Notizen zum

Repetitorium
Einführung in die Algebra

Wintersemester 2017/18

Jendrik Stelzner
s6jestel@uni-bonn.de

Letzte Änderung:
16. März 2018

Online verfügbar unter
goo.gl/SUyfxp*

*https://github.com/cionx/einfuehrung-in-die-algebra-review-ws-17-18

Inhaltsverzeichnis

1 Gruppentheorie

Es seien G, H zwei Gruppen.

Definition 1.1. *Eine Abbildung $f\colon G \to H$ ist ein* Gruppenhomomorphismus*, wenn $f(g_1g_2) = f(g_1)f(g_2)$ für alle $g_1, g_2 \in G$ gilt.*

Definition 1.2. *Eine Teilmenge $H \subseteq G$ ist eine* Untergruppe *von G, wenn $1 \in H$ gilt, und für alle $h, h_1, h_2 \in H$ auch $h^{-1} \in H$ und $h_1h_2 \in H$ gelten. Dies wird dann mit $H \leq G$ notiert.*

Ist $H \leq G$ eine Untergruppe, so lässt sich die Verknüpfung von G auf H einschränken, wodurch H ebenfalls wieder eine Gruppe ist.

Beispiel 1.3. Es ist $\mathrm{Z}(G) = \{g \in G \mid \forall h \in G : gh = hg\} \leq G$ das *Zentrum* von G.

Definition 1.4. *Ein Gruppenelement $g \in \mathrm{Z}(G)$ ist* zentral *in G.*

Definition 1.5. *Der* Kern *eines Gruppenhomomorphismus $f\colon G \to H$ ist*

$$\ker(f) \coloneqq \{g \in G \mid f(g) = 1\} \leq G\,.$$

Definition 1.6. *Zwei Gruppenelemente $g_1, g_2 \in G$ sind* konjugiert (zueinander)*, wenn es ein $h \in G$ mit $hg_1h^{-1} = g_2$ gibt. Zwei Untergruppen $H_1, H_2 \leq G$ sind* konjugiert (zueinander)*, wenn es ein $g \in G$ mit $gH_1g^{-1} = H_2$ gibt.*

1.1 Nebenklassen und Satz von Lagrange

Es sei G eine Gruppe und $H \leq G$ eine Untergruppe.

Definition 1.7. *Für alle $a \in G$ ist $aH \coloneqq \{ah \mid h \in H\}$ die* Linksnebenklasse von a bezüglich H*, und $Ha \coloneqq \{ha \mid h \in H\}$ die* Rechtsnebenklasse von a bezüglich H*.*

Für alle $a \in G$ gilt dabei

$$aH = H \iff a \in H \iff Ha = H\,.$$

Auf G werden nun durch

$$a \sim_L b \iff aH = bH \quad \text{und} \quad a \sim_R b \iff Ha = Hb$$

zwei Äquivalenzrelationen definiert. Dabei gilt für alle $a, b \in G$, dass

$$a \sim_L b \iff aH = bH \iff b^{-1}aH = H \iff b^{-1}a \in H \iff a^{-1}b \in H\,,$$

sowie analog

$$a \sim_R b \iff Ha = Hb \iff H = Hba^{-1} \iff ba^{-1} \in H \iff ab^{-1} \in H\,.$$

Dabei ist $x = a^{-1}b$ das eindeutige Gruppenelement mit $a \cdot x = b$. Es folgt somit, dass

$$\begin{aligned}[a]_{\sim_L} = \{b \in G \mid a \sim_L b\} &= \{b \in G \mid a^{-1}b \in H\} \\ &= \{b \in G \mid \exists h \in H : ah = b\} = \{ah \mid h \in H\} = aH\,,\end{aligned}$$

sowie analog, dass $[a]_{\sim_R} = Ha$. Die Äquivalenzklassen von $\sim_L$ und $\sim_R$ sind also genau die Linksnebenklassen Rechtsnebenklassen bezüglich H, also verschobene Versionen von H selbst. Dabei ist für jedes $a \in H$ die Abbildung

$$H \to aH\,, \quad h \mapsto ah$$

bijektiv, weshalb $|aH| = |H|$ gilt, sowie analog auch $|Ha| = |H|$.

Es ist nun G die disjunkte Vereinigung der Äquivalenzklassen von $\sim_L$, d.h. G zerfällt in disjunkte verschobene Versionen von H. Ist G endlich, so folgt somit, dass $|G|$ ein Vielfaches von $|H|$ ist.

Definition 1.8. *Die* Ordnung *einer Gruppe G ist* $\operatorname{ord}(G) \coloneqq |G|$.

Korollar 1.9 (Satz von Lagrange)**.** *Ist G endlich, so gilt* $\operatorname{ord}(H) \mid \operatorname{ord}(G)$.

Definition 1.10. *Es ist $G/H \coloneqq G/{\sim_L} = \{aH \mid a \in H\}$ die Menge der Linksnebenklassen und $H\backslash G \coloneqq G/{\sim_R} = \{Ha \mid a \in G\}$ die Menge der Rechtsnebenklassen.*

Für die Inversions-Abbildung $(-)^{-1} \colon G \to G$, $g \mapsto g^{-1}$ gilt

$$(aH)^{-1} = H^{-1}a^{-1} = Ha^{-1}\,,$$

weshalb $(-)^{-1}$ eine Bijektion $G/H \to H\backslash G$ induziert. Es gibt deshalb gleich viele Links- und Rechtsnebenklassen, d.h. es gilt $|G/H| = |H\backslash G|$.

Definition 1.11. *Der* Index *von H in G ist* $[G : H] \coloneqq |G/H| = |H\backslash G|$.

Korollar 1.12. *Ist G endlich, so gilt* $\operatorname{ord}(G) = \operatorname{ord}(H)[G : H]$*, sowie äquivalent* $[G : H] = \operatorname{ord}(G)/\operatorname{ord}(H)$*. Insbesondere ist auch $[G : H]$ ein Teiler von* $\operatorname{ord}(G)$.

Lemma 1.13. *Für $K \leq H \leq G$ gilt $[G : K] = [G : H][H : K]$.*

1.2 Normalteiler und Quotientengruppen

1.2.1 Definition von Normalteilern

Für eine Untergruppe $N \leq G$ sind die folgenden Bedingungen äquivalent:

1. Für alle $a \in G$ gilt $aN = Na$.

2. Für alle $a \in G$ gilt $aNa^{-1} = N$.

3. Für alle $a \in G$ gilt $aNa^{-1} \subseteq N$.

Definition 1.14. *Eine Untergruppe $N \leq G$, die eine (und damit alle) der obigen Bedingungen erfüllt, ist* normal*, bzw. ein* Normalteiler*. Dies wird mit $N \trianglelefteq G$ notiert.*

Beispiel 1.15. 1. Ist G abelsch, so ist jede Untergruppe $N \leq G$ normal.

2. Für $N \trianglelefteq G$ und $H \leq G$ mit $N \leq H$ gilt auch $N \trianglelefteq H$

3. Jede Untergruppe $N \leq G$ vom Index $[G : N] = 2$ ist normal.

4. Für jeden Gruppenhomomorphismus $f\colon G \to H$ ist $\ker(f)$ ein Normalteiler in G.
   a) Für alle $n \geq 0$ ist $A_n \coloneqq \{\sigma \in S_n \mid \operatorname{sgn}(\sigma) = 1\} \trianglelefteq S_n$.
   b) Für alle $n \geq 0$ ist $\mathrm{SO}(n) = \{A \in \mathrm{O}(n) \mid \det(A) = 1\} \trianglelefteq \mathrm{O}(n)$.

Definition 1.16. *Der* Normalisator *einer Untergruppe $H \leq G$ ist*

$$N_G(H) \coloneqq \{g \in G \mid gHg^{-1} = H\},$$

d.h. $N_G(H)$ ist die größte Untergruppe von G, in der H normal ist.

1.2.2 Konstruktion von Quotientengruppen

Ist $N \trianglelefteq G$ ein Normalteiler, so lässt sich auf G/N durch

$$gN \cdot hN \coloneqq (gh)N$$

eine Gruppenstruktur definieren.

Definition 1.17. *Für $N \trianglelefteq G$ ist G/N die* Quotientengruppe *von G nach N.*

Die Gruppenstruktur auf G/N ist eindeutig dadurch bestimmt, dass die *kanonische Projektion*

$$p\colon G \to G/N \quad g \mapsto \overline{g} \coloneqq gN$$

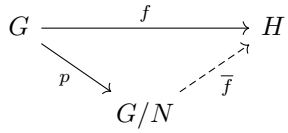
ein Gruppenhomomorphismus ist. Dabei gilt $\ker(p) = N$.

Korollar 1.18. *Eine Untergruppe $N \leq G$ ist genau dann normal, wenn es einen Gruppenhomomorphismus $f\colon G \to H$ mit $\ker(f) = N$ gibt.*

Bemerkung 1.19. Es handelt sich bei dem obigen Vorgehen um eine von mehreren möglichen Vorgehensweisen, Quotientengruppen zu konstruieren. Inbesondere lassen sich Quotientengruppen auch ohne Verwendung von Nebenklassen konstruieren. Entscheident ist für die Quotientengruppe G/N nur, dass die kanonische Projektion $p\colon G \to G/N$ ein Gruppenhomomorphismus mit $\ker(p) = N$ ist, welcher die folgende universelle Eigenschaft besitzt:

1.2.3 Universelle Eigenschaft der Quotientengruppe

Satz 1.20 (Homomorphiesatz für Gruppen)**.** *Ist $f\colon G \to H$ ein Gruppenhomomorphismus mit $N \subseteq \ker(f)$, so induziert f einen eindeutigen Gruppenhomomorphismus $\overline{f}\colon G/N \to H$ mit $f = \overline{f} \circ p$, d.h. so dass das folgende Diagramm kommutiert:*



In anderen Worten: Es ergibt sich eine Bijektion

$$\{\textit{Gruppenhomo. } \overline{f}\colon G/N \to H\} \xrightarrow{\sim} \{\textit{Gruppenhomo. } f\colon G \to H \textit{ mit } N \subseteq \ker(f)\}\,,$$
$$\overline{f} \mapsto \overline{f} \circ p\,.$$

Korollar 1.21 (1. Isomorphiesatz)**.** *Jeder Gruppenhomomorphismus $f\colon G \to H$ induziert einen Isomorphismus*

$$G/\ker(f) \xrightarrow{\sim} \mathrm{im}(f)\,, \quad \overline{g} \mapsto f(g)\,.$$

Korollar 1.22 (2. Isomorphiesatz)**.** *Es seien $N, K \trianglelefteq G$ zwei Normalteiler mit $N \leq K$. Dann ist K/N normal in G/N, und es gibt einen wohldefinierten Isomorphismus*

$$(G/N)/(K/N) \xrightarrow{\sim} G/K\,, \quad \overline{\overline{g}} \mapsto \overline{g}\,.$$

Korollar 1.23 (3. Isomorphiesatz)**.** *Es sei $H \leq G$ eine Untergruppe und $N \trianglelefteq G$ eine normale Untergruppe. Dann ist $HN = \{hn \mid h \in H, n \in N\}$ eine Untergruppe von G, $H \cap N$ eine normale Untergruppe von H, und es gibt einen wohldefinierten Isomorphismus*

$$H/(H \cap N) \xrightarrow{\sim} HN/N\,, \quad \overline{h} \mapsto \overline{h}\,.$$

1.2.4 Korrespondenz von (normalen) Untergruppen

Proposition 1.24. *Es sei $N \trianglelefteq G$ eine normale Untergruppe und $p\colon G \to G/N$, $g \mapsto \overline{g}$ die kanonische Projektion.*

1. Es gibt eine 1:1-Korrespondenz von Untergruppen

$$\{\textit{Untergruppen } H \leq G \textit{ mit } N \leq H\} \overset{1:1}{\longleftrightarrow} \{\textit{Untergruppen } H' \leq G/N\}\,,$$
$$H \longmapsto p(H) = H/N\,,$$
$$p^{-1}(H') \longmapsfrom H'\,.$$

2. Es gibt eine eingeschränkte 1:1-Korrespondenz zwischen normalen Untergruppen

$$\{\textit{Normalteiler } K \trianglelefteq G \textit{ mit } N \leq K\} \overset{1:1}{\longleftrightarrow} \{\textit{Normalteiler } K' \trianglelefteq G/N\}\,,$$
$$K \longmapsto p(K) = K/N\,,$$
$$p^{-1}(K') \longmapsfrom K'\,.$$

3. *Für jeden Normalteiler $K \trianglelefteq G$ mit $N \leq K$ gilt dabei für den zugehörigen Normalteiler $K' = p(K) = K/N$ nach dem 2. Isomorphiesatz, dass*

$$G/K \cong (G/N)/(K/N) \cong (G/N)/K' .$$

Auf beiden Seiten der obigen 1:1-Korrespondenz erhält man somit (bis auf Isomorphie) die gleichen Quotientengruppen.

1.3 Erzeugte Untergruppen

1.3.1 Definition erzeugter Untergruppen

Es sei G eine Gruppe und $S \subseteq G$ eine Teilmenge. Für eine Untergruppe $H \subseteq G$ sind die folgenden Bedingungen äquivalent:

1. Es ist H die kleinste Untergruppe von G, die S enthält, d.h. es gilt $S \subseteq H$, und für jede Untergruppe $K \leq G$ mit $S \subseteq K$ gilt $H \leq K$.
2. Es gilt $H = \bigcap_{K \leq G, S \subseteq K} K$.
3. Es gilt $H = \{s_1^{\varepsilon_1} \cdots s_n^{\varepsilon_n} \mid n \in \mathbb{N}, s_i \in S, \varepsilon_i = \pm 1\}$.

Definition 1.25. *Die Untergruppe H, die eine (und damit alle) der obigen Bedingungen erfüllt, ist die* von S erzeugte *Untergruppe, und wird mit $\langle S \rangle$ notiert. Es ist S ein* Erzeugendensystem *von H.*

Beispiel 1.26. 1. Die symmetrische Gruppe S_n wird von der Menge der Transpositionen $\{(i,j) \mid 1 \leq i \neq j \leq n\}$ erzeugt. Ein weiteres Erzeugendensystem ist die Menge der einfachen Transpositionen $\{(i, i+1) \mid 1 \leq i < n\}$.

2. Ist K ein Körper, so wird die Gruppe $\mathrm{GL}_n(K)$ von der Menge der Elementarmatrizen erzeugt.

1.3.2 Klassifikation zyklischer Gruppen

Definition 1.27. *Ein Gruppe G* zyklisch*, wenn es ein $g \in G$ mit $G = \langle g \rangle$ gibt.*

Beispiel 1.28. 1. Die Gruppe $\mathbb{Z}$ ist zyklisch mit Erzeuger 1.

2. Wird G von $g \in G$ zyklisch erzeugt, so wird für jeden Normalteiler $N \trianglelefteq G$ die Quotientengruppe G/N von $\overline{1}$ zyklisch erzeugt.

3. Insbesondere ist für alle $n \in \mathbb{Z}$ die Quotientengruppe $\mathbb{Z}/n \coloneqq \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\langle n \rangle$ zyklisch mit Erzeuger $\overline{1} \in \mathbb{Z}/n$.

4. Ist K ein Körper, so ist jede endliche Untergruppe $H \leq K^\times$ zyklisch. Inbesondere ist $K^\times$ zyklisch, wenn K endlich ist.

Es gilt auch die Umkehrung der obigen Beispiele, d.h. jede zyklische Gruppe ist zu genau einer der Gruppen $\mathbb{Z}/n$ mit $n \geq 0$ isomorph:

Lemma 1.29. *Jede Untergruppe $H \leq \mathbb{Z}$ ist von der Form $H = \langle n \rangle = n\mathbb{Z}$ für ein eindeutiges $n \geq 0$. Für $H = \{0\}$ gilt $n = 0$, und sonst gilt $n = \min\{k > 0 \mid k \in H\}$.*

Ist G zyklisch mit Erzeuger $g \in G$, so ist die Abbildung

$$f \colon \mathbb{Z} \to G\,, \quad n \mapsto g^n$$

ein surjektiver Gruppenhomomorphismus, und induziert somit einen Isomorphismus

$$\overline{f} \colon \mathbb{Z}/\ker(f) \to G\,, \quad \overline{n} \mapsto g^n\,.$$

Es gibt es eindeutiges $n \geq 0$ mit $\ker(f) = n\mathbb{Z}$. Gilt $n = 0$, so ist gilt $\mathbb{Z} \cong G$, und G ist unendlich. Ansonsten gilt $n > 1$ und somit $G \cong \mathbb{Z}/n$ mit $\operatorname{ord}(G) = n$.

Korollar 1.30 (Klassifikation zyklischer Gruppen)**.** *Jede zyklische Gruppe G ist zu genau einer der Gruppen $\mathbb{Z}$, $\mathbb{Z}/n$ mit $n \geq 1$ isomorph. Dabei gilt*

$$G \cong \begin{cases} \mathbb{Z} & \text{falls } G \text{ unendlich ist}, \\ \mathbb{Z}/n & \text{falls } n = \operatorname{ord}(G) \text{ endlich ist}. \end{cases}$$

Korollar 1.31. *Untergruppen zyklischer Gruppen sind ebenfalls zyklisch.*

Definition 1.32. *Für $g \in G$ ist* $\operatorname{ord}(g) = \operatorname{ord}(\langle g \rangle)$ *die* Ordnung von g.

Lemma 1.33. *Es sei $g \in G$.*

1. *Ist G eine endliche Gruppe, so gilt* $\operatorname{ord}(g) \mid \operatorname{ord}(G)$. *Insbesondere gilt* $g^{\operatorname{ord}(G)} = 1$.
2. *Hat g endliche Ordnung, so gilt* $\operatorname{ord}(g) = \min\{n \geq 1 \mid g^n = 1\}$, *sowie genau dann* $g^m = 1$, *wenn* $\operatorname{ord}(g) \mid m$.

