Ideal $m \trianglelefteq R$ (d.h. R/m ist ein Körper).*

Proposition 4.17. *Sei F ein Körper. Dann existiert eine Körpererweiterung L/F, so daß jedes nichtkonstante Polynom $f(x) \in F[x] \setminus F$ eine Nullstelle in L hat.*

5. Irreduzible Polynome

Definition 5.1. Sei R faktoriell und $f = \sum_{i=0}^{n} a_i x^i \in R[x]$.
$c(f) := ggT(a_0, \ldots, a_n) \in R$ heißt *Inhalt* (content) des Polynoms f. (Der Inhalt $c(f)$ ist nicht eindeutig, sondern repräsentiert eine Klasse von assoziierten Elementen.)
f heißt *primitiv* $:\Leftrightarrow c(f) = 1$ bzw. $c(f) \in R^*$ (eine Einheit in R).

Lemma 5.2. *(Lemma von Gauß, 1. Version): Sei R faktoriell. Wenn $f, g \in R[X]$ beide primitiv sind, ist auch $f \cdot g \in R[X]$ primitiv.*

Definition 5.3. Sei R faktoriell, $K := Quot(R)$, $f \in K[x]$ und $a \neq 0, a \in R$, so daß $af \in R[x]$. Dann ist $c_K(f) := \frac{c(af)}{a}$.

Lemma 5.4. *(Lemma von Gauß, 2. Version): Für $f, g \in K[x]$ gilt $c_K(fg) = c_K(f) \cdot c_K(g)$ (d.h. Repräsentanten von $c_K(fg)$ und $c_K(f) \cdot c_K(g)$ sind zueinander assoziiert).*

Korollar 5.5. *Sei $f \in R[x]$. Dann gilt:*

(a) *Sei $f = g \cdot h$ eine Zerlegung mit $g, h \in K[x] - K^* \Rightarrow f = (c(f) \cdot \frac{g}{c_K(g)}) \cdot \frac{h}{c_K(h)}$ ist eine Zerlegung in $R[x]$.*
Wenn f in $R[x]$ unzerlegbar ist und $\deg f \geq 1$, dann ist f auch in $K[x]$ unzerlegbar.

(b) *Ist f unzerlegbar in $K[x]$ und primitiv, dann ist f unzerlegbar in $R[x]$.*

Theorem 5.6. *(Satz von Gauß): Sei R faktoriell. Dann ist $R[x]$ faktoriell.*
Die unzerlegbaren Elemente von $R[x]$ sind:

(I) *die unzerlegbaren Elemente in R, sowie*
(II) *alle primitiven Polynome in $R[x]$, die in $K[x]$ unzerlegbar sind.*

Theorem 5.7. *(Kriterium von Eisenstein): Sei R ein faktorieller Ring, $K = Quot(R)$ der Quotientenkörper und $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$ mit $n \geq 1$. Sei $p \in R$ irreduzibel mit $p \mid a_1$ für $i = 0, \ldots, n-1$, $p \nmid a_n$ und $p^2 \nmid a_0$. Dann ist $f(x)$ irreduzibel in $K[x]$.*
Falls $f(x)$ primitiv ist, dann ist es auch irreduzibel in $R[x]$.

Proposition 5.8. *(Reduktionskriterium): Sei R faktoriell, S ein Integritätsbereich und $\varphi : R \to S$ ein Ringhomomorphismus, fortgesetzt zu $\phi : R[x] \to S[x]$ mit $\phi(x) = x$. Sei $f \in R[x]$ primitiv mit $\deg(f) = \deg(\phi(f))$, so daß $\phi(f)$ in $S[x]$ unzerlegbar ist.*
Dann ist f unzerlegbar in $R[x]$.

6. Körpererweiterungen, Isomorphismen und Automorphismen

Definition 6.1. Seien L_1/K und L_2/K Körpererweiterungen von K. Ein Ringhomomorphismus $\varphi : L_1 \to L_2$ heißt *K-Homomorphismus* $:\Leftrightarrow \forall \lambda \in K : \varphi(\lambda) = \lambda$. Wenn φ zusätzlich bijektiv ist, heißt es *K-Isomorphismus*, und falls weiterhin $L_1 = L_2$ heißt es *K-Automorphismus*.

Lemma 6.2. *Sei L/K eine Körpererweiterung und $\varphi : L \to L$ ein K-Automorphismus. Sei $f \in K[x]$ und $x_0 \in L$ eine Nullstelle von $f(x)$. Dann ist auch $\varphi(x_0)$ eine Nullstelle von $f(x)$.*

Proposition 6.3. *Seien K_1 und K_2 Körper und L_1/K_1 und L_2/K_2 Körpererweiterungen sowie $\sigma : K_1 \to K_2$ ein Isomorphismus und $\sigma^* : K_1[x] \to K_2[x]$ die induzierte Abbildung $\sum \lambda_i x^i \mapsto \sum \sigma(\lambda_i) x^i$.*

