LEHRPLAN: ALGEBRA UND ZAHLENTHEORIE

VICTORIA HOSKINS

Webseite: `http://userpage.fu-berlin.de/hoskins/AZT.html`

Diese Lehrplan ist kein Skript, nur meine Notizen zur Vorlesung. Fehler können und werden vorkommen. Wenn Sie einen Fehler finden, senden Sie mir eine E-Mail: `hoskins@math.fu-berlin.de`.

Inhaltsverzeichnis

[16.10.18]

Überblick. In diesem Kurs werden wir einige bekannte algebraische Strukturen (Gruppen, Ringe und Körper) studieren, um die *Galois Theorie* einzuführen und den *Hauptsatz der Galoistheorie* zu beweisen. Die Motivation für die Galois Theorie war das klassische Problem der Auflösbarkeit einer Polynomgleichung:

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0.$$

Idealerweise möchte man die Lösungen in Form von Koeffizienten durch algebraische Operationen (wie Addition, Subtraktion, Multiplikation, Division und Wurzelziehen) ausdrücken. Diese ist die berühmte und klassische Frage nach der *Auflösbarkeit algebraischer Gleichungen durch Radikale* (d.h. die obige Operationen).

Eine kurze Geschichte der Auflösbarkeit algebraischer Gleichungen:

- Quadratische Gleichungen: $ax^2 + bx + c = 0$ (wobei $a \neq 0$) hat die Lösungen:
$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$
Bereits 2000 vor Christus. könnten babylonische Mathematiker quadratische Gleichungen lösen. Geometrische Methoden wurden verwendet, um quadratische Gleichungen in Babylonien, Ägypten, Griechenland, China und Indien zu lösen. Wenn a, b und c reelle Zahlen sind, können die Nullstellen in den *komplexen Zahlen* liegen. Falls die Nullstellen komplex sind, gibt es eine Symmetrie zwischen den Nullstellen: sie sind komplex konjugiert.
- Gleichungen von Grad 3 und 4: Eine Hauptmotivation, die komplexen Zahlen zu untersuchen, bestand darin, algebraische Lösungen für algebraische Gleichungen von Grad 3 und 4 zu finden. Im 16. Jahrhundert wurden algebraische Lösungen für die Nullstellen von kubischen und quartären Polynomen von italienischen Mathematikern entdeckt.
- Gleichungen höheren Grades und Galois Theorie: Zu diesem Thema gab es keinen Fortschritt, bis das folgende Theorem bewiesen wurde.

  Satz von Abel-Ruffini, 1824. Für jede $n \geq 5$ existieren Polynome vom Grad n, die nicht durch Radikale lösbar sind.

Einige Polynome vom Grad n könnten jedoch gelöst werden (z.B. $(x-1)^n = 0$). Daher war die Frage, wann eine Gleichung lösbar war. Dieses Problem wurde von Évariste Galois (1811 - 1831, französische Mathematiker) gelöst: er zeigte, dass die Frage, ob ein Polynom lösbar war oder nicht, äquivalent dazu war, ob die Permutationsgruppe ihrer Nullstellen (in der modernen Terminologie ihre *Galois Gruppe*) eine gewisse Struktur hatte (eine sogenannte *lösbare* Gruppe).

Anwendungen: Eine Anwendung der Galois Theorie, die für LehrerInnen besonders relevant ist, ist die Untersuchung von Problemen in der *Konstruktion von Zirkel und Lineal*. In der aktuellen mathematischen Forschung spielt die Galois-Theorie eine wichtige Rolle in der *Zahlentheorie* und der *algebraischen Geometrie*.

1. Gruppentheorie

1.1. **Gruppen und Untergruppen.** Eine *Gruppe* ist eine Menge G mit einer Verknüpfung $\star : G \times G \to G$ mit der folgenden Eigenschaften (G1-G3):

(G1) Die Verknüpfung ist assoziativ: für alle $a, b, c \in G$ gilt

$$a \star (b \star c) = (a \star b) \star c.$$

(G2) G hat ein *linksneutrales Element* $e \in G$ (d.h. für alle $g \in G$ gilt $e \star g = g$).

(G3) Für jedes Element $g \in G$ gibt es ein *linksinverses Element* $g' \in G$ (d.h. $g' \star g = e$ und normalerweise schreibt man $g^{-1} := g'$).

Eine Gruppe $(G, \star)$ heißt *abelsch*, wenn $\star$ kommutativ ist (d.h. $a \star b = b \star a$ für alle $a, b \in G$).

Bemerkung. Diese ist eine schwache Definition einer Gruppe, da wir nur fordern, dass e linksneutral ist und jedes Element g ein linksinverses Element hat. Jedoch nach dem folgenden Aussagen ist e auch rechtsneutral (so dass, wir e ein neutrales Element nennen können) und ein linksinverses Element g' von $g \in G$ ist auch ein rechtsinverses Element (so dass, wir g' ein inverses Element von g nennen können). Für eine Gruppe gilt die folgenden Aussagen:

(1) Das neutrale Element e ist eindeutig bestimmt.
(2) Für $g \in G$ gilt $g \star e = g$.
(3) Das inverse Element von einem Element $g \in G$ ist eindeutig besimmt.
(4) Sei g' das inverse Element von $g \in G$. Dann gilt $g \star g' = e$.
(5) (Kürzungsregeln): für $a, b, c \in G$:

$$\text{i)} \quad a \star b = a \star c \implies b = c,$$
$$\text{ii)} \quad a \star b = c \star b \implies a = c.$$

(6) Für $g \in G$, gilt $(g^{-1})^{-1} = g$, wobei g^{-1} ist das inverse Element von g und $(g^{-1})^{-1}$ ist das inverse Element von g^{-1}.
(7) Für $g, h \in G$ gilt $(g \star h)^{-1} = h^{-1} \star g^{-1}$.

Beispiel.

(1) $(\mathbb{Z}, +)$ ist eine abelsche Gruppe mit dem neutralen Element 0. Das inverse Element von $a \in \mathbb{Z}$ ist $-a \in \mathbb{Z}$.
(2) Jeder Körper K ist eine abelsche Gruppe unter Addition: z.B. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.
(3) Jeder Körper ohne Null $K^\times = K \setminus \{0\}$ ist eine abelsche Gruppe unter Multiplikation.
(4) $\mathbb{Z}/n\mathbb{Z} \cong \{[0]_n, \cdots, [n-1]_n\}$ mit Addition modulo n ist eine abelsche Gruppe. Zür Erinnerung $\mathbb{Z}/n\mathbb{Z} := \mathbb{Z}/\sim_n$ wobei $a \sim_n b \iff n|a-b$. Sei $[a]_n = a + n\mathbb{Z}$ die Äquivalenzklass von $a \in \mathbb{Z}$.[1]
(5) Für eine Menge X ist die Menge $\mathrm{Isom}(X)$ von Isomorphismen $f : X \to X$ mit der Verknüpfung $\circ$ (Komposition) eine Gruppe.
(6) $(\mathrm{Mat}_{n\times n}(K), +)$ ist eine abelsche Gruppe.
(7) $(\mathrm{GL}_n(K), \cdot)$ ist eine Gruppe. Für $n = 1$ ist diese Gruppe abelsche $\mathrm{GL}_1(K) = K^\times$ und für $n > 1$ ist diese Gruppe nicht-kommutativ.

[1]Wir werden bald eine Konstruktion von $\mathbb{Z}/n\mathbb{Z}$ als eine Quotientengruppe sehen.

(8) $\mathbb{N} = \{0, 1, 2 \dots\}$ mit Addition ist keine Gruppe: die Addition ist assoziativ und $0 \in \mathbb{N}$ ist ein neutrales Element, aber jede positive Zahlen n hat ein inverses Element $-n \in \mathbb{Z} \setminus \mathbb{N}$ (d.h. Axiom (G3) gilt nicht).

Definition. Für $n \in \mathbb{N}$ ist die *symmetrische Gruppen* $S_n := \mathrm{Isom}(\{1, \dots, n\})$. Ein Element σ von S_n heißt *Permutation* und wir schreiben σ wie folgt:

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

Beispiel. Die symmetrische Gruppe S_1 hat nur ein Element, die Identität. Die symmetrische Gruppe S_2 hat zwei Elemente

$$e = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \quad \sigma := \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix},$$

da jedes Element eine *bijektive* Abbildung $\{1, 2\} \to \{1, 2\}$ ist. Es gilt $\sigma \circ \sigma = e$.

Jetzt betrachen wir die symmetrische Gruppe S_3. Um eine bijektive Abbildung $\sigma : \{1, 2, 3\} \to \{1, 2, 3\}$ zu definieren, muss man $\sigma(1) \in \{1, 2, 3\}$ wählen (es gibt 3 Möglichkeiten) und dann $\sigma(2) \in \{1, 2, 3\} \setminus \{\sigma(1)\}$ wählen (es gibt 2 Möglichkeiten), dann $\sigma(3) \in \{1, 2, 3\} \setminus \{\sigma(1), \sigma(2)\}$ wählen (es gibt nur eine Möglichkeit). Daher hat S_3 sechs ($6 = 3 \times 2 \times 1$) Elemente:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \sigma_1 := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \sigma_2 := \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \tau_1 := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \tau_2 := \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

und S_3 ist nicht kommutativ, da $\sigma_1 \circ \sigma_2 = \tau_2 \neq \tau_1 = \sigma_2 \circ \sigma_1$.

Definition. Das Produkt von zwei Gruppen $(G, \star_G)$ und $(H, \star_H)$ ist

$$(G \times H, \star), \quad \text{wobei } (g, h) \star (g', h') := (g \star_G g', h \star_H h').$$

Übung. Zeigen Sie, dass $G \times H$ eine Gruppe ist.

Definition. Eine *Untergruppe* einer Gruppe $(G, \star)$ ist eine Teilmenge $H \subset G$ mit den folgenden Eigenschaften:

(1) Das neutrale Element $e \in G$ ist ein Element von H.
(2) Für $h \in H$ gilt $h^{-1} \in H$.
(3) Für $h_1, h_2 \in H$ gilt $h_1 \star h_2 \in H$.

Man schreibt $H < G$ für eine Untergruppe H von G.

Bemerkung. $(H, \star)$ ist eine Gruppe (für eine Untergruppe $H < G$).

Beispiel. Die Gruppe $(\mathbb{Z}, +)$ hat die Untergruppen

$$n\mathbb{Z} := \{a \in \mathbb{Z} : \exists k \in \mathbb{Z} \text{ mit } a = kn\} = \{0, \pm n, \pm 2n, \cdots\}$$

für $n \in \mathbb{N}$.

Proposition. Jede Untegruppe H von $(\mathbb{Z}, +)$ hat die Form $H = n\mathbb{Z}$ für eine natürliche Zahl n.

1.2. **Nebenklassen und Quotientengruppen.** Es gibt 2 Motivationen für Quotientengruppen (deren Elemente die so-genannte Nebenklassen sind):

- Man kann neue Gruppen aus alten Gruppen konstruieren (z.B. $\mathbb{Z}/n\mathbb{Z}$ ist die Quotientengruppe von $\mathbb{Z}$ durch die normale Untergruppe $n\mathbb{Z}$).
- Die Untersuchung von Gruppenhomomorphismen (z.B. siehe den Homomorphiesatz).

Definition. Für eine Untergruppe $H < G$ und $a \in G$ definiert man die die *Linksnebenklasse* (LNK) aH und die *Rechtsnebenklasse* (RNK) Ha

$$aH := \{a' \in G : a' = a \star h \text{ für } h \in H\} \qquad Ha := \{a' \in G : a' = h \star a \text{ für } h \in H\}.$$

Man schreibt $G/H = \{aH : a \in G\}$ und $H\backslash G = \{Ha : a \in G\}$ für die Menge der LNK und RNK von H in G bzw.

Bemerkung. Wenn G eine abelsche Gruppe ist, dann gilt $aH = Ha$ für alle $a \in G$ (d.h. die Linksnebenklassen und Rechtsnebenklasse übereinstimmen). Falls G eine Gruppe mot Addition ist (z.B. $G = \mathbb{Z}$) schreiben wir $a + H$ für die LNK von $a \in G$.

Lemma. Für eine Untergruppe $H < G$ ist die Relation $\sim_H$ auf G

$$\text{für } a, b \in G: \quad a \sim_H b :\iff a^{-1} \star b \in H$$

eine Äquivalenzrelation. Ferner ist die Äquivalenzklasse von $a \in G$ die Linksnebenklassen

$$aH := \{a \star h : h \in H\}.$$

Deshalb sind zwei Linksnebenklassen entweder gleich oder disjunkt (d.h. ihr Durchschnitt ist leer) und G ist die disjunkte Vereinigung[2] der Linksnebenklassen

$$G = \bigsqcup_{aH \in G/H} aH.$$

[18.10.18]

Definition. Seien $(G, \star_G)$ und $(H, \star_H)$ Gruppen. Eine Abbildung $\varphi : G \to H$ heißt *Gruppenhomomorphismus* (GH.), wenn für alle $g_1, g_2 \in G$ gilt

$$\varphi(g_1 \star_G g_2) = \varphi(g_1) \star_H \varphi(g_2).$$

Der Kern von φ ist $\mathrm{Ker}(\phi) := \phi^{-1}(e_G)$.

Beispiel. Sei $H < G$ eine Untergruppe einer Gruppe G. Dann ist die Inklusionsabbildung $i : H \to G$, die durch $i(h) = h$ definiert wird, ein Gruppenhomomorphismus.

Beispiel. Sei $(G, \star)$ eine Gruppe und $a \in G$. Dann ist

$$\varphi_a : G \to G, \quad \varphi_a(g) := aga^{-1}$$

ein Gruppenhomomorphismus.

Bemerkung. Der bijektive Abbildung $f : G \to G$ mit $g \mapsto g^{-1}$ ist keine GH, aber das Bild einer Linksnebenklasse aH ist die Rechtsnebenklasse Ha^{-1} (d.h. $f(aH) = Ha^{-1}$). Deshalb gibt es eine bijektive Abbildung

$$G/H \to H\backslash G, \quad aH \mapsto Ha^{-1}.$$

Definition. Sei G eine Gruppe.

(1) Die *Ordnung* $|G| \in \mathbb{N} \cup \{\infty\}$ von G ist die Anzahl der Elemente in G.
(2) Ein Element $g \in G$ hat endlich Ordung, wenn es $n \in \mathbb{N}$ mit $g^n = e$ gibt. In diesem Fall ist die Ordnung von g die kleinste Zahl $n \in \mathbb{N} \setminus \{0\}$ so dass $g^n = e$ (man schreibt $|g| = n$). Sonst hat g unendliche Ordnung und man schreibt $|g| = \infty$.
(3) Für $H < G$ ist der *Index* $|G : H| \in \mathbb{N} \cup \{\infty\}$ die Anzahl der LNK von H in G (oder die Anzahl von RNK von H in G).

Beispiel. Die symmetrische Gruppe S_n hat die Ordnung $|S_n| = n!$

[2]eine Vereinigung $A = \cup_i A_i$ ist disjunkt, wenn $A_i \cap A_j = \emptyset$ für alle $i \neq j$, und man schreibt $A = \sqcup_i A_i$

Satz 1.1 (Lagrange)**.** *Sei G eine endliche Gruppe und $H \leq G$ eine Untergruppe. Dann gilt*

$$|G| = |G : H||H|.$$

Beweisidee. Für $a \in G$ gibt es eine bijektive Abbildung $\phi_a : H \to aH$, die durch $\phi_a(h) = ah$ definiert wird. Daher gilt $|H| = |aH|$. Da $\sim_H$ eine Äquivalenzrelation auf G ist, ist G die disjunkte Vereinigung von Äquivalenzklassen. Die Äquivalenzklassen sind die Linksnebenklassen, so dass

$$G = \bigsqcup_{aH \in G/H} aH.$$

Daher gilt

$$|G| = \sum_{aH \in G/H} |aH| = \sum_{aH \in G/H} |H| = |G : H||H|.$$

□

Korollar. Sei G eine endliche Gruppe. Für jedes $g \in G$ ist $|g|$ ein Teiler von $|G|$.

Definition. Eine Untergruppe H einer Gruppe G heißt *normale Untergruppe*, wenn für alle $a \in G$ gilt $aH = Ha$. Man schreibt $H \triangleleft G$ für eine normale Untergruppe H von G.

Bemerkung.

(1) Die Untergruppen $\{e\}$ und G sind normale Untegruppen von G.
(2) Jede Untergruppe einer abelschen Gruppe ist eine normale Untergruppe.
(3) Es gilt $aH = Ha$, wenn $aHa^{-1} = H$. Zeigen Sie, dass $H < G$ genau dann eine normale Untergruppe ist, wenn $aHa^{-1} \subset H$ für alle $a \in G$ gilt.

Lemma. Sei $\varphi : G \to H$ ein Gruppenhomomorphismus. Dann gelten die folgende Aussagen.

(1) $\varphi(e_G) = e_H$.
(2) $\varphi(g)^{-1} = \varphi(g^{-1})$ für alle $g \in G$.
(3) Das Bild $\varphi(G)$ ist eine Untergruppe von H.
(4) Der Kern ist eine normale Untergruppe von G.
(5) φ ist genau dann injektiv, wenn $\ker(\varphi) = \{e_G\}$.
(6) Wenn φ bijektiv ist, ist die Umkehrfunktion φ^{-1} ein Gruppenhomomorphismus.

Satz 1.2. *Sei H eine normale Untergruppe einer Gruppe G. Dann gibt es eine Abbildung*

$$\begin{array}{ccc} G/H \times G/H & \to & G/H \\ (aH, bH) & \mapsto & abH \end{array}$$

die auf G/H die Struktur einer Gruppe definiert. Ferner ist die Abbildung $\pi : G \to G/H$ mit $\pi(a) = aH$ ein Gruppenhomomorphismus mit $\ker(\pi) = H$ *und* $\text{Bild}(\pi) = G/H$.

Beweisidee. Wir müssen zeigen, dass diese Abbildung wohldefiniert ist (d.h. wenn $a_1H = a_2H$ und $b_1H = b_2H$ gelten, dann ist $a_1b_1H = a_2b_2H$). Wir nehmen an, dass $a_1 = a_2h$ und $b_1 = b_2\tilde{h}$ mit $h, \tilde{h} \in H$. Dann

$$(a_2b_2)^{-1}(a_1b_1) = b_2^{-1}a_2^{-1}a_1b_1 = b_2^{-1}hb_1 = b_2^{-1}hb_2\tilde{h}$$

ist ein Element von H, weil $b_2^{-1}hb_2 \in H$ nach der Normalität von $H \triangleleft G$ ist. Daher gilt $a_1b_1 \sim_H a_2b_2$ und $a_1b_1H = a_2b_2H$.

Das neutrale Element in G/H ist die Linksnebenklasse $eH = H$ und das inverse Element von aH in G/H ist $a^{-1}H$. Die Assoziativität von G/H folgt aus der Assoziativität von G.

Es gilt $\pi(ab) = abH = (aH)(bH) = \pi(a)\pi(b)$, d.h. π ist ein Gruppenhomomorphismus. □

Definition. Für eine normale Untergruppe $H \triangleleft G$ nennen wir die Gruppe G/H von Linksnebenklassen die *Quotientengruppe* (oder die Faktorgruppe).

Beispiel. Sei $H = n\mathbb{Z} \triangleleft G = \mathbb{Z}$. Die Äquivalenzrelation $\sim_H$ ist

$$a \sim_H b \iff (-a) + b \in n\mathbb{Z} \iff n|b-a$$

und deshalb ist $[a]_n := a + n\mathbb{Z}$ die Äquivalenzklass von $a \in \mathbb{Z}$. Dann gilt

$$\mathbb{Z}/n\mathbb{Z} = \{[0]_n, \cdots, [n-1]_n\}$$

ist eine Gruppe mit Addition modulo n.