Beispiel 1.34 (Gruppen von Ordnung p)**.** Es sei p prim und G eine Gruppe von Ordnung $\operatorname{ord}(G) = p$. Dann gibt es ein nicht-triviales Element $g \in G$. Dann ist $\operatorname{ord}(g) \neq 1$ ein Teiler von $\operatorname{ord}(G) = p$, und somit $\operatorname{ord}(g) = \operatorname{ord}(G)$, also $\langle g \rangle = G$. Somit ist G zyklisch, also $G \cong \mathbb{Z}/p$.

1.4 Gruppenwirkungen

1.4.1 Grundlegende Definitionen

Definition 1.35. *Es sei G eine Gruppe und X eine Menge. Eine* (Gruppen)wirkung *von G auf X ist eine Abbildung $G \times X \to X$, $(g, x) \mapsto g.x$ mit $1.x = x$ und $g.(h.x) = (gh).x$ für alle $g, h \in G$, $x \in X$.*

*Eine G-*Menge *ist eine Menge X zusammen mit einer Wirkung von G auf X.*

Es sei G eine Gruppe und X eine Menge.

- Wirkt G auf X, so ist für jedes $g \in G$ die Abbildung $\lambda_g \colon X \to X$, $x \mapsto g.x$ eine Bijektion, und die Abbildung $G \to S(X)$, $g \mapsto \lambda_g$ ist ein Gruppenhomomorphismus.
- Ist andererseits $\varphi \colon G \to S(X)$ ein Gruppenhomomorphismus, so wird durch $g.x \coloneqq \varphi(g)(x)$ eine Wirkung von G auf X definiert.

Diese beiden Konstruktionen sind invers zueinander, weshalb eine Wirkung von G auf X einem Gruppenhomomorphismus $G \to S(X)$ entspricht.

Definition 1.36. *Es sei X eine G-Menge und $x \in X$.*

1. *Die* G-Bahn *von x ist $G.x \coloneqq \{g.x \mid g \in G\}$.*
2. *Es ist $X/G \coloneqq \{G.x \mid x \in X\}$ die Menge der G-Bahnen.*
3. *Der* Stabilisator *von x ist $G_x \coloneqq \{g \in G \mid g.x = x\}$.*
4. *Die* Fixpunktmenge *von X ist $X^G \coloneqq \{x \in X \mid \forall g \in G : g.x = x\}$.*

Lemma 1.37. *Es sei X eine G-Menge.*

1. *Für alle $x \in X$ ist $G_x \leq G$ eine Untergruppe.*
2. *Für alle $g \in G$, $x \in X$ gilt $G_{g.x} = gG_xg^{-1}$.*

Beispiel 1.38. Die Gruppe $\mathrm{GL}_n(K)$ wirkt auf dem Vektorraum K^n durch $A.x \coloneqq Ax$ für alle $A \in \mathrm{GL}_n(K)$, $x \in K^n$. Für alle $x, y \in K^n$ mit $x, y \neq 0$ gibt es ein $A \in \mathrm{GL}_n(K)$ mit $Ax = y$, weshalb diese Gruppenwirkung zwei Bahnen besitzt: $\{0\}$ und $K^n \smallsetminus \{0\}$. Insbesondere ist im Allgemeinen 0 der einzige Fixpunkt dieser Wirkung; einzige Ausnahme ist der Fall $K = \mathbb{F}_2$, $n = 1$, dann sind beide Elemente Fixpunkte. Der Stabilisator des Standardbasisvektors e_1 ist die Untergruppe

$$H \coloneqq \left\{ \begin{pmatrix} 1 & * \\ 0 & A \end{pmatrix} \,\middle|\, A \in \mathrm{GL}_{n-1}(K) \right\};$$

der Stabilisator eines beliebigen Vektors $x \in K^n$, $x \neq 0$ ist konjugiert zu H.

Definition 1.39. *Es sei X eine G-Menge.*

1. *Die Wirkung von G auf X ist* transitiv*, wenn es für alle $x, y \in X$ ein $g \in G$ mit $g.x = y$ gibt.*
2. *Die Wirkung von G auf X ist* treu*, wenn es für alle $g, h \in G$ aus*

   $$g.x = h.x \text{ für alle } x \in X$$

   folgt, dass $g = h$ gilt.

Bemerkung 1.40. Eine Wirkung von G auf X ist genau dann treu, wenn der zugehörige Gruppenhomomorphismus $G \to S(X)$ injektiv ist.

Beispiel 1.41. Die symmetrische Gruppe S_n wirkt auf der Menge $X \coloneqq \{1, \dots, n\}$ durch $\sigma.i \coloneqq \sigma(i)$ für alle $\sigma \in S_n$, $i \in X$. Dies Wirkung ist transitiv und treu. Der zugehörige Gruppenhomomorphismus $S_n \to S(X) = S_n$ ist die Identität id_{S_n}. Der Stabilisator von $i \in X$ ist $\{\sigma \in S_n \,|\, \sigma(i) = i\} \cong S_{n-1}$.

Beispiel 1.42. Jede Gruppe G wirkt auf sich selbst, d.h. auf $X \coloneqq G$, auf zwei Weisen:

1. Die Gruppe G wirkt auf sich selbst durch Linksmultiplikation, d.h. durch $g.x \coloneqq gx$ für alle $g \in G$, $x \in X$. Diese Wirkung ist transitiv und treu, und für jedes $x \in X$ ist der Stabilisator G_x trivial.

   Man bemerke, dass diese treue Wirkung einem injektiven Gruppenhomomorphismus $G \hookrightarrow S(X)$ entspricht, durch den sich G als eine Untergruppe der symmetrischen Gruppe $S(X)$ auffassen lässt. Dies ist der *Satz von Cayley*: Jede Gruppe ist isomorph zu einer Gruppe von Permutationen.

2. Die Gruppe G wirkt auf sich selbst durch Konjugation, d.h. für alle $g \in G$, $x \in X$ ist $g.x \coloneqq gxg^{-1}$. Die Bahnen dieser Wirkung sind die *Konjugationsklassen* von G. Für alle $g \in G$ $x \in X$ gilt

   $$g.x = x \iff gxg^{-1} = x \iff gx = xg$$

   die Fixpunktmenge X^G dieser Wirkung ist deshalb das Zentrum $\mathrm{Z}(G)$, und für jedes $x \in X$ ist $G_x = \{g \in G \,|\, gx = xg\} =: \mathrm{Z}_G(x)$ der *Zentralisator* von x; dies ist die größte Untergruppe von G, in der x zentral ist.

1.4.2 Die Bahnenformel

Es sei X eine G-Menge. Durch

$$x \sim y \iff \exists g \in G : g.x = y$$

wird eine Äquivalenzrelation auf X definiert. Für alle $x \in X$ gilt dann $[x]_\sim = G.x$. Je zwei Bahnen $G.x$ und $G.y$ sind also entweder gleich oder disjunkt, und X ist die disjunkte Vereinigung der G-Bahnen. Ist $(x_i)_{i \in I}$ ein Repräsentantensystem der G-Bahnen von X, so gilt deshalb

$$|X| = \sum_{i \in I} |G.x_i| = \left|X^G\right| + \sum_{\substack{i \in I \\ x_i \notin X^G}} |G.x_i| \,. \tag{1}$$

Für jedes $x \in X$ ist dabei die Abbildung $G \to G.x$, $g \mapsto g.x$ surjektiv, und es gilt

$$g.x = h.x \iff h^{-1}g.x = x \iff h^{-1}g \in G_x \iff gG_x = hG_x \,.$$

Korollar 1.43. *Für jedes $x \in G$ ist die Abbildung*

$$G/G_x \to G.x \,, \quad gG_x \mapsto g.x$$

eine wolhdefinierte Bijektion. Insbesondere gilt $|G.x| = |G/G_x| = [G : G_x]$.

Bemerkung 1.44. Man bemerke, dass somit $|G.x|$ stets ein Teiler von $|G|$ ist!

Durch Lemma 1.43 lässt sich Gleichung (1) zu

$$|X| = \sum_{i \in I} [G : G_{x_i}] = \left|X^G\right| + \sum_{\substack{i \in I \\ x_i \notin X^G}} [G : G_{x_i}]$$

umschreiben.

Korollar 1.45 (Bahnenformel)**.** *Ist X eine G-Menge und $(x_i)_{i \in I}$ ein Repräsentantensystem der G-Bahnen von X, so gilt*

$$|X| = \left|X^G\right| + \sum_{\substack{i \in I \\ x_i \notin X^G}} [G : G_{x_i}].$$

1.5 p-Gruppen und Sylowsätze

Es sei G eine endliche Gruppe und p prim.

Definition 1.46. *Gilt* $\mathrm{ord}(G) = p^n$ *für ein* $n \in \mathbb{N}$*, so ist* G *eine* p-Gruppe.

Beispiel 1.47. 1. Es ist $\mathbb{Z}/p$ bis auf Isomorphie die einzige Gruppe der Ordnung p.

2. Jede Gruppe der Ordnung p^2 ist abelsch, und isomorph zu entweder $\mathbb{Z}/p^2$ oder $\mathbb{Z}/p \times \mathbb{Z}/p$.

3. Die Heisenberg-Gruppe

$$H \coloneqq \left\{ \begin{pmatrix} 1 & a & b \\ & 1 & c \\ & & 1 \end{pmatrix} \middle| \, a, b, c \in \mathbb{F}_p \right\} \leq \mathrm{GL}_3(\mathbb{F}_p)$$

ist eine nicht abelsche Gruppe der Ordnung p^3.

Lemma 1.48. *Ist* G *eine nicht-triviale* p*-Gruppe, so ist auch* $\mathrm{Z}(G)$ *nicht-trivial.*

Korollar 1.49. *Ist* G *eine* p*-Gruppe, so besitzt* G *eine Normalenreihe*

$$\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq G_3 \trianglelefteq \cdots \trianglelefteq G_n = G$$

mit Quotienten $G_i/G_{i-1} \cong \mathbb{Z}/p$ *für alle* $i = 1, \ldots, n$*, d.h. es gilt* $|G_r| = p^r$ *für alle* r*.*

Definition 1.50. *Eine* p-Sylowuntergruppe *von* G *ist eine* p*-Untergruppe* $S \leq G$ *mit* $p \nmid [G : S]$*, d.h. für* $\mathrm{ord}(G) = p^r m$ *mit* $p \nmid m$ *gilt* $\mathrm{ord}(S) = p^r$*.*

Satz 1.51 (Sylowsätze)**.** *Es gelte* $G = p^r m$ *mit* $p \nmid m$*.*

1. *Jede* p*-Untergruppe* $H \leq G$ *ist in einer* p*-Sylowuntergruppe von* G *enthalten. Insbesondere ergibt sich für* $H = \{1\}$*, dass* G *eine* p*-Sylowuntergruppe besitzt.*

2. *Je zwei* p*-Sylowuntergruppen* $S, S' \leq G$ *sind konjugiert zueinander, d.h. es gibt ein* $g \in G$ *mit* $gSg^{-1} = S'$*.*

3. *Bezeichnet* n_p *die Anzahl der* p*-Sylowuntergruppen von* G*, so gilt*

$$n_p \equiv 1 \pmod{p} \qquad \textit{und} \qquad n_p \mid m\,.$$

Korollar 1.52. *Eine* p*-Sylowuntergruppe* $S \leq G$ *ist genau dann normal, wenn* $n_p = 1$*.*

Korollar 1.53. *Ist* G *abelsch, so besitzt* G *eine eindeutige* p*-Sylowuntergruppe.*

1.6 Klassifikation endlicher abelscher Gruppen

Satz 1.54. *Es sei G eine endliche abelsche Gruppe, und für jede Primzahl p sei S_p die eindeutige p-Sylowuntergruppe von G. Sind $p_1, \ldots, p_n$ die Primfaktoren von $|G|$, so ist die Abbildung*

$$S_{p_1} \times \cdots \times S_{p_n} \xrightarrow{\sim} G\,, \quad (g_1, \ldots, g_n) \mapsto g_1 \cdots g_n$$

ein Isomorphismus.

Proposition 1.55. *Es sei p prim. Jede abelsche p-Gruppe G ist isomorph zu einem Produkt zyklischer p-Gruppen, d.h. es gilt*

$$G \cong \mathbb{Z}/p^{n_1} \times \cdots \times \mathbb{Z}/p^{n_r}$$

mit $n_1, \ldots, n_r \geq 1$.

Korollar 1.56 (Klassifikation endlicher abelscher Gruppen)**.** *Jede endliche abelsche Gruppe G ist isomorph zu einem Produkt zyklischer p-Gruppen, d.h. es gilt*

$$G \cong \mathbb{Z}/p_1^{n_1} \times \cdots \times \mathbb{Z}/p_r^{n_r}$$

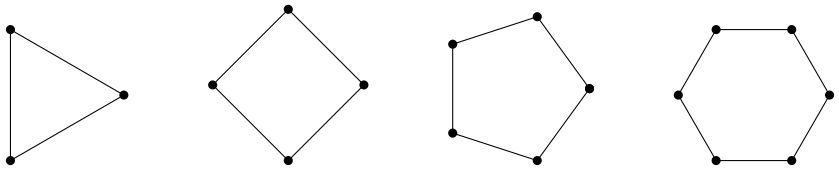
mit $p_1, \ldots, p_r$ prim und $n_1, \ldots, n_r \geq 1$.

Man bemerke, dass dabei $|G| = p_1^{n_1} \cdots p_r^{n_r}$ gilt.

Bemerkung 1.57. Tatsächlich ist diese Zerlegung bereits eindeutig bis auf Permutation der Faktoren, d.h. die Paare $(p_1, n_1), \ldots, (p_r, n_r)$ sind eindeutig bis auf Permutation. Diese Eindeutigkeit wurde in der Vorlesung allerdings nicht gezeigt.

1.7 Beispiel: Die Diedergruppe D_n

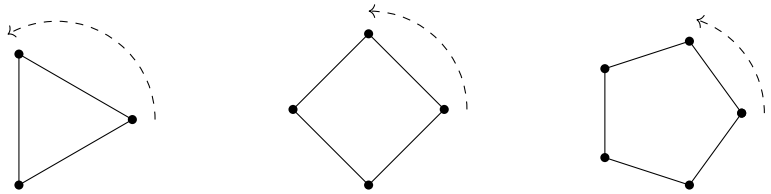
Es sei $n \geq 3$. Die *Diedergruppe* D_n ist die Symmetriegruppe eines regelmäßigen n-Ecks.



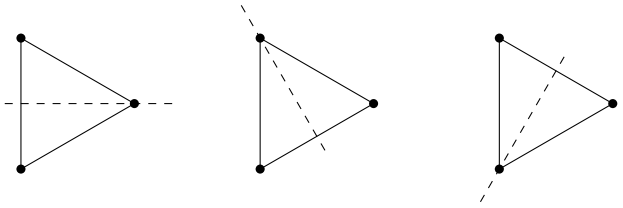
Ein regelmäßiges n-Eck für $n = 3, 4, 5, 6$.

Die Gruppe D_n besteht also aus zwei Arten von Elementen:

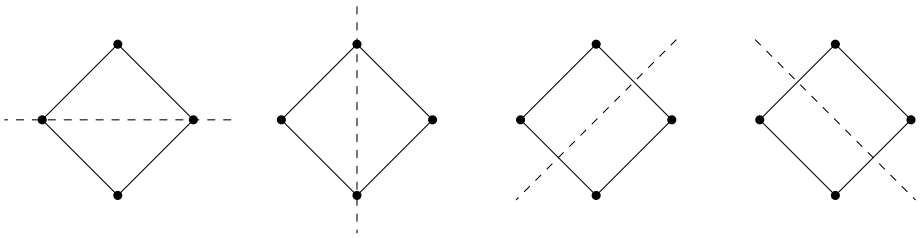
- Die insgesamt n Rotationen um Vielfache des Winkels $2\pi/n$.



- Ingesamt n Spiegelungen:
  - Ist n ungerade, so gehen die Spiegelungsachsen durch jeweils einen der Eckpunkte sowie den Mittelpunkt der gegenüberliegenden Seite:

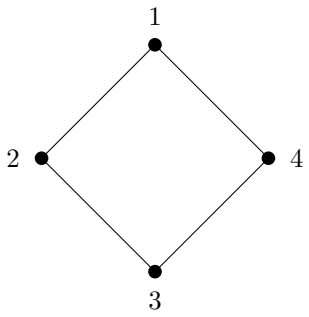


  - Ist n gerade, so gibt es $n/2$ Spiegelungen, deren Achsen durch einen der Eckpunkte sowie den gegenüberliegenden Eckpunkt gehen, sowie $n/2$ Spiegelungen, die durch einen der Seitenmittelpunkte sowie den gegenüberliegenden Seitenmittelpunkt gehen:



Insgesamt besteht die Diedergruppe D_n somit aus $2n$ Elementen, davon n Rotationen und n Spiegelungen. Jedes $\sigma \in D_n$ permutiert die Eckpunkte des regelmäßigen n-Ecks, wobei die Wirkung von σ auf dem gesamten n-Eck bereits eindeutig durch die Wirkung auf den Eckpunkten bestimmt ist. Indem man die Eckpunkte mit $1, \ldots, n$ durchnummeriert, lässt sich D_n auf diese Weise mit einer Untergruppe von S_n identifizieren.

Beispiel 1.58. Es sei $n = 4$.



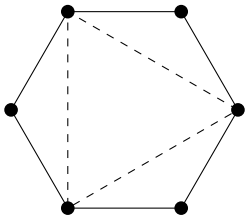
Spiegelungen mit Achse durch die Eckpunkte	$(1,3)$ und $(2,4)$
Spiegelungen mit Achse durch die Seitenmittelpunkte	$(1,2)(3,4)$ und $(1,4)(2,3)$
Rotationen um $0°$, $90°$, $180°$, $270°$	id, $(1,2,3,4)$, $(1,3)(2,4)$, $(4,3,2,1)$

Für $n = 3$ gilt $|D_3| = 2 \cdot 3 = 6 = 3! = |S_3|$, weshalb die Einbettung $D_3 \hookrightarrow S_3$ bereits ein Isomorphismus ist.

Korollar 1.59. *Es gilt $D_3 \cong S_3$.*

Proposition 1.60. *Es seien $n, m \geq 3$.*

1. Gilt $n \mid m$, so gibt es eine Einbettung $D_n \hookrightarrow D_m$:



Beispiel: $D_3 \hookrightarrow D_6$.