(a) *Für $a_1 \in L_1$ und $a_2 \in L_2$ mit $m_{a_2,K_2} = \sigma^*(m_{a_1,K_1})$ existiert genau ein Isomorphismus $\varphi : K_1(a_1) \mapsto K_2(a_2)$ mit $\varphi(a_1) = a_2$ und $\varphi \mid_{K_1} = \sigma$.*

(b) *Für $a \in L_1$ gilt:*

$$|\{\varphi : K_1(a) \to L_2 \text{ mit } \varphi \mid_{K_1} = \sigma\}| = |\{b \in L_2 : \sigma^*(m_{a,K_1})(b) = 0\}|$$

Theorem 6.4. *Sei K ein Körper.*

(a) *Sei L/K eine algebraische Erweiterung, $M = \overline{M}$ ein algebraisch abgeschlossener Körper und $\sigma : K \to M$ ein Homomorphismus. Dann existiert eine Fortsetzung $\varphi : L \to M$, d. h. ein Homomorphismus mit $\varphi|_K = \sigma$. Damit ist das folgende Diagramm kommutativ:*

$$\begin{array}{ccc} \tau : K & \longrightarrow & M = \overline{M} \ . \\ \cap & \nearrow_{\exists \psi} & \\ L & & \end{array}$$

(b) *Sei $K \simeq K'$ und $\bar{K}$ bzw. $\bar{K}'$ ein algebraischer Abschluß von K bzw. K'. Dann existiert ein Isomorphismus $\psi : \bar{K} \xrightarrow{\sim} \bar{K}'$ mit $\psi|_K = \tau$; das folgende Diagramm ist also kommutativ:*

$$\begin{array}{ccc} \tau : K & \xrightarrow{\sim} & K' \\ \cap & & \cap \\ \exists\psi : \overline{K} & \xrightarrow{\sim} & \overline{K}' \end{array}$$

(c) *Seien L_1 und L_2 zwei algebraische Abschlüsse von K. Dann existiert ein K-Isomorphismus $\alpha : L_1 \xrightarrow{\sim} L_2$. Insbesondere ist $\alpha|_K = id_K$.*

Definition 6.5. Sei K ein Körper und $f(x) \in K[x]$ ein Polynom vom Grad $n \geq 1$. Sei L/K eine Körpererweiterung. Dann heißt L *Zerfällungskörper* von $f(x) :\Leftrightarrow \exists a_1, \ldots, a_n \in L, c \in K$, so daß $f(x) = c\prod_{i=1}^{n}(x - a_i)$ und $L = K(a_1, \ldots, a_n)$.

Definition 6.6. Sei L/K eine Körpererweiterung und $\Lambda \subset K[x]$ eine Menge von nichtkonstanten Polynomen. L heißt *Zerfällungskörper* von Λ über K, wenn über L alle Polynome in Λ in Produkte von Linearfaktoren zerfallen und kein K' mit $K \subset K' \subsetneq L$ diese Eigenschaft hat. Eine Körpererweiterung L/K heißt *normal*, wenn es eine Menge $\Lambda \subset K[x] - K$ gibt, so daß L der Zerfällungskörper von Λ über K ist.

Theorem 6.7. *Sei $K \subset L \subset \bar{K}$ eine Kette von Körpererweiterungen. Dann sind äquivalent:*

(a) *$\forall f \in K[x], f$ irreduzibel über K: Wenn f eine Nullstelle in L hat, dann ist es über L ein Produkt von Linearfaktoren, d. h. alle Nullstellen von f liegen schon in L.*
(b) *L/K ist normal.*
(c) *Jeder K-Homomorphismus $\varphi : L \to \bar{K}$ erfüllt $\varphi(L) = L$.*

Definition 6.8. Ein Element $a \in \bar{K}$ heißt *separabel* über $K :\Leftrightarrow m_{a,K}(x)$ hat in $\bar{K}$ nur einfache Nullstellen.

Lemma 6.9. *Sei $a \in \bar{K}$. Dann ist a separabel über $K \Leftrightarrow m'_{a,K} \neq 0$.*

Sei K ein Körper. Die *Charakteristik* von K ist $char(K) := \min\{n \in \mathbb{N} : \underbrace{1 + 1 + \cdots + 1}_{\text{n mal}} = 0\}$ bzw. $char(K) = 0$, falls $\underbrace{1 + \cdots + 1}_{\text{n mal}} \neq 0 \ \forall n \in \mathbb{N}$.

Definition 6.10. Sei $K \subset L \subset \bar{K}$. Der *Separabilitätsgrad* $[L : K]_s$ (von L über K) ist definiert als die Anzahl der verschiedenen K-Homomorphismen $L \to \bar{K}$. Wenn L/K endlich ist, heißt L/K *separabel* $:\Leftrightarrow [L : K]_s = [L : K]$.