Satz 1.3 (Homomorphiesatz)**.** *Sei $\varphi : G \to G'$ ein Gruppenhomomorphismus und H eine normale Untergruppe einer Gruppe G mit $H \subset \ker(\varphi)$. Dann gibt es einen eindeutig bestimmten Gruppenhomomorphismus $\overline{\varphi} : G/H \to G'$ mit $\varphi = \overline{\varphi} \circ \pi$ für $\pi : G \to G/H$. Ferner gilt*

$$\text{Bild}(\varphi) = \text{Bild}(\overline{\varphi}) \quad \textit{und} \quad \ker(\overline{\varphi}) = \pi(\ker(\varphi)).$$

Insbesondere ist $\overline{\varphi}$ genau dann injektiv, wenn $H = \ker(\varphi)$.

Beweisidee. Die Eindeutigkeit von $\overline{\varphi}$ folgt, da $\overline{\varphi}(aH) = \overline{\varphi}(\pi(a)) = \varphi(a)$. Wir definieren $\overline{\varphi}$ durch $\overline{\varphi}(aH) = \varphi(a)$ und wir müssen überprüfen, dass diese Abbildung wohldefiniert ist (d.h. unabhängig der Auswahl des Repräsentants a von aH). Falls $aH = bH$ müssen wir zeigen, dass $\varphi(a) = \varphi(b)$. Aus $aH = bH$ folgt $a^{-1}b \in H \subset \ker(\varphi)$ und deshalb gilt

$$e_G = \varphi(a^{-1}b) = \varphi(a)^{-1}\varphi(b) \quad d.h.\ \varphi(a) = \varphi(b).$$

Die Abbildung $\overline{\varphi}$ ist ein Gruppenhomomorphismus:

$$\overline{\varphi}(aH \cdot bH) = \overline{\varphi}(abH) = \varphi(ab) = \varphi(a)\varphi(b) = \overline{\varphi}(aH)\overline{\varphi}(bH).$$

Es gilt

$$aH \in \ker(\overline{\varphi}) \iff \overline{\varphi}(aH) = \varphi(a) = e_{G'} \iff a \in \ker(\varphi).$$

Da π surjektiv ist, gilt $\text{Bild}(\varphi) = \text{Bild}(\overline{\varphi})$. □

Korollar. Wenn $\varphi : G \to G'$ ein surjektiver Gruppenhomomorphismus ist, dann gibt es einen Isomorphismus $G/\ker(\varphi) \cong G'$.

Satz 1.4 (Erster Isomomorphiesatz)**.** *Sei G eine Gruppe, $H < G$ eine Untergruppe und $N \triangleleft G$ eine normale Untergruppe. Dann ist $HN := \{hn : h \in H, n \in N\} < G$ eine Untergruppe, $N \triangleleft HN$ eine normale Untergruppe, $H \cap N \triangleleft H$ eine normale Untergruppe. Ferner ist der kanonische Gruppenhomomorphismus*

$$H/(H \cap N) \to HN/N$$

ein Isomorphismus.

Beweisidee. Die Normalität von N impliziert $HN < G$: für $h_i n_i \in HN$ gilt $h_1 n_1 h_2 n_2 = (h_1 h_2)(h_2^{-1} n_1 h_2 n_2) \in HN$ und $(h_1 n_1)^{-1} = n_1^{-1} h_1^{-1} = h_1^{-1}(h_1 n_1^{-1} h_1^{-1}) \in HN$. Es gilt $N \triangleleft HN$: für $hn \in HN$ und $n' \in N$ gilt $(hn)n'(hn)^{-1} = hnn'n^{-1}h^{-1} \in N$, weil $N \triangleleft G$.

Wir betrachten $\varphi : H \hookrightarrow HN \twoheadrightarrow HN/N$ für die inklusion und die kanonische surjection $\pi : HN \twoheadrightarrow HN/N$. Der Kern ist

$$\ker(\varphi) = \{h \in H : hN = eN\} = \{h \in H : h \in N\} = H \cap N$$

und deshalb gilt $H \cap N \triangleleft H$. Sei $hnN \in HN/N$ dann gilt $hnN = hN = \varphi(h)$, d.h. φ ist surjektiv. Dann benutzen wir das Korollar des Homomorphiesatzes für φ. □

[23.10.18]

Satz 1.5 (Zweiter Isomomorphiesatz)**.** *Sei G eine Gruppe, $H, N \triangleleft G$ normale Untergruppen mit $N \subset H$. Dann ist $N \triangleleft H$ eine normale Untergruppe und $H/N \triangleleft G/N$ ist eine normale Untergruppe. Ferner ist der kanonische Gruppenhomomorphismus*

$$(G/N)/(H/N) \to G/H$$

ein Isomorphismus.

Beweisidee. Für den Beweis von $N \triangleleft H$: Sei $h \in H$ und $n \in N$, dann gilt $hnh^{-1} \in N$ (da $N \triangleleft G$ und $h \in G$).

Die Komposition $\varphi : H \hookrightarrow G \twoheadrightarrow G/N$ ist ein Gruppenhomomorphismus mit $N = \ker(\varphi)$ und deshalb gibt es eine injektive Gruppenhomomorphismus $\overline{\varphi} : H/N \hookrightarrow G/N$ (d.h. H/N ist eine Untergruppe von G/N). Diese Untergruppe ist normal: für $hN \in H/N$ und $gN \in G/N$ gilt

$$(gN)(hN)(gN)^{-1} = (gN)(hN)(g^{-1}N) = ghg^{-1}N \in H/N$$

weil $ghg^{-1} \in H$ (nach der Normalität der Untergruppe $H \triangleleft G$).

Für $\pi : G \twoheadrightarrow G/H$ wir haben $N \subset H = \ker(\pi)$. Nach dem Satz 1.3 gibt es einen surjektiven Gruppenhomomorphismus $\overline{\pi} : G/N \to G/H$ mit dem Kern $\ker(\overline{\pi}) = \ker(\pi)/N = H/N$. Nach dem Korollar des Satzes 1.3 gibt es einen Isomorphismus $(G/N)/(H/N) \cong G/H$. □

Beispiel. Sei $G = \mathbb{Z}$ und $N = 4\mathbb{Z} \subset H = 2\mathbb{Z}$. Dann gilt $H/N = 2\mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}$ und

$$(\mathbb{Z}/4\mathbb{Z})/(2\mathbb{Z}/4\mathbb{Z}) \cong (\mathbb{Z}/4\mathbb{Z})/(\mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}.$$

1.3. **Erzeugendensysteme und zyklische Gruppen.** Sei G eine Gruppe und sei $S \subset G$ eine Teilmenge von G. Die kleinste Untegruppe von G, die S enthält, wird $< S >$ bezeichnet. Wir sagen, dass S die Gruppe G *erzeugt* (oder S ein *Erzeugendensystem* von G ist), wenn $G =< S >$. Eine *zyklische Gruppe* ist eine Gruppe G, die von einem Element g erzeugt wird (d.h. $G =< g >$).

Bemerkung. Jede zyklische Gruppe ist abelsch.

.

Beispiel.

(1) Die symmetrische Gruppe S_2 ist eine zyklische Gruppe: $S_2 =< \sigma >$, wobei σ das Element von Ordnung 2 ist. Die symmetrische Gruppe S_3 ist keine zyklische Gruppe, aber $S_3 =< \sigma, \tau >$ für ein Element σ von Ordnung 2 und ein Element τ von Ordnung 3.
(2) Sei $n \in \mathbb{N}$ mit $n > 1$. Dann ist $\mathbb{Z}/n\mathbb{Z}$ eine zyklische Gruppe, da $\mathbb{Z}/n\mathbb{Z} =< [1]_n >$.

Lemma. Sei G eine zyklische Gruppe und G' eine Gruppe. Es gilt:

(1) Jede Untergruppe $H < G$ ist zyklische.
(2) Für einen Gruppenhomomorphismus $\varphi : G \to G'$ sind $\ker(\varphi)$ und $\text{Bild}(\varphi)$ zyklische.

Satz 1.6. *Sei G eine zyklische Gruppe. Dann gibt es einen Isomorphismus*

$$G \cong \begin{cases} \mathbb{Z}/n\mathbb{Z} & \text{falls } |G| = n \\ \mathbb{Z} & \text{falls } |G| = \infty \end{cases}$$

Beweisidee. Da $G =< g >$ zyklisch ist, ist die Abbildung $\varphi : \mathbb{Z} \to G$ mit $\varphi(n) = g^n$ ein surjektiver Gruppenhomomorphismus. Der Kern von φ ist eine Untergruppen von $\mathbb{Z}$ (d.h. $\ker(\varphi) = n\mathbb{Z}$ für $n \in \mathbb{N} = \{0, 1, \dots\}$). Falls $|G| = \infty$ gilt $\varphi(n) = g^n \neq e$ für all $n \neq 0$ und deshalb ist $\ker(\varphi) = 0$, also φ ist injektiv und $\mathbb{Z} \cong G$. Falls $|G| = n$ (also $n \geq 1$) dann $g^n = e \implies n \in \ker(\varphi)$ und nach der Minimalität von n folgt $\ker(\varphi) = n\mathbb{Z}$ und $G \cong \mathbb{Z}/n\mathbb{Z}$ nach dem Korollar des Homomorphiesatzes. □

2. Ringe und Polynome

2.1. **Ringe.** Ein *Ring* ist ein Tripel $(R, +, \cdot)$, das aus einer Menge R und zwei Verknüpfungen $+ : R \times R \to R$ ('die Addition') und $\cdot : R \times R \to R$ ('die Multiplikation') besteht, mit den folgenden Eigenschaften (R1-R3).

(R1): Die Menge R mit Addition $(R, +)$ ist eine abelsche Gruppe.
(R2): Die Multiplikation $\cdot$ ist assoziativ.
(R3): Die Distributivgesetze: $\forall a, b, c \in R$ gelten

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{und} \quad (a + b) \cdot c = a \cdot c + b \cdot c.$$

Schreibweise: das neutrale Element für die Addition ist die Null $0_R \in R$.

- $(R, +, \cdot)$ ist *kommutativ*, wenn die Multiplikation kommutativ ist.

- Ein *Ring mit Eins* ist ein Ring $(R, +, \cdot)$ mit einem neutralen Element 1_R für die Multiplikation.
- Ein Element $r \in R$ heißt *Nullteiler*, wenn es $s \in R \setminus \{0_R\}$ mit $rs = 0_R$ oder $sr = 0_R$ gibt. Fall 0_R ist der einzige Nullteiler von R nennen wir R *nullteilerfrei*. Ein nullteilerfrei kommutativer Ring $R \neq \{0_R\}$ heißt *Integritätsbereich*.
- Für einen Ring R mit Eins sei $R^\times := \{r \in R : \exists s \in R \text{ mit } rs = sr = 1_R\}$ die Menge der multiplikativ invertierbaren Elemente. Diese Menge ist eine Gruppe unter Multiplikation (Übung). Ein Element $r \in R^\times$ heißt *Einheit* von R und $R^\times$ heißt die *Einheitsgruppe* von R.

Übung. Für einen Ring mit Eins ist $(R^\times, \cdot)$ ist eine Gruppe.

Beispiel.

(1) $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring mit Eins und ein Integritätsbereich. Die Einheitsgruppe ist $R^\times = \{\pm 1\}$.
(2) Jeder Körper ist ein kommutativer Ring mit Eins und ein Integritätsbereich mit $R^\times = R \setminus \{0\}$.
(3) $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring mit Eins. $\mathbb{Z}/n\mathbb{Z}$ ist genau dann ein Integritätsbereich, wenn n prim ist. Es gilt $(\mathbb{Z}/n\mathbb{Z})^\times = \{[a]_n : 0 < a < n \text{ und } \mathrm{ggT}(a, n) = 1\}$. Insbesondere ist $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ ein Körper für eine Primzahl p.
(4) $(\mathrm{Mat}_{n\times n}(K), +, \cdot)$ ist ein Ring mit Eins, der kommutativ nur für $n = 1$ ist. Die Einheitsgruppe ist $\mathrm{Mat}_{n\times n}(K)^\times = \mathrm{GL}_n(K)$. Dieser Ring ist genau dann ein Integritätsbereich, wenn $n = 1$.
(5) Für einen K-Vektorraum V ist $(\mathrm{End}_K(V), +, \circ)$ ein Ring mit Eins mit $\mathrm{End}_K(V)^\times = \mathrm{Aut}_K(V)$.

Definition. Seien $(R, +_R, \cdot_R)$ und $(S, +_S, \cdot_S)$ Ringe. Ein Ringhomomorphismus ist eine Abbildung $\varphi : R \to S$, so dass für $r_1, r_2 \in R$:

(1) $\varphi(r_1 +_R r_2) = \varphi(r_1) +_S \varphi(r_2)$,
(2) $\varphi(r_1 \cdot_R r_2) = \varphi(r_1) \cdot_S \varphi(r_2)$,
(3) (Falls R und S Ringe mit Eins sind) $\varphi(1_R) = 1_S$.

Beispiel. Für $n > 1$ ist die Abbildung $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ mit $a \mapsto [a] := a + n\mathbb{Z}$ ein Ringhomomorphismus.

Bemerkung. Für einen Ringhomomorphismus $\varphi : R \to S$ gilt

(1) $\varphi(0_R) = \varphi(0_S)$ (nach dem ersten Axiom),
(2) $\varphi(-r) = -\varphi(r)$ für $r \in R$ (nach dem ersten Axiom),
(3) Die dritte Bedingung $\varphi(1_R) = \varphi(1_S)$ folgt nicht aus den anderen Axiomen (z.B. Seien $R = \{0\}$ und $S = \mathbb{Z}$, dann gelten die erste und zweite Bedingungen für die Nullabbildung $\varphi : R \to S$, aber $\varphi(1_R) = \varphi(0_R) = 0_\mathbb{Z} \neq 1_\mathbb{Z}$).
(4) φ ist genau dann injektiv, wenn $\ker(\varphi) = \{0_R\}$ (nach dem ersten Axiom),
(5) Wenn φ bijektiv ist, dann ist $\varphi^{-1} : S \to R$ auch ein Ringhomomorphismus.

Definition. Ein *Körper* ist ein Tripel $(K, +, \cdot)$, das aus einer Menge K und zwei Verknüpfungen $+ : K \times K \to K$ ('die Addition') und $\cdot : K \times K \to K$ ('die Multiplikation') besteht, mit den folgenden Eigenschaften (K1-K3).

(K1): $(K, +)$ ist eine abelsche Gruppe (mit neutralem Element $0_K \in K$).
(K2): $(K \setminus \{0_K\}, \cdot)$ ist eine abelsche Gruppe (mit neutralem Element $1_K \in K^\times$).
(K3): Die Distributivgesetze: $\forall a, b, c \in K$ gelten

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{und} \quad (a + b) \cdot c = a \cdot c + b \cdot c.$$

Beispiel. $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ sind Körper.

Polynomringe. Sei R ein Ring. Wir definieren [25.10.18]

$$R[t] := \{(a_i)_{i\geq 0} : a_i \in R, a_i = 0 \text{ für fast alle } i \in \mathbb{N}\} \subset \mathrm{Abb}(\mathbb{N}, R).$$

Sei $(a_i)_{i\geq 0} \in K[t]$ dann gibt es $n \in \mathbb{N}$ so dass $a_i = 0$ für alle $i > n$. Dann definiert diese Folge ein *Polynom* in eine Variabel t

$$f(t) = a_0 + a_1 t + \cdots + a_n t^n$$

mit Koeffizienten $a_i \in R$. Das Nullpolynom 0 ist das Polynom, dessen Koeffizienten alle Null sind. Der *Grad* eines Polynoms $f(t) = a_0 + \cdots + a_n t^n$ ist

$$\mathrm{grad}(f) := \begin{cases} -\infty & \text{falls } f \equiv 0, \\ \max\{m : a_m \neq 0\} & \text{sonst.} \end{cases}$$

Deshalb ist $R[t]$ die Menge aller Polynome.

Man kann Polynome miteinander addieren und multiplizieren: Seien $f, g \in R[t]$

$$f(t) = \sum_{i=0}^{n} a_i t^i = a_0 + a_1 t + \cdots + a_n t^n \quad \text{und} \quad g(t) = \sum_{j=0}^{m} b_j t^j = b_0 + b_1 t + \cdots + b_m t^m.$$

Dann

$$(f+g)(t) := \sum_{i=0}^{n} a_i t^i + \sum_{j=0}^{m} b_j t^j = \sum_{l=0}^{\max\{n,m\}} (a_l + b_l) t^l,$$

wobei $a_l = 0$ für $l > n$ und $b_l = 0$ für $l > m$, und

$$(f \cdot g)(t) = \sum_{l=0}^{n+m} c_l t^l, \quad \text{wobei } c_l = \sum_{\substack{i,j \\ i+j=l}} a_i b_j.$$

Die Addition auf $R[t]$ ist assoziativ und kommutativ, weil die Addition auf R assoziativ und kommutativ ist. Die Multiplikation auf $R[t]$ ist assoziativ (und kommutativ, falls R kommutativ ist). Das Nullpolynom ist ein neutrales Element für die Addition und wenn R ein Ring mit Eins ist, dann ist das Polynom $1(t) = 1$ ein neutrales Element für die Multiplikation. Das Polynom $f(t) = \sum_{i=0}^{n} a_i t^i$ hat das additiv inverse Element $-f(t) = \sum_{i=0}^{n} (-a_i) t^i$. Ferner gelten die Distributivgesetze. Deshalb ist $R[t]$ ein Ring. Es gilt

- $\mathrm{grad}(f+g) \leq \max(\mathrm{grad}(f), \mathrm{grad}(g))$,
- $\mathrm{grad}(fg) \leq \mathrm{grad}(f) + \mathrm{grad}(f)$ (mit Gleichheit für einen Integritätsbereich R).

Bemerkung.

(1) Wenn R ein kommutativer Ring (bzw. mit Eins) ist, dann ist $R[t]$ ein kommutativer Ring (bzw. mit Eins).
(2) Es gibt einen injektiven Ringhomomorphismus $R \hookrightarrow R[t]$ mit $r \mapsto f(t) = r$ (das konstante Polynoma).
(3) Wenn $R \hookrightarrow R'$ ein injektiver Ringhomomorphismus ist, dann gibt es einen injektiven Ringhomomorphismus $R[t] \hookrightarrow R'[t]$. Zum Biespiel

$$\mathbb{Z}[t] \subset \mathbb{Q}[t] \subset \mathbb{R}[t] \subset \mathbb{C}[t].$$

(4) Für einen Integritätsbereich R gilt $R[t]^\times = R^\times$, da $f(t)g(t) = 1 \implies \mathrm{grad}(f) + \mathrm{grad}(g) = \mathrm{grad}(1) = 0$ und deshalb sind f und g konstant.
(5) Wenn R ein Integritätsbereich ist, dann ist $R[t]$ auch ein Integritätsbereich.

Erinnerung: (Division mit Rest in $\mathbb{Z}$) Für $a, b \in \mathbb{Z}$ mit $b > 0$ gibt es eindeutig bestimmte Zahlen $q, r \in \mathbb{Z}$ mit $a = bq + r$ und $0 \leq r < b$.

Satz 2.1 (Division mit Rest für Polynomringe)**.** *Sei R ein kommutativer Ring mit Eins und $f, g \in R[t]$ mit* $\operatorname{grad}(g) = m \geq 0$ *und der höchste Koeffizient b_m von g ist ein Einheit (d.h. $b_m \in R^\times$). Dann gibt es eindeutige bestimmte Polynome $q, r \in R[t]$ mit $f = gq + r$ und* $\operatorname{grad}(r) < \operatorname{grad}(g)$.

Beweisidee. Eindeutigkeit: Übung.