2. Gilt $n = 2m$ mit m ungerade, so gilt bereits $D_n \cong D_m \times (\mathbb{Z}/2)$.

2 Ringtheorie

Es seien R, S zwei Ringe.

Definition 2.1. *Eine Abbildung $f\colon R \to S$ ist ein Ringhomomorphismus, wenn*

$$f(r_1 + r_2) = f(r_1) + f(r_2), \quad f(r_1 r_2) = f(r_1) f(r_2), \quad f(1) = 1$$

für alle $r_1, r_2 \in R$ gilt.

Definition 2.2. *Der* Kern *eines Ringhomomorphismus $f\colon R \to S$ ist*

$$\ker(f) \coloneqq \{x \in R \mid f(x) = 0\}.$$

Definition 2.3. *Eine Teilmenge $S \subseteq R$ ist ein* Unterring*, wenn*

$$s_1 + s_2 \in S, \quad s_1 s_2 \in S, \quad 1 \in S$$

für alle $s_1, s_2 \in S$ gilt.

Ist $X \subseteq R$ eine Teilmenge, so sind für jeden Unterring $S \subseteq R$ die folgenden Bedingungen äquivalent:

1. Es ist S der kleinste Unterring, der X enthält, d.h. es gilt $X \subseteq S$, und für jeden Unterring $S' \subseteq R$ mit $X \subseteq S'$ gilt $S \subseteq S'$.
2. Es gilt $S = \bigcap_{\text{Unterring } S' \subseteq S,\ X \subseteq S'} S'$.
3. Es gilt $S = \{\sum_{i=1}^{n} \varepsilon_i x_{i,1} \cdots x_{i,m_i} \mid n, m_i \in \mathbb{N}, \varepsilon_i = \pm 1, x_{i,j} \in X\}$.

Definition 2.4. *Der Unterring $S \subseteq R$ der eine (und damit alle) der obigen Bedingungen erfüllt, ist der* von X erzeugte *Unterring von R. Es ist X ein* Erzeugendensystem *von R.*

Definition 2.5. *Für $x, y \in R$ ist x ein* Teiler *von y wenn es ein $z \in R$ mit $y = xz$ gibt. Dies wird mit $x \mid y$ notiert.*

2.1 Einheiten und Nullteiler

Es sei R ein Ring.

Definition 2.6. *Ein Element $u \in R$ ist eine* Einheit*, wenn es ein $r \in R$ mit $ur = 1$ und $ru = 1$ gibt. Es ist $R^\times \coloneqq \{u \in R \mid u \text{ ist eine Einheit}\}$ die* Einheitengruppe *von R.*

Es bildet $R^\times$ bezüglich der Multiplikation von R eine Gruppe, was den Begriff der Einheiten*gruppe* rechtfertigt.

Beispiel 2.7. 1. Ist K ein Körper, so gilt $\mathrm{M}_n(K)^\times = \mathrm{GL}_n(K)$.

2. Ein kommutativer Ring R ist genau dann ein Körper, wenn $R^\times = R \setminus \{0\}$ gilt.

3. Es gilt $\mathbb{Z}^\times = \{1, -1\}$.

4. Für $n \geq 1$ ist ein Element $\overline{k} \in \mathbb{Z}/n$ ist genau dann eine Einheit, wenn n und k teilerfremd sind.

Definition 2.8. *Ein Element $r \in R$ ist ein* Linksnullteiler *bzw.* Rechtsnullteiler*, wenn es ein $x \in R$ mit $x \neq 0$ und $rx = 0$, bzw. $xr = 0$ gibt. Ist r ein Links- und Rechtsnullteiler, so ist r ein* (beidseitiger) Nullteiler.

Beispiel 2.9. 1. Für $n \geq 1$ ist $\overline{k} \in \mathbb{Z}/n$ genau dann ein Nullteiler, wenn k und n nicht teilerfremd sind.

2. Ist V ein Vektorraum, so ist $f \in \mathrm{End}(V)$ genau dann ein
   - Linksnullteiler, wenn f nicht injektiv ist,
   - Rechtsnullteiler, wenn f nicht surjektiv ist.

   Ist V endlichdimensional, so sind beide Bedingungen äquivalent. Ist V unendlichdimensional, so gibt es ein $f \in \mathrm{End}(V)$, das surjektiv aber nicht injektiv ist, und somit ein Linksnullteiler aber kein Rechtsnullteiler ist; analog gibt es in $\mathrm{End}(V)$ auch Rechtsnullteiler, die keine Linkssnullteiler sind.

Definition 2.10. *Ein* Integritätsbereich *ist ein kommutativer Ring R mit $R \neq \{0\}$, so dass 0 der einziger Nullteiler in R ist.*

2.2 Polynomringe

Es sei R ein Ring.

2.2.1 Polynomring in einer Variables

Definition 2.11. *Der* Grad *eines Polynoms $f = \sum_{i=0}^{n} a_i t^i \in R[t]$ ist für $f \neq 0$ durch*

$$\deg(f) \coloneqq \max\{i \mid a_i \neq 0\}$$

definiert, und für $f = 0$ durch $\deg(0) \coloneqq -\infty$.

Proposition 2.12. *1. $R[t]$ ist genau dann kommutativ, wenn R kommutativ ist.*

2. Für alle $f, g \in R[t]$ gilt $\deg(fg) \leq \deg(f) + \deg(g)$.

3. Dabei gilt genau dann Gleichheit für alle $f, g \in R[t]$, wenn R keinen von 0 verschiedenen Linksnullteiler (und somit auch keinen von 0 verschiedenen Rechtsnullteiler) besitzt. Dies gilt insbesondere, wenn R ein Integritätsbereich ist.

4. $R[t]$ ist genau dann ein Integritätsbereich, wenn R ein Integritätsbereich ist.

5. Ist R ein Integritätsbereich, so gilt $R[t]^\times = R^\times$.

Proposition 2.13 (Polynomdivision)**.** *Es sei K ein Körper. Für alle $f, g \in K[t]$ mit $g \neq 0$ gibt es eindeutige Polynome $q, r \in K[t]$ mit*

$$f = qg + r\,, \qquad \textit{wobei } \deg(r) < \deg(g)\,.$$

Es sei nun R kommutativ. Ist S ein kommutativer Ring, so dass $R \subseteq S$ ein Unterring ist, so lassen sich Elemente $s \in S$ in Polynome $f = \sum_{i=0}^n a_i t^i \in R[t]$ einsetzen:

$$f(s) \coloneqq \sum_{i=0}^n a_i s^i\,.$$

Die Abbildung $R[t] \to S$, $f \mapsto f(s)$ ist dabei ein Ringhomomorphismus. Ist allgemeiner $\varphi\colon R \to S$ ein Ringhomomorphismus, so ergibt sich für jedes $s \in S$ ein Ringhomomorphismus ,

$$R[t] \to S\,, \quad \sum_{i=0}^n a_i t^i \mapsto \sum_{i=0}^n \varphi(a_i) s^i\,.$$

Satz 2.14 (Universelle Eigenschaft des Polynomrings)**.** *Sind R, S kommutative Ringe, so gibt es für jeden Ringhomomorphismus $\varphi\colon R \to S$ und jedes Element $s \in S$ einen eindeutigen Ringhomomorphismus $\hat\varphi\colon R[t] \to S$ mit $\hat\varphi|_R = \varphi$ und $\hat\varphi(t) = s$; dabei gilt*

$$\hat\varphi\left(\sum_{i=0}^n a_i t^i\right) = \sum_{i=0}^n \varphi(a_i) s^i\,.$$

In anderen Worten: Es ergibt sich eine Bijektion

$$\begin{aligned}\{\textit{Ringhomo. } \hat\varphi\colon R[t] \to S\} &\xrightarrow{\sim} \{(\varphi, s) \mid \textit{Ringhomo. } \varphi\colon R \to S,\ s \in S\}\,,\\ \hat\varphi &\longmapsto (\hat\varphi|_R, \hat\varphi(t))\ .\end{aligned}$$

2.2.2 Polynomringe in endlich vielen Variablen

Ist R ein Ring, so lässt sich der Polynomring $R[t_1, \ldots, t_n]$ in endlich vielen Variablen induktiv als $R[t_1, \ldots, t_n] \coloneqq R[t_1, \ldots, t_{n-1}][t_n]$ definieren.

Beispiel 2.15. Es gilt $3tu^2 + 2u^2 + t^2u - 4u + t + 6 \in \mathbb{Z}[t, u]$. Unter der Identifikation $\mathbb{Z}[t, u] \cong \mathbb{Z}[t][u]$ entspricht dies dem Polynom $(3t+2)u^2 + (t^2-4)u + (t+6)$, und unter der Identifikation $\mathbb{Z}[t, u] \cong \mathbb{Z}[u][t]$ dem Polynom $ut^2 + (3u^2+1)t + (2u^2 - 4u + 6)$.

Satz 2.16 (Universelle Eigenschaft des Polynomrings)**.** *Sind R, S kommutative Ringe, so gibt es für jeden Ringhomomorphismus $\varphi\colon R \to S$ und alle Elemente $s_1, \ldots, s_n \in S$ einen eindeutigen Ringhomomorphismus $\hat\varphi\colon R[t_1, \ldots, t_n] \to S$ mit $\hat\varphi|_R = \varphi$ und $\hat\varphi(t_i) = s_i$ für alle $i = 1, \ldots, n$; dabei gilt*

$$\hat\varphi\left(\sum_{\alpha \in \mathbb{N}^n} a_\alpha t_1^{\alpha_1} \cdots t_n^{\alpha_n}\right) = \sum_{\alpha \in \mathbb{N}^n} a_\alpha s_1^{\alpha_1} \cdots s_n^{\alpha_n}\,.$$

In anderen Worten: Es ergibt sich eine Bijektion

$$\begin{aligned} &\{\textit{Ringhomo. } \hat{\varphi}\colon R[t_1,\dots,t_n] \to S\} \\ \xrightarrow{\sim}\ &\{(\varphi, s_1,\dots,s_n) \mid \textit{Ringhomo. } \varphi\colon R \to S,\ s_i \in S\} \\ \hat{\varphi} \longmapsto\ &(\hat{\varphi}|_R, \hat{\varphi}(t_1),\dots,\hat{\varphi}(t_n))\,. \end{aligned}$$

Bemerkung 2.17. Es lassen sich auch allgemeiner Polynomringe $R[t_i \mid i \in I]$ für eine beliebige Indexmenge I konstruieren.

Lemma 2.18. *Es seien R, S kommutative Ringe, so dass $R \subseteq S$ ein Unterring ist. Für $s_1,\dots,s_n \in S$ sei*

$$\mathrm{ev}_{s_1,\dots,s_n}\colon R[t_1,\dots,t_n] \to S$$

der eindeutige Ringhomomorphismu mit

$$\mathrm{ev}_{s_1,\dots,s_n}|_R = \mathrm{id}_R \qquad \textit{und} \qquad \mathrm{ev}_{s_1,\dots,s_n}(t_i) = s_i$$

für alle i. Dann ist $\mathrm{im}(\mathrm{ev}_{s_1,\dots,s_n})$ der von R und $s_1,\dots,s_n$ erzeugte Unterring von S.

Definition 2.19. *In der obigen Situation ist $\mathrm{ev}_{s_1,\dots,s_n}$ der* Einsetzhomomorphismus *und $R[s_1,\dots,s_n] \coloneqq \mathrm{im}(\mathrm{ev}_{s_1,\dots,s_n})$ der von R und den s_i erzeugte Unterring von S.*

2.3 Ideale und Quotientenringe

Es sei R ein Ring.

Definition 2.20. *Eine Teilmenge $I \subseteq R$ ist ein* Linksideal*, wenn I eine additive Untergruppe ist, und $RI \subseteq I$ gilt, d.h. für alle $r \in R$, $x \in I$ gilt $rx \in I$. Gilt $IR \subseteq I$, so ist I ein* Rechtsideal*. Ist I ein Links- und Rechtsideal, so ist I ein* (beidseitiges) Ideal*. Dies wird dann mit $I \trianglelefteq R$ notiert.*

Beispiel 2.21. 1. Die Ideale in $\mathbb{Z}$ sind genau $n\mathbb{Z}$ mit $n \in \mathbb{Z}$.

2. Für jeden Ring R sind $\{0\}$ und R Ideale in R.

3. Ein kommutativer Ring K ist genau dann ein Körper, wenn $\{0\}$ und K die einzigen beiden Ideale in K sind.

4. Für jeden Ringhomomorphismus $f\colon R \to S$ ist $\ker(f)$ ein Ideal in R.

Ein *Ideal* in R ist das analog zu einem Normalteiler einer Gruppe:

Gruppe G	$\rightsquigarrow$	Ring R
Untergruppe $H \leq G$	$\rightsquigarrow$	Unterring $S \subseteq R$
Normalteiler $N \trianglelefteq G$	$\rightsquigarrow$	Ideal $I \trianglelefteq G$

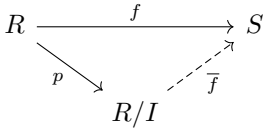
Man beachte jedoch, dass $I \trianglelefteq R$ für $I \neq R$ kein Unterring ist, da dann $1 \notin I$ gilt.

So wie sich Quotientegruppen G/N konstruieren lassen, gibt es nun auch Quotientenringe R/I: Es sei $I \trianglelefteq R$ ein Ideal. Dann wird auf der Quotientengruppe R/I durch

$$\overline{x} \cdot \overline{y} = \overline{xy} \quad \text{für alle } x, y \in R$$

eine Ringstruktur definiert. Dies ist die eindeutige Ringstruktur auf R/I, welche die kanonische Projektion $p\colon R \to R/I$, $r \mapsto \overline{r}$ zu einem Ringhomomorphismus macht, und es gilt $\ker(p) = I$.

Satz 2.22 (Homomorphiesatz für Ringe)**.** *Ist $f\colon R \to S$ ein Ringhomomorphismus mit $I \subseteq \ker f$, so induziert f einen eindeutigen Ringhomomorphismus $\overline{f}\colon R/I \to S$ mit $f = \overline{f} \circ p$, d.h. so dass das folgende Diagramm kommutiert:*



In anderen Worten: Es ergibt sich eine Bijektion

$$\{\text{Ringhomo. } \overline{f}\colon R/I \to S\} \xrightarrow{\sim} \{\text{Ringomo. } f\colon R \to S \text{ mit } I \subseteq \ker(f)\}\,,$$
$$\overline{f} \mapsto \overline{f} \circ p\,.$$

Korollar 2.23 (1. Isomorphiesatz)**.** *Jeder Ringhomomorphismus $f\colon R \to S$ induziert einen Ringisomorphismus*

$$\overline{f}\colon R/\ker(f) \to \operatorname{im}(f)\,, \quad \overline{r} \mapsto f(r)\,.$$

Korollar 2.24 (2. Isomorphiesatz)**.** *Sind $I, J \trianglelefteq R$ Ideale mit $J \subseteq I$, so ist I/J ein Ideal in R/J und es gibt einen wohldefinierten Ringisomorphismus*

$$(R/J)/(I/J) \xrightarrow{\sim} R/I\,, \quad \overline{\overline{r}} \mapsto \overline{r}\,.$$

Korollar 2.25 (3. Isomorphiesatz)**.** *Es sei $S \subseteq R$ ein Unterring und $I \trianglelefteq R$ ein Ideal. Dann ist $S + I$ ein Unterring von R, I ein Ideal in $S + I$, $S \cap I$ ein Ideal in S, und es gibt einen wohldefinierten Ringisomorphismus*

$$R/(R \cap I) \xrightarrow{\sim} (R + I)/I\,, \quad \overline{r} \mapsto \overline{r}\,.$$

Lemma 2.26. *Es sei $I \trianglelefteq R$ ein Ideal und $p\colon R \to R/I$ die kanonische Projektion.*

1. Es gibt es eine 1:1-Korrespondenz

$$\{\text{Unterringe } S \subseteq R \text{ mit } I \subseteq S\} \overset{1:1}{\longleftrightarrow} \{\text{Unterringe } S' \subseteq R/I\}\,,$$
$$S \longmapsto p(S) = S/I\,,$$
$$p^{-1}(S') \longmapsfrom S'\,.$$

2. Es gibt es eine 1:1-Korrespondenz

$$\begin{aligned}\{\textit{Ideale } J \trianglelefteq R \textit{ mit } I \subseteq J\} &\overset{1:1}{\longleftrightarrow} \{\textit{Ideale } J' \trianglelefteq R/I\}\,,\\ J &\longmapsto p(J) = J/I\,,\\ p^{-1}(J') &\longmapsto J'\,.\end{aligned}$$

3. Für jedes Ideal $J \trianglelefteq R$ mit $I \subseteq J$ gilt dabei für das zugehörige Ideal $J' = p(J) = J/I$ nach dem 2. Isomorphiesatz, dass

$$(R/I)/J' \cong (R/I)/(J/I) \cong R/J\,.$$

Auf beiden Seiten der obigen 1:1-Korrespondenz erhält man also (bis auf Isomorphie) die gleichen Quotientenringe.

Es sei $X \subseteq R$ eine Teilmenge. Für jedes Ideal $I \subseteq R$ sind dann die folgenden Bedingungen äquivalent:

1. Es ist I das kleinste Ideal, das X enthält, d.h. es gilt $X \subseteq I$, und für jedes Ideal $J \trianglelefteq R$ mit $X \subseteq J$ gilt $I \subseteq J$.
2. Es gilt $I = \bigcap_{J \trianglelefteq R, X \subseteq J} J$.
3. Es gilt $I = \{r_1 x_1 r_1' + \cdots + r_n x_n r_n' \mid n \in \mathbb{N}, r_i, r_i' \in R, x_i \in X\}$

Definition 2.27. *Das Ideal $I \trianglelefteq R$, dass eine (und damit alle) der obigen Bedingungen erfüllt, ist das* von X erzeugte *Ideal, und wird mit (X) notiert. Es ist dann X ist ein* Erzeugendensystem *von I.*

Definition 2.28. *Gibt es für $I \trianglelefteq R$ ein $x \in R$ mit $I = (x)$, so ist I ein* Hauptideal.