Lemma 6.11. *Sei L/K endlich. Dann ist $[L : K] \geq [L : K]_s$.*

Theorem 6.12. *Sei L/K eine endliche Körpererweiterung. Dann sind äquivalent:*

(a) *L/K ist separabel.*
(b) *$\forall a \in L : a$ ist separabel über K.*
(c) *$\exists a_1, \ldots, a_n$ separabel über K mit $L = K(a_1, \ldots, a_n)$*
Weiterhin ist L/K separabel, falls (d) oder (e) gilt:
(d) *$char(K) = 0$*
(e) *$char(K) = p \neq 0$ und $p \nmid [L : K]$*

Für $K \subset M \subset L$ gilt: L/K separabel $\Leftrightarrow L/M$ und M/K separabel

Theorem 6.13. *(Satz vom primitiven Element): Sei L/K endlich und separabel. Dann existiert ein $a \in L$ mit $L = K(a)$. Also ist L eine einfache Körpererweiterung.*

Lemma 6.14. *Sei L ein Körper und $G \subset L^*$ eine endliche multiplikative Untergruppe von L^*. Dann ist G zyklisch. Wenn $|L| < \infty$, ist also L^* selbst eine zyklische Gruppe.*

Theorem 6.15. *Für jede Primzahl p und jedes $n \in \mathbb{N}$ gibt es bis auf Isomorphie genau einen Körper $\mathbb{F}_q$ mit $q := p^n$ Elementen.*
$\mathbb{F}_q$ ist algebraisch als Körpererweiterung über $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, separabel und normal. Die Elemente von $\mathbb{F}_q$ sind genau die Nullstellen von $f(x) = x^q - x$ als Polynom über $\mathbb{F}_p$.
Genauer:

(a) *Sei $n \in \mathbb{N}, p$ eine Primzahl und $q := p^n$. Der Zerfällungskörper L von $f(x) = x^q - x \in \mathbb{F}_p[x]$ ist ein Erweiterungskörper von $\mathbb{F}_p$ mit $[L : \mathbb{F}_p] = n$. Es gilt $|L| = q$ und $L = \{$Nullstellen von $f(x) \in \mathbb{F}_p[x]\}$. Die Erweiterung $L/\mathbb{F}_p$ ist algebraisch, separabel und normal.*

(b) *$\mathbb{F}_q$ ist bis auf Isomorphie der einzige Körper mit $q = p^n$ Elementen. Jeder endliche Körper ist zu genau einem $\mathbb{F}_q$ isomorph.*

(c) *Die Automorphismengruppe $Aut_{\mathbb{F}_p}(\mathbb{F}_q)$ ist zyklisch von Ordnung n und erzeugt vom Frobenius-Automorphismus $Fr : x \mapsto x^p$.*

7. Konstruktionen mit Zirkel und Lineal

Erlaubte Konstruktionen mit Zirkel und unmarkiertem Lineal:

(I) Schnittpunkte zweier Geraden
(II) Schnittpunkte einer Geraden mit einem Kreis
(III) Schnitt von zwei Kreisen

Definition 7.1. Sei $M \subset \mathbb{R}^2 = \mathbb{C}, (0,0), (1,0) = 1_{\mathbb{C}} \in M$. Ein Punkt $p \in \mathbb{C}$ heißt aus M mit Zirkel und Lineal *konstruierbar*, genau dann wenn ein $n \in \mathbb{N}$ und eine Kette $M = M_0 \subset M_1 \subset \cdots \subset M_n$ existieren mit $p \in M_n$, sodass alle Elemente von M_i Ergebnisse der Konstruktionen I, II und III angewandt auf Punkte in M_{i-1} sind, für $1 \leq i \leq n$.
Notation: $Kon(M) := \{p \in \mathbb{R}^2 : p$ ist aus M konstruierbar$\}$

Theorem 7.2. *Sei $0, 1 \in M \subset \mathbb{C}$. Dann gilt:*

(a) *$Kon(M)$ ist ein Teilkörper von $\mathbb{C}$.*
(b) *$Kon(M) = \overline{Kon(M)} = \{\bar{z} : z \in Kon(M)\}$.*
(c) *$\mathbb{Q}(M \cup \bar{M})$ ist ein Teilkörper von $Kon(M)$.*
(d) *$Kon(M)$ ist quadratisch abgeschlossen, d. h. für $b \in \mathbb{C}$ gilt:*
$b^2 \in Kon(M) \Rightarrow b \in Kon(M)$.

Theorem 7.3. *Sei $0, 1 \in M \subset \mathbb{C}$. Dann gilt:*

(a) *$Kon(M)/\mathbb{Q}(M \cup \bar{M})$ ist eine algebraische Körpererweiterung.*
(b) *Ein $z \in \mathbb{C}$ ist genau dann aus M konstruierbar, wenn es eine Kette von Körpererweiterungen $\mathbb{Q}(M \cup \bar{M}) = L_0 \subset L_1 \subset \cdots \subset L_n$ gibt, so daß $z \in L_n$ und $\forall j : [L_j : L_{j-1}] \in \{1, 2\}$.*
(c) *Für $z \in Kon(M \cup \bar{M})$ ist $[L_0(z) : L_0]$ eine Zweierpotenz.*

Korollar 7.4. *Das Delische Problem ist nicht lösbar, d.h. Würfelverdopplung mit Zirkel und Lineal ist unmöglich.*