Existenz: Falls $\operatorname{grad}(f) < \operatorname{grad}(g)$, setzen wir $r := f$ und $q := 0$. Falls $n := \operatorname{grad}(f) \geq m := \operatorname{grad}(g) \geq 0$ beweisen wir die Existenz durch Induktion über n. Der Induktionsanfang $(n = m = 0)$ gilt, da für konstante Polynome $f(t) = a$ und $g(t) = b$ mit $b \in R^\times$ gilt $a = qb$ mit $q = a/b$ (da b invertierbar für die Multiplikation ist). Für den Induktionsschritt: wenn

$$f(t) = \sum_{i=0}^{n} a_i t^i = a_0 + a_1 t + \cdots a_n t^n \quad \text{und} \quad g(t) = \sum_{j=0}^{m} b_j t^j = b_0 + b_1 t + \cdots b_m t^m$$

mit $a_n \neq 0$ und $b_m \neq 0$ und $b_m \in R^\times$, dann ist der Grad von $f_1 := f - \frac{a_n}{b_m} t^{n-m} \cdot g$ kleiner als der Grad von f. Nach der Induktionsvoraussetzung kann man die Division durch g von f_1 durchführen, so dass $\exists q', r \in R[t]$ mit $f_1 = gq' + r$ und $\operatorname{grad}(r) < \operatorname{grad}(g)$. Dann gilt $f = gq + r$ für $q := q' + \frac{a_n}{b_m} t^{n-m}$. □

Bemerkung. Wenn $R = K$ ein Körper ist, dann funktioniert Division mit Rest für alle $f, g \in K[t]$ mit $g \neq 0$ (da $K^\times = K \setminus \{0\}$).

2.2. **Ideale und Quotientenringe.** In diesem Abschnitt ist R ein kommutativer Ring. Wir werden Ideale einführen, um Quotientenringe zu definieren. Wir werden sehen, dass der Kern eines Ringhomomorphismuses ein Ideal ist und dann werden wir einen Homomorphiesatz für Ringe beweisen.

Definition. Sei $(R, +, \cdot)$ ein kommutative Ring.

a) Ein *Unterring* von R ist eine Teilmenge $S \subset R$, so dass S unter die Addition und Multiplikation abgeschlossen ist und S mit der Einschränkung der Addition und Multipliktation von R ein Ring ist (Wenn R ein Ring mit Eins ist, soll ein Unterring S auch das neutralelement 1_R erhalten).
b) Ein *Ideal* von R ist eine Teilmenge $I \subset R$, so dass (I1) - (I2) gelten:
   (I1) I ist eine Untergruppe von $(R, +)$,
   (I2) Für $i \in I$ und $r \in R$ gilt $r \cdot i \in I$.

Ein Unterring $S \subset R$ (bzw. Ideal $I \subset R$) heißt *echt* wenn $S \neq R$ (bzw. $I \neq R$).

Bemerkung.

(1) Eine Teilmenge S eines Rings R ist genau dann ein Unterring, wenn S unter die Subtraktion $-$ und die Multiplikation $\cdot$ abgeschlossen ist (und $1 \in S$ falls R Ring mit Eins ist).
(2) Für einen nicht kommutativen Ring gibt es Begriffe von Links- und Rechtsideale. In einem kommutativen Ring stimmen die Recht- und Linksideale überein.
(3) Ein Ideal ist eine Untergruppe von $(R, +)$, die unter Multiplikation von Elemente aus R abgeschlossen ist. Insbesondere ist I unter $+$, $-$ und $\cdot$ abgeschlossen.

Beispiel.

(1) R und $\{0_R\}$ sind immer Ideale von R. Wenn $R \neq \{0_R\}$ ein Ring mit Eins ist, dann ist $\{0_R\}$ kein Unterring von R.
(2) Sei I ein Ideal eines Rings mit Eins R. Wenn $1_R \in I$, folgt $I = R$.
(3) Der Ring $R = \mathbb{Z}$ hat keine echten Unterringe: die Untergruppen von $(\mathbb{Z}, +)$ sind genau die Teilmengen $n\mathbb{Z}$ für $n \in \mathbb{N}$, aber $1 \in n\mathbb{Z}$ genau dann, wenn $n = 1$. Allerdings sind die Untergruppen $n\mathbb{Z}$ Ideale: für $r \in \mathbb{Z}$ und $na \in n\mathbb{Z}$ gilt

$$r \cdot na = n(ra) \in n\mathbb{Z}.$$

(4) Die Teilmenge $\mathbb{Z}$ des Rings $(\mathbb{Q}, +, 0)$ ist ein Unterring aber kein Ideal: $1 \in \mathbb{Z}$ und $\frac{1}{2} \in \mathbb{Q}$, aber $\frac{1}{2} \cdot 1 \notin \mathbb{Z}$).

Übung. Sei $R \neq \{0\}$ ein kommutativer Ring mit Eins. Beweisen Sie, dass R genau dann ein Körper ist, wenn R genau 2 Ideale hat.

Definition. Sei R ein kommutativer Ring mit Eins[3].

(1) Für $a \in R$ definieren wir das *von a erzeugte Ideal*
$$(a) = Ra := \{r \cdot a : r \in R\}.$$
Ideale von R der Form (a) werden *Hauptideale* genannt.
(2) Für eine Teilmenge $A \subset R$ definieren wir das *von A erzeugte Ideal*
$$(A) = \{\sum_{i=1}^{n} r_i a_i : n \in \mathbb{N}, r_i \in R, a_i \in A\}.$$
(3) Ein Integritätsbereich heißt *Hauptidealring*, wenn jedes Ideal von R ein Hauptideal ist.

Beispiel.

(1) Es gilt $(0_R) = \{0_R\}$ und falls $1_R \in R$ gilt $(1_R) = R$.
(2) Für $R = \mathbb{Z}$ ist $(n) = n\mathbb{Z}$. Insbesondere ist $\mathbb{Z}$ ein Hauptidealring.

Übung. Der Durchschnitt einer Familie von Idealen eines kommutativen Rings R ist ein Ideal. Für eine Teilmenge A eines kommutativen Rings mit Eins R ist die Menge (A) ein Ideal von R mit $A \subset (A)$. Ferner gilt
$$(A) = \bigcap_{\substack{A \subset J \subset R \\ J \text{ Ideal}}} J,$$
und (A) ist das kleinste Ideal in R, das A enthält.

Definition. Für zwei Ideale I und J eines kommutativen Rings mit Eins R definieren wir

a) $I + J := \{i + j : i \in I, j \in J\}$ und
b) $I \cdot J := (IJ) = (\{i \cdot j : i \in I, j \in J\})$.

Bemerkung. Es gilt
$$I \cdot J := \left\{ r \in R : \exists n \in \mathbb{N} \text{ und } i_l \in I, j_l \in J \text{ für } 1 \leq l \leq n \text{ mit } r = \sum_{l=1}^{n} i_l j_l \right\}.$$

Lemma. Für zwei Ideale I und J eines kommutativen Rings mit Eins R sind $I + J$ und $I \cdot J$ Ideale von R. Es gilt $I + J = (I \cup J)$ und $I \cdot J \subset I \cap J$.

[30.10.18]

Beispiel. Für $R = \mathbb{Z}$ und $n, m \in \mathbb{Z}$ gilt:

a) $(m) \subset (n) \iff n | m$,
b) $(m) + (n) = (\text{ggT}(n, m))$,
c) $(m) \cdot (n) = (mn)$,
d) $(m) \cap (n) = (\text{kgV}(n, m))$,
e) $(n) + (m) = \mathbb{Z} \iff (n) \cdot (m) = (n) \cap (m)$.

Lemma. Sei R ein Integritätsbereich und (a) und (b) zwei Hauptideale von R. Dann
$$(a) = (b) \iff \exists c \in R^\times \text{ mit } a = cb.$$

[3]Die Definition für nicht kommutative Ringe und Ringe ohne Eins ist ein bisschen mehr kompliziert

Definition Die Relation auf einem Integritätsbereich R

$$a \sim b \iff \exists c \in R^\times \text{ mit } a = cb$$

ist eine Äquivalenzrelation (Übung). Diese Relation heißt *Assoziiertheit*.

Übung. $\mathbb{Z}[t]$ ist kein Hauptidealring. Man hat die folgende Ideale:

$$(2) = \{\sum a_i t^i \in \mathbb{Z}[t] : a_i \in 2\mathbb{Z}\ \forall i\} \quad \text{und} \quad (t) = \{\sum a_i t^i \in \mathbb{Z}[t] : a_0 = 0\}$$

aber $(2,t) := \{\sum a_i t^i \in \mathbb{Z}[t] : a_0 \in 2\mathbb{Z}\}$ ist kein Hauptideal.

Satz 2.2. *Seien R und S kommutative Ringe mit Eins und $\varphi : R \to S$ ein Ringhomomorphismus. Dann gilt*

(1) Das Bild von φ ist ein Unterrring von S.
(2) Für einen Unterring $R' \subset R$ ist $\varphi(R')$ ein Unterring von S.
(3) Der Kern $\ker(\varphi)$ ist ein Ideal von R.
(4) Für ein Ideal $J \subset S$ ist das Urbild $\varphi^{-1}(J)$ ein Ideal von R.

Beweisidee. Es ist hinreichend nur (2) und (4) zu beweisen. Beide sind ähnlich, und deshalb schreiben wir den Beweis nur für (4). Da das Ideal $J \subset S$ eine Untergruppe für die Addition ist und φ ein Gruppenhomomorphismus ist, ist $\varphi^{-1}(J) < (R, +_R)$ eine Untergruppe. Für $r \in R$ und $r' \in \varphi^{-1}(J)$ (d.h. $\varphi(r') \in J$) gilt $r \cdot_R r' \in \varphi^{-1}(J)$, weil

$$\varphi(r \cdot_R r') = \varphi(r) \cdot_S \varphi(r') \in J$$

nach dem Axiom $(I2)$ für das Ideal $J \subset S$. □

Beispiel.

(1) Für den Ringhomomorphismus $\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ mit $a \mapsto [a] = a + n\mathbb{Z}$ ist

$$\ker(\varphi) = \{a \in \mathbb{Z} : a \equiv 0 \mod n\} = n\mathbb{Z}.$$

und $\text{Bild}(\varphi) = \mathbb{Z}/n\mathbb{Z}$.

(2) Sei K ein Körper und $\lambda \in K$. Dann ist die Abbildung $\varphi : K[t] \to K$ mit

$$\varphi(P(t)) = P(\lambda)$$

ein surjetiver Ringhomomorphismus mit

$$\ker(\varphi) = \{P(t) \in K[t] : P(\lambda) = 0\} = \{P(t) \in K[t] : (t-\lambda) | P(t)\} = (t-\lambda).$$

Satz 2.3. *Sei I ein Ideal eines kommutativen Rings R. Dann gilt*

(1) Die Menge $R/I := \{r + I : r \in R\}$ ist ein Ring (ein Quotientenring*) mit den folgenden Addition und Multiplikation:*

$$(r+I) +_{R/I} (r'+I) := r + r' + I \quad \text{und} \quad (r+I) \cdot_{R/I} (r'+I) = r \cdot r' + I$$

und das Nullelement ist $0_R + I = I$.
(2) Wenn R ein Ring mit Eins ist, dann ist R/I ein Ring mit Eins.
(3) Die Abbildung $\pi : R \to R/I$, die durch $r \mapsto r + I$ definiert wird, ist ein surjektiver Ringhomomorphismus mit $\ker(\pi) = I$.
(4) Die Abbildung

$$\begin{array}{rccc} \alpha: & \mathcal{A} := \{\text{Ideale } J \text{ von } R/I\} & \to & \mathcal{B} := \{\text{Ideale } M \text{ von } R \text{ mit } I \subset M\} \\ & J & \mapsto & \pi^{-1}(J) \end{array}$$

ist bijektiv mit der Umkehrfunktion $M \mapsto \pi(M)$.

Beweisidee. Da $(R,+)$ eine abelsche Gruppe ist, ist $I < (R,+)$ eine normale Untergruppe. Deshalb ist $(R/I, +_{R/I})$ eine abelsche Gruppe und $\pi : R \to R/I$ ein Gruppenhomomorphismus (unter Addition).

Die Multiplikation $\cdot_{R/I}$ ist wohldefiniert (d.h. unabhängig der Wahl des Repräsentant): falls $r = s + i$ und $r' = s + i'$ mit $i, i' \in I$ gilt

$$rr' - ss' = (s+i)(s'+i') - ss' = is' + si' \in I$$

also $rr' + I = ss' + I$. Die Assoziativität von $\cdot_{R/I}$ und die Distributivegesetze folgt von R. Deshalb ist R/I ein Ring und wenn $1 \in R$, ist $1 + I$ das neutrale Element für die Multiplikation auf R/I.

Der Gruppenhomomorphismus $\pi : R \to R/I$ ist auch ein Ringhomomorphismus

$$\pi(r \cdot s) = r \cdot s + I = (r + I) \cdot_{R/I} (s + I) = \pi(r) \cdot_{R/I} \pi(s)$$

und falls $1 \in R$, gilt $\pi(1) = 1 + I = 1_{R/I}$.

Für (4): Die Abbildung α ist wohldefiniert (in diesem Fall d.h. $\alpha(J) \in \mathcal{B}$ für alle $J \in \mathcal{A}$): $\pi^{-1}(J) \subset R$ ist ein Ideal (Satz 2.2) und $I = \ker(\pi) = \pi^{-1}(0_{R/I}) \subset \pi^{-1}(J)$, da $0_{R/I} \in J$. Wir behaupten, dass die Abbildung $\beta : \mathcal{B} \to \mathcal{A}$ mit $\beta(M) := \pi(M)$ eine Umkehrfunktion von α ist. Zuerst ist β wohldefiniert (d.h. $\beta(M) \in \mathcal{A}$ für alle $M \in \mathcal{B}$): das Bild $\pi(M) < (R/I, +)$ ist eine Untergruppe (da π ein Gruppenhomomorphismus ist) und für $r + I \in R/I$ und $m + I \in \pi(M)$ gilt

$$(r + I) \cdot_{R/I} (m + I) = rm + I \in \pi(M),$$

da $M \subset R$ ein Ideal ist. Deshalb ist $\pi(M)$ ein Ideal von R/I. Wegen der Surjektivität von π gilt $\beta \circ \alpha(J) = \pi(\pi^{-1}(J)) = J$ für $J \in \mathcal{A}$. Für $M \in \mathcal{B}$ gilt $\alpha \circ \beta(M) = \pi^{-1}(\pi(M)) \supset M$ und wir behaupten, die andere Inklusion gilt. Sei $r \in \pi^{-1}(\pi(M))$, d.h. $r + I = m + I$ für $m \in M$. Dann gilt $r - m \in I \subset M$ und $r = m + (r - m) \in M$. □

Beispiel. Für $R = \mathbb{Z}$ und $I = n\mathbb{Z}$ mit $n \in \mathbb{N}$ ist $\mathbb{Z}/n\mathbb{Z} = \{x + n\mathbb{Z} : x \in \mathbb{Z}\} \cong \mathbb{Z}_n$. Die Ideale von $\mathbb{Z}/n\mathbb{Z}$ sind genau die Mengen

$$\pi(m\mathbb{Z}) = \{x + n\mathbb{Z} : x \in m\mathbb{Z}\}$$

für $m|n$. Insbesondere ist $\mathbb{Z}/p\mathbb{Z}$ ein Körper für eine Primzahl p (weil $\mathbb{Z}/p\mathbb{Z}$ nur zwei Ideale hat).

Beispiel. Sei $R = \mathbb{F}_2[t]$ und $I = (f)$ wobei $f = t^2 + t + 1 \in \mathbb{F}_2[t]$. Für $P \in \mathbb{F}_2[t]$ betrachten wir die Linksnebenklasse $P + (f) \in \mathbb{F}_2[t]/(f)$. Nach Division mit Rest für Polynome gibt et $Q, R \in \mathbb{F}_2[t]$ mit $P = Qf + R$ und $\operatorname{grad}(R) < \operatorname{grad}(f) = 2$. Es gibt 4 Möglichkeiten für den Rest: 0, 1, t oder $t + 1$. Ferner gilt $P - R = Qf \in (f)$, also $P + (f) = R + (f)$. Deshalb hat der Quotientenring

$$\mathbb{F}_2[t]/(f) = \{0 + (f), 1 + (f), t + (f), t + 1 + (f)\}$$

4 Elementen. Dieser Ring ist ein Körper: das multiplikative inverse Element von $t + (f)$ ist $t + 1 + (f)$, da $(t + (f)) \cdot (t + 1 + (f)) = t^2 + 2 + (f) = 1 + (f)$.

Satz 2.4. *(Homomorphiesatz für Ringe) Sei $\varphi : R \to S$ ein Ringhomomorphismus zwischen kommutativen Ringen. Dann gibt es einen Ringisomorphismus* [1.11.18]

$$\bar{\varphi} : R/\ker(\varphi) \to \varphi(R)$$

mit $\bar{\varphi} \circ \pi = \varphi$, wobei $\pi : R \to R/\ker(\varphi)$ der natürliche surjektive Ringhomomorphismus ist.

Beweisidee. Da $\varphi : (R,+) \to (S,+)$ ein Gruppenhomomorphismus ist, gibt es einen Gruppenisomorphismus $\bar{\varphi} : R/\ker(\varphi) \to \varphi(R)$ für die Addition mit $\bar{\varphi} \circ \pi = \varphi$. Man überprüft, dass $\bar{\varphi}$ auch ein Ringhomomorphismus ist. □

Beispiel. Für den Polynomring $R[t]$ und ein Polynom $f \in R[t]$ kann man das Hauptideal $I = (f)$ betrachten und den Ring $R[t]/(f)$ konstruieren. Mit dieser Konstruktion werden wir neue Körper bauen (siehe Satz 2.13).

(1) Es gilt $\mathbb{R}[t]/(t^2+1) \cong \mathbb{C}$. Der surjektive Ringhomomorphismus $\varphi : \mathbb{R}[t] \to \mathbb{C}$ mit $f(t) \mapsto f(i)$ hat Kern $\ker(\varphi) = (t^2+1)$.
(2) Für $d \in \mathbb{Z}$ quadratfrei (d.h. $n^2 \nmid d$ für $n > 1$) gilt $\mathbb{Z}[t]/(t^2-d) = \mathbb{Z}[\sqrt{d}] := \{a + \sqrt{d}b : a, b \in \mathbb{Z}\}$. Falls $d > 0$ gibt es $\sqrt{d} \in \mathbb{R}$ und $\mathbb{Z}[\sqrt{d}] \subset \mathbb{R}$. Falls $d < 0$ gibt es $\sqrt{d} \in \mathbb{C}$ und $\mathbb{Z}[\sqrt{d}] \subset \mathbb{C}$.

Definition. Zwei Ideale I und J eines kommutativen Rings mit Eins R heißen relativ prim, wenn $I + J = R$.

Lemma. Seien $I_1, \cdots I_n$ Ideale eines kommutativen Rings mit Eins R, so dass I_j und I_k relativ prim für $1 \leq j < k \leq n$ sind. Dann gilt

$$\prod_{k=1}^{n} I_k = \bigcap_{k=1}^{n} I_k.$$

Beweisidee. Wir wissen schon, dass $\prod_{k=1}^n I_k \subset \bigcap_{k=1}^n I_k$ und man zeigt $\bigcap_{k=1}^n I_k \subset \prod_{k=1}^n I_k$ durch Induktion nach $n \geq 2$.

Für den Induktionsanfang: Seien I_1, I_2 relativ prim. Dann gilt $1 = i_1 + i_2$ mit $i_i \in I_j$. Sei $a \in I_1 \cap I_2$. Dann gilt $a = a \cdot 1 = ai_1 + ai_2 \in I_1 \cdot I_2$.