2.4 Prim- und maximale Ideale

Es sei R ein kommutativer Ring.

Definition 2.29. *1. Ein Ideal $P \trianglelefteq R$ ist ein* Primideal*, bzw.* prim*, wenn $P \neq R$ gilt, und für alle $x, y \in P$ mit $xy \in P$ bereits $x \in P$ oder $y \in P$ gilt.*

2. Ein Ideal $M \trianglelefteq R$ ist ein maximales Ideal*, wenn $M \neq R$ gilt, und für jedes Ideal $I \trianglelefteq R$ mit $M \subsetneq I$ bereits $I = R$ gilt; es gibt also bzgl. $\subseteq$ kein größeres echtes Ideal.*

Lemma 2.30. *1. $P \trianglelefteq R$ ist genau dann prim, wenn R/P ein Integritätsbereich ist.*

2. $M \trianglelefteq R$ ist genau dann maximal, wenn R/M ein Körper ist.

Korollar 2.31. *Maximale Ideale sind prim.*

Korollar 2.32. *Ist $I \trianglelefteq R$ ein Ideal und $p\colon R \to R/I$ die kanonische Projektion, so schränkt sich die 1:1-Korrespondenz*

$$\begin{aligned} \{\text{Ideale } J \trianglelefteq R \text{ mit } I \subseteq J\} &\overset{1:1}{\longleftrightarrow} \{\text{Ideale } J' \trianglelefteq R/I\}\,, \\ J &\longmapsto p(J) = J/I\,, \\ p^{-1}(J') &\longmapsfrom J' \end{aligned}$$

aus Lemma 2.26 zu 1:1-Korrespondenzen

$$\{\text{Primideale } P \trianglelefteq R \text{ mit } I \subseteq P\} \overset{1:1}{\longleftrightarrow} \{\text{Primideale } P' \trianglelefteq R/I\}$$

und

$$\{\text{maximale Ideale } M \trianglelefteq R \text{ mit } I \subseteq M\} \overset{1:1}{\longleftrightarrow} \{\text{maximale Ideale } M' \trianglelefteq R/I\}$$

ein.

Lemma 2.33 (Existenz maximaler Ideale)**.** *Für jedes echte Ideal $I \trianglelefteq R$, $I \neq R$ gibt es ein maximales Ideal $M \trianglelefteq R$ mit $I \subseteq M$.*

Korollar 2.34. *Ist $R \neq 0$, so gibt es ein maximales Ideal $M \trianglelefteq R$.*

2.5 Lokalisierung

2.5.1 Für allgemeinen kommutative Ringe

Es sei R ein kommutativer Ring.

Definition 2.35. *Eine Teilmenge $S \subseteq R$ ist* multiplikativ (abgeschlossen)*, wenn $1 \in S$ gilt, und für alle $s, t \in S$ auch $st \in S$ gilt.*

Ist $S \subseteq R$ eine multiplikative Teilmenge, so wird auf $R \times S$ durch

$$(r, s) \sim (r', s') \iff \exists t \in S : rs't = r'st \tag{1}$$

eine Äquivalenzrelation definiert. Für alle $r \in R$, $s \in S$ ist

$$\frac{r}{s} \coloneqq [(r, s)]_\sim ,$$

und es ist

$$S^{-1}R \coloneqq (R \times S)/\sim = \left\{ \frac{r}{s} \,\middle|\, r \in R, s \in S \right\}.$$

Auf $S^{-1}R$ wird durch

$$\frac{r}{s} + \frac{r'}{s'} \coloneqq \frac{rs' + r's}{ss'} \qquad \text{und} \qquad \frac{r}{s} \cdot \frac{r'}{s'} \coloneqq \frac{rr'}{ss'}$$

die Struktur eines kommutativen Rings definiert. Das Nullelement ist durch $0/1$ gegeben, und das Einselement durch $1/1$.

Definition 2.36. *Der Ring $S^{-1}R$ ist die* Lokalisierung *von R an S.*

Für alle $r/s \in S^{-1}R$ und $t \in S$ gilt dabei

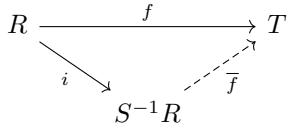
$$\frac{rt}{st} = \frac{r}{s}.$$

Für jedes $s \in S$ ist deshalb $s/1$ eine Einheit mit

$$\left(\frac{s}{1}\right)^{-1} = \frac{1}{s}.$$

Dies spiegelt sich in der universellen Eigenschaft des kanonischen Ringhomomorphismus $i \colon R \to S^{-1}R$, $r \mapsto r/1$ wieder:

Satz 2.37 (Universelle Eigenschaft der Lokalisierung)**.** *Ist $f \colon R \to T$ ein Ringhomomorphismus, so dass $f(s)$ für jedes $s \in S$ eine Einheit ist, so induziert f einen eindeutigen Ringhomomorphismus $\overline{f} \colon S^{-1}R \to T$ mit $f = \overline{f} \circ i$, d.h. so dass das folgende Diagramm kommutiert:*



In anderen Worten: Es ergibt sich eine Bijektion

$$\{\textit{Ringhomo. } \overline{f}\colon S^{-1}R \to T\} \xrightarrow{\sim} \{\textit{Ringhomo. } f\colon R \to T \textit{ mit } f(S) \subseteq T^\times\}\,,$$
$$\overline{f} \mapsto \overline{f} \circ i\,.$$

Warnung 2.38. Der kanonische Ringhomomorphismus $i\colon R \to S^{-1}R$ ist im Allgemeinen nicht injektiv. Es ist i genau dann injektiv, wenn S keinen Nullteiler enthält.

2.5.2 Für Integritätsbereiche

Es sei R ein Integritätsbereich.

Gilt $0 \in S$, so ist $S^{-1}R = 0$ der Nullring. Gilt hingegen $0 \notin S$, so enthält S keinen Nullteiler, weshalb der kanonische Ringhomomorphismus $i\colon R \to S^{-1}R$ dann injektiv ist. Außerdem lässt sich die rechte Seite von (1) dann zu $rs' = r's$ vereinfachen.

Da S ein Integritätsbereich ist, lässt sich $S = R \setminus \{0\}$ wählen. Die Lokalisierung $S^{-1}R$ ist dann bereits ein Körper, denn für jedes $r/s \in S^{-1}R$ mit $r/s \neq 0$ gilt $r \neq 0$, weshalb $s/r \in S^{-1}R$ ein wohldefinierter Bruch ist, für den

$$\frac{r}{s} \cdot \frac{s}{r} = \frac{rs}{rs} = \frac{1}{1} = 1_{S^{-1}R}$$

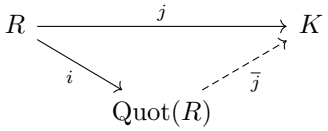
gilt.

Definition 2.39. *Ist R ein Integritätsbereich, so ist* $\mathrm{Quot}(R) \coloneqq S^{-1}R$ *für* $S = R \setminus \{0\}$ *der* Quotientenkörper *von R.*

Der kanonische Ringhomomorphismus $i\colon R \to \mathrm{Quot}(R)$ injektiv, weshalb sich R als ein Unterring des Körpers $\mathrm{Quot}(R)$ auffassen lässt.

Korollar 2.40. *Integritätsbereiche sind genau die Unterring von Körpern, d.h. ein Ring R ist genau dann ein Integritätsbereich, wenn es einen Körper K gibt, so dass $R \subseteq K$ ein Unterring ist.*

Es ist $\mathrm{Quot}(R)$ der „kleinste“ Körper, der R enthält: Ist K ein Körper und $j\colon R \to K$ ein injektiver Ringhomomorphismus, so faktorisiert j eindeutig über i, d.h. es gibt einen eindeutigen Körperhomomorphismus $\overline{j}\colon \mathrm{Quot}(R) \to K$, der das folgende Diagramm zum Kommutieren bringt:



Beispiel 2.41. 1. Es gilt $\mathrm{Quot}(\mathbb{Z}) = \mathbb{Q}$.

2. Ist K ein Körper, so ist der kanonische Ringhomomorphismus $i\colon K \to \mathrm{Quot}(K)$ ein Isomorphismus.

3. Ist K ein Körper, so ist $\mathrm{Quot}(K[t_1, \ldots, t_n]) =: K(t_1, \ldots, t_n)$ der *Funktionenkörper* oder *Körper der rationalen Funktionen* in den Variablen $t_1, \ldots, t_n$.

2.6 Hauptideal- und euklidische Ringe

Definition 2.42. *Ein* Hauptidealring *ist ein Integritätsbereich R, so dass jedes Ideal $I \trianglelefteq R$ ein Hauptideal ist.*

Definition 2.43. *Ein* euklidischer Ring *ist ein Integritätsbereich R zusammen mit einer* Gradabbildung $\delta\colon R \setminus \{0\} \to \mathbb{N}$*, so dass es für alle $f, g \in R$ mit $g \neq 0$ Elemente $q, r \in R$ gibt, so dass*

$$f = qg + r\,, \qquad \text{wobei } r = 0 \text{ oder } \delta(r) < \delta(g)\,.$$

Lemma 2.44. *Jeder euklidische Ring R ist ein Hauptidealring: Ist $I \trianglelefteq R$ mit $I \neq \{0\}$ und hat $x \in I$ minimalen Grad unter allen Elementen in $I \setminus \{0\}$, so gilt $I = (x)$.*

Beispiel 2.45. 1. Der Ring $\mathbb{Z}$ ist ein euklidischer Ring bezüglich der Gradabbildung $\delta(n) \coloneqq |x|$. Die Folgerung, dass $\mathbb{Z}$ ein Hauptidealring ist, sowie die obige explizite Beschreibung eines Erzeugers eines Ideal $I \trianglelefteq R$, entspricht genau Lemma 1.29.

2. Ist K ein Körper, so ist der Polynomring $K[t]$ ein euklidischer Ring bezüglich der üblichen Gradabbildung $\delta \coloneqq \deg$. Insbesondere ist $K[t]$ ein Hauptidealring.

Bemerkung 2.46. Ist R ein Integritätsbereich Ring, so ist für jedes $a \in R$ ist das Ideal $(t, a) \trianglelefteq R[t]$ genau dann ein Hauptideal, wenn a eine Einheit in R ist. Deshalb ist $R[t]$ genau dann ein Hauptidealring, wenn R ein Körper ist.

So sind etwa $\mathbb{Z}[t]$ und $K[t, u] \cong K[t][u]$ für einen Körper K keine Hauptidealringe, denn $(t, 2) \trianglelefteq \mathbb{Z}[t]$ und $(t, u) \trianglelefteq K[t][u]$ sind keine Hauptideale.

Beispiel 2.47. Es ist $\mathbb{Z}[\sqrt{-1}] \coloneqq \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ ein Unterring von $\mathbb{C}$, der Ring der *Gaußschen Zahlen*. Für jedes $z = a + ib \in \mathbb{Z}[i]$ ist $N(z) \coloneqq |z|^2 = a^2 + b^2 \in \mathbb{N}$ die *Norm* von z. Dann ist $\mathbb{Z}[i]$ zusammen mit der Norm N ein euklidischer Ring:

Für jedes $z \in \mathbb{C}$ gibt es ein Element $w \in \mathbb{Z}[i]$ mit $|z - w| \leq \sqrt{2}/2 = 1/\sqrt{2}$. Sind nun $f, g \in \mathbb{Z}[i]$ mit $g \neq 0$, so lässt sich in $\mathbb{C}$ der Quotient f/g bilden. Dann gibt es ein $q \in \mathbb{Z}[i]$ mit $|f/g - q| < 1/\sqrt{2}$. Für den Rest $r \coloneqq f - qg$ gilt dann $f = qg + r$, sowie

$$N(r) = |r|^2 = |f - qg|^2 = |f/g - q|^2|g|^2 \leq \frac{1}{2}|g|^2 < |g|^2 = N(g)\,.$$

2.7 Faktorielle Ringe

Es sei R ein kommutativer Ring.

Definition 2.48. *Zwei Elemente $a, b \in R$ sind* assoziiert (zueinander)*, wenn sie „gleich bis auf Einheit“ sind, d.h. wenn es eine Einheit $\varepsilon \in R^\times$ mit $b = \varepsilon a$ gibt.*

Lemma 2.49. *Assoziiertheit ist eine Äuquivalenzrelation auf R.*

Bemerkung 2.50. Ist R ein Integritätsbereich, so sind zwei Elemente $a, b \in R$ genau dann assoziiert, wenn $(a) = (b)$ gilt, wenn also $a \mid b$ und $b \mid a$ gelten. Wenn wir im Folgenden von „Eindeutigkeit bis auf Assoziiertheit“ von Elementen sprechen, so geht es also eigentlich um eindeutige Hauptideale.

2.7.1 Definition faktorieller Ringe

Es sei R ein Integritätsbereich.

Definition 2.51. *Es sei $p \in R$ eine Nichteinheit mit $p \neq 0$.*

1. *p ist* irreduzibel, *wenn für jede Zerlegung $p = xy$ bereits $x \in R^\times$ oder $y \in R^\times$ gilt.*
2. *p ist prim, wenn für alle $x, y \in R$ mit $p \mid (xy)$ bereits $p \mid x$ oder $p \mid y$ gilt, d.h. wenn das Ideal (p) prim ist.*

Definition 2.52. *Der Ring R ist* faktoriell, *wenn jedes $r \in R$, $r \neq 0$ eine Zerlegung*

$$r = \varepsilon p_1 \cdots p_n \tag{2}$$

besitzt, wobei

- *$\varepsilon \in R^\times$ eine Einheit ist,*
- *$p_1, \ldots, p_n$ irreduzibel sind, und*
- *diese Zerlegung eindeutig „bis auf Assoziiertheit und Permutation“ ist:*

  Falls $r = \varepsilon' p_1' \cdots p_m'$ eine weitere solche Zerlegung ist, so gilt $n = m$, und es gibt Einheiten $\delta_1, \ldots, \delta_n \in R^\times$ uond eine Permutation $\pi \in S_n$ mit $p_i' = \delta_i p_{\pi(i)}$ für alle $i = 1, \ldots, n$.

Lemma 2.53. *Ist R faktoriell, so ist $p \in R$ genau dann irreduzibel, wenn p prim ist.*

In faktoriellen Ringen muss also nicht zwischen Prim- und irreduziblen Elementen unterschieden werden. Deshalb bezeichnet man für $r \in R$, $r \neq 0$ die Zerlegung (2) als *Primfaktorzerlegung.*

Bemerkung 2.54. Ist R faktoriell und $\mathcal{P} \subseteq R$ ein Repräsentantensystem der Assoziiertheitsklassen der Primelemente, so lässt sich jedes Element $r \in R$, $r \neq 0$ als

$$r = \varepsilon \prod_{p \in \mathcal{P}} p^{\nu_p}$$

schreiben, wobei $\varepsilon \in R^\times$ eine Einheit ist, und $\nu_p = 0$ für fast alle $p \in \mathcal{P}$ gilt. Diese Zerlegung ist dann eindeutig (bis auf Permutation der p^{ν_p}).

Proposition 2.55. *Hauptidealringe sind faktoriell.*

Beispiel 2.56. 1. Der Ring der ganzen Zahlen $\mathbb{Z}$ ist faktoriell. Für $\mathcal{P}$ lässt sich die Menge der üblichen Primzahlen wählen.

2. Ist K ein Körper, so ist der Polynomring $K[t]$ faktoriell. Für $\mathcal{P}$ lässt sich die Menge der normierten irreduziblen Polynome wählen.

3. Der Ring der gaußschen Zahlen $\mathbb{Z}[i]$ ist faktoriell.

Beispiel 2.57. Es ist $\mathbb{Z}[\sqrt{-5}] \coloneqq \mathbb{Z}[i\sqrt{5}] = \{a + ib\sqrt{5} \mid a, b \in \mathbb{Z}\}$ ein Unterring von $\mathbb{C}$, der *nicht* faktoriell ist: Es sei $R \coloneqq \mathbb{Z}[\sqrt{-5}]$ und für jedes $z = a + ib\sqrt{5} \in R$ sei $N(z) \coloneqq |z|^2 = a^2 + 5b^2$ die *Norm* von z. Dann gilt

- $N(z) \in \mathbb{N}$ für alle $z \in R$, und
- $N(zw) = N(z)N(w)$ für alle $z, w \in R$.

Mithilfe der Norm N lassen sich die Einheiten von R bestimmen: Aus $zw = 1$ in R folgt $N(z)N(w) = 1$ in $\mathbb{N}$, also $N(z) = N(w) = 1$ in $\mathbb{N}$ und somit $z, w = \pm 1$. Somit gilt $R^\times = \{1, -1\} = \{z \in R \mid N(z) = 1\}$.

Hieraus ergibt sich, dass die Elemente $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ irreduzibel in R sind: Gilt etwa $2 = zw$ für $z, w \in R$, so gilt $4 = N(2) = N(z)N(w)$. Es gilt somit

$$N(z) = 1, N(w) = 4\,, \quad \text{oder} \quad N(z) = 2, N(w) = 2\,, \quad \text{oder} \quad N(z) = 4, N(w) = 1\,.$$

Da es aber kein $z' \in R$ mit $N(z') = 2$ gibt, muss $N(z) = 1$ oder $N(w) = 1$ gelten. Somit ist z oder w eine Einheit. Die Irreduziblität von $3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ ergibt sich analog.

Nun gilt aber $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Dabei sind die irreduziblen Elemente $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ paarweise nicht assoziiert zueinander (denn $z \in R$ ist nur zu $\pm z$ assoziiert). Somit besitzt $6 \in R$ zwei nicht-äquivalente Zerlegungen in irreduzible Elemente.

2.7.2 Prim- und irreduzible Elemente im Allgemeinen

Es sei R ein Integritätsbereich, und $p \in R$.

Lemma 2.58. *Ist p prim, so ist p auch irreduzibel.*

Lemma 2.59. *Ist R ein Hauptidealring, so sind die folgenden Bedingungen äquivalent:*

1. *Das Ideal (p) ist maximal.*
2. *Das Ideal (p) ist prim.*
3. *Das Element p ist prim.*
4. *Das Element p ist irreduzibel.*

Inbesondere ist jedes Primideal in R schon maximal.

2.7.3 ggT und kgV

Es sei R ein kommutativer Ring

Definition 2.60. *Es seien $a_i \in R$, $i \in I$.*

1. *Ein* größter gemeinsamer Teiler *der a_i ist ein Element $a \in R$ mit $a \mid a_i$ für alle $i \in I$, so dass für jedes andere $b \in R$ mit $b \mid a_i$ für alle $i \in I$ bereits $b \mid a$ gilt. Man schreibt $a = \mathrm{ggT}(a_i \mid i \in I)$.*

2. *Ein* kleinstes gemeinsames Vielfaches *der a_i ist ein Element $a \in R$ mit $a_i \mid a$ für alle $i \in I$, so dass für jedes andere $b \in R$ mit $a_i \mid b$ für alle $i \in I$ bereits $a \mid b$ gilt. Man schreibt $a = \mathrm{kgV}(a_i \mid i \in I)$.*

Lemma 2.61. *Ist R ein Integritätsbereich, so sind größte gemeinsame Teiler und kleinste gemeinsame Vielfache (sofern sie existieren) eindeutig bis auf Assoziiertheit.*

Lemma 2.62 (Berechnung von ggT und kgV in faktoriellen Ringen)**.** *Es sei R ein faktorieller Ring und $\mathcal{P} \subseteq R$ ein Repräsentantensystem der Assoziiertheitsklassen der Primelement von R. Es seien $a_1, \ldots, a_n \in R$, $a_i \neq 0$ mit Primfaktorzerlegungen*

$$a_i = \varepsilon_i \prod_{p \in \mathcal{P}} p^{\nu_{p,i}} .$$

Dann existieren $\mathrm{ggT}(a_1, \ldots, a_n)$ und $\mathrm{kgV}(a_1, \ldots, a_n)$, und es gilt

$$\mathrm{ggT}(a_1, \ldots, a_n) = \prod_{p \in \mathcal{P}} p^{\min\{\nu_{p,1}, \ldots, \nu_{p,n}\}}$$

und

$$\mathrm{kgV}(a_1, \ldots, a_n) = \prod_{p \in \mathcal{P}} p^{\max\{\nu_{p,1}, \ldots, \nu_{p,n}\}} .$$

Definition 2.63. *Es sei R ein faktorieller Ring und es seien $a_1, \ldots, a_n \in R$. Die Elemente $a_1, \ldots, a_n$ sind* (insgesamt) teilerfremd*, wenn $\mathrm{ggT}(a_1, \ldots, a_n) = 1$ gilt. In anderen Worten: Jedes Element $a \in R$ mit $a \mid a_i$ für alle i ist bereits eine Einheit.*

Lemma 2.64 (Charakterisierung von ggT und kgV in Hauptidealringen)**.** *Ist R ein Hauptidealring, so gilt für alle $a_1, \ldots, a_n \in R$, dass*

$$(a_1) + \cdots + (a_n) = (a_1, \ldots, a_n) = (\mathrm{ggT}(a_1, \ldots, a_n))$$

sowie

$$(a_1) \cap \cdots \cap (a_n) = (\mathrm{kgV}(a_1, \ldots, a_n)) .$$

Inbesondere gibt es Koeffizienten $c_1, \ldots, c_n \in R$ mit

$$\mathrm{ggT}(a_1, \ldots, a_n) = c_1 a_1 + \cdots + c_n a_n .$$

Korollar 2.65. *Ist R ein Hauptidealring, so sind $a, b \in R$ genau dann teilerfremd, wenn $(a) + (b) = R$ gilt.*

Ist R ein euklidischer Ring mit Gradabbildung δ, so lässt sich der größte gemeinsame Teiler von $f, g \in R$, $g \neq 0$ mithilfe des *euklidischen Algorithmus* berechnen: Es gibt $q, r \in R$ mit $a = qb + r$, wobei $r = 0$ oder $\delta(r) < \delta(b)$ gilt. Es gilt dann

$$\mathrm{ggT}(a, b) = \mathrm{ggT}(qb + r, b) = \mathrm{ggT}(r, b) = \mathrm{ggT}(b, r) .$$

Iteriert man dieses Vorgehen, so ergibt sich aus $\delta(r) < \delta(b)$, dass nach endlich vielen Schritten der Fall $r = 0$ eintritt. Dann lässt sich nutzen, dass

$$\mathrm{ggT}(a, 0) = a$$

gilt. Es lassen sich dann auch Koeffizienten $c, d \in R$ mit $\mathrm{ggT}(a, b) = ca + db$ bestimmen.

Beispiel 2.66. Es gilt

$$\begin{aligned} &\mathrm{ggT}(84,30) = \mathrm{ggT}(2\cdot 30+24,30)\\ &= \mathrm{ggT}(30,24) = \mathrm{ggT}(24+6,24)\\ &= \mathrm{ggT}(24,6) = \mathrm{ggT}(4\cdot 6+0,6)\\ &= \mathrm{ggT}(6,0) = 6\,. \end{aligned}$$

Wir erhalten außerdem, dass

$$\mathrm{ggT}(84,30) = 6 = 30-24 = 30-(84-2\cdot 30) = 3\cdot 30-84\,.$$

2.7.4 Der Satz von Gauß

Es sei R ein faktorieller Ring.

Definition 2.67. *Ein Polynom $f=\sum_{i=0}^{n} a_i t^i \in R[t]$ ist* primitiv*, wenn die Koeffizienten $a_0,\dots,a_n$ insgesamt teilerfremd sind.*

Satz 2.68 (Satz von Gauß)**.** *Der Polynomring $R[t]$ ist ebenfalls faktoriell. Dabei ist ein Polynom $p\in R[t]$ genau dann irreduzibel, wenn eine der folgenden beiden Bedingungen erfüllt ist:*

- *Es gilt $p\in R$, und p ist irreduzibel in R.*
- *Das Polynom p ist primitiv und irreduzibel in* $\mathrm{Quot}(R)[t]$.

Ein primitives Polynom $p\in R[t]$ ist genau dann irreduzibel in $R[t]$, wenn p irreduzibel in $\mathrm{Quot}(R)[t]$ *ist.*

Korollar 2.69. *Der Polynomring $R[t_1,\dots,t_n]$ ist faktoriell.*

Beispiel 2.70. 1. Ist K ein Körper, so ist $K[t_1,\dots,t_n]$ faktoriell.

2. $\mathbb{Z}[t_1,\dots,t_n]$ ist faktoriell.

2.8 Irreduziblitätskriterien

Es sei R ein faktorieller Ring.

Lemma 2.71. *Es sei K ein Körper und $f\in K[t]$ nicht-konstant.*

1. *Gilt* $\deg(f)=1$*, so ist f irreduzibel.*
2. *Gilt* $\deg(f)=2$ *oder* $\deg(f)=3$ *so ist f genau dann irreduzibel, wenn f keine Nullstelle in K besitzt.*
3. *Gilt* $\deg(f)\geq 2$ *und besitzt f eine Nullstelle in K, so ist f reduzibel.*

Beispiel 2.72. Jedes Polynom $f\in\mathbb{R}[t]$ ungeraden Grades besitzt nach dem Zwischenwertsatz eine Nullstelle; für $\deg(f)\neq 1$ ist f somit reduzibel.

Proposition 2.73 (Eisenstein)**.** *Es sei* $f = \sum_{i=0}^{n} a_i t^i \in R[t]$ *primitiv, und es gebe* $p \in R$ *prim mit*

$$p \nmid a_n\,, \qquad p \mid a_i \text{ für alle } i < n\,, \qquad p^2 \nmid a_0\,.$$

Dann ist f *irreduzibel in* $R[t]$*, und somit auch in* $\mathrm{Quot}(R)[t]$*.*

Proposition 2.74 (Reduktionskriterium)**.** *Es sei* $f \in R[t]$ *primitiv und* $p \in R$ *prim, so dass der Leitkoeffizient von* f *nicht von* p *geteilt wird. Für jedes Polynom* $g = \sum_{j=0}^{m} b_j t^j \in R[t]$ *sei*

$$\overline{g} \coloneqq \sum_{j=0}^{m} \overline{b_j} t^j \in (R/(p))[t]$$

das Polynom, dass durch Reduzieren der Koeffizienten modulo p *entsteht. Ist* $\overline{f}$ *irreduzibel in* $(R/(p))[t]$*, so ist* f *irreduzibel in* $R[t]$*, und somit auch in* $\mathrm{Quot}(R)[t]$*.*

2.9 Chinesischer Restsatz

Es sei R ein Ring. Für Ideale $I_1, \ldots, I_n \trianglelefteq R$ induzieren die kanonischen Projektionen $p_j \colon R \to R/I_j$ einen Ringhomomorphismus

$$p \coloneqq (p_1, \ldots, p_n) \colon R \to (R/I_1) \times \cdots \times (R/I_n)\,, \quad r \mapsto (\overline{r}, \ldots, \overline{r})$$

mit $\ker(p) = \bigcap_{j=1}^{n} \ker(p_j) = \bigcap_{j=1}^{n} I_j$. Gilt dabei $I_j + I_k = R$ für alle $j \neq k$, so ist p auch surjektiv:

Satz 2.75 (Chinesischer Restsatz)**.** *Sind* $I_1, \ldots, I_n \trianglelefteq R$ *Ideale mit* $I_j + I_k = R$ *für alle* $j \neq k$*, so gibt es einen wohldefinierten Isomorphismus*

$$R/\bigcap_{j=1}^{n} I_j \xrightarrow{\sim} (R/I_1) \times \cdots \times (R/I_n)\,, \quad \overline{r} \mapsto (\overline{r}, \ldots, \overline{r})\,.$$

Korollar 2.76. *Es sei* R *ein Hauptidealring, und es seien* $a_1, \ldots, a_n \in R$ *paarweise teilerfremd. Dann gibt es einen wohldefinierten Ringisomorphismus*

$$R/(\mathrm{kgV}(a_1, \ldots, a_n)) \xrightarrow{\sim} R/(a_1) \times \cdots \times R/(a_n)\,, \quad \overline{r} \mapsto (\overline{r}, \ldots, \overline{r})\,.$$

Korollar 2.77. *Für jedes* $n \geq 1$ *mit Primfakorzerlegung* $n = p_1^{n_1} \cdots p_r^{n_r}$ *gilt*

$$\mathbb{Z}/n \cong \mathbb{Z}/p_1^{n_1} \times \cdots \times \mathbb{Z}/p_r^{n_r}\,.$$

Korollar 2.78. *Sind* $n_1, \ldots, n_k \in \mathbb{Z}$ *und* $b_1, \ldots, b_k \in \mathbb{Z}$*, und ist* $x_0 \in \mathbb{Z}$ *eine Lösung des Systems simultaner Kongruenzen*

$$\begin{cases} x \equiv b_1 \pmod{n_1}\,, \\ x \equiv b_2 \pmod{n_2}\,, \\ \quad \vdots \\ x \equiv b_k \pmod{n_k}\,, \end{cases}$$

so ist die Lösungsmenge dieses Systems von Kongruenzen durch

$$x_0 + \mathrm{kgV}(n_1, \ldots, n_k)\mathbb{Z}$$

gegeben. Sind $n_1, \ldots, n_k$ paarweise teilerfremd, so existert eine solche Lösung x_0.

Beispiel 2.79. Wir betrachten das folgende System simultaner Kongruenzen:

$$\begin{cases} x & \equiv & 6 & \pmod{11}, \\ x & \equiv & 7 & \pmod{13}, \end{cases}$$

Da 11 und 13 teilerfremd sind, besitzt gibt es eine Lösung x_0. Die Lösungsmenge ist dann $x_0 + 143\mathbb{Z}$. Die Lösungen der ersten Kongruenz sind

$$6, 17, 28, 39, 50, 61, 72, \ldots$$

Dabei gilt $11 \equiv -2 \pmod{13}$, weshalb die obigen Gleichungen modulo 13 zu

$$\overline{6}, \overline{4}, \overline{2}, \overline{0}, \overline{-2} = \overline{11}, \overline{9}, \overline{7}, \ldots$$

werden. Es lässt sich somit $x_0 = 72$ wählen.

Beispiel 2.80. Wir betrachten das folgende System simultaner Kongruenzen:

$$\begin{cases} x & \equiv & 7 & \pmod{6}, \\ x & \equiv & 5 & \pmod{15}, \end{cases}$$

Mithilfe des chinesischen Restklassensatzen können wir die einzelnen Kongruenzen auftrennen:

$$\begin{cases} x & \equiv & 7 & \pmod{2}, \\ x & \equiv & 7 & \pmod{3}, \\ x & \equiv & 5 & \pmod{3}, \\ x & \equiv & 5 & \pmod{5}, \end{cases} \iff \begin{cases} x & \equiv & 1 & \pmod{2}, \\ x & \equiv & 1 & \pmod{3}, \\ x & \equiv & 2 & \pmod{3}, \\ x & \equiv & 0 & \pmod{5}. \end{cases}$$

Die mittleren beiden Kongruenzen stehen im Widerspruch, weshalb es keine Lösungen gibt.

Beispiel 2.81. Wir betrachten das abgeänderte System

$$\begin{cases} x & \equiv & 8 & \pmod{6}, \\ x & \equiv & 5 & \pmod{15}, \end{cases}$$

Durch Aufteilen der einzelnen Kongruenzen erhalten wir nun

$$\begin{cases} x & \equiv & 8 & \pmod{2}, \\ x & \equiv & 8 & \pmod{3}, \\ x & \equiv & 5 & \pmod{3}, \\ x & \equiv & 5 & \pmod{5}, \end{cases} \iff \begin{cases} x & \equiv & 0 & \pmod{2}, \\ x & \equiv & 2 & \pmod{3}, \\ x & \equiv & 0 & \pmod{5}. \end{cases}$$

Die äußeren beiden Kongruenzen lassen sich zu $x \equiv 2 \pmod{10}$ zusammenfassen, und wir erhalten das kleinere System

$$\begin{cases} x & \equiv & 2 & \pmod 3\,, \\ x & \equiv & 0 & \pmod{10}\,. \end{cases}$$

Die Lösungen der unteren Kongruenz sind

$$0, 10, 20, \ldots,$$

und modulo 3 wir dies zu

$$\overline{0}, \overline{1}, \overline{2}, \ldots\,.$$

Eine Lösung ist also durch $x_0 = 20$ gegeben. Die Lösungsmenge ist insgesamt

$$x_0 + \mathrm{kgV}(6, 15)\mathbb{Z} = 20 + 30\mathbb{Z}\,.$$

Bemerkung 2.82. Simultane Kongruenzen lassen sich aus mithilfe des euklidischen Algorithmus lösen. Ein entsprechende Erklärung, sowie das Ausrechnen der Beispiele von Übungsblatt 6, findet sich unter goo.gl/J2ML2r[1].

[1] https://github.com/cionx/einfuehrung-in-die-algebra-tutorial-ws-17-18/raw/master/sheet_06/sheet_06.pdf

3 Körpererweiterungen

Definition 3.1. *Es seien K, L zwei Körper. Ist K ein Unterring von L, so ist K ein* Unterkörper *von L. Dann ist L eine* Körpererweiterung *von K, notiert als L/K.*

Lemma 3.2. *Ist L ein Körper, so ist eine Teilmenge $K \subseteq L$ genau dann ein Unterkörper, wenn für alle $x, y, z \in K$, $z \neq 0$ auch*

$$1 \in K\,, \qquad x + y \in K\,, \qquad xy \in K\,, \qquad z^{-1} \in K\,.$$

Definition 3.3. *Ein Ringhomomorphismus $K \to L$ zwischen Körpern K, L ist ein* Körperhomomorphismus.

Lemma 3.4. *Jeder Körperhomomorphismus ist injektiv.*

Ist $\varphi\colon K \to L$ ein Körperhomomorphismus, so induziert φ einen Körperisomorphismus $\overline{\varphi}\colon K \to \mathrm{im}(\varphi)$. Indem man K mit dem Unterkörper $\mathrm{im}(\varphi)$ von L identifiziert, lässt sich K als ein Unterkörper von L auffassen.

Definition 3.5. *Ist K ein Körper und $S \subseteq K$ eine Teilmenge, so ist*

$$\langle S \rangle_{Körper} \coloneqq \bigcap_{\substack{Unterkörper \\ K' \subseteq K \\ S \subseteq K'}} K'$$

der von S erzeugte Unterkörper. *Für jeden Unterkörper $K' \subseteq K$ mit $S \subseteq K'$ gilt also $\langle S \rangle_{Körper} \subseteq K'$.*

Ist L/K eine Körpererweiterung und $S \subseteq L$ eine Teilmenge, so ist

$$K(S) \coloneqq \langle K \cup S \rangle_{Körper} = \bigcap_{\substack{Zwischenkörper \\ K \subseteq L' \subseteq L \\ S \subseteq L'}} L'$$

die von S erzeugt *Zwischenerweiterung. Für jeden Zwischenkörper $K \subseteq L' \subseteq L$ mit $S \subseteq L'$ gilt also $K(S) \subseteq L$.*

3.1 Der Primkörper

Es sei K ein Körper. Dann ist

$$P \coloneqq \bigcap_{\substack{\text{Unterkörper} \\ K' \subseteq K}} K' = \langle 1 \rangle_{\text{Körper}} = \langle \emptyset \rangle_{\text{Körper}}$$

ein Unterkörper von K. Es handelt sich um den kleinsten Unterkörper, der in K enthalten ist, d.h. für jeden anderen Unterkörper $K' \subseteq L$ gilt $P \subseteq K'$.