Für den Induktionsschritt ($n \to n+1$): Seien $I_1, \ldots, I_{n+1}$ paarweise relativ prim. Es ist hinreichend zu zeigen, dass $J := \prod_{i=1}^n I_i$ und I_{n+1} relativ prim sind (da $J = \cap_{i=1}^n I_i$ nach der Induktionsvoraussetzung und dann gilt $J \cdot I_{n+1} = J \cap I_{n+1}$). Für alle $1 \leq j \leq n$ gilt $R = I_j + I_{n+1}$, also gibt es $r_j \in I_j$ und $s_j \in I_{n+1}$ mit $1 = r_j + s_j$. Dann gilt

$$J \ni r := \prod_{j=1}^{n} r_j = \prod_{j=1}^{n} (1 - s_j) = 1 - s$$

wobei $s = 1 - \prod_{j=1}^n (1 - s_j) \in I_{n+1}$. Deshalb gilt $1 = r + s$ und $J + I_{n+1} = R$. □

Bemerkung. Seien $I_1, \cdots I_n$ Ideale eines Rings R. Dann gibt es surjektive Ringhomomorphismen $\pi_k : R \to R/I_k$, mit $\pi_k(a) = a + I_k$ für $1 \leq k \leq n$. Das kartesische Produkt $R/I_1 \times \cdots \times R/I_n$ hat die Struktur eines kommutativen Rings mit Eins, wobei für $\star = +$ und $\star = \cdot$

$$(a_1 + I_1, \ldots, a_n + I_n) \star (b_1 + I_1, \ldots, b_n + I_n) := (a_1 \star b_1 + I_1, \ldots, a_n \star b_n + I_n).$$

Die Abbildung

$$\begin{array}{rccc} \varphi : & R & \to & R/I_1 \times \cdots R/I_n \\ & r & \mapsto & (r + I_1, \cdots, r + I_n) \end{array}$$

ist ein Ringhomomorphismus mit $\ker(\varphi) := \{r \in R : r + I_k = I_k \text{ für } 1 \leq k \leq n\} = \cap_{k=1}^n I_k$. Deshalb ist die Abbildung

$$\tilde{\varphi} : R/\cap_{k=1}^n I_k \to R/I_1 \times \cdots R/I_n$$

ein injektiver Ringhomomorphismus.

Satz 2.5 (Chinesischer Restsatz)**.** *Seien $I_1, \cdots I_n$ Ideale eines kommutativen Rings R mit Eins, so dass I_j und I_k relativ prim für $1 \leq j < k \leq n$ sind. Dann gibt es einen Ringisomorphismus*

$$\tilde{\varphi} : R/\prod_{k=1}^{n} I_k \to R/I_1 \times \cdots R/I_n$$

Beweisidee. Nach dem obigen Lemma gilt $\prod_{k=1}^n I_k = \cap_{k=1}^n I_k$ und in der Bemerkung haben wir schon einen injektiven Ringhomomorphismus $\tilde{\varphi}$ konstruiert.

Um der Surjektivität von $\tilde{\varphi}$ zu überprüfen, ist es hinreichend zu zeigen, dass $f_1, \cdots, f_n \in \text{Bild}(\tilde{\varphi})$, wobei

$$f_j = (0 + I_1, \ldots, 0 + I_{j-1}, 1 + I_j, 0 + I_{j+1}, \ldots, 0 + I_n) \in R/I_1 \times \cdots R/I_n$$

(da $\tilde{\varphi}$ ein Ringhomomorphismus ist). Es gilt $f_j \in \text{Bild}(\tilde{\varphi})$, wenn es $a_j \in R$ mit

$$a_j + I_j = 1 + I_j \quad \text{und} \quad \forall k \neq j a_j + I_k = 0 + I_k$$

gibt (d.h. $a_j - 1 \in I_j$ und $a_j \in I_k$ für alle $k \neq j$). Aus $I_k + I_j = R$ für alle $k \neq j$ folgt $1 = s_k + r_k$ mit $s_k \in I_k$ und $r_k \in I_j$. Sei $a_j = \prod_{k \neq j} s_k$. Dann gilt $a_j \in I_k$ für alle $k \neq j$. Ferner gilt

$$a_j = \prod_{k \neq j} (1 - r_k) = 1 + \tilde{r_j}$$

wobei $\tilde{r_j} = \prod_{k \neq j}(1 - r_k) - 1 \in I_j$. Deshalb folgt $a_j - 1 = \tilde{r_j} \in I_j$ und $f_j \in \text{Bild}(\tilde{\varphi})$. □

Korollar. Sei $a = p_1^{m_1} \cdots p_n^{m_n}$ die Primzerlegung einer ganzen Zahl $a \in \mathbb{Z}$. Dann gilt

$$\mathbb{Z}/(a) \cong \mathbb{Z}/(p_1^{m_1}) \times \cdots \times \mathbb{Z}/(p_n^{m_n}).$$

Für $b_1, \cdots, b_n \in \mathbb{Z}$ gibt es $b \in \mathbb{Z}$ mit $b \equiv b_k \mod p_k^{m_k}$ für $1 \leq k \leq n$ und die Zahl b ist eindeutig modulo $a = p_1^{m_1} \cdots p_n^{m_n}$.

Bemerkung. Seien $r_1, \ldots, r_n$ ganze Zahlen mit $\text{ggT}(r_i, r_j) = 1$ für alle $i \neq j$. Für Zahlen $b_1, \ldots, b_n \in \mathbb{Z}$ hat die Gleichungen

$$\begin{cases} x \equiv b_1 \mod r_1 \\ \vdots \\ x_n \equiv b_n \mod r_n \end{cases}$$

eine eindeutig bestimmte Lösung x modulo $\prod_{i=1}^n r_i$. Um eine solche Lösung konkret zu konstruieren, sei $q_k := \prod_{i \neq k} r_i$ für $1 \leq k \leq n$. Wegen $\text{ggT}(q_k, r_k) = 1$ gibt es Zahlen $s_k, t_k \in \mathbb{Z}$ mit

$$s_k q_k + t_k r_k = 1$$

d.h. $s_k q_k \equiv 1 \mod r_k$ und für $i \neq k$ gilt es $s_k q_k \equiv 0 \mod r_i$, da $r_i | q_k$ für alle $i \neq k$. Dann ist

$$x = \sum_{k=1}^{n} b_k s_k q_k$$

eine Lösung.

[6.11.18]

2.3. **Primfaktorzerlegung.** In diesem Abschnitt ist R ein kommuativer Ring mit Eins.

Definition. Ein echtes Ideal I von R heißt

(1) *maximal*, wenn es für jedes Ideal J von R mit $I \subset J$ gilt $J = I$ oder $J = R$.
(2) *Primideal*, wenn es für alle $a, b \in R$ gilt: $a \cdot b \in I \implies a \in I$ oder $b \in I$.

Bemerkung. Das Nullideal $\{0\}$ ist geanu dann ein Primideal (bzw. maximales Ideal), wenn R ein Integritätsbereich (bzw. Körper) ist.

Beispiel. Die Primideale von $\mathbb{Z}$ sind die Ideale $p\mathbb{Z}$ für Primzahlen $p \in \mathbb{Z}$ und $0\mathbb{Z}$. Die maximale Ideale sind die Ideale $p\mathbb{Z}$ für Primzahlen p.

Satz 2.6. *Sei $I \subset R$ ein Ideal. Dann gilt*

(1) I ist genau dann ein maximales Ideal, wenn R/I ein Körper ist
(2) I ist genau dann ein primes Ideal, wenn R/I ein Integritätsbereich ist

Insbesondere ist jedes maximale Ideal $I \subset R$ ein Primideal.

Beweisidee. (1) Nach dem Satz 2.3 gibt es eine Bijektion

$$\{\text{Ideale von } R/I\} \cong \{\text{Ideale } J \text{ von } R \text{ mit } I \subset J\}.$$

R/I ist genau dann ein Körper, wenn es genau 2 Ideale hat. R/I hat genau 2 Ideale, wenn es genau 2 Ideale J von R mit $I \subset J$ gibt (nämlich $J = I$ und $J = R$), d.h. wenn I maximal ist.

(2) Für $a \in R$ ist äquivalent: $a \in I \iff a + I = 0_{R/I}$. Dann folgt Aussage (2) nach der Definitionen. □

Definition. Sei R ein Integritätsbereich und $\delta : R \setminus \{0\} \to \mathbb{N}$ eine Abbildung. Dann heißt (R, δ) ein *Euklidischer Ring*, wenn für alle $f, g \in R$ mit $g \neq 0$ es $q, r \in R$ mit

$$f = gq + r \quad \text{und} \quad \delta(r) < \delta(g) \ \text{ falls } \ r \neq 0$$

gibt.

Beispiel.

(1) Sei K ein Körper und $\delta : K \setminus \{0\} \to \mathbb{N}$ beleibig, dann ist (K, δ) ein Euklidischer Ring.
(2) $(\mathbb{Z}, |-|)$ ist ein Euklidischer Ring.
(3) Für einen Körper K ist $(K[t], \text{grad}(-))$ ein Euklidischer Ring.

Beispiel. (Der Ring der ganzen Gaußschen Zahlen) Die Teilmenge

$$\mathbb{Z}[i] := \{a + ib : a, b \in \mathbb{Z}\} \subset \mathbb{C}$$

ist ein Unterring. Der Ring $\mathbb{Z}[i]$ heißt der Ring der ganzen Gaußschen Zahlen. Mit der Abbiluding $\delta : \mathbb{Z}[i] \setminus \{0\} \to \mathbb{N}$

$$\delta(a + ib) = |a + ib|^2 = a^2 + b^2$$

ist $\mathbb{Z}[i]$ ein Euklidischer Ring (Übung).

Bemerkung: $\mathbb{Z}[\sqrt{d}]$. Sei $d \in \mathbb{Z} \setminus \{0, 1\}$, die quadratfrei ist (d.h. $n^2 \nmid d$ für alle $n \in \mathbb{N}$ mit $n > 1$). Es gibt $\sqrt{d} \in \mathbb{C}$ und wir definieren den Unterring

$$\mathbb{Z}[\sqrt{d}] := \{a + \sqrt{d}b : a, b \in \mathbb{Z}\} \subset \mathbb{C}$$

Für $d = -1$ ist $\mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i]$ wie oben. Im Allgemeinen ist $\mathbb{Z}[\sqrt{d}]$ nicht Euklidisch für $\delta(a + \sqrt{d}b) := a^2 + db^2$ (siehe Bosch §2.4, S.45).

Satz 2.7. *Jeder Euklidische Ring ist ein Hauptidealring.*

Beweisidee. Sei I ein Ideal eines Euklidischen Rings (R, δ). Falls $I = \{0\}$ ist $I = (0)$. Falls $I \neq \{0\}$ wählen wir $a \in I \setminus \{0\}$ mit der Eigenschaft, dass $\delta(a)$ minimal ist. Dann gilt $(a) \subset I$. Sei $b \in I$ dann gilt $b = aq + r$ für $q, r \in R$ mit $\delta(r) < \delta(a)$ falls $r \neq 0$. Der Rest $r = b - aq$ ist auch ein Element von I und deshalb gilt $r = 0$ (nach der Minimalität von $\delta(a)$). Dann gilt $b = aq \in (a)$ und diese Aussage gilt für alle $b \in I$. Dies zeigt $I = (a)$. □

Korollar. $\mathbb{Z}$, $\mathbb{Z}[i]$ und $K[t]$ sind Hauptidealringe.

Definition. Sei R ein Integritätsbereich und $p \in R \setminus (R^\times \cup \{0\})$.

(1) p heißt *irreduzibel*, wenn für jede Zerlegung $p = rs$ mit $r, s \in R$ gilt: $r \in R^\times$ oder $s \in R^\times$. Falls nichts nennen wir p reduzibel.
(2) p heißt *prim*, wenn für all $r, s \in R$ mit $p | rs$ gilt: $p | r$ oder $p | s$.

Bemerkung. Sei $p \in R \setminus (R^\times \cup \{0\})$ für einen Integritätsbereich R.

(1) p ist genau dann prim, wenn das Hauptideal (p) prim ist (nach der Definition).
(2) Wenn (p) ein maximales Ideal ist, dann is p prim (da jede maximales Ideal ist prim).
(3) Wenn p prim ist, dann ist p irreduzibel. Für den Beweis: falls $p = rs$ mit $r, s \in R$ gilt $p | r$ oder $p | s$ (da p prim ist). O.E.d.A. $p | r$ dann $pa = r$ für $a \in R$ und aus $p = rs = pas$ folgt $as = 1$ (da R ein Integritätsbereich ist und $p \neq 0$) d.h. $s \in R^\times$.

Satz 2.8. *Sei R ein Hauptidealring und $p \in R \setminus (R^\times \cup \{0\})$. Dann ist äquivalent:*

(1) p ist irreduzibel,
(2) p ist prim,
(3) (p) ist maximales Ideal in R.

Beweisidee. Jeder Hauptidealring ist ein Integritätsbereich (per Definition), also gilt (3) $\implies$ (2) $\implies$ (1) nach der obigen Bemerkung. Deshalb müssen wir nur zeigen (1) $\implies$ (3). Sei p irreduzibel. Sei (a) ein Ideal von R mit $(p) \subset (a) \subset R$. Da $p \in (a)$ gilt $p = ab$ für $b \in R$ und es folgt, dass a oder b ein Einheit ist (nach der Irreduzibilität von p). Falls $a \in R^\times$ gilt $(a) = R$ und falls $b \in R^\times$ gilt $(p) = (a)$. Somit ist (p) maximal. □

Satz 2.9. *(Primfaktorzerlegung) Sei R ein Hauptidealring und $r \in R \setminus (R^\times \cup \{0\})$. Dann kann man r als ein endliches Produkt von Primelementen schreiben.* [8.11.18]

Beweisidee. Wenn r irreduzibel ist, dann ist r prim (Satz 2.8) und r ist ein Produkt von Primelementen. Wenn r reduzibel ist, gibt es eine Zerlegung $r = ab$ mit $a, b \notin R^\times \cup \{0\}$. Dann kann man diese Konstruktion wiederholen mit a und b: Wenn a und b beide irreduzibel sind, dann sind beide prim und r hat eine Primfaktorzerlegung. Falls nicht o.E.d.A. ist a reduzibel und wir weiderholen diese Verfahren mit a. Wir müssen nur zeigen das diese Verfahren nach endliche vielen Schritten endet. Falls nichts konstruieren wir eine unendliche Folge $(r_i)_{i\geq 0}$ mit $r_0 = r$ und $r_1 = a$, alle r_i reduzibel, so dass $r_i = r_{i+1}s_{i+1}$ mit $r_i, s_i \notin R^\times \cup \{0\}$). Dann haben wir eine unendliche Kette von Ideale

$$(r_0) \subset (r_1) \subset (r_2) \subset \cdots \subset R.$$

Die Vereinigung $I = \cup_{n\in\mathbb{N}}(r_i)$ ist auch ein Ideal und müss ein Hauptideal sein d.h. $I = (s)$ für $s \in R$. Da $s \in I$, gibt es $n \in \mathbb{N}$ mit $s \in (r_n)$. Dann gilt

$$(r_0) \subset (r_1) \subset (r_2) \subset \cdots\cdots (r_n) = (s) = (r_{n+i})$$

und aus $(r_n) = (r_{n+1})$ folgt $r_{n+1} = r_n c$. Deshalb gilt $r_n = r_{n+1}s_{n+1} = r_n c s_{n+1}$ und es folgt $cs_{n+1} = 1$ d.h. $s_{n+1} \in R^\times$. Dies liefert ein Widerspruch: r_n ist nicht reduzibel, da $s_{n+1} \in R^\times$. Deshalb endet die Verfahren nach endliche vielen Schritten. □

Bemerkung. Der Beweis zeigt, dass jeder Hauptidealring Noethersch ist (Ein Ring heißt *Noethersch*, wenn jede aufsteigende Kette von Idealen $I_0 \subset I_1 \subset I_2 \subset \cdots$ stationär wird, d.h. es gibt $n \in \mathbb{N}$ mit $I_n = I_{n+i}$ für alle $i \geq 0$).

Korollar. Für $R = \mathbb{Z}$ hat jede ganze Zahl $r \in \mathbb{Z} \setminus \{0, \pm 1\}$ eine Primfaktorzerlegung.

Lemma. Sei r ein Element eines Integritätsbereichs R mit Zerlegungen

$$r = p_1 \cdots p_n = q_1 \cdots q_m$$

für p_i prim und q_j irreduzibel. Dann gilt $n = m$ und es gibt eine Permutation $\sigma \in S_n$, so dass p_i assoziiert zu $q_{\sigma(i)}$ für alle $1 \leq i \leq n$ ist (d.h. es gibt Einheiten $\epsilon_1, \cdots \epsilon_n$, so dass $\epsilon_i p_i = q_{\sigma(i)}$). *Beweisidee.* Aus $p_1 | q_1 \cdots q_m$ und p_1 prim folgt es, dass es ein j mit $p_1 | q_j$ gibt (d.h. $q_j = \epsilon_1 p_1$ und $\epsilon_1 \in R^\times$, da q_j irreduzibel ist). Sei $\sigma(1) := j$. Dann folgt

$$p_2 \cdots p_n = \epsilon_1 q_1 \cdots q_{j-1} q_{j+1} \cdots q_m$$

und man kann das Verfahren wiederholen mit p_2: es gibt $\sigma(2) \in \{1, \ldots, j-1, j+1, \cdots m\}$ mit $p_2 | q_{\sigma(2)}$ (wir bemerken, dass $p_2 \nmid \epsilon_1$, da p keine Einheit ist). Falls $n > m$ haben wir

$$p_{m+1} \cdots p_n = \epsilon_1 \cdots \epsilon_m$$

aber p_{m+1} ist prim und $p_{m+1} \nmid \epsilon_i$, so diese Gleichung ist nicht möglich. Falls $n < m$ haben wir

$$1 = \epsilon_1 \cdots \epsilon_n \prod_{j \neq \sigma(i)} q_j$$

aber q_j ist kein Einheit. Daher müss $n = m$ gelten. □

Satz 2.10. *Sei R ein Integritätsbereich. Dann ist äquivalent:*

(1) Jedes $r \in R \setminus (R^\times \cup \{0\})$ lässt sich als Produkt von Primelementen schreiben.
(2) Jedes $r \in R \setminus (R^\times \cup \{0\})$ lässt sich als eindutig (bis auf Reihenfolge und Assoziiertheit) als Produkt von irreduziblen Elementen schreiben.

Beweisidee. (1) $\implies$ (2) Jedes Primelement in R ist irreduzibel und deshalb gilt die Existenz einer Zerlegung bei (2). Für die Eindeutigkeit verwenden wir das obige Lemma.

(2) $\implies$ (1): Es ist hinreichend zu zeigen, dass jedes irreduzibles Element $r \in R$ prim ist. Wir nehmen an, dass $r|ab$ und wollen zeigen dass $r|a$ oder $r|b$. Wir betrachten die Zerlegungen bei (2) von a und b als Produkten von irreduziblen Elementen a_i und b_j:

$$a = a_1 \cdots a_n \quad \text{und} \quad b = b_1 \cdots b_m.$$

Dann $r|a_1 \cdots a_n b_1 \cdots b_m$ und nach der Eindeutigkeit der Zerlegung bei (2) folgt $r = a_i\epsilon$ oder $r = b_j\epsilon$ für ein Einheit $\epsilon \in R^\times$. Dann folgt $r|a$ oder $r|b$. □

Definition. Ein Integritätbereich R, der die äquivalenten Bedingungen des Satzes 2.10 erfüllt, heißt *fakoriell*.

Bemerkung. Nach dem Beweis des Satzes 2.10 gilt für einen faktoriellen Ring R: ein Element $r \in R$ ist genau dann irreduzibel, wenn es prim ist.

Korollar (des Satzes 2.9). Jeder Hauptidealring ist faktoriell.

Definition. Sei R ein faktorieller Ring und $\mathcal{P} \subset R$ die Menge aller Primelementen. Eine Teilmenge $P \subset \mathcal{P}$ heißt *Repräsentantensystem der Primelementen*, wenn für jedes $p \in \mathcal{P}$ es genau ein Primelement $p' \in P$ gibt, so dass p assoziiert zu p' ist.

Bemerkung. Sei R ein faktorieller Ring, $P \subset R$ ein Repräsentantensystem der Primelementen und $a \in R \setminus \{0\}$. Dann gibt es eine eindeutig bestimmte Zerlegung

$$a = \epsilon \prod_{p \in P} p^{\nu_p(a)}$$

wobei $\epsilon \in R^\times$ und $\nu_p(a) \in \mathbb{N}$ mit $\nu_p(a) = 0$ für fast alle $p \in P$.