Definition 3.6. *Der Körper P wie oben ist der* Primkörper *von K.*

Zur näheren Bestimmung des Primkörpers betrachtet man den Ringhomomorphismus

$$\varphi\colon \mathbb{Z} \to K\,, \quad n \mapsto n \cdot 1_K\,.$$

Gilt $\operatorname{char}(K) = p > 0$, so gilt $\ker(\varphi) = (p)$, weshalb φ einen Körperhomomorphismus

$$\overline{\varphi}\colon \mathbb{F}_p \to K\,, \quad \overline{n} \mapsto n \cdot 1_K$$

induziert. Gilt $\operatorname{char}(K) = 0$, so induziert φ hingegen einen Körperhomomorphismus

$$\overline{\varphi}\colon \mathbb{Q} \to K\,, \quad \frac{n}{m} \mapsto \frac{n \cdot 1_K}{m \cdot 1_K}\,.$$

In beiden Fällen ist $\operatorname{im}(\overline{\varphi})$ der von 1_K erzeugte Unterkörper von K, also der Primkörper P. Es gilt also

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

Mithilfe des obigen Isomorphismus $\overline{\varphi}$ wird P im Folgenden mit $\mathbb{F}_p$, bzw. $\mathbb{Q}$ identifiziert. Ist dabei $K' \subseteq K$ ein Unterkörper, so haben K und K' den gleichen Primkörper.

Korollar 3.7. *Sind K und L zwei Körper mit $\operatorname{char}(K) \neq \operatorname{char}(L)$, so gibt es keinen Körperhomomorphismus $K \to L$.*

3.2 Der Grad einer Körpererweiterung

Es seien $M/L/K$ Körpererweiterungen.

Definition 3.8. *Der* Grad *einer Körpererweiterung L/K ist $[L : K] \coloneqq \dim_K(L)$.*

Lemma 3.9. *Es sei V ein L-Vektorraum mit L-Basis $(v_i)_{i\in I}$ und $(b_j)_{j\in J}$ eine K-Basis von L. Dann ist $(b_j v_i)_{i\in I, j\in J}$ eine K-Basis von V, also $\dim_K(V) = \dim_K(L)\dim_L(V)$.*

Beispiel 3.10. Für jeden komplexen Vektorraum V gilt $\dim_{\mathbb{R}}(V) = 2\dim_{\mathbb{C}}(V)$.

Korollar 3.11 (Multiplikativität des Grades)**.** *Es gilt $[M : K] = [M : L][L : K]$.*

Definition 3.12. *Die Körpererweiterung L/K ist* endlich*, wenn $[L : K]$ endlich ist.*

3.3 Algebraizität

Es seien $M/L/K$ eine Körpererweiterung.

Lemma 3.13. *Für $a \in L$ sind die folgenden Bedingungen äquivalent:*

1. *Die Körpererweiterung $K(a)/K$ ist endlich.*
2. *Es gibt ein Polynom $p \in K[t]$ mit $p \neq 0$ und $p(a) = 0$.*
3. *Es gilt $K[a] = K(a)$.*

Definition 3.14. *Ein Element $a \in L$ ist* algebraisch (über K)*, wenn es eine (und damit alle) der obigen Bedingungen erfüllt; andernfalls ist a* transzendent (über K)*.*

Die Körpererweiterung L/K ist algebraisch*, wenn jedes $a \in L$ algebraisch über K ist; andernfalls ist L/K* transzendent*.*

Lemma 3.15. *Ist M/K algebraisch, so sind auch M/L und L/K algebraisch.*

Lemma 3.16. *Ist die Erweiterung L/K endlich, so ist L/K auch algebraisch.*

Korollar 3.17. *Sind $a, b \in L$ algebraisch, so sind auch $a+b$ und $a \cdot b$ algebraisch. Gilt $a \neq 0$, so ist auch $1/a$ algebraisch.*

Korollar 3.18. *Es ist $(L/K)^{\mathrm{alg}} := \{x \in L \mid x \text{ ist algebraisch über } K\}$ ein Zwischenkörper der Erweiterung L/K.*

Korollar 3.19. *Für die Erweiterung L/K sind die folgenden Bedingungen äquivalent:*

1. *L/K ist endlich.*
2. *L/K wird von endlich vielen algebraischen Elementen $a_1, \ldots, a_n \in L$ erzeugt.*

Korollar 3.20 (Transitivität von Algebraizität)**.** *Sind die Erweiterungen M/L und L/K beide algebraisch, so ist auch M/K algebraisch.*

Korollar 3.21. *Die folgenden beiden Bedingungen sind äquivalent:*

1. *Die Erweiterung L/K ist algebraisch.*
2. *Die Erweiterung L/K wird von algebraischen Elementen erzeugt, d.h. es gibt algebraische Elemente $a_i \in L$, $i \in I$ mit $L = K(a_i \mid i \in I)$.*

3.4 Einfache Körpererweiterungen

Es sei L/K eine Körpererweiterung.

Definition 3.22. *L/K ist* einfach*, wenn es ein $a \in L$ mit $L = K(a)$ gibt.*

Es sei zunächst $a \in L$ algebraisch über K. Dann gilt $K(a) = K[a]$, weshalb $K(a)$ das Bild des Ringhomomorphismus

$$\varphi\colon K[t] \to L\,, \quad p \mapsto p(a)$$

ist. Dann ist $\ker(\varphi)$ ein Ideal in $K[t]$, weshalb es ein eindeutiges normiertes Polynom $m_a \in K[t]$ mit $\ker(\varphi) = (m_a)$ gibt.

Definition 3.23. *Ist $a \in L$ algebraisch über K, so ist $m_a \in K[t]$ wie oben das* Minimalpolynom von a (über K).

Der Ringhomomorphismus φ induziert einen Ringisomorphismus

$$K[t]/(m_a) \xrightarrow{\sim} K(a)\,, \quad \overline{p} \mapsto p(a)\,.$$

Insbesondere gilt $K[t]/(m_a) \cong K(a)$, weshalb $K[t]/(m_a)$ ein Körper ist. Das Ideal (m_a) ist also maximal, und das Polynom m_a somit irreduzibel. Ist $p \in K[t]$ ein weiteres irreduzibles normiertes Polynom mit $p(a) = 0$, so gilt $m_a \mid p$ und somit bereits $p = m_a$.

Korollar 3.24. *Ist $a \in L$ algebraisch über K, so ist $m_a \in K[t]$ das eindeutige normierte irreduzible Polynom, das a als Nullstelle hat.*

Beispiel 3.25. 1. Für die Erweiterung $\mathbb{C}/\mathbb{R}$ ist $f \coloneqq t^2+1 \in \mathbb{R}[t]$ das Minimalpolynom von $i \in \mathbb{C}$: Das Polynom f ist normiert mit $f(i) = 0$. Es ist irreduzibel in $\mathbb{R}[t]$, da es quadratisch ist, und keine Nullstelle in $\mathbb{R}$ besitzt.

2. Für die Erweiterung $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ ist $f \coloneqq t^2 - 2 \in \mathbb{Q}[t]$ das Minimalpolynom von $\sqrt{2} \in \mathbb{Q}(\sqrt{2})$: Das Polynom f ist normiert mit $f(\sqrt{2}) = 0$, und irreduzibel nach dem Eisenstein-Kriterium.

Der Körperisomorphismus $\overline{\varphi}$ ist auch K-linear, und somit ein Isomorphismus von K-Vektorräumen. Dabei ist für $\deg(m_a) = d$ eine K-Basis von $K[t]/(m_a)$ durch $\overline{1}, \overline{t}, \ldots, \overline{t^{d-1}}$ gegeben.

Korollar 3.26. *Ist $a \in L$ algebraisch über K, so gilt $[K(a) : K] = \deg(m_a)$.*

Ist hingegen $a \in L$ transzendent über K, so ist der Ringhomomorphismus φ injektiv, und induziert deshalb einen Körperhomomorphismus

$$\overline{\varphi}\colon K(t) \to L\,, \quad \frac{p}{q} \mapsto \frac{p(a)}{q(a)}\,,$$

dessen Bild gerade $K(a)$ ist. Also gilt dann $K(a) \cong K(t)$.

3.5 Das Kompositum

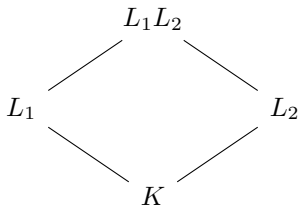
Es sei L/K eine Körpererweiterung, und es seien L_1, L_2 zwei Zwischenkörper dieser Erweiterung, d.h. es seien $L_1, L_2 \subseteq L$ Unterkörper mit $K \subseteq L_1, L_2$.

Definition 3.27. *Das* Kompositum *der Zwischenkörper L_1, L_2 ist der Zwischenkörper*

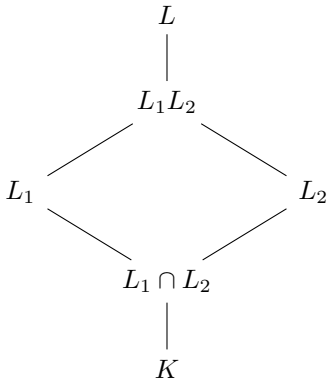
$$L_1L_2 \coloneqq K(L_1 \cup L_2) = L_1(L_2) = L_2(L_1)\,,$$

also der kleinste Zwischenkörper der Erweiterung L/K, der L_1 und L_2 enthält.

Dies lässt sich wie folgt darstellen:



Dabei lässt sich auch noch die Zwischenerweiterung $L_1 \cap L_2$ einzeichnen:



Proposition 3.28. *Es seien L_1/K, L_2/K algebraisch.*

1. *Es gelten $[L_1 : K], [L_2 : K] \mid [L_1L_2 : K]$.*
2. *Ist $(a_i)_{i\in I}$ eine K-Basis von L_1 und $(b_j)_{j\in J}$ eine K-Basis von L_2, so ist $(a_ib_j)_{i\in I, j\in J}$ ein K-Erzeugendensystem von L_1L_2.*
3. *Es gilt $[L_1L_2 : K] \leq [L_1 : K][L_2 : K]$.*

Korollar 3.29. *Sind L_1/K, L_2/K endlich und $[L_1 : K]$, $[L_2 : K]$ teilerfremd, so gilt*

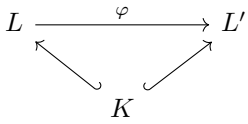
$$[L_1L_2 : K] = [L_1 : K][L_2 : K]\,.$$

3.6 K-Homomorphismen

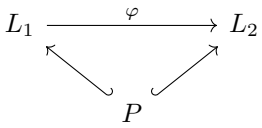
Es seien L/K und L'/K zwei Körpererweiterungen eines Körpers K.

Definition 3.30. *Ein K-linearer Körperhomomorphismus $\varphi\colon L \to L'$ ist ein* K-Homomorphismus. *Ist φ zudem ein Isomorphismus, bzw. Automorphismus, so ist φ ein* K-Isomorphismus, *bzw.* K-Automorphismus.

Bemerkung 3.31. Die K-Linearität von φ ist äquivalent dazu, dass $\varphi|_K = \mathrm{id}_K$ gilt, sowie äquivalent zur Kommutativität des folgenden Diagramms:



Beispiel 3.32. Fasst man zwei Körper L, L' gleicher Charakteristik als Körpererweiterungen L/P, L'/P des gemeinsamen Primkörpers P auf, so ist jeder Körperhomomorphismus $\varphi\colon L \to L'$ bereits P-linear, und somit ein P-Homomorphismus: Es gibt nämlich nur genau einen Körperhomomorphismus $P \to L'$, weshalb das Diagramm



notwendigerweise kommutiert.

Definition 3.33. *Es ist* $\mathrm{Aut}(L/K) \coloneqq \{K\text{-Automorphismen } L \to L\}$ *die* Automorphismengruppe *der Erweiterung L/K.*

Wie der Name vermuten lässt, bildet $\mathrm{Aut}(L/K)$ zusammen mit der Komposition von Abbildungen eine Gruppe.

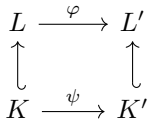
Lemma 3.34. *Ist L/K endlich, so ist jeder K-Homomorphismus $L \to L$ bereits ein K-Automorphismus.*

Bemerkung 3.35. Lemma 3.34 gilt allgemeiner für algebraische Erweiterungen L/K.

Lemma 3.36. *Es sei $a \in L$.*

1. *Ist $\varphi\colon L \to L'$ ein K-Homomorphismus, so gilt für jedes Polynom $f \in K[t]$, dass $f(\varphi(a)) = \varphi(f(a))$.*
2. *Es ist a genau dann eine Nullstelle von f, wenn $\varphi(a)$ eine Nullstelle von f ist.*
3. *Es ist a genau dann algebraisch über K, wenn $\varphi(a)$ algebraisch über K ist, und es gilt dann $m_a = m_{\varphi(a)}$.*

Bemerkung 3.37. Es seien allgemeiner L/K und L'/K' Körpererweiterungen und $\psi\colon K \to K'$, $\varphi\colon L \to L'$ Körperhomomorphismen mit $\varphi|_K = \psi$, d.h. so dass das folgende Diagramm kommutiert:



Dann ist $a \in L$ genau dann eine Nullstelle von $f \in K[t]$, wenn $\varphi(a)$ eine Nullstelle von $\psi_*(f) \in K'[t]$ ist, wobei ψ_* der von ψ induzierte Ringhomomorphismus

$$\psi_* \colon K[t] \to K'[t]\,, \quad \sum_{i=0}^{n} a_i t^i \mapsto \sum_{i=0}^{n} \psi(a_i) t^i$$

ist.

Satz 3.38. *Es sei $a \in L$ algebraisch. Für jede Nullstelle $a' \in L'$ des Minimalpolynoms $m_a \in K[t]$ gibt es dann einen eindeutigen K-Homomorphismus $\varphi \colon K(a) \to L'$ mit $\varphi(a) = a'$. In anderen Worten: Es ergibt sich eine Bijektion*

$$\begin{aligned} \{K\text{-Homomorphismen } K(a) \to L'\} &\xrightarrow{\sim} \{\text{Nullstellen von } m_a \text{ in } L'\}\,, \\ \varphi &\longmapsto \varphi(a)\,. \end{aligned}$$

Beispiel 3.39. Die Erweiterung $\mathbb{C}/\mathbb{R}$ ist endlich mit $\mathbb{C} = \mathbb{R}(i)$, wobei $t^2 + 1 \in \mathbb{R}[t]$ das Minimalpolynom von i ist. Es gilt somit

$$\begin{aligned} \mathrm{Aut}(\mathbb{C}/\mathbb{R}) &\overset{3.34}{=\!=} \{\mathbb{R}\text{-Homomorphismen } \mathbb{R}(i) \to \mathbb{C}\} \\ &\overset{3.38}{\longleftrightarrow} \{\text{Nullstellen von } t^2 + 1 \in \mathbb{C}\} \\ &=\!=\!= \{i, -i\}\,. \end{aligned}$$

3.7 Der Algebraische Abschluss

Es sei K ein Körper.

3.7.1 Hinzuadjungieren von Nullstellen

Ist $f \in K[t]$ irreduzibel, so ist $L \coloneqq K[t]/(f)$ ein Körper, und durch den Körperhomomorphismus $K \to L$, $x \mapsto \overline{x}$ ergibt sich eine Körpererweiterung L/K. Dabei gilt für das Element $a \coloneqq \overline{t} \in L$, dass $f(a) = 0$. Es lässt sich also eine Körperweiterung L/K konstruieren, in der f eine Nullstelle hat, und diese Körpererweiterung wird von dieser Nullstelle erzeugt. Man kann also Nullstellen von Polynomen zu K „hinzuadjungieren“.

3.7.2 Definition des algebraischen Abschluss

Lemma 3.40. *Für K sind die folgenden Bedingungen äquivalent:*

1. *Jedes nicht-konstante Polynom $p \in K[t]$ besitzt eine Nullstelle in K.*
2. *Jedes Polynom $p \in K[t]$ zerfällt in Linearfaktoren.*
3. *Die normierten irreduziblen Polynome in $K[t]$ sind genau die Linearfaktoren.*
4. *Für jede algebraische Körpererweiterung L/K gilt bereits $L = K$.*

Definition 3.41. *Erfüllt K eine (und damit alle) der obigen Bedingungen, so ist K* algebraisch abgeschlossen.

Beispiel 3.42. Der *Fundamentalsatz der Algebra* besagt, dass der Körper der komplexen Zahlen $\mathbb{C}$ algebraisch abgeschlossen ist.

Definition 3.43. *Ist L/K eine Körpererweiterung, so ist L ein* algebraischer Abschluss von K*, wenn*

- *die Erweiterung L/K algebraisch ist, und*
- *der Körper L algebraisch abgeschlossen ist.*

Beispiel 3.44. 1. Nach dem Fundamentalsatz der Algebra ist $\mathbb{C}$ ein algebraischer Abschluss von $\mathbb{R}$. (Die Algebraizität der Erweiterung $\mathbb{C}/\mathbb{R}$ folgt aus ihrer Endlichkeit.)

2. Es ist $\mathbb{C}$ kein algebraischer Abschluss von $\mathbb{Q}$, da $\mathbb{C}/\mathbb{Q}$ nicht algebraisch ist.

3.7.3 Existenz des Algebraischen Abschlusses

Zur Konstruktion eines algebraischen Abschlusses von K adjungiert man für alle nicht-konstanten Polynome $f \in K[t]$ „gleichzeitig“ eine Nullstelle hinzu, und iteriert diesen Prozess anschließend:

Es sei $\mathcal{F} \subseteq K[t]$ die Menge aller nicht-konstanten Polynome. Für den Polynomring $R \coloneqq K[X_f \mid f \in \mathcal{F}]$ sei $I \coloneqq (f(X_f) \mid f \in \mathcal{F})$. Dann ist I ein echtes Ideal in R, und somit in einem maximalen Ideal $M \trianglelefteq R$ enthalten. Dann ist $L_1 \coloneqq R/M$ ein Körper, und jedes $f \in \mathcal{F}$ has eine Nullstelle in L_1 (nämlich $\overline{X_f}$). Induktiv ergibt sich, ausgehend von $L_0 \coloneqq K$, eine aufsteigende Folge von Körpern

$$K = L_0 \subseteq L_1 \subseteq L_2 \subseteq L_3 \subseteq \cdots,$$

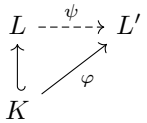
so dass L_{i+1}/L_i für alle i algebraisch ist, und alle nicht-konstanten Polynome aus $L_i[t]$ in L_{i+1} eine Nullstelle haben. Dann ist $L \coloneqq \bigcup_{i\geq 0} L_i$ eine Körper, so dass L/K algebraisch ist, und jedes nicht-konstante Polynom aus $L[t]$ eine Nullstelle in L hat. Also ist L ein algebraischer Abschluss von K.