Beispiel. Für $R = \mathbb{Z}$ ist $R^\times = \{\pm 1\}$ und $\mathcal{P} = \{\pm 2, \pm 3, \pm 5, \cdots\}$ und wir nehmen $P := \{2, 3, 5, \cdots\}$ die Menge aller positiven Primzahlen.

Übung. Zeigen Sie, dass $\mathbb{Z}[\sqrt{-5}]$ nicht faktoriell ist, da

$$2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

und $2, 3, (1 + \sqrt{-5}), (1 - \sqrt{-5})$ irreduzibel sind, aber $(1 + \sqrt{-5})$ ist nicht assoziiert zu entweder 2 oder 3. Überprüfen Sie, dass $\mathbb{Z}[\sqrt{-5}]$ ein Integritätsbereich ist.

Bemerkung. Man hat die folgenden Inklusionen:

$$\begin{array}{ccccccc} \text{Körper} & \subsetneq & \text{Euklidische Ringe} & \subsetneq & \text{Hauptidealringe} & \subsetneq & \\ \text{z.B. } \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p & & \text{z.B. } \mathbb{Z}, \mathbb{Z}[i], K[t] & & \text{z.B.}(*)\ \mathbb{Z}[\tfrac{1}{2}(1 + \sqrt{-19})] & & \end{array}$$

$$\begin{array}{ccccccc} \subset & \text{Faktorielle Ringe} & \subsetneq & \text{Integritätsbereich} & \subsetneq & \text{kommutative Ringe} & \\ & \text{z.B.}(*)\ \mathbb{Z}[x, y] & & \text{z.B. } \mathbb{Z}[\sqrt{-5}] & & \text{z.B. } \mathbb{Z}/n\mathbb{Z} \text{ für } n = ab & \end{array}$$

Die Beispiele hier sind so gewählt, dass sie keine Beispiele für die vorherige Klasse sind (z.B. $\mathbb{Z}$ ist ein Euklidische Ring, aber kein Körper). Wir haben nicht die Sterne markierten Beispiele gesehen, aber wir werden bald einige dieser Beispiele sehen.

Definition. Sei R ein Integritätsbereich und $r_1, \ldots, r_n \in R$. Ein Element $d \in R$ heißt *größter gemeinsamer Teiler* (ggT) von $r_1, \ldots r_n$ (man schreibt $\text{ggT}(r_1, \ldots, r_n) = d$) wenn gilt:

- $d|r_i$ für alle i (d.h. d ist ein gemeinsamer Teiler von $r_1, \ldots r_n$),
- für jeden gemeinsamen Teiler c von $r_1, \ldots r_n$ gilt $c|d$.

Bemerkung.

(1) Die Existenz eines größten gemeinsamen Teilers gilt für einen faktoriellen Ring R: Sei $P \subset R$ ein Repräsentantensystem der Primelementen dann hat $r_1, \dots, r_n \in R$ Primfaktorzerlegungen:

$$r_i = \epsilon_i \prod_{p \in P} p^{\nu_p(r_i)}.$$

(Übung) Zeigen Sie, dass

$$\mathrm{ggT}(r_1, \dots, r_n) = \prod_{p \in P} p^{\min(\nu_p(r_1), \dots, \nu_p(r_n))}.$$

(2) Der Ring $R = \mathbb{Z}[\sqrt{-5}]$ ist ein Integritätsbereich aber nicht faktoriell. Ein größter gemeinsamer Teiler von $r_1 = 6$ und $r_2 = 2(1 + \sqrt{-5})$ existiert nicht: beide 2 und $1 + \sqrt{-5}$ sind gemeinsame Teiler von r_1, r_2, aber $2 \nmid 1 + \sqrt{-5}$ und $1 + \sqrt{-5} \nmid 2$.

(3) Der größter gemeinsamer Teiler ist bis auf Assoziiertheit eindeutig.

Satz 2.11. *(Euklidischer Algorithmus) Sei (R, δ) ein Euklidischer Ring und $r_1, r_2 \in R \setminus \{0\}$. Sei r_{i+1} der Rest von r_{i-1} bei Division durch r_i für $i > 2$. Dann gibt es einen maximalen Index n mit $r_n \neq 0$ und es gilt $\mathrm{ggT}(r_1, r_2) = r_n$.* [13.11.18]

Beweisidee. Nach Division mit Rest haben wir

$$\begin{aligned} r_1 &= r_2 q_2 + r_3 && \delta(r_3) < \delta(r_2) \text{ falls } r_3 \neq 0 \\ r_2 &= r_3 q_3 + r_4 && \delta(r_4) < \delta(r_3) \text{ falls } r_4 \neq 0 \\ &\vdots \\ r_{i-1} &= r_i q_i + r_{i+1} && \delta(r_{i+1}) < \delta(r_i) \text{ falls } r_{i+1} \neq 0 \end{aligned}$$

Die Existenz von n folgt, da

$$0 \leq \cdots \delta(r_{i+1}) < \delta(r_i) < \cdots \delta(r_3) < \delta(r_2),$$

(d.h. $\delta(r_i)_{i \geq 2}$ ist eine fallende Folge der naturlichen Zahlen). Dann folgt der Beweis nach dem Lemma: wenn $a, b, q, r \in R$ und $a = bq + r$, dann folgt $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, r)$. □

Satz 2.12. *Seien $r_1, \dots, r_n$ Elemente eines Integritätsbereich R. Falls das Ideal $(r_1, \dots, r_n)$ ein Hauptideal ist (z.B. in einem Hauptidealring ist jedes Ideal ein Hauptideal), dann gilt*

$$(r_1, \dots, r_n) = (\mathrm{ggT}(r_1, \dots, r_n)).$$

Insbesondere existiert ein größter gemeinsamer Teiler von $r_1, \dots, r_n$ in diesem Fall.

Beweisidee. Falls $(r_1, \dots, r_n) = (r)$, gilt $r | r_i$ für $1 \leq i \leq n$ und $r = \sum_{i=1}^n a_i r_i$ für Elemente $a_1, \dots, a_n \in R$. Deshalb ist r ein gemeinsame Teiler von $r_1, \dots r_n$ und jeder andere gemeinsame Teiler von $r_1, \dots r_n$ ist auch ein Teiler von $r = \sum_{i=1}^n a_i r_i$, d.h. $r = \mathrm{ggT}(r_1, \dots, r_n)$. □

Satz 2.13. *Sei K ein Körper und $f \in K[t]$ ein nicht-konstantes Polynom. Dann ist äquivalent:*

(1) f ist irreduzibel,

(2) Der Quotientring ist $K[t]/(f)$ ein Körper.

Beweisidee. Der Polynomring $K[t]$ ist ein Hauptidealring und deshalb ist $f(t)$ genau dann irreduzibel, wenn das Ideal (f) maximal ist (Satz 2.8). Nach dem Satz 2.6 ist (f) genau dann maximal, wenn $K[t]/(f)$ ein Körper ist. □

Beispiel. Da $t^2 + t + 1 \in \mathbb{F}_2[t]$ irreduzibel ist, ist

$$\mathbb{F}_2[t]/(t^2 + t + 1) := \{0 + (f), 1 + (f), t + (f), t + 1 + (f)\}$$

ein Körper mit 4 Elementen.

2.4. **Satz von Gauß.** Mit dem Satz von Gauß kann man neue faktorielle Ringe konstruieren.

Definition. Sei R ein Integritätsbereich. Dann ist der *Quotientenkörper* von R

$$Q(R) := \{(a,b) : a \in R, b \in R \setminus \{0\}\}/\sim$$

wobei $(a,b) \sim (a',b') \iff ab' = a'b$. Für $(a,b) \in R \times R \setminus \{0\}$ schreiben wir $\frac{a}{b} := [(a,b)]$ und wir definieren Addition und Multiplikation auf $Q(R)$ wie folgt

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \quad \text{und} \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Übung. Beweisen Sie, dass $\sim$ eine Äquivalenzrelation ist, die Addition und Multiplikation auf $Q(R)$ wohldefiniert sind und $Q(R)$ ein Körper ist.

Beispiel. $Q(\mathbb{Z}) = \mathbb{Q}$.

Lemma. Sei R ein faktorieller Ring und $P \subset R$ ein Repräsentantensystem der Primelementen. Dann besitzt jedes $x = \frac{a}{b} \in Q(R)^\times$ eine eindutige Darstellung

$$x = \epsilon \prod_{p \in P} p^{\nu_p(x)}$$

wobei $\epsilon \in R^\times$ und $\nu_p(x) \in \mathbb{Z}$ mit $\nu_p(x) = 0$ für fast alle $p \in P$.

Definition. Sei R ein faktorieller Ring und $P \subset R$ ein Repräsentantensystem der Primelementen. Für $p \in P$ definieren wir eine Abbildung $\nu_p : Q(R) \to \mathbb{Z} \cup \{\infty\}$ durch $\nu_p(0) = \infty$ und für $x \in Q(R)^\times$ ist $\nu_p(x)$ die Potenz von p in der obigen Primfaktorzerlegung von x. Wir definieren $\tilde{\nu}_p : Q(R)[t] \to \mathbb{Z} \cup \{\infty\}$ durch

$$\tilde{\nu}_p(\sum_{i \geq 0} a_i t^i) = \min_i \nu_p(a_i).$$

Ein Polynom $f \in R[t]$ heißt *primitiv*, wenn der größte gemeinsame Teiler der Koeffizienten von f gleich 1 ist.

Bemerkung.

(1) Für $f \in Q(R)[t]$ gilt: $f = 0 \iff \tilde{\nu}_p(f) = \infty$ für ein Primelement $p \in R$.
(2) Für $f \in Q(R)[t]$ gilt: $f \in R[t] \iff \tilde{\nu}_p(f) \geq 0$ für alle $p \in P$.
(3) Ein Polynom $f \in R[t]$ ist genau dann primitiv, wenn $\tilde{\nu}_p(f) = 0$ für alle $p \in P$.
(4) Sei $p \in R$ ein Primelement. Es gilt $\nu_p(xy) = \nu_p(x) + \nu_p(y)$ für $x, y \in Q(R)$. Deshalb folgt $\nu_p(\epsilon) = 0$ für alle $\epsilon \in R^\times$ (da $0 = \nu_p(1) = \nu_p(\epsilon) + \nu_p(\epsilon^{-1})$ und $\nu_p(\epsilon), \nu_p(\epsilon^{-1}) \geq 0$)
(5) Für $f(t) = \sum_{i=0}^n a_i t^i \in Q(R)[t]$ gibt es $c \in Q(R)^\times$ und ein primitives Polynom $\tilde{f} \in R[t]$ mit $f = c\tilde{f}$. Nämlich

$$c := \prod_{p \in P} p^{\tilde{\nu}_p(f)} = \mathrm{ggT}(a_0, \ldots, a_n)$$

teilt jeden Koeffizient a_i von f und deshalb existiert $\tilde{f} := c^{-1}f \in Q(R)[t]$. Es gilt $\mathrm{ggT}(c^{-1}a_0, \ldots, c^{-1}a_n) = 1$, d.h. $\tilde{f} \in R[t]$ und $\tilde{f}$ ist primitiv.
(6) Sei $f \in Q(R)[t]$ ein normierte Polynom. Dann gilt $\tilde{\nu}_p(f) \leq 0$ für jedes Primelement $p \in R$.

[15.11.18] **Lemma (Gauß).** Sei R ein faktorieller Ring und $p \in R$ prim. Dann gilt für $f, g \in Q(R)[t]$

$$\tilde{\nu}_p(fg) = \tilde{\nu}_p(f) + \tilde{\nu}_p(g).$$

Beweisidee. Die Aussage gilt für konstante Polynome f und g. Die Aussage ist auch klar falls nur f oder g konstant ist. Daher nehmen wir an, dass f, g nicht-konstant sind und wir können f und g mit Konstante aus $Q(R)^\times$ multiplizieren. Nach der Bemerkung gibt es primitive Polynome $\tilde{f}, \tilde{g} \in R[t]$ und $c, d \in Q(R)^\times$ mit $f = c\tilde{f}$ und $g = d\tilde{g}$. O.E.d.A nehmen wir an, dass $f, g \in R[t]$

und es gilt $\tilde{\nu}_p(f) = \tilde{\nu}_p(g) = 0$. Dann müssen wir zeigen, dass $\tilde{\nu}_p(fg) = 0$. Sei $R' = R/(p)$ dann gibt es einen Homomorphismus $\Phi : R[t] \to R'[t]$, der die Koeffizienten reduziert. Ein Polynom $h \in R[t]$ ist genau dann in dem Kern von Φ, wenn p aller koeffizienten von h teilt:

$$\ker(\Phi) = \{h \in R[t] : \tilde{\nu}_p(h) > 0\}$$

und wegen $\tilde{\nu}_p(f) = \tilde{\nu}_p(g) = 0$ gilt $f, g \notin \ker(\Phi)$. Es gilt

$$0 \neq \Phi(fg) = \Phi(f)\Phi(g)$$

da $R' = R/(p)$ und deshalb auch $R'[t]$ Integritätsbereiche sind (siehe Satz 2.6). Insbesondere gilt $\tilde{\nu}_p(fg) = 0 = \tilde{\nu}_p(f) + \tilde{\nu}_p(g)$. □

Korollar. Sei R ein faktorieller Ring und $h \in R[t]$ ein normiert Polynom (d.h. der höchste nicht-Null-Koeffizient ist 1). Aus einer Gleichung $h = f \cdot g$ in $Q(R)[t]$ mit f und g normierte Polynome in $Q(R)[t]$ folgt $f, g \in R[t]$.

Beweisidee. Da $h \in R[t]$ normiert ist, gilt $\tilde{\nu}_p(h) = 0$ für alle prim $p \in R$. Da $g, h \in Q(R)[t]$ normiert sind, gilt $\tilde{\nu}_p(f) \leq 0$ und $\tilde{\nu}_p(g) \leq 0$. Nach dem Lemma gilt

$$0 \geq \tilde{\nu}_p(f) + \tilde{\nu}_p(g) = \tilde{\nu}_p(h) = 0$$

und sogar gilt $\tilde{\nu}_p(f) = \tilde{\nu}_p(g) = 0$ und es folgt, dass $f, g \in R[t]$. □

Beispiel. Sei $R = \mathbb{Z}$ mit $Q(R) = \mathbb{Q}$. Seien $h \in \mathbb{Z}[t]$ und $f, g \in \mathbb{Q}[t]$ normierte Polynome. Dann gilt

$$h = f \cdot g \in \mathbb{Q}[t] \implies f, g \in \mathbb{Z}[t].$$

Satz 2.14. *(Gauß) Sei R ein faktorieller Ring. Dann ist auch $R[t]$ faktoriell. Ferner ist ein Polynom $q \in R[t]$ genau dann prim ($\star$), wenn entweder*

(1) $q \in R$ prim ist oder,
(2) $q \in R[t]$ primitiv ist und $q \in Q(R)[t]$ prim ist.

Beweisidee. (1) $\implies$ ($\star$): Falls $q \in R$ prim ist, dann ist $R/(q)$ ein Integritätsbereich (Satz 2.6). Dann ist $(R/(q))[t] = R[t]/(q)$ auch ein Integritätsbereich (rechts ist $(q) = qR[t]$ ein Ideal von $R[t]$) und nach dem Satz 2.6 ist das Ideal $(q) \subset R[t]$ prim und es folgt, dass $q \in R[t]$ ein Primelement ist.

(2) $\implies$ ($\star$): Sei $q \in R[t]$, so dass $q(t) \in R[t]$ primitiv ist (d.h. $\tilde{\nu}_p(q) = 0$ für alle $p \in R$ prim) und $q \in Q(R)[t]$ ein Primelement ist. Wir wollen zeigen, dass q ein Primelement in $R[t]$ ist. Seien $f, g \in R[t]$ mit $q \mid fg$ in $R[t]$. Dann gilt $q \mid fg \in Q(R)[t]$ und in $Q(R)[t]$ ist q prim, also $q \mid f$ oder $q \mid g$ in $Q(R)[t]$. O.E.d.A. $q \mid f$ in $Q(R)[t]$, d.h. es $h \in Q(R)[t]$ gibt mit $f = qh$. Nach dem Lemma von Gauß gilt für jedes Primelement $p \in R$

$$0 \leq \tilde{\nu}_p(f) = \tilde{\nu}_p(q) + \tilde{\nu}_p(h) = \tilde{\nu}_p(h)$$

da $q \in R[t]$ primitiv (was äquivalent zu $\tilde{\nu}_p(q) = 0$ für jedes Primelement $p \in R$ ist) ist und $f \in R[t]$ (was äquivalent zu $\tilde{\nu}_p(f) \geq 0$ für jedes Primelement $p \in R$ ist). Deshalb gilt $h \in R[t]$ und $q | f \in R[t]$.

$R[t]$ ist faktoriell: Es ist hinreichend zu zeigen, dass jedes $f \in R[t] \setminus (R[t]^\times \cup \{0\})$ ein Produkt von Primelementen in $R[t]$ ist. Nach der obigen Bemerkung gibt es $c \in Q(R)^\times \cap R = R \setminus \{0\}$ und ein primitives Element $\tilde{f} \in R[t]$ mif $f = c\tilde{f}$. Das Element c ist genau dann eine Einheit, wenn f schon primitiv ist. Sonst ist $c \in R \setminus (R^\times \cup \{0\})$. Da R faktoriell ist, hat c eine Zerlegung als Produkt von Primlelementen in R und nach dem Fall (1) $\implies$ ($\star$) ist jedes Primelement in R auch ein Primelement in $R[t]$. Deshalb ist es hinreichend, eine Primfaktorzerlegung für jedes primitive Polynom $\tilde{f} \in R[t]$ zu finden. Als Element des faktoriellen Rings $Q(R)[t]$ hat $\tilde{f}$ eine Primfaktorzerlegung

$$\tilde{f} = f_1 \cdots f_n$$

mit $f_1, \cdots, f_n$ Primelemente in $Q(R)[t]$. Für $1 \leq i \leq n$ gibt es $a_i \in Q(R)^\times$ und primitive Elemente $\tilde{f}_i \in R[t]$ mit $f_i = a_i \tilde{f}_i$. Nach dem Fall (2) $\implies$ $(\star)$ sind $\tilde{f}_1, \ldots, \tilde{f}_n$ Primelemente in $R[t]$, da $\tilde{f}_i \in R[t]$ primitiv sind und $f_i \sim \tilde{f}_i \in Q(R)[t]$ prim sind. Dann haben wir eine Zerlegung

$$\tilde{f} = a\tilde{f}_1 \cdots \tilde{f}_n$$

mit $a = \prod_{i=1}^n a_i \in Q(R)^\times$ und $\tilde{f}_1, \ldots, \tilde{f}_n$ Primelemente in $R[t]$. Wir müssen nur zeigen, dass $a \in R$ (und deshalb hat a auch eine Primfaktorzerlegung). Nach dem Lemma von Gauß gilt

$$0 = \tilde{\nu}_p(\tilde{f}) = \tilde{\nu}_p(a) + \sum_{i=1}^n \tilde{\nu}_p(\tilde{f}_i) = \tilde{\nu}_p(a) \quad \forall p \in R \text{ prim},$$

da $\tilde{f}, \tilde{f}_1, \ldots, \tilde{f}_n$ primitive Elemente in $R[t]$ sind. Deshalb folgt $a \in R$ und dann hat $\tilde{f}$ eine Primfaktorzerlegung.

$(\star) \implies$ (1) oder (2): Wir müssen zeigen, dass jedes Primelement $q \in R[t]$ von Typ (1) oder (2) ist. Da $R[t]$ faktoriell ist, hat q eine Zerlegung

$$q = c_1 \cdots c_m \tilde{f}_1 \cdots \tilde{f}_n$$

für Primelement $c_1, \ldots, c_m$ vom Typ (1) und Primelement $\tilde{f}_1, \ldots, \tilde{f}_n$ von Typ (2). Nach dem Lemma vor dem Satz 2.10 ist eine Primfaktorzerlegung eindeutig bis auf Reihenfolge und Assoziiertheit. Deshalb gilt $n + m = 1$ und entweder $q = c_i$ oder $q = \tilde{f}_j$ (d.h. q ist ein Primelement vom Typ (1) oder (2). □

Bemerkung. Man kann Polynomringe in mehreren Variablen induktiv konstruieren

$$R[t_1, \ldots, t_n] := (R[t_1, \ldots, t_{n-1}])[t_n].$$

Beispiel. Für einen faktoriellen Ring R ist $R[t_1, \ldots, t_n]$ faktoriell. Insbesondere sind $\mathbb{Z}[t]$ und $\mathbb{Z}[t_1, \ldots, t_n]$ faktoriell.