Satz 3.45. *Jeder Körper K besitzt einen algebraischen Abschluss.*

3.7.4 Eindeutigkeit des Algebraischen Abschlusses

Lemma 3.46 (Forsetzungssätze für algebraische Abschlüsse)**.**

1. *Ist L/K eine algebraische Körpererweiterung und L' ein algebraisch abgeschlossener Körper, so setzt sich jeder Körperhomomorphismus $\varphi\colon K \to L'$, also jede Einbettung $K \hookrightarrow L'$ zu einem Körperhomomorphismus $\psi\colon L \to L'$, also zu einer Einbettung $L \hookrightarrow L'$ fort, d.h. es gilt $\psi|_K = \varphi$.*



2. *Sind K, K' zwei Körper mit zugehörigen algebraischen Abschlüssen L, L', so setzt sich jeder Körperisomorphismus $\varphi\colon K \to K'$ zu einem Körperisomorphismus $\psi\colon L \to L'$ fort, d.h. es gilt $\psi|_K = \varphi$.*

$$\begin{array}{ccc} L & \overset{\sim}{\underset{\psi}{\dashrightarrow}} & L' \\ \uparrow & & \uparrow \\ K & \xrightarrow[\varphi]{\sim} & K' \end{array}$$

Korollar 3.47. *Je zwei algebraische Abschlüsse $\overline{K}, \overline{K}'$ von K sind K-isomorph.*

Wegen dieser Eindeutigkeit bis auf K-Isomorphismus spricht man auch von *dem* algebraischen Abschluss von K, und notiert diesen mit $\overline{K}$.

3.8 Zerfällungskörper

Es sei L/K eine Körpererweiterung.

Definition 3.48. *Es ist L ein* Zerfällungskörper *einer Familie $(f_i)_{i\in I}$ von Polynomen $f_i \in K[t]$, wenn jedes f_i über L in Linearfaktoren zerfällt, und die Erweiterung L/K von den Nullstellen der f_i erzeugt wird.*

Ist L/K ein Zerfällungskörper, so wird die Erweiterung L/K von algebraischen Elementen (nämlich den Nullstellen der f_i) erzeugt, und ist somit algebraisch.

Lemma 3.49 (Existenz von Zerfällungskörpern)**.** *Für jede Familie $(f_i)_{i\in I}$ nichtkonstanter Polynome $f_i \in K[t]$ existiert ein Zerfällungskörper.*

Lemma 3.50. *Es sei $(f_i)_{i\in I}$ eine Familie von Polynomen $f_i \in K[t]$. Es sei $\varphi\colon K \to K'$ ein Körperisomorphismus und $\varphi_*\colon K[t] \to K'[t]$, $\sum_{i=0}^n a_i t^i \mapsto \sum_{i=0}^n \varphi(a_i)t^i$ der induzierte Ringisomorphismus. Ist L ein Zerfällungkörper der Familie $(f_i)_{i\in I}$ und L' ein Zerfällungskörper der entsprechenden Familie $(\varphi_*(f_i))_{i\in I}$, so setzt sich φ zu einem Körperisomorphismus $\psi\colon L \to L'$ fort, d.h. es gilt $\psi|_K = \varphi$.*

$$\begin{array}{ccc} L & \overset{\psi}{\dashrightarrow} & L' \\ \uparrow & & \uparrow \\ K & \xrightarrow{\varphi} & K' \end{array}$$

Korollar 3.51 (Eindeutigkeit von Zerfällungskörpern)**.** *Je zwei Zerfällungskörper L, L' einer Familie $(f_i)_{i\in I}$ von Polynomen $f_i \in K[t]$ sind K-isomorph.*

Ist L ein Zerfällungskörper einer Familie von Polynom $(f_i)_{i\in I}$, so wird die Erweiterung L/K von den Nullstellen der f_i erzeugt. Ist L'/K eine weitere Körpererweiterung und $\varphi\colon L \to L'$ ein K-Homomorphismus, so ist für jede Nullstelle $a \in L$ von f_i auch $\varphi(a) \in L'$ eine Nullstelle von f_i. Für die Menge $N = \{a_1, \ldots, a_n\}$ aller Nullstellen von

f_i in L ist deshalb das Bild $\varphi(N)$ die Menge aller Nullstellen von f_i in L'. Deshalb ist $\varphi(N)$ unabhängig von der Wahl von φ, d.h. für jeden weiteren K-Homomorphismus $\psi\colon L \to L'$ gilt $\varphi(N) = \psi(N)$. Da L von den Nullstellen der f_i erzeugt wird, ist somit das gesamte Bild $\varphi(L)$ unabhängig von der Wahl von φ.

Beispiel 3.52. Für jeden $\mathbb{R}$-Homomorphismus $\varphi\colon \mathbb{C} \to \mathbb{C}$ gilt $\varphi(\{i, -i\}) = \{i, -i\}$.

Proposition 3.53. *Ist L/K algebraisch, so sind die folgenden Bedingungen äquivalent:*

1. *Es ist L der Zerfällungskörper einer Familie $(f_i)_{i\in I}$ von Polynomen $f_i \in K[t]$.*
2. *Für jede Körpererweiterung L'/K haben alle K-Homomorphismen $L \to L'$ das gleiche Bild.*
3. *Für jede algebraische Körpererweiterung L'/K haben alle K-Homomorphismen $L \to L'$ das gleiche Bild.*
4. *Ist $\overline{K}$ ein algebraischer Abschluss von K, so haben alle K-Homomorphismen $L \to \overline{K}$ das gleiche Bild.*
5. *Ist $\overline{K}$ ein algebraischer Abschluss von K mit $L \subseteq \overline{K}$, so hat jeder K-Homomorphismus $L \to \overline{K}$ das Bild $\varphi(L) = L$.*
6. *Ist $\overline{K}$ ein algebraischer Abschluss von K mit $L \subseteq \overline{K}$, so schränkt sich jeder K-Homomorphismus $L \to \overline{K}$ zu einem K-Automorphismus $L \to L$ ein.*
7. *Jedes irreduzible Polynom $f \in K[t]$, das in L eine Nullstelle hat, zerfällt in L bereits in Linearfaktoren.*

Definition 3.54. *Erfüllt die Erweiterung L/K eine (und damit alle) der obigen Bedingungen, so ist die Erweiterung L/K* normal.

Beispiel 3.55. Jede Körpererweiterung L/K vom Grad $[L : K] = 2$ ist normal.

Lemma 3.56. *Sind $M/L/K$ Körpererweiterungen, so dass M/K normal ist, so ist auch M/L normal.*

Warnung 3.57. 1. Ist M/K normal, so ist L/K nicht notwendigerweise normal.

2. Sind M/L und L/K normal, so ist M/K nicht notwendigerweise normal.

3.9 Separablität

Es sei K ein Körper.

Definition 3.58. *Die* (formale) Ableitung *eines Polynoms* $f = \sum_{i=0}^{n} a_i t^i \in K[t]$ *ist das Polynom*

$$f' := \sum_{i=1}^{n} i a_i t^{i-1} = \sum_{i=0}^{n-1} (i+1) a_{i+1} t^i \,.$$

Lemma 3.59. *Für alle* $f, g \in K[t]$, $\lambda \in K$ *gelten die Gleichheiten.*

$$(f+g)' = f' + g' \,, \qquad (\lambda f)' = \lambda f' \,, \qquad (fg)' = fg' + f'g \,.$$

3.9.1 Mehrfache Nullstellen

Lemma 3.60. *Ein Element* $a \in K$ *ist genau dann eine mehrfache Nullstelle eines Polynoms* $f \in K[t]$*, wenn* a *eine gemeinsame Nullstelle von* f *und* f' *ist.*

Ist K algebraisch abgeschlossen, so besitzen je zwei Polynome $f, g \in K[t]$ genau dann eine gemeinsame Nullstelle, wenn sie einen gemeinsamen Linearfaktoren besitzten. Da die Linearfaktoren ein Repräsentantensystem der irreduziblen Elemente von $K[t]$ bilden, ist dies äquivalent dazu, dass f und g nicht teilerfremd sind, dass also $\mathrm{ggT}(f, g) \neq 1$ gilt. Da sich der ggT zweier Polynome mithilfe des euklidischen Algorithmus und Polynomdivison berechen lässt, hängt dieser ggT dabei nicht von dem Körper K ab:

Lemma 3.61. *Ist* L/K *eine Körperweiterung, so haben* $f, g \in K[t]$ *den gleichen* ggT *in* $K[t]$ *und* $L[t]$*, d.h. ein Polynom* $h \in K[t]$ *ist genau dann ein* ggT *von* f *und* g *in* $K[t]$*, wenn* h *in* $L[t]$ *ein* ggT *von* f *und* g *ist. Inbesondere sind* f *und* g *genau dann teilerfremd in* $K[t]$*, wenn sie es in* $L[t]$ *sind.*

Dies führt zu der folgenden Charakterisierung gemeinsamer Nullstellen:

Korollar 3.62. *Für* $f, g \in K[t]$ *sind die folgenden Bedingungen äquivalent:*

1. *Ist* $\overline{K}$ *ein algebraischer Abschluss von* K*, so haben* f *und* g *eine gemeinsame Nullstelle in* K*.*
2. *Es gibt eine Körpererweiterung* L/K*, so dass* f *und* g *eine gemeinsame Nullstelle in* L *haben.*
3. *Es gibt eine algebraische Körpererweiterung* L/K*, so dass* f *und* g *eine gemeinsame Nullstelle in* L *haben.*
4. *Die Polynome* f *und* g *sind nicht teilerfremd.*

Korollar 3.63. *Für ein Polynom* $f \in K[t]$ *sind die folgenden Bedingungen äquivalent:*

1. *Für keine Körpererweiterung* L/K *hat* f *eine mehrfache Nullstelle in* L*.*

2. *Das Polynom f hat in einem algebraischen Abschluss $\overline{K}$ keine mehrfache Nullstelle.*

3. *Das Polynom f hat in einem Zerfällungkörper von f keine mehrfache Nullstelle.*

4. *Die Polynome f und f' sind teilerfremd.*

Definition 3.64. *Ein Polynom $f \in K[t]$, das eine (und damit alle) der obigen Bedingungen erfüllt, ist* separabel.

Beispiel 3.65. 1. Gilt $\mathrm{char}(K) = 0$, so ist jedes irreduzible Polynom $f \in K[t]$ separabel: Es gilt $\deg(f') = \deg(f) - 1$, weshalb f kein Teiler von f' ist, und somit f und f' teilerfremd sind.

2. Das Polynom $f := t^p - u \in \mathbb{F}_p(u)[t]$ ist nicht separabel, denn es gilt $f' = 0$, und somit $\mathrm{ggT}(f, f') = f \neq 1$.

3. Gilt allgemeiner $\mathrm{char}(K) = p > 0$ und ist $f \in K[t]$ irreduzibel, so gilt

$$f \text{ ist nicht separabel} \iff f' = 0 \iff \exists g \in K[t] : f(t) = g(t^p)\,.$$

3.9.2 Separable Elemente und Erweiterungen

Es sei L/K ein Körpererweiterung.

Lemma 3.66. *Für jedes Element $a \in L$ sind die folgenden Bedingungen äquivalent:*

1. *Es gibt ein separables Polynom $f \in K[t]$ mit $f(a) = 0$.*

2. *Das Element a ist algebraisch, und das Minimalpolynom $m_a \in K[t]$ ist separabel.*

Definition 3.67. *Ein Element $a \in L$ ist* separabel (über K)*, wenn es eine (und damit alle) der obigen Bedingungen erfüllt; ansonsten ist a* inseparabel.

Die Erweiterung L/K ist separabel*, wenn jedes Element $a \in L$ separabel über K ist; ansonsten ist die Erweiterung* inseparabel.

Beispiel 3.68. Gilt $\mathrm{char}(K) = 0$, so ist jedes algebraische Element $a \in L$ separabel, und somit jede algebraische Körpererweiterung L/K separabel.

Lemma 3.69. *Sind $M/L/K$ Erweiterungen, so dass M/K separabel ist, so sind auch M/L und L/K separabel.*

3.9.3 Der Separablitätsgrad

Definition 3.70. *Der* Separablitätsgrad *der algebraischen Erweiterung L/K ist die Anzahl der K-Homomorphismen $L \to \overline{K}$, und wird mit $[L : K]_{\mathrm{sep}}$ notiert.*

Lemma 3.71 (Multiplikativität des Separablitätsgrades)**.** *Für alle algebraischen Körpererweiterungen $M/L/K$ gilt $[M : K]_{\mathrm{sep}} = [M : L]_{\mathrm{sep}}[L : K]_{\mathrm{sep}}$.*

Lemma 3.72. *Es sei $a \in L$ algebraisch.*

1. *Es gilt $[K(a) : K]_{\text{sep}} \leq [K(a) : K]$.*

2. *Es gilt genau dann Gleichheit, wenn $K(a)/K$ separabel ist.*

Korollar 3.73. *Die Erweiterung L/K sei endlich.*

1. *Es gilt $[L : K]_{\text{sep}} \leq [L : K]$.*

2. *Es gilt genau dann Gleichheit, wenn L/K separabel ist.*

Korollar 3.74. *Sind M/L und L/K endliche separable Körpererweiterungen, so ist auch M/K separabel.*

Korollar 3.75. *Sind $a, b \in L$ separabel, so sind auch $a + b$ und $a \cdot b$ separabel; gilt $a \neq 0$, so ist auch $1/a$ separabel.*

Korollar 3.76. *Es ist $L' = \{x \in L \mid x \text{ ist separabel}\}$ ein Zwischenkörper von L/K.*

Korollar 3.77. *Die Erweiterung L/K ist genau dann separabel, wenn sie von separablen Elementen erzeugt wird.*

Satz 3.78 (Satz vom primitiven Element)**.** *Ist L/K endlich und separabel, so gibt es ein $a \in L$ mit $L = K(a)$, d.h. die Erweiterung L/K ist einfach.*

3.9.4 Perfekte Körper

Definition 3.79. *Ein Körper K ist* perfekt *oder* vollkommen*, wenn jede algebraische Körpererweiterung L/K separabel ist.*

Beispiel 3.80. Jeder Körper von Charakteristik 0 ist perfekt.

Ob ein Körper K der Charakteristik $\text{char}(K) = p > 0$ perfekt ist, hängt vom Verhalten des *Frobenius-Homomorphismus* ab:

Lemma 3.81. *Ist R ein Ring mit $\text{char}(R) = p > 0$, so ist die Abbildung $\sigma \colon R \to R$, $x \mapsto x^p$ ein Ringhomomorphismus.*

Definition 3.82. *Der Ringhomomorphismus σ wie oben ist der* Frobenius-Homomorphismus *von R.*

Proposition 3.83. *Ein Körper K von Charakteristik $\text{char}(K) = p > 0$ ist genau dann perfekt, wenn der Frobenius-Homomorphismus $\sigma \colon K \to K$, $x \mapsto x^p$ surjektiv ist.*

Beispiel 3.84. 1. Endliche Körper sind perfekt.

2. Algebraisch abgeschlossene Körper sind perfekt.

3. Der Körper $\mathbb{F}_p(u)$ ist nicht perfekt, denn es gibt kein $a \in \mathbb{F}_p(u)$ mit $a^p = u$.

3.10 Klassifikation endlicher Körper

Es sei p eine Primzahl. Im Folgenden seien alle Körper von Charakteristik p; der zugehörige Primkörper ist also stets $\mathbb{F}_p$.

Lemma 3.85. *Ist K ein endlicher Körper, so gilt $|\mathbb{F}_p| = p^n$ für $n = [K : \mathbb{F}_p]$.*

Es sei K ein Körper mit $|K| = q$. Dann gilt $|K^\times| = q - 1$, und somit $x^{q-1} = 1$ für alle $x \in K^\times$. Für alle $x \in K$ gilt somit $x^q = x$.

Lemma 3.86. *Ist K ein endlicher Körper mit $|K| = p^n = q$, so gilt besteht K aus den q verschiedenen Nullstellen des Polynomes $t^q - t \in \mathbb{F}_p[t]$. Inbesondere ist K ein Zerfällungskörper des Polynoms $t^q - t$.*

Korollar 3.87. *Je zwei endliche Körper K, K' mit $|K| = p^n = |K'|$ sind isomorph.*

Es sei andererseits $n \geq 1$, $q \coloneqq p^n$ und K ein Zerfällungskörper des Polynoms $f \coloneqq t^q - t \in \mathbb{F}_p[t]$. Dann ist die Menge der Nullstellen $K' \coloneqq \{x \in K \mid x^q = x\}$ ein Unterkörper von K, denn es ist $K' = \{x \in K \mid \sigma^n(x) = \mathrm{id}(x)\}$ die Übereinstimmungsmenge zweier Körperhomomorphismen. Es gilt somit $K = K'$. Es gilt $f' = -1$, weshalb f und f' teilerfremd sind. Es ist also f separabel, und somit $|K| = \deg(f) = q = p^n$.

Satz 3.88 (Klassifikation endlicher Körper)**.** *Es sei p eine Primzahl. Dann gibt es für alle $n \geq 0$ einen Körper $\mathbb{F}_{p^n}$ mit p^n Elementen, dieser ist eindeutig bis auf Isomorphie, und jeder endliche Körper von Charakteristik p ist von dieser Form. Der Körper $\mathbb{F}_{p^n}$ besteht aus den Nullstellen des Polynoms $t^{p^n} - t \in \mathbb{F}_p[t]$.*

Lemma 3.89. *Für alle $n, m \geq 1$ gibt es genau dann eine Einbettung (d.h. einen Körperhomomorphismus) $\mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$, wenn $n \mid m$ gilt.*

Beispiel 3.90. Für alle $n \leq m$ lässt sich $\mathbb{F}_{p^{n!}}$ als Unterkörper von $\mathbb{F}_{p^{m!}}$ auffassen. Dann ist $\mathbb{F}_{p^\infty} \coloneqq \bigcup_{n \geq 0} \mathbb{F}_{p^{n!}}$ ein algebraischer Abschluss von $\mathbb{F}_p$.