3. Körpererweiterungen

[20.11.18]

3.1. **Charakteristik.** Für einen Integritätsbereich R gibt es einen Ringhomomorphismus $\varphi : \mathbb{Z} \to R$ mit $\varphi(n) = n \cdot 1$. Der Kern von φ ist ein Hauptideal von $\mathbb{Z}$ und φ induziert einen injektiven Homomorphismus $\overline{\varphi} : \mathbb{Z}/\ker(\varphi) \hookrightarrow R$. Insbesondere ist $\mathbb{Z}/\ker(\varphi)$ auch ein Integritätsbereich und es folgt, dass $\ker(\varphi) \subset \mathbb{Z}$ ein Primideal ist (Satz 2.6). Deshalb gilt $\ker(\varphi) = (n)$ mit $n \in \{0\} \cup \{p : \text{Primzahl}\}$.

Definition. Die *Charakteristik* eines Integritätsbereichs R ist $\mathrm{Char}(R) := n$ mit $\ker(\varphi) = (n)$.

Beispiel. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ haben Charakteristik 0. Der endliche Körper $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (mit p prim) hat Charakteristik p.

Definition. Sei K ein Körper.

(1) Ein *Teilkörper* ist ein Unterring $T \subset K$, der selbst ein Körper ist.
(2) Der *Primkörper* von K ist der Durchschnitt $P := \cap_T T$ aller Teilkörper $T \subset K$.

Übung. Der Primkörper P von K ist der kleinste Teilkörper von K und $\mathrm{Char}(P) = \mathrm{Char}(K)$.

Satz 3.1. *Sei P der Primkörper eines Körper K. Dann gilt*

(1) $\mathrm{Char}(K) = 0 \iff P \cong \mathbb{Q}$,
(2) $\mathrm{Char}(K) = p > 0 \iff P \cong \mathbb{F}_p$.

Beweisidee. $\Leftarrow$ ist trivial, weil $\mathrm{Char}(P) = \mathrm{Char}(K)$.

$\Rightarrow$: Der Ringhomomorphismus $\varphi : \mathbb{Z} \to K$ mit $\varphi(n) = n \cdot 1$ faktorisiert durch jeden Teilkörper von K und insbesondere P. Deshalb gilt $\mathrm{Bild}(\varphi) \subset P \subset K$ und $\mathrm{Bild}(\varphi) \cong \mathbb{Z}/(\mathrm{Char}(K))$. Falls

$\mathrm{Char}(K) = 0$, dann ist $\mathbb{Z} = \mathbb{Z}/(0) \cong \mathrm{Bild}(\varphi) \subset P$ und deshalb ist $\mathbb{Q} = Q(\mathbb{Z}) \cong Q(\mathrm{Bild}(\varphi)) \subset P$. Dann folgt $P \cong \mathbb{Q}$, da P der kleinste Teilkörper von K ist. Falls $\mathrm{Char}(K) = p > 0$, dann ist $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \cong \mathrm{Bild}(\varphi) \subset P$ und dann folgt $P \cong \mathbb{F}_p$. □

Übung. Sei K ein Körper mit $\mathrm{Char}(K) = p > 0$. Dann gilt

$$\forall a, b \in K, n \in \mathbb{N}: \quad (a \pm b)^{p^n} = a^{p^n} \pm b^{p^n}$$

und deshalb ist $F : K \to K$ mit $F(a) = a^p$ ein Körperhomomorphismus. F heißt *Frobenius-Homomorphismus*.

3.2. **Endliche und algebraische Körpererweiterungen.** Eine *Körpererweiterung* ist $K \subset L$, wobei K ein Teilkörper von L ist. Man schreibt $K \subset L$ oder K/L und sagt 'K über L'.

Bemerkung. Für eine Körpererweiterung $K \subset L$ können wir L als ein Vektorraum über K betrachten (z.B. Für $K = \mathbb{R} \subset L = \mathbb{C}$ ist $\mathbb{C}$ ein $\mathbb{R}$-Vektorraum der Dimension 2 über $\mathbb{R}$).

Definition. Der *Grad* einer Körpererweiterung $K \subset L$ ist $[L : K] := \dim_K(L)$. Die Körpererweiterung $K \subset L$ heißt *(un)endlich*, wenn der Grad (un)endlich ist.

Bemerkung. Es gilt $[L : K] = 1 \iff K = L$.

Satz 3.2 (Gradsatz)**.** *Seien $K \subset L \subset M$ Körpererweiterungen. Dann gilt*

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

Beweisidee. Falls L/K und M/L beide endliche Grade n und m haben, dann gibt es Basen

- $x_1, \ldots, x_n$ des K-Vektorraums L,
- $y_1, \ldots, y_m$ des L-Vektorraums M.

Wir behaupten, dass $x_i \cdot y_j$ mit $1 \le i \le n$, $1 \le j \le m$ eine Basis des K-Vektorraums M ist. Für die lineare Unabhängigkeit: aus $\sum_{i,j} c_{ij} \cdot x_i \cdot y_j = 0$ mit $c_{ij} \in K$, folgt $\sum_j (\sum_i c_{ij} x_i) y_j = 0$ mit $\sum_i c_{ij} x_i \in L$. Da $y_1, \ldots, y_m$ eine L-Basis von M ist, folgt $\sum_i c_{ij} x_i = 0$ für alle $1 \le j \le m$. Dann folgt $c_{ij} = 0$ für alle $1 \le i \le n$, da $x_1, \ldots, x_n$ eine K-Basis von L ist. Die Vektoren sind ein Erzeugendensystem: $r \in M$ hat eine Darstellung $r = \sum_{j=1}^m \lambda_j y_j$ mit $\lambda_j \in L$ (da $y_1, \ldots, y_m$ eine L-Basis von M ist). Für alle $1 \le j \le n$ hat λ_j eine Darstellung $\lambda_j = \sum_{i=1}^n \mu_{ij} x_i$ mit $\mu_{ij} \in K$ (da $x_1, \ldots, x_n$ eine K-Basis von L ist). Dann folgt $r = \sum_{i,j} \mu_{ij} \cdot (x_i \cdot y_j)$ mit $\mu_{ij} \in K$.

Falls $K \subset L$ oder $L \subset M$ unendlichen Grad hat, dann gilt für alle $n \in N$ stets $[L : K] \ge n$ oder $[M : L] \ge n$. Nach dem obigen Argument folgt $[M : K] \ge n$ für alle n und deshalb gilt die Gleichung. □

Korollar. Seien $K \subset L \subset M$ Körpererweiterungen mit $p = [M : K]$. Dann folgt $L = K$ oder $L = M$.

Definition. Sei $K \subset L$ eine Körpererweiterung.

(1) $\alpha \in L$ heißt *algebraisch über K*, wenn α eine Gleichung

$$\alpha^n + c_{n-1}\alpha^{n-1} + \cdots c_1\alpha + c_0 = 0 \quad \text{mit } c_i \in K$$

erfüllt. Sonst heißt *transzendent über K*.

(2) Die Körpererweiterung heißt *algebraisch*, wenn jedes $\alpha \in L$ algebraisch über K ist.

Bemerkung. Sei $K \subset L$ eine Körpererweiterung. Für $\alpha \in K$ ist äquivalent:

(1) α ist algebraisch über K,
(2) α ist eine Nullstelle eines nicht-Null Polynoms in $K[t]$,
(3) Der Kern des Ringhomomorphismuses $\varphi_\alpha : K[t] \to L$ mit $\varphi_\alpha(g) := g(\alpha)$ ist nicht Null.

Beispiel. Sei $K = \mathbb{Q} \subset L = \mathbb{C}$. Dann ist $i \in \mathbb{C}$ algebraisch über $\mathbb{Q}$, da i eine Nullstelle von t^2+1 ist. Für $q \in \mathbb{Q}$ und $n \in \mathbb{N}$ ist $\sqrt[n]{q}$ algebraisch über $\mathbb{Q}$, da $\sqrt[n]{q}$ eine Nullstelle von $t^n - q$ ist. Diese Körpererweiterung ist nicht algebraisch, da $\pi \in \mathbb{C}$ transzendent über $\mathbb{Q}$ ist (wir werden nicht diese Aussage beweisen).

Definition. Sei $K \subset L$ eine Körpererweiterung und $\alpha \in L$ algebraisch über K. Ein normiertes Polynom $f \in K[t]$ heißt *Minimalpolynom* von α (über K), wenn $f(\alpha) = 0$ und für alle $0 \neq g \in K[t]$ mit $g(\alpha) = 0$ gilt $\text{grad}(f) \leq \text{grad}(g)$. Man schreibt m_α für das Minimalpolynom von α.

Lemma. Sei $K \subset L$ eine Körpererweiterung und $\alpha \in L$ algebraisch über K. Dann gilt

(1) Das Minimalpolynom m_α von α existiert und ist eindeutig bestimmt. Ferner gilt $\ker(\varphi_\alpha) = (m_\alpha)$ für $\varphi_\alpha : K[t] \to L$ mit $\varphi_\alpha(g) := g(\alpha)$,
(2) m_α ist prim und somit irreduzibel,
(3) $K[t]/(m_\alpha)$ ist ein Körper

Beweisidee. (1): Das Ideal $\ker(\varphi_\alpha) \subset K[t]$ ist ein nicht-Null Hauptideal (da α algebraisch über K ist und $K[t]$ ein Hauptidealring ist). Deshalb gibt es ein Polynom $0 \neq f_\alpha \in K[t]$ mit $\ker(\varphi_\alpha) = (f_\alpha)$. Das erzeugendes Element f_α ist bis auf Assoziiertheit eindeutig und wegen $K[t]^\times = K \subset \{0\}$ gibt es genau ein normiertes Polynom $m_\alpha \sim f_\alpha$ mit $\ker(\varphi_\alpha) = (m_\alpha)$. Nach der Definition von φ_α und des Kerns gilt $m_\alpha(\alpha) = 0$. Falls $0 \neq g \in K[t]$ mit $g(\alpha) = 0$ existiert, dann ist $g \in \ker(\varphi_\alpha) = (m_\alpha)$ und es folgt, dass $\text{grad}(g) \geq \text{grad}(m_\alpha)$.

(2) und (3): $\text{Bild}(\varphi_\alpha) \subset L$ ist ein Integritätsbereich und deshalb ist $\text{Bild}(\varphi_\alpha) \cong K[t]/(m_\alpha)$ ein Integritätsbereich und es folgt, dass (m_α) ein Primideal ist und m_α ein Primelement ist. Es folgt, dass m_α auch irreduzibel ist und (3) gilt nach dem Satz 2.13. □

Satz 3.3. *Sei $K \subset L$ eine Körpererweiterung und $\alpha \in L$ algebraisch über K mit Minimalpolynom $m_\alpha \in K[t]$. Sei $K[\alpha] = \text{Bild}(\varphi_\alpha)$ den von α und K erzeugten Unterring von L. Dann gibt es einen Ringisomorphismus $\overline{\varphi_\alpha} : K[t]/(m_\alpha) \cong K[\alpha]$ und insbesondere ist $K[\alpha]$ ein Körper und eine Körpererweiterung von K. Ferner gilt $[K[\alpha] : K] = \text{grad}(m_\alpha)$.*

Beweisidee. Nach dem obigen Lemma müssen wir nur $[K[\alpha] : K]$ berechnen. Sei $n = \text{grad}(m_\alpha)$. Dann behaupten wir, dass $1 + (m_\alpha), t + (m_\alpha), \ldots, t^{n-1} + (m_\alpha)$ eine K-Basis von $K[t]/(m_\alpha)$ ist. Sei $f + (m_\alpha) \in K[t]/(m_\alpha)$. Nach Division mit Rest gibt es $r = \sum_{i=0}^{n-1} c_i t^i \in K[t]$ mit $\text{grad}(r) < n$ und $f + (m_\alpha) = r + (m_\alpha)$. Dann ist $r + (m_\alpha) = \sum_{i=0}^{n-1} c_i (t^i + (m_\alpha))$ eine K-Linearkombination der Basisvektoren. Die lineare Unabhängigkeit der Basisvektoren folgt, da $\text{grad}(m_\alpha) = n$. Deshalb gilt $[K[\alpha] : K] = n$. □

[22.11.18] **Bemerkung.** Für α algebraisch über K mit $\text{grad}(m_\alpha) = n$ ist $\alpha^0, \ldots, \alpha^{n-1}$ eine K-Basis von $K[\alpha]$.

Satz 3.4. *Jede endliche Körpererweiterung $K \subset L$ ist algebraisch.*

Beweisidee. Sei $n := [L : K]$ und $\alpha \in L$. Dann sind $\alpha^0, \ldots, \alpha^n \in L$ lineare abhängig über K, d.h. es gibt $c_i \in K$ mit $c_n \alpha^n + \cdots + c_0 \alpha^0 = 0$. Sei $m = \max\{i : c_i \neq 0\}$. Dann gilt $m > 0$ und α ist eine Nullstelle des normierten Polynoms $f(t) = t^m + \frac{c_{m-1}}{c_m} t^{m-1} + \cdots + \frac{c_0}{c_m}$ mit K-Koeffizienten, d.h. α ist algebraisch über K. □

Definition. Sei $K \subset L$ eine Körpererweiterung und $A \subset L$ eine Teilmenge

(1) Der *von A erzeugter Teilköper von L über K* ist der Durschnitt $K(A) = \cap_T T$ aller Teilköper $T \subset L$ mit $K \cup A \subset T$.
(2) Die Körpererweiterung $K \subset L$ heißt *einfach*, wenn es ein Element $\alpha \in L$ mit $L = K(\alpha)$ gibt. Man schriebt $\text{grad}(\alpha) = [K(\alpha) : K]$.
(3) Die Körpererweiterung $K \subset L$ heißt *endlich erzeugt*, wenn es endlich viele Elemente $\alpha_1, \ldots, \alpha_n \in L$ mit $L = K(\alpha_1, \ldots, \alpha_n)$ gibt.

Bemerkung. Sei $K \subset L$ eine Körpererweiterung und $A \subset L$ eine Teilmenge.

(1) Nach der Konstruktion ist $K(A)$ ein Teilkörper von L mit $K \subset K(A) \subset L$. Der Teilkörper $K(A)$ ist der kleinste Teilkörper von L, der A und K enthält.
(2) Für $A = \{\alpha_1, \ldots, \alpha_n\}$ eine endliche Teilmenge betrachten wir den Ringhomomorphismus $\varphi_A : K[t_1, \ldots, t_n] \to L$ mit $f(t_1, \ldots, t_n) \mapsto f(\alpha_1, \ldots, \alpha_n)$. Sei
$$K[\alpha_1, \ldots, \alpha_n] := \text{Bild}(\varphi_A) \subset L,$$
der ein Unterring von L ist. $K[\alpha_1, \ldots, \alpha_n]$ ist der kleinste Unterring von L, der $\{\alpha_1, \ldots \alpha_n\}$ und K enthält. Dann gilt $K[\alpha_1, \ldots, \alpha_n] \subset K(\alpha_1, \ldots, \alpha_n)$ und der Quotientenkörper
$$Q(K[\alpha_1, \ldots, \alpha_n]) = \left\{ \frac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)} : f, g \in K[t_1, \ldots, t_n],\ g(\alpha_1, \ldots, \alpha_n) \neq 0 \right\}$$
ist ein Teilkörper von $K(\alpha_1, \ldots, \alpha_n)$. Aus $\{\alpha_1, \ldots, \alpha_n\} \cup K \subset Q(K[\alpha_1, \ldots, \alpha_n])$ folgt $Q(K[\alpha_1, \ldots, \alpha_n]) = K(\alpha_1, \ldots, \alpha_n)$ (wegen der Minimalität von $K(A)$). Im Allgemeinen gilt $K[\alpha_1, \ldots, \alpha_n] \subsetneq K(\alpha_1, \ldots, \alpha_n)$, aber wir werden sehen, dass wenn α_i algebraisch über K sind, dann haben wir Gleichheit (Satz 3.5).
(3) Falls $A = \{\alpha_i : i \in I\}$ unendlich ist, dann ist
$$K(A) = \bigcup_{\substack{J \subset I \\ |J| < \infty}} K(\alpha_j : j \in J).$$
Man kann einen Polynomring in unendliche Variablen $K[t_i : i \in I]$ betrachen und den Ringhomomorphismus $\varphi_A : K[t_i : i \in I] \to L$ mit $f(t_i : i \in I) \mapsto f(\alpha_i : i \in I)$ bilden. Den ist $K(A) = Q(\text{Bild}(\varphi_A))$.
(4) Falls $\alpha \in L$ algebraisch über K ist gilt $K[\alpha] = K(\alpha)$ (Satz 3.3).

Satz 3.5. *Sei $K(\alpha_1, \ldots, \alpha_n)$ eine endliche erzeugte Körpererweiterung von K mit $\alpha_1, \ldots, \alpha_n$ algebraisch über K. Dann gilt*

(1) $K[\alpha_1, \ldots, \alpha_n] = K(\alpha_1, \ldots, \alpha_n)$,
(2) $K \subset K(\alpha_1, \ldots, \alpha_n)$ ist algebraisch und insbesondere algebraisch.

Beweisidee. Durch Induktion nach n. Der Induktionsanfang (n=1) ist Satz 3.3. Wir nehmen an, dass $K[\alpha_1, \ldots, \alpha_{n-1}] = K(\alpha_1, \ldots, \alpha_{n-1})$ eine endliche Körpererweiterung von K ist. Nach dem Satz 3.3 ist
$$K[\alpha_1, \ldots, \alpha_{n-1}] \subset K[\alpha_1, \ldots, \alpha_n] = K[\alpha_1, \ldots, \alpha_{n-1}][\alpha_n] = K(\alpha_1, \ldots, \alpha_n)$$
eine endliche Körpererweiterung. Nach dem Gradsatz 3.2 ist $K \subset K[\alpha_1, \ldots, \alpha_n]$ endlich. □

Beispiel. $\mathbb{Q} \subset \mathbb{Q}(e^{\pi i/n})$ ist eine einfache algebraische Körpererweiterung (da $e^{\pi i/n}$ eine Nullstelle von $t^{2n} - 1$ ist). Deshalb ist $\cos(\pi/n) = (e^{\pi i/n} + e^{-\pi i/n})/2$ algebraisch über K.

Satz 3.6. *Sei $K \subset L$ eine Körpererweiterung. Dann ist äquivalent*

(1) L/K ist endlich,
(2) L wird von endlich viele algebrasichen Elementen über K erzeugt,
(3) L/K ist algebraisch und endlich erzeugt.

Beweisidee. Nach dem Satz 3.5 folgt (2) $\implies$ (3) und (2) $\implies$ (1). Offentscihtlich gilt (3) $\implies$ (2) und nach dem Satz 3.4 folgt (1) $\implies$ (2). □

Bemerkung. Für eine Körpererweiterung $K \subset L$ ist äquivalent:

(1) L/K ist algebraisch,
(2) L wird von algebrasichen Elementen über K erzeugt.