4 Galois-Theorie

4.1 Galois-Erweiterungen

Es sei L/K eine endliche Körpererweiterung.

Definition 4.1. *Der* Fixkörper *einer Untergruppe $H \leq \mathrm{Aut}(L/K)$ ist*

$$L^H \coloneqq \{x \in L \mid \sigma(x) = x \text{ für alle } \sigma \in H\}.$$

Lemma 4.2. *1. Es gilt $|\mathrm{Aut}(L/K)| \leq [L:K]_{\mathrm{sep}} \leq [L:K]$.*

2. Die Eweiterung L/K ist genau dann normal, wenn $|\mathrm{Aut}(L/K)| = [L:K]_{\mathrm{sep}}$ gilt.

Proposition 4.3. *Für L/K sind die folgenden Bedingungen äquivalent:*

1. *Es gilt $|\mathrm{Aut}(L/K)| = [L:K]$.*
2. *Die Erweiterung L/K ist normal und separabel.*
3. *Für jedes $a \in L$ zerfällt das Minimalpolynom m_a über L in die Linearfaktoren $t - \sigma(a)$ mit $\sigma \in \mathrm{Gal}(L/K)$, jeweils mit Vielfachheit 1.*
4. *Es gilt $K = L^{\mathrm{Aut}(L/K)}$.*

Definition 4.4. *Erfüllt die Erweiterung L/K eine (und damit alle) der obigen Bedingungen, so ist L/K* galoissch. *Es ist dann $\mathrm{Gal}(L/K) \coloneqq \mathrm{Aut}(L/K)$ die* Galoisgruppe *der Erweiterung L/K.*

Satz 4.5 (Hauptsatz der Galoistheorie)**.** *Die Erweiterung L/K sei galoissch mit Galoisgruppe $G \coloneqq \mathrm{Gal}(L/K)$.*

1. *Es gibt es eine inklusionsumkehrende Bijektion*

$$\begin{aligned} \{\text{Zwischenkörper } K \subseteq M \subseteq L\} &\xrightarrow{\sim} \{\text{Untergruppen } H \leq G\}, \\ M &\longmapsto \mathrm{Aut}(L/M), \\ L^H &\longmapsfrom H. \end{aligned}$$

Dies lässt sich wie folgt veranschaulichen:

$$\begin{array}{ccc} L & & 1 \\ \uparrow & & \downarrow \\ M & \leftrightsquigarrow & H \\ \uparrow & & \downarrow \\ K & & G \end{array}$$

2. *Es sei $K \subseteq M \subseteq L$ ein Zwischenkörper mit zugehöriger Untergruppe $H \leq G$.*
   a) *Es ist L/M galoissch mit Galoisgrouppe H. Insbesondere gilt $[L : M] = |H|$.*
   b) *Es gilt $[M : K] = [G : H]$.*

   Dies lässt sich wie folgt veranschaulichen:

$$\begin{array}{ccc} L & & 1 \\ {\scriptstyle [L:M]}\uparrow & & \downarrow{\scriptstyle |H|=[H:1]} \\ M & \leftrightsquigarrow & H \\ {\scriptstyle [M:K]}\uparrow & & \downarrow{\scriptstyle [G:H]} \\ K & & G \end{array}$$

3. *Die Erweiterung M/K ist genau dann normal, wenn die zugehörige Untergruppe $N \leq G$ normal ist. Dann ist M/K ebenfalls galoissch, und es gilt*

$$\mathrm{Gal}(M/K) \cong G/N\,.$$

Definition 4.6. *Die obige inklusionsumkehrende Korrespondenz zwischen Unterkörpern und Untergruppen ist die* Galoiskorrespondenz.

4.2 Beispiel: $\mathbb{C}/\mathbb{R}$

Die Körpererweiterung $\mathbb{C}/\mathbb{R}$ ist normal, da $\mathbb{C} = \mathbb{R}(i)$ ein Zerfällungskörper des Polynoms $f := t^2 + 1 \in \mathbb{R}[t]$ ist. Die Erweiterung ist separabel, da $\mathbb{R}$ perfekt ist, da $\mathrm{char}(\mathbb{R}) = 0$ gilt. Somit ist die Erweiterung $\mathbb{C}/\mathbb{R}$ galoissch.

Aus $|\mathrm{Gal}(\mathbb{C}/\mathbb{R})| = [\mathbb{C} : \mathbb{R}] = 2$ ergibt sich bereits, dass $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \cong \mathbb{Z}/2$ gilt. Ein nicht-trivialer $\mathbb{R}$-Automorphismus $\mathbb{C} \to \mathbb{C}$ ist durch die Konjugationsabbildung $c\colon \mathbb{C} \to \mathbb{C}$, $z \mapsto \overline{z}$ gegeben. Somit gilt $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}, c\}$.

$$\begin{array}{ccc} \{\mathrm{id}, c\} & & \mathbb{R} \\ {\scriptstyle 2}\uparrow & \leftrightsquigarrow & {\scriptstyle 2}\downarrow \\ 1 & & \mathbb{C} \end{array}$$

4.3 Beispiel: $\mathbb{F}_{p^n}/\mathbb{F}_p$

Die Erweiterung $\mathbb{F}_{p^n}/\mathbb{F}_p$ ist normal, denn nach der Klassifikation endlicher Körper ist $\mathbb{F}_{p^n}$ ein Zerfällungskörper des Polynoms $f := t^{p^n} - t \in \mathbb{F}_p[t]$. Die Erweiterung ist separabel, da $\mathbb{F}_p$ endlich, und somit perfekt ist. Also ist $\mathbb{F}_{p^n}/\mathbb{F}_p$ galoissch.

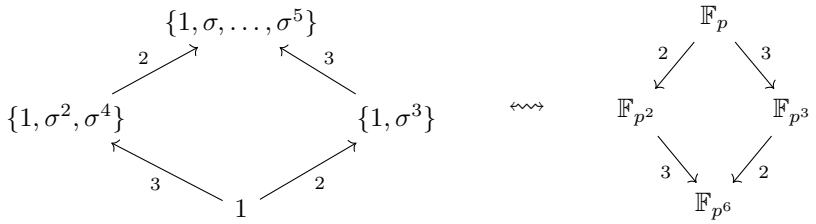
Der Frobenius-Homomorphismus $\sigma\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, $x \mapsto x^p$ ist ein Körperautomorphismus von $\mathbb{F}_{p^n}$; er ist $\mathbb{F}_p$-linear, da $\mathbb{F}_p$ der Primkörper von $\mathbb{F}_{p^n}$ ist. Somit gilt $\sigma \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$.

Gilt dabei $\sigma^m = \mathrm{id}$ für ein $m \geq 1$, so gilt $x^{p^m} - x = 0$ für alle $x \in \mathbb{F}_{p^n}$, d.h. alle Elemente von $\mathbb{F}_{p^n}$ sind Nullstellen des Polynoms $g \coloneqq t^{p^m} - t \in \mathbb{F}_p[t]$. Dann gilt allerdings $p^n = |\mathbb{F}_{p^n}| \leq \deg(g) = p^m$, und somit $m \geq n$. Es gilt also $\mathrm{ord}(\sigma) \geq n$. Andererseits gilt

$$\mathrm{ord}(\sigma) \mid \mathrm{ord}(\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)) = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n\,.$$

Ingesamt gilt also $\mathrm{ord}(\sigma) = n = \mathrm{ord}(\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p))$. Somit ist die Galoisgruppe $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ zyklisch, und wird vom Frobenius-Homomorphismus σ erzeugt. Es gilt insbesondere $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n$.

Für $n = 6$ ergibt sich die folgende Galoiskorrespondenz:



4.4 Beispiel: $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$

4.4.1 Die Erweiterung ist galoissch

Es sei $L \coloneqq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Dann ist $L = \mathbb{Q}(\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3})$ ein Zerfällungskörper des Polynoms $f \coloneqq (t^2 - 2)(t^2 - 3) \in \mathbb{Q}[t]$, und die Erweiterung $L/\mathbb{Q}$ somit normal. Diese Erweiterung ist auch separabel, da $\mathbb{Q}$ perfekt ist, da $\mathrm{char}(\mathbb{Q}) = 0$ gilt.

4.4.2 Bestimmung des Grades

Es gilt $[L : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$. Dabei gilt $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, denn das Minimalpolynom von $\sqrt{2}$ ist $t^2 - 2 \in \mathbb{Q}[t]$ (siehe Beispiel 3.25). Da $\sqrt{3}$ Nullstelle des Polynoms $t^2 - 3 \in \mathbb{Q}(\sqrt{2})[t]$ ist, gilt $[\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}(\sqrt{2})] \leq 2$. Im Fall $[\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 1$ wäre $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$, was aber nicht gilt:

Lemma 4.7. *Es gilt $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$.*

Es gilt also $[\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$. Insgesamt gilt somit $[L : \mathbb{Q}] = 4$.

4.4.3 Bestimmung einer Basis

Es ist $1, \sqrt{2}$ eine $\mathbb{Q}$-Basis von $\mathbb{Q}(\sqrt{2})$, und $1, \sqrt{3}$ eine $\mathbb{Q}(\sqrt{2})$-Basis von $\mathbb{Q}(\sqrt{2})(\sqrt{3}) = L$. Eine $\mathbb{Q}$-Basis von L ist deshalb durch

$$1 \cdot 1 = 1\,, \quad \sqrt{2} \cdot 1 = \sqrt{2}\,, \quad 1 \cdot \sqrt{3} = \sqrt{3}\,, \quad \sqrt{2} \cdot \sqrt{3} = \sqrt{6}$$

gegeben.

4.4.4 Bestimmung der Galoisgruppe

Jeder $\mathbb{Q}$-Automorphismus $\varphi\colon L \to L$ muss die Nullstellen der beiden rationalen Polynome $t^2-2, t^2-3 \in \mathbb{Q}[t]$ jeweils permutieren; es muss also $\varphi(\sqrt{2}) = \pm\sqrt{2}$ und $\varphi(\sqrt{3}) = \pm\sqrt{3}$ gelten. Dabei ist φ durch die Werte $\varphi(\sqrt{2})$ und $\varphi(\sqrt{3})$ bereits eindeutig bestimmt. Es gibt also höchstens 4 $\mathbb{Q}$-Automorphismen $L \to L$, und diese sind durch die folgenden Zuordnungen festgelegt:

$$\mathrm{id}\colon \begin{cases} \sqrt{2} \mapsto & \sqrt{2} \\ \sqrt{3} \mapsto & \sqrt{3} \end{cases} \qquad \tau_1\colon \begin{cases} \sqrt{2} \mapsto & -\sqrt{2} \\ \sqrt{3} \mapsto & \sqrt{3} \end{cases}$$

$$\tau_2\colon \begin{cases} \sqrt{2} \mapsto & \sqrt{2} \\ \sqrt{3} \mapsto & -\sqrt{3} \end{cases} \qquad \tau_1\tau_2\colon \begin{cases} \sqrt{2} \mapsto & -\sqrt{2} \\ \sqrt{3} \mapsto & -\sqrt{3} \end{cases}$$

Da die Erweiterung $L/\mathbb{Q}$ galoissch ist, gilt dabei $|\mathrm{Gal}(L/K)| = [L:\mathbb{Q}] = 4$. Somit muss jede der obigen 4 Zuordnungen tätsächlich schon einen $\mathbb{Q}$-Automorphismus definieren.

Insbesondere gilt $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/2 \times \mathbb{Z}/2$; dabei entspricht etwa τ_1 dem Element $(1,0)$, und τ_2 dem Element $(0,1)$.

4.4.5 Bestimmung der Untergruppen der Galoisgruppe

Die Untergruppen von $\mathbb{Z}/2 \times \mathbb{Z}/2$ sind

- die triviale Gruppe 0,
- die zyklischen Untergruppen $\langle(1,0)\rangle$, $\langle(1,1)\rangle$, $\langle(0,1)\rangle$,
- die gesamte Gruppe $\mathbb{Z}/2 \times \mathbb{Z}/2$.

Die Untergruppen von $G \coloneqq \mathrm{Gal}(L/\mathbb{Q})$ sind also

- die triviale Gruppe 1,
- die zyklischen Untergruppen $\langle\tau_1\rangle$, $\langle\tau_2\rangle$, $\langle\tau_1\tau_2\rangle$,
- die gesamte Gruppe G.

4.4.6 Bestimmung der Fixkörper

Für $x \in L$,

$$x = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$$

mit $a, b, c, d \in \mathbb{Q}$ gilt etwa

$$\tau_1(x) = a - b\sqrt{2} + c\sqrt{2} - d\sqrt{6}\,,$$

und deshalb genau dann $\tau_1(x) = x$, wenn $b = d = 0$. Also gilt

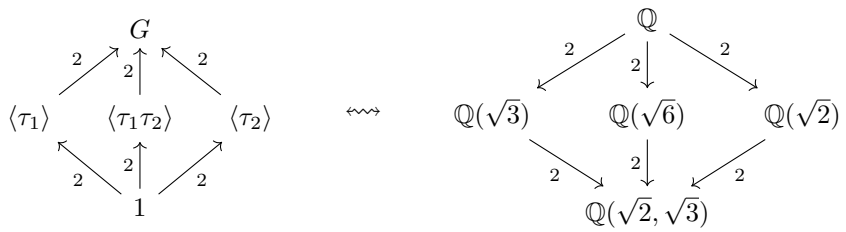
$$L^{\langle\tau_1\rangle} = \{a + c\sqrt{3} \mid a, c \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{3})\,.$$

Analog ergibt sich, dass

$$L^{\langle\tau_2\rangle} = \mathbb{Q}(\sqrt{2})\,, \qquad L^{\langle\tau_1\tau_2\rangle} = \mathbb{Q}(\sqrt{6})\,.$$

4.4.7 Die Galoiskorrespondenz

Die gesamte Galoiskorrespondenz sieht somit wie folgt aus:



4.5 Beispiel: Kreisteilungskörper $\mathbb{Q}(\zeta_n)/\mathbb{Q}$

Definition 4.8. *Für alle $n \geq 1$ ist $W_n \coloneqq \{z \in \mathbb{C} \mid z^n = 1\}$ die Gruppen der n-ten Einheitswurzeln. Eine n-te Einheitswurzel $\zeta \in W_n$ ist* primitiv*, wenn $W_n = \langle\zeta\rangle$ gilt.*

Ist ζ eine primitive n-te Einheitswurzeln, so ist die Abbildung

$$\mathbb{Z}/n \to W_n\,, \quad \overline{k} \mapsto \zeta^k$$

ein Gruppenisomorphismus. Dabei gilt

$$\begin{aligned} & \zeta_k \text{ ist primitiv} \\ \iff & \overline{k} \in \mathbb{Z}/n \text{ ist ein zyklischer Erzeuger} \\ \iff & k \text{ und } n \text{ sind teilerfremd} \\ \iff & \overline{k} \text{ ist eine Einheit in } \mathbb{Z}/n\,. \end{aligned}$$

Also ist ζ^k genau dann primitiv, wenn $\overline{k}$ ein Erzeuger von $\mathbb{Z}/n$ ist, wenn also k und n teilerfremd sind, wenn also $\overline{k}$ eine Einheit in $\mathbb{Z}/n$ ist.

Definition 4.9. *Für alle $n \geq 1$ ist $\Phi_n \coloneqq \prod_{\zeta \text{ primitive } n\text{-te Einheitswurzel}}(t-\zeta)$ das n-te* Kreisteilungspolynom*.*

Satz 4.10. *Es sei $n \geq 1$.*

1. *Das Polynom Φ_n ist normiert.*
2. *Es gilt $t^n - 1 = \prod_{d|n} \Phi_d$.*
3. *Für p prim gilt $\Phi_p = t^{p-1} + \cdots + t + 1 = (t^p - 1)/(t-1)$.*
4. *Es gilt $\Phi_n \in \mathbb{Z}[t]$.*
5. *Das Polynom Φ_n ist irreduzibel.*

Korollar 4.11. *Φ_n ist das Minimalpolynom jeder primitiven n-ten Einheitswurzel*

Bemerkung 4.12. Für p prim lässt sich die Irreduziblität von Φ_p dadurch zeigen, dass man auf

$$\Phi_p(t+1) = \frac{(t+1)^p - 1}{t} = \sum_{k=1}^{p} \binom{p}{k} t^{k-1} = \sum_{k=0}^{p-1} \binom{p}{k+1} t^k$$

das Eisenstein-Kriterium bezüglich der Primzahl p anwendet.

Es sei im Folgenden ζ_n eine primitive n-te Einheitswurzel.

4.5.1 Die Erweiterung ist galoissch

Es ist $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_n^k \,|\, k \in \mathbb{Z})$ ein Zerfällungskörper von $t^n - 1$, und $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ somit normal. Die Erweiterung ist separabel, da $\mathbb{Q}$ perfekt ist, da $\mathrm{char}(\mathbb{Q}) = 0$ gilt.

4.5.2 Bestimmung der Galoisgruppe

Es gilt

$$\begin{aligned}
\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) &= \{\mathbb{Q}\text{-Automorphismen } \mathbb{Q}(\zeta_n) \to \mathbb{Q}(\zeta_n)\} \\
&= \{\mathbb{Q}\text{-Homomorphismen } \mathbb{Q}(\zeta_n) \to \mathbb{Q}(\zeta_n)\} \\
&\leftrightarrow \{\text{Nullstellen von } \Phi_n \text{ in } \mathbb{Q}(\zeta_n)\} \\
&= \{\text{primitive } n\text{-te Einheitswurzeln}\} \\
&\leftrightarrow (\mathbb{Z}/n)^\times ,
\end{aligned}$$

wobei für jedes $\overline{k} \in (\mathbb{Z}/n)^\times$ das zugehörige Gruppenelement $\psi_{\overline{k}} \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ durch

$$\psi_{\overline{k}}(\zeta_n) = \zeta_n^k$$

eindeutig bestimmt ist. Dabei gilt

$$\psi_{\overline{k}} \psi_{\overline{\ell}} = \psi_{\overline{k} \cdot \overline{\ell}}$$

weshalb es sich bereits um einen Gruppenisomorphismus handelt. Es gilt also

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n)^\times .$$