Beweisidee. (1) $\implies$ (2) ist klar (wir können $A := L$ nehmen). Für (2) $\implies$ (1) ist $L = K(A)$ mit $A \subset L$ eine Teilmenge von algebraischen Elementen über K ist $K(\alpha_1, \ldots, \alpha_n)$ algebraisch über K für jede endliche Teilmenge $\{\alpha_1, \ldots, \alpha_n\} \subset A$. Da $K(A)$ die Vereinigung von Teilkörper $K(\alpha_1, \ldots, \alpha_n)$ über alle endliche Teilmenge $\{\alpha_1, \ldots, \alpha_n\} \subset A$ ist, ist $K(A)$ auch algebraisch über K. □

Satz 3.7. *Seien $K \subset L \subset M$ Körpererweiterungen. Dann ist M/K genau dann algebraisch, wenn M/L und L/K algebraisch sind.*

Beweisidee. '$\Rightarrow$' ist trivial. '$\Leftarrow$' : Sei $\alpha \in M$. dann gibt es $m_\alpha(t) = t^n + c_{n-1}t^{n-1} + \cdots + c_0 \in L[t]$ mit $m_\alpha(\alpha) = 0$ (da M/L algebraisch ist). Dann ist α algebraisch über $K(c_0, \ldots, c_{n-1})$ und die Körpererweiterung $K(c_0, \ldots, c_{n-1}) \subset K(c_0, \ldots, c_{n-1}, \alpha)$ ist endlich (Satz 3.3). Da $c_i \in L$ und L/K algebraisch ist, ist $K \subset K(c_0, \ldots, c_{n-1})$ endlich (Satz 3.5). Nach dem Gradsatz 3.2 ist $K \subset K(c_0, \ldots, c_{n-1}, \alpha)$ endlich und deshalb algebraisch nach dem Satz 3.6 und es folgt, dass α algebraisch über K ist. □

Beispiel. Wir betrachten $\mathbb{Q} \subset L := \{\alpha \in \mathbb{C} : \alpha \text{ ist algebraisch über } \mathbb{Q}\} \subset \mathbb{C}$. Wir bemerken, dass L ein Körper ist: falls $\alpha, \beta \in L$ gilt $\mathbb{Q}(\alpha, \beta) \subset L$ (nach dem Satz 3.5) und deshalb sind $\alpha \pm \beta$, $\alpha\beta$ und α/β (falls $\beta \neq 0$) Elemente von L. Nach der Definition ist $L/\mathbb{Q}$ algebraisch, aber diese Körpererweiterung ist unendlich: für jede Primzahl p und $n \in \mathbb{N}$ gilt $\mathbb{Q}(\sqrt[n]{p}) \subset L$ und es folgt, dass $[L : \mathbb{Q}] \geq [\mathbb{Q}(\sqrt[n]{p}) : \mathbb{Q}] = n$. Insbesondere gilt $[\mathbb{C} : \mathbb{Q}] = \infty$. Wir werden sehen, dass $L = \overline{\mathbb{Q}}$ der algebraische Abschluss von $\mathbb{Q}$ in $\mathbb{C}$ ist.

Übung. Sei $K \subset L$ eine Körpererweiterung. Beweisen Sie, dass

$$\mathbb{A}_{L/K} := \{\alpha \in L : \alpha \text{ ist algebraisch über } K\}$$

eine algebraische Körpererweiterung von K ist.

3.3. **Algebraischer Abschluss.** Für einen Körper K finden wir einen minimalen Körper $\overline{K}$ (*den algebraischen Abschluss von K*), so dass $\overline{K}$ algebraisch abgeschlossen ist und $K \subset \overline{K}$ eine algebraische Körpererweiterung ist.

Definition. Ein Körper K heißt *algebraisch abgeschlossen*, wenn jedes nicht-konstante Polynom aus $K[t]$ eine Nullstelle in K besitzt.

Übung. Wenn K algebraisch abgeschlossen ist, hat jedes Polymom $f \in K[t]$ eine Zerlegung in Linearfaktoren $f(t) = c\prod_{i=1}^n (t - a_i)$ mit $c, a_i \in K$ und $n \in \mathbb{N}$.

Beispiel. $\mathbb{R}$ ist nicht algebraisch abgeschlossen $t^2 + 1 \in \mathbb{R}[t]$ hat keine Nullstelle in $\mathbb{R}$, aber eine Nullstelle in $\mathbb{C}$. Daher gilt $\mathbb{C} \subset \overline{\mathbb{R}}$ und es folgt, dass $\overline{\mathbb{R}} = \mathbb{C}$.

[27.11.18]

Satz 3.8. *Sei K ein Körper und $f \in K[t]$ mit $\mathrm{grad}(f) \geq 1$. Dann existiert eine algebraische Körpererweiterung L/K, so dass f eine Nullstelle in L besitzt. Falls f irreduzibel ist, kann mann $L := K[t]/(f)$ setzen.*

Beweisidee. Falls f irreduzibel ist, dann ist $L := K[t]/(f)$ ein Körper (Satz 2.13). Der Ringhomomorphismus $K \hookrightarrow K[t] \twoheadrightarrow K[t]/(f) = L$ hat den Kern $\{0\}$, da $\mathrm{grad}(f) \geq 1$. Deshalb ist $K \subset L$ eine Körpererweiterung mit $[L : K] = \mathrm{grad}(f) < \infty$. Insbesondere ist $K \subset L$ algebraisch (Satz 3.4). Ferner hat $f = \sum_{i=0}^n c_i t^i$ eine Nullstelle $t + (f) \in L = K[t]/(f)$:

$$f(t + (f)) = \sum_{i=0}^n c_i (t + (f))^i = \sum_{i=0}^n c_i t^i + (f) = f + (f) = 0 + (f).$$

Falls f reduzibel ist betrachten wir eine Primfaktorzerlegung $f = f_1 \cdots f_n$ mit f_i Primelement (und deshalb sind f_i auch irreduzibel). Dann hat f_1 eine Nullstelle in der algebraischen Körpererweiterung $L := K[t]/(f_1)$ von K. Jede Nullstelle von f_1 ist auch eine Nullstelle von f und deshalb hat f eine Nullstelle in L. □

Lemma. Ein Körper K ist genau dann algebraisch abgeschlossen, wenn es keine echte algebraisch Körpererweiterung $K \subsetneq L$ zulässt.

Partielle geordnete Mengen und das Lemma von Zorn. Eine *partielle Ordnung* auf einer Menge M ist eine Relation $\leq$, die reflexiv ($\forall a \in M : a \leq a$), transitiv ($\forall a, b, c \in M : a \leq b, b \leq$

$c \implies a \leq c$) und antisymmetrisch ($\forall a, b \in M : a \leq b, b \leq a \implies a = b$) ist. Die Ordnung ist total, wenn $\forall a, b \in M : a \leq b$ oder $b \leq a$ gilt.

(1) $a \in M$ heißt größtes Element von M, wenn $b \leq a$ für alle $b \in M$ gilt.
(2) $a \in M$ heißt maximales Element von M, wenn $a \leq b$ mit $b \in M \implies b = a$.
(3) $a \in M$ heißt obere Schranke einer Teilmenge $N \subset M$, wenn $b \geq a$ für alle $b \in N$ gilt.

Lemma von Zorn.[4] Sei $(M, \leq)$ eine partielle geordnete Menge, so dass jede total geordnete Teilmenge von M eine obere Schranke hat. Dann hat M ein maximales Element.

Satz 3.9. *Sei R ein kommutativer Ring mit Eins. Für jedes Ideal $I \subsetneq R$ gibt es ein maximales Ideal J mit $I \subset J \subsetneq R$. Insbesondere falls $R \neq \{0\}$ hat R ein maximales Ideal.*

Beweisidee. Sei $M := \{I' \subsetneq R \text{ Ideal } : I \subset I'\}$ mit der partiellen Ordnung $I' \leq I'' :\iff I' \subset I''$. Es gilt $M \neq \emptyset$, da $I \in M$. Sei $N \subset M$ eine total geordnete Teilmenge. Falls $N = \emptyset$ ist $I \in M$ eine obere Schranke von N. Sonst definieren wir $I_N := \cup_{I' \in N} I'$ und wir behaupten, dass $I_N \in M$ eine obere Schranke von N ist. Die Teilmenge I_N ist ein Ideal von R, da N eine total geordnete Teilmenge ist. Es gilt $I \subset I_N$, da $I \subset I'$ für alle $I' \in N$. Falls $I_N = R$ ist $1 \in I_N$ und es gibt $I' \in N$ mit $1 \in I'$, aber dann gilt $I' = R$ und $I' \notin M$. Deshalb folgt $I_N \subsetneq R$ und $I_N \in M$. Für $I' \in N$ gilt $I' \leq I_N$ d.h. I_N ist eine obere Schranke von N. Nach dem Lemma von Zorn hat M ein maximales Element J und insbesondere ist $J \subsetneq R$ ein maximales Ideal, das I enthält. Falls $R \neq \{0\}$ gibt es für $I := \{0\} \subsetneq R$ ein maximales Ideal J mit $I \subset J \subsetneq R$. □

Satz 3.10. *Jeder Körper K hat eine Körpererweiterung $K \subset L$ mit L algebraische abgeschlossen.*

Beweisidee. Wir werden eine Kette von Körpererweiterungen $K = L_0 \subset L_1 \subset \cdots$ konstruieren, so dass jedes nicht-konstante Polynom $f(t) \in L_n[t]$ eine Nullstelle in L_{n+1} hat. Dann setzen wir $L = \cup_{n \geq 0} L_n$.

Für die Konstruktion von L_1 definieren wir eine Indexmenge $\mathcal{A} := \{f \in K[t] : \text{grad}(f) \geq 1\}$ und betrachten den Polynomring $K[t_f : f \in \mathcal{A}]$ in Variablen t_f für alle $f \in \mathcal{A}$. Sei $I = (f(t_f) : f \in \mathcal{A}) \subset K[t_f : f \in \mathcal{A}]$ das von $\{f(t_f) : f \in \mathcal{A}\}$ erzeugte Ideal. Falls $I = K[t_f : f \in \mathcal{A}]$ ist $1 \in I$, d.h. es gibt $n \in \mathbb{N}$ und $f_1, \ldots, f_n \in \mathcal{A}$ und $g_1, \ldots, g_n \in K[t_f : f \in \mathcal{A}]$ mit $1 = \sum_{i=1}^n g_i f_i(t_{f_i})$. Nach Verwendungen des Satzes 3.8 für $f_1, \ldots, f_n$ gibt es eine algebraische Körpererweiterung $K \subset K'$, so dass jedes Polynom f_i eine Nullstelle $\alpha_i \in K'$ hat. Dann betrachten wir die Familie $\{\alpha_f : f \in \mathcal{A}\}$ von Elementen $\alpha_f \in K'$, wobei $\alpha_f = \alpha_i$ falls $f = f_i$ und sonst ist $\alpha_f = 0$. Die Evaluation bei $\{\alpha_f : f \in \mathcal{A}\}$ definiert einen Ringhomomorphismus

$$\Phi : K[t_f : f \in \mathcal{A}] \to K' \qquad P(f_f : f \in \mathcal{A}) \mapsto P(\alpha_f : f \in \mathcal{A}).$$

Dann folgt einen Widerspruch: $1 = \Phi(1) = \Phi(\sum_{i=1}^n g_i f_i(t_{f_i})) = \sum_{i=1}^n g_i(\alpha_f : f \in \mathcal{A}) f_i(\alpha_i) = 0$. Daher gilt $I \neq K[t_f : f \in \mathcal{A}]$ und es gibt es ein maximales Ideal $J \subsetneq K[t_f : f \in \mathcal{A}]$ mit $I \subset J$ nach dem Satz 3.9. Wir definieren $L_1 := K[t_f : f \in \mathcal{A}]/J$, der ein Körper ist (Satz 2.6). Der Ringhomomorphismus

$$K \hookrightarrow K[t_f : f \in \mathcal{A}] \twoheadrightarrow L_1 := K[t_f : f \in \mathcal{A}]/J$$

ist injektiv: für $\lambda \in K \neq \{0\}$ aus $\lambda \in J$ folgt $1 = \lambda\lambda^{-1} \in J$ (aber $J \neq K[t_f : f \in \mathcal{A}]$). Insbesondere hat jedes $f \in \mathcal{A} = \{f \in K[t] : \text{grad}(f) \geq 1\}$ eine Nullstelle $t_f + J$ in L_1.

Wir konstruieren $L_n \subset L_{n+1}$, wie die obige Konstruktion von $L_0 = K \subset L_1$, so dass jedes nicht-konstante Polynom $f(t) \in L_n[t]$ eine Nullstelle in L_{n+1} hat. Sei $L = \cup_{n \geq 0} L_n$. Sei $f = \sum_{i=0}^m c_i t^i \in L[t]$ ein nicht-konstantes Polynom. Für $0 \leq i \leq m$ gibt es n_i mit $c_i \in L_{n_i}$. Dann gilt $f \in L_n[t]$, wobei $n = \max\{n_i : 0 \leq i \leq m\}$, und f hat eine Nullstelle in $L_{n+1} \subset L$. Deshalb ist L algebraisch abgeschlossen. □

Definition. Ein *algebraischer Abschluss* eines Körpers K ist eine algebraische Körpererweiterung $K \subset L$ mit L algebraische abgeschlossen. Normalerweise schreibt man $L = \overline{K}$ für einen

[4]Der Beweis benutzt das Auswahlaxiom (z.B. siehe Tuschik und Wolter 'Mathematische Logik' Satz 5.13).

algebraischen Abschluss von K.

Korollar. Jeder Körper K hat einen algebraischen Abschluss.

[29.11.18]

Beweisidee. Sei L der Körper in dem Beweis des Satzes 3.10. Dann müssen wir zeigen, dass $K \subset L$ eine algebraische Körpererweiterung ist. Nach Konstruktion $L = \cup_{n\geq 0} L_n$ für eine Kette $K = L_0 \subset L_1 \subset \cdots$ von Körpererweiterungen. Die Körpererweiterung $L_0 = K \subset L_1 = k[t_f : f \in \mathcal{A}]/J$ ist algebraisch: da L_1 von die Familie $\{t_f + J : f \in \mathcal{A}\} \subset L_1$ von algebraischen Elementen über K erzeugt wird ($t_f + J$ ist eine Nullstelle von $f(t) \in K[t]$). Ebenso ist $L_{n-1} \subset L_n$ algebraisch und es folgt aus dem Satz 3.6, dass $K \subset L_n$ algebraisch ist. Dann ist $L = \cup_{n\geq 0} L_n$ algebraisch über K. □

Bemerkung. Sie $K \subset L$ eine Körpererweiterung mit L einem algebraischen abgeschlossen Körper. Wir haben schon gesehen, dass

$$\mathbb{A}_{L/K} := \{\alpha \in L : \alpha \text{ ist algebraisch über } K\}$$

eine algebraische Körpererweiterung von K ist. Wir behaupten, dass $\mathbb{A}_{L/K}$ ein algebraisher Abschluss von K ist. Wir müssen nur zeigen, dass $\mathbb{A}_{L/K}$ algebraisch abgeschlossen ist. Sei $f \in \mathbb{A}_{L/K}[t]$ ein nicht-konstantes Polynom. Dann hat f eine Nullstelle $\alpha \in L$ und $\mathbb{A}_{L/K} \subset \mathbb{A}_{L/K}(\alpha)$ ist algebraisch. In der Kette $K \subset \mathbb{A}_{L/K} \subset \mathbb{A}_{L/K}(\alpha)$ sind $K \subset \mathbb{A}_{L/K}$ und $\mathbb{A}_{L/K} \subset \mathbb{A}_{L/K}(\alpha)$ algebraische Körpererweiterungen und deshalb ist $K \subset \mathbb{A}_{L/K}(\alpha)$ algebraisch (Satz 3.7). Insbesondere ist α algebraisch über K, d.h. $\alpha \in \mathbb{A}_{L/K}$.

Notation. Für einen Körperhomomorphismus $\varphi : K \to L$ und $f = \sum_{i=0}^n a_i t^i \in K[t]$ schreiben wir $f^\varphi = \sum_{i=0}^n \varphi(a_i) t^i$ für das Bild von f unter den Ringhomomorphismus $K[t] \to L[t]$.

Lemma. Sei K ein Körper und $j : K \hookrightarrow K(\alpha)$ eine algebraische Körpererweiterung mit dem Minimalpolynom $m := m_\alpha \in K[t]$. Sei $\varphi : K \to L$ ein Körperhomomorphismus. Dann gilt

(1) Wenn $\varphi = \varphi' \circ j$ für einen Körperhomomorphismus $\varphi' : K(\alpha) \to L$, ist $\varphi'(\alpha) \in L$ eine Nullstelle von $m^\varphi \in L[t]$.
(2) Zu jeder Nullstelle $\beta \in L$ von $m^\varphi \in L[t]$ gibt es einen Körperhomomorphismus $\varphi_\beta : K(\alpha) \to L$ mit $\varphi = \varphi_\beta \circ j$ und $\beta = \varphi_\beta(\alpha)$.

Ferner ist die Anzahl von Körperhomomorphismus $\varphi' : K(\alpha) \to L$ mit $\varphi = \varphi' \circ j$ gleich die Anzahl der verschiedenen Nullstellen von m in L (und diese Zahl ist kleiner oder gleich $\text{grad}(m)$).
Beweisidee. Für (1): Es gilt $m^\varphi(\varphi'(\alpha)) = \varphi'(m(\alpha)) = 0$. Für (2): Seien

$$\Phi_\alpha : K[t] \to K(\alpha) \quad \text{und} \quad \Psi_\beta : K[t] \to L$$

die Ringhomomorphismen mit $\Phi_\alpha(f) = f(\alpha)$ und $\Psi_\beta(f) = f^\varphi(\beta)$. Dann gilt $\ker(\Phi_\alpha) = (m)$ und $(m) \subset \ker(\Psi_\beta)$. Daher gibt es Körperhomomorphismen $\overline{\Phi_\alpha} : K[t]/(m) \to K(\alpha)$ und $\overline{\Psi_\beta} : K[t]/(m) \to L$, so dass $\Phi_\alpha = \overline{\Phi_\alpha} \circ \pi$ und $\Psi_\beta = \overline{\Psi_\beta} \circ \pi$ für $\pi : K[t] \to K[t]/(m)$. Ferner ist $\overline{\Phi_\alpha}$ ein Isomorphismus (Satz 3.3). Wir definieren einen Körperhomomorphismus $\varphi_\beta := \overline{\Psi_\beta} \circ \overline{\Phi_\alpha}^{-1} : K(\alpha) \to L$. Dann gilt $\varphi = \varphi_\beta \circ j$ und $\varphi_\beta(\alpha) = \psi_\beta(t) = \beta$. Aus die Aussagen (1) und (2) definieren ein paar von Funktionen zwischen der Mengen

$$\left\{ \begin{array}{c} \text{Körperhomomorphismus } \varphi' : K(\alpha) \to L \\ \text{mit } \varphi = \varphi_\beta \circ j \text{ und } \beta = \varphi_\beta(\alpha) \end{array} \right\} \longleftrightarrow \{\text{Nullstellen } \beta \in L \text{ von } m_\alpha^\varphi \in L[t]\}$$

und wir überlassen es dem Leser, zu überprüfen, ob diese Funktionen Umkehrfunktionen voneinander sind. Dann folgt die letzte Aussage. □

Satz 3.11 (Eindeutigkeit des algebraischen Abschlusses bis auf Isomorphie)**.** *Sei $j : K \hookrightarrow K'$ eine algebraische Körpererweiterung und $\varphi : K \to L$ ein Körperhomomorphismus, wobei L algebraisch abgeschlossen ist.*

(1) Dann hat φ eine Erweiterung zu einem Körperhomomorphismus $\varphi' : K' \to L$ mit $\varphi = \varphi' \circ j$ (d.h. $\varphi'|_K = \varphi$).
(2) Wenn K' auch algebraisch abgeschlossen ist und $\mathrm{Bild}(\varphi) \subset L$ *algebraisch ist, dann ist jede $\varphi' : K' \to L$ mit $\varphi = \varphi' \circ j$ ein Isomorphismus.*
(3) Wenn K' und L zwei algebraische Abschlüsse von K sind, dann existiert einen Isomorphismus $\varphi' : K' \to L$, so dass die Einschränkung $\varphi'|_K$ die Identität auf K ist.

Beweisidee. Für (1) : Sei $M = \{(F, \tau) : K \subset F \subset K', \tau : F \to L \text{ mit } \tau|_K = \varphi\}$ mit der partiellen Ordnung $(F, \tau) \leq (F', \tau') \iff F \subset F'$ und $\tau = \tau'|_F$. Wir überlassen es dem Leser, zu überprüfen, dass jede total geordnete Teilmenge $N \subset M$ eine obere Schranke hat. Dann hat M ein maximales Element (F, τ) nach dem Lemma von Zorn. Wir behaupten, dass $F = K'$. Falls nicht gibt es $\alpha \in K' \setminus F$ und es gilt $K \subset F \subset F(\alpha) \subset K'$. Da K'/K algebraische ist, ist α algebraische über K und deshalb auch algebraisch über F. Sei $m_\alpha \in F[t]$ das Minimalpolynom von α über F und sei $\beta \in L = \overline{L}$ eine beliebige Nullstelle von $m_\alpha^\tau \in L[t]$. Nach dem Lemma 2) gibt es einen Körperhomomorphismus $\tau_\beta : F(\alpha) \to L$ mit $\tau_\beta|_F = \tau$ und $\tau_\beta(\alpha) = \beta$. Aber dann gilt $(F(\alpha), \tau_\beta) \in M$ und $(F(\alpha), \tau_\beta) > (F, \tau)$, was einen Widerspruch zu der Maximalität von F gibt. Deshalb gilt $F = K'$ und insbesondere gibt es eine Körperhomomorphismus $\varphi' = \tau : K' \to L$, so dass $\varphi = \varphi' \circ j$.

Für (2): Wir nehmen an, dass $K' = \overline{K'}$ und $\varphi' : K' \to L$ ein Körperhomomorphismus mit $\varphi = \varphi' \circ j$ ist. Es gilt $\varphi(K) \subset \varphi'(K') \subset L$ und da $L/\varphi(K)$ algebraische ist, dann ist $L/\varphi'(K')$ algebraisch. Aber $\varphi'(K')$ ist algebraisch abgeschlossen und deshalb hat keine echte algebraische Körpererweiterungen, also gilt $L = \varphi'(K')$. Deshalb ist φ' surjektiv und auch injektiv (da jeder Körperhomomorphismus injektiv ist).

Für (3) gibt es einen Isomorphismus $\varphi' : K' \to L$ nach (1) und (2) und man überprüft, dass $\varphi'|_K = \mathrm{Id}_K$. □

3.4. **Irreduzibilitätskriterien.** Um das Minimalpolynom eines algebraischen Elements zu finden, werden wir einige Irreduzibilitätskriterien beweisen.

Bemerkung. Sei R ein faktorieller Ring mit Quotientenkörper $K = Q(R)$. Dann hat jedes nicht-konstante Polynom $f \in K[t]$ eine Darstellung $f = c\tilde{f}$ mit $c \in K^\times$ und $\tilde{f} \in R[t]$ primitiv. Beide $R[t]$ und $K[t]$ sind faktorielle (nach dem Satz von Gauß) und in einem faktoriellen Ring stimmen die Begriffe 'prim ' und 'irreduzibel' überein. Dann ist äquivalent:

(1) $f \in K[t]$ ist irreduzibel,
(2) $\tilde{f} \in K[t]$ ist irreduzibel,
(3) $\tilde{f} \in R[t]$ ist irreduzibel,

da $f \sim \tilde{f}$ in $K[t]$ (also gilt (1) $\iff$ (2)) und die Äquivalenz (2) $\iff$ (3) folgt aus dem Satz 2.14.

Satz 3.12. *(Eisensteinsche Kriterium) Sei R ein faktorieller Ring, $p \in R$ ein Primelement und $f(t) = \sum_{i=0}^n a_i t^i \in R[t]$ ein primitives Polynom mit $n = \mathrm{grad}(f) \geq 1$, so dass*

$$p \nmid a_n \quad \textit{und} \quad p \mid a_i \, \forall \, 0 \leq i < n \quad \textit{und} \quad p^2 \nmid a_0.$$

Dann ist $f \in R[t]$ (und auch $f \in Q(R)[t]$) irreduzibel.

Beweisidee. Wenn f reduzibel ist gilt $f = gh$ mit $g = \sum_{i=0}^r b_i t^i$ und $h = \sum_{i=0}^s c_i t^i \in R[t]$. Da f primitiv ist, gilt $r = \mathrm{grad}(g), s = \mathrm{grad}(h) \geq 1$. Man hat die Gleichungen

$$a_j = \sum_{i=0}^{j} b_i c_{j-i}.$$

Aus $p \nmid a_b = b_r c_s$ folgt $p \nmid b_r$ und $p \nmid c_s$. Aus $p \mid a_0 = b_0 c_0$ und $p^2 \nmid a_0$ folgt entweder $p \mid b_0$ und $p \nmid c_0$ oder $p \nmid b_0$ und $p \mid c_0$. Ohne Einschränkung der Allgemeinheit nehmen wir an, dass $p \mid b_0$ und $p \nmid c_0$. Sei $t = \max\{i : p \mid b_j \, \forall 0 \leq j \leq i\} < r$. Dann folgt $p \nmid a_{t+1} = \sum_{j=0}^{t+1} b_j c_{t+1-j}$, da $p \mid b_j$ für $0 \leq j \leq t$ und $p \nmid b_{t+1} c_0$. Deshalb gilt $t + 1 = n$ und es folgt, dass $r = n$ und $s = 0$, was

einen Widerspruch gibt. □

Beispiel. Sei $R = \mathbb{Z}$ und $Q(R) = \mathbb{Q}$. Für eine Primzahl p und $N \in \mathbb{N}_{>0}$ ist $t^n - p \in \mathbb{Z}[t]$ (und $\mathbb{Q}[t]$) irreduzibel nach dem Eisensteinschen Kriterium.

Bemerkung. Sei R ein Integritätsbereich und $a \in R$. Dann ist $f(t) \in R[t]$ genau dann irreduzibel, wenn $f(t+a)$ irreduzibel ist (da $\Phi_a : R[t] \to R[t]$ mit $\Phi_a(f) := f(t+a)$ ein Ringisomorphismus ist).

Beispiel. Sei p eine Primzahl. Dann ist $f(t) = t^{p-1} + \cdots + 1 = (t^p - 1)/(t-1)$ irreduzibel in $\mathbb{Z}[t]$ und $\mathbb{Q}[t]$, da

$$g(t) := f(t+1) = \sum_{i=0}^{p-1} \binom{p}{i} t^{p-i-1}$$

irreduzibel ist (nach dem Eisensteinschen Kriterium).

Satz 3.13. *(Reduktionskriterium) Sei R ein faktorieller Ring, $p \in R$ ein Primelement und $f(t) = \sum_{i=0}^n a_i t^i \in R[t]$ ein Polynom mit $n = \operatorname{grad}(f) \geq 1$, so dass $p \nmid a_n$. Sei $\Phi : R[t] \to (R/(p))[t]$ der kanonische Ringhomomorphismus mit $\Phi(\sum_{i=0}^m b_i t^i) = \sum_{i=0}^m (b_i + (p))t^i$. Dann gilt*

(1) Wenn $\Phi(f) \in (R/(p))[t]$ irreduzibel ist, ist $f \in Q(R)[t]$ irreduzibel.
(2) Wenn $\Phi(f) \in (R/(p))[t]$ irreduzibel ist und $f \in R[t]$ primitiv ist, ist $f \in R[t]$ irreduzibel.

Beweisidee. Für (2): Falls f reduzibel in $R[t]$ ist, gibt es eine Zerlegung $f = gh$ mit $= \sum_{i=0}^s b_i t^i$ und $h = \sum_{i=0}^r c_i t^i \in R[t]$ und $s = \operatorname{grad}(g), r = \operatorname{grad}(h) \geq 1$ (da f primitiv ist). Aus $p \nmid a_n = b_s c_r$ folgt $p \nmid b_s$ und $p \nmid c_r$. Daher sind die Klassen $b_s + (p), c_r + (p) \in R/(p)$ nicht-Null. Dann folgt $\Phi(f) = \Phi(g)\Phi(h)$ mit $s = \operatorname{grad}(\Phi(g)), r = \operatorname{grad}(\Phi(h)) \geq 1$, aber $\Phi(f)$ ist irreduzibel und deshalb müss f irreduzibel sein. Für (1) schreiben wir $f = c\tilde{f}$ mit $c \in R$ und $\tilde{f} = \sum_{i=0}^n \tilde{a_i} t^i \in R[t]$ ein primitives Polynom. Aus $p \nmid a_n = c\tilde{a_n}$ folgt $p \nmid c$ (d.h. $\Phi(c) \neq 0$) und $p \nmid \tilde{a_n}$. Aus $\Phi(f) = \Phi(c)\Phi(\tilde{f})$ und die Irreduzibilität von $\Phi(f)$ folgt die irreduzibilität von $\Phi(\tilde{f})$ und aus (2) folgt die Irreduzibilität von $\tilde{f} \in R[t]$. Nach der ersten Bermerkung in diesem Abschnitt folgt die Irreduzibilität von $f \in Q(R)[t]$. □

Beispiel. Sei $f(t) = t^3 + 3t^2 - 4t - 1 \in \mathbb{Z}[t]$ und $p = 3$. Dann betrachten wir $\Phi : \mathbb{Z}[t] \to \mathbb{F}_3[t]$, wobei $\mathbb{F}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$. Es gilt $\Phi(f) = \overline{1}t^3 - \overline{1}t - \overline{1} \in \mathbb{F}_3[t]$ und diese Polynom ist irreduzibel, da es keine Nullstellen hat und $\operatorname{grad}(\Phi(f)) = 3$. Nach dem Reduktionskriterium ist $f \in \mathbb{Z}[t]$ und $f \in \mathbb{Q}[t]$ irreduzibel.

3.5. **Zerfällungskörper.**

Definition. Sei K ein Körper und $\mathcal{F} = \{f_i : i \in I\}$ eine Familie nicht-konstanter Polynome $f_i \in K[t]$. Ein *Zerfällungskörper* von $\mathcal{F}$ über K ist ein Erweiterungskörper L von K mit den folgenden Eigenschaften:

(1) Jedes Polynom $f_i \in \mathcal{F}$ zerfällt in Linearfaktoren über L,
(2) L wird von der Nullstellen der Polynome f_i für alle $i \in I$ über K erzeugt.

Lemma. Jede Familie nicht-konstanter Polynome aus $K[t]$ hat ein Zerfällungskörper. Ferner ist ein Zerfällungskörper einer endlichen Familie von Polynome aus $K[t]$ ein endliche Körpererweiterung von K.

Beweisidee. Sei $\overline{K}$ ein algebraischer Abschluss von K und sei $\mathcal{F} = \{f_i : i \in I\}$ eine Familie nicht-konstanter Polynome $f_i \in K[t]$. Seien $\alpha_{i,j} \in \overline{K}$ für $1 \leq j \leq n_i$ die Nullstellen von f_i. Dann ist $K(\{\alpha_{i,j} : i \in I, 1 \leq j \leq n_i\})$ ein Zerfällungskörper von $\mathcal{F} \subset K[t]$. □

Definition. Sei $K \subset L$ und $K \subset L'$ Körpererweiterungen und $\mathrm{Hom}(L, L')$ die Menge aller Körperhomomorphismus $L \to L'$. Wir definieren

$$\mathrm{Hom}_K(L, L') := \{\varphi : L \to L' \in \mathrm{Hom}(L, L') : \varphi|_K = \mathrm{id}_K\}$$

und wir nennen die Elemente K-Homomorphismen. Falls $L = L'$ schreiben wir $\mathrm{End}_K(L) := \mathrm{Hom}_K(L, L) \subset \mathrm{End}(L) := \mathrm{Hom}(L, L)$. Ebenso definieren wir $\mathrm{Aut}_K(L) \subset \mathrm{Aut}(L)$ mit Körperautomorphismen.

Satz 3.14. *Seien L_1 und L_2 zwei Zerfällungskörper einer Familie $\mathcal{F} = \{f_i : i \in I\}$ nichtkonstanter Polynome $f_i \in K[t]$ und sei $\varphi : L_1 \to \overline{L_2}$ ein K-Homomorphismus zu einem algebraischen Abschluss von L_2. Dann beschränkt sich φ zu einem Isomorphismus $\varphi|_{L_1} : L_1 \to L_2$.*

Beweisidee. Falls $\mathcal{F} = \{f_1, \dots, f_n\}$ endlich ist: sei $f = \prod_{i=1}^n f_i$. Seien $a_1, \dots a_m \in L_1$ (bzw. $b_1, \dots, b_m \in L_2$) die Nullstellen von f (wobei $m = \mathrm{grad}(f)$), so dass $L_1 = K(a_1, \dots, a_m)$ und $L_2 = K(b_1, \dots, b_m)$. Für die Inklusion $i_j : K \hookrightarrow L_j$ gilt

$$f^{i_1}(t) = \prod_{i=1}^m (t - a_i) \in L_1[t] \quad \text{und} \quad f^{i_2}(t) = \prod_{i=1}^m (t - b_i) \in L_2[t].$$

Für $\varphi \in \mathrm{Hom}_K(L_1, \overline{L_2})$ gilt $\Pi_{i=1}^m (t - \varphi(a_i)) = f^{\varphi \circ i_1}(t) = f^{i_2} = \Pi_{i=1}^m (t - b_i)$ und deshalb definiert φ eine Bijektion $\{a_1, \dots, \alpha_m\} \cong \{b_1, \dots, b_m\}$. Insbesondere gilt $\varphi(L_1) = K(\varphi(a_1), \dots, \varphi(a_m)) = K(b_1, \dots, b_m) = L_2$.

Falls $\mathcal{F} = \{f_i : i \in I\}$ unendlich ist: seien $a_{i,1}, \dots a_{i,n_i} \in L_i$ (bzw. $b_{i,1}, \dots, b_{i,n_i} \in L_2$) die Nullstellen von f_i (wobei $n_i = \mathrm{grad}(f_i)$). Für jede endliche $J \subset I$ beschränkt sich φ zu einem Isomorphismus

$$\varphi| : K(\{a_{j,k} : j \in J, 1 \le k \le n_j\}) \to K(\{b_{j,k} : j \in J, 1 \le k \le n_j\})$$

Da $L_1 = \cup_J K(\{a_{j,k} : j \in J, 1 \le k \le n_j\})$ und $L_2 = \cup_J K(\{b_{j,k} : j \in J, 1 \le k \le n_j\})$ für endliche Teilmengen $J \subset I$, folgt die Behauptung, dass $\varphi|_{L_1} : L_1 \to L_2$ ein Isomorphismus ist. □

Korollar. Ein Zerfällungskörper einer Familie $\mathcal{F} = \{f_i : i \in I\}$ nicht-konstanter Polynome $f_i \in K[t]$ ist eindeutig bis auf (nicht-kanonische) Isomorphie.

Beweisidee. Nach dem Satz 3.14 ist es hinreichend zu zeigen, dass es einen K-Homomorphismus $\varphi : L_1 \to \overline{L_2}$ gibt. Da $K \subset L_1$ algebraische ist gibt es einen Homomorphismus $\varphi : L_1 \to \overline{L_2}$, so dass $\varphi|_K$ die Inklusion $K \subset L_2 \subset \overline{L_2}$ ist (Satz 3.11). □

Bemerkung. Als ein Teilkörper von $\overline{K}$ ist der Zerfällungskörper von $\mathcal{F} = \{f_i : i \in I\} \subset K[t]$ eindeutig (als der von der Nullstellen von f_i in $\overline{K}$ erzeugter Körper).

Beispiel. Ein Zerfällungskörper von $t^3 - 2$ über $\mathbb{Q}$ ist $\mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$.

3.6. **Normale und Separable Körpererweiterungen.** [11.12.18]

Definition. Eine algebraische Körpererweiterung $K \subset L$ heißt *normal*, wenn jedes irreduzible Polynom in $K[t]$, welches in L eine Nullstelle besitzt, vollstandig über L in Linearfaktoren zerfällt.

Beispiel.

(1) $K \subset \overline{K}$ ist eine normale Körpererweiterung.
(2) Jede algebraische Körpererweiterung $K \subset L$ vom Grad 2 ist normal: Sei $f \in K[t]$ irreduzibel mit einer Nullstelle $\alpha \in L$. Dann gibt es $\lambda \in K^\times$, so dass $\tilde{f} := \lambda f$ normiert ist und daher ist $\tilde{f}$ das Minimalpolynom von α und es gilt $\mathrm{grad}(f) \le 2$ (da $K \subset K(\alpha) \subset L$ und $[L : K] = 2$). Jedes Polynom von Grad 2 mit K-Koeffizienten zerfällt in Linearfaktoren über L, sofern es eine Nullstelle in L besitzt.

Satz 3.15. *Für eine algebraische Körpererweiterung $K \subset L$ ist äquivalent:*

(1) *Jeder K-Homomorphismus $\varphi : L \to \overline{L}$ (wobei $\overline{L}$ ein algebraischer Abschluss von L ist) beschränkt sich zu einem K-Automorphismen von L (d.h. $\varphi(L) = L$, so dass $\varphi|_L \in \mathrm{Aut}_K(L)$).*
(2) *L ist ein Zerfällungskörper einer Familie von Polynomen aus $K[t]$.*
(3) *$K \subset L$ ist eine normale Körpererweiterung.*

Beweisidee. (1) $\implies$ (3) : Sei $f \in K[t]$ ein irreduzible Polynom mit einer Nullstelle $\alpha \in L$ von f. Sei $\beta \in \overline{L}$ eine andere Nullstelle von f und sei $\varphi : K \hookrightarrow \overline{L}$ die Inklusion. Nach dem Lemma vor Satz 3.11 gibt es einen K-Homomorphismus $\varphi' : K(\alpha) \to \overline{L}$, so dass $\varphi'|_K = \varphi$ und $\varphi'(\alpha) = \beta$. Nach dem Satz 3.11 hat φ' eine Erweiterung $\varphi'' : L \to \overline{L}$, so dass $\varphi''|_{K(\alpha)} = \varphi'$. Nach 1) gilt $\varphi''(L) = L$ und daher ist $\beta = \varphi''(\alpha) \in L$. Deshalb zerfällt f in Linearfaktoren über L.

(3) $\implies$ (2) : Da $K \subset L$ algebraische ist, gibt es eine Familie $\mathcal{A} = \{\alpha_i : i \in I\} \subset L$ von algebraischen Elementen über K mit $L = K(\mathcal{A})$. Sei $m_i \in K[t]$ das Minimalpolynom von α_i für alle $i \in I$. Nach (3) zerfällt f_i in Linearfaktoren über L und deshalb ist L ein Zerfällungskörper von $\mathcal{F} := \{m_i : i \in I\}$.

(2) $\implies$ (1) : Wir nehmen an, dass L ein Zerfällungskörper einer Familie $\mathcal{F} := \{f_i : i \in I\} \subset K[t]$ nicht-konstanter Polynomen ist. Sei $\varphi : L \to \overline{L}$ ein K-Homomorphismus. Dann ist $\varphi(L) \subset \overline{L}$ auch ein Zerfällungskörper von $\mathcal{F}$ und da der Zefällungskörper eindeutig als ein Teilkörper von $\overline{L}$ ist, gilt $\varphi(L) = L$. Deshalb ist die Einschränkung von φ zu L ein K-Automorphismus von L.□

Korollar. Seien $K \subset L \subset M$ eine Kette von algebraischen Körpererweiterungen. Wenn M/K normal ist, dann ist M/L normal.

Beweisidee. Die Aussage folgt aus dem Satz 3.15 (2). □

Bemerkung. Für eine Kette $K \subset L \subset M$ von algebraischen Körpererweiterungen folgt die Normalität von M/K nicht aus der Normalität von M/L und L/K. Zum Beispiel hat man eine Kette

$$K = \mathbb{Q} \subset L = \mathbb{Q}(\sqrt{2}) \subset M = \mathbb{Q}(\sqrt[4]{2}),$$

wobei L/K und M/L normal sind (da $[L : K] = [M : L] = 2$), aber M/K ist nicht normal: das irreduzible Polynom $t^4 - 2 \in \mathbb{Q}[t]$ hat eine Nullstelle $\sqrt[4]{2} \in M$, aber es gibt andere Nullstellen $\pm i\sqrt[4]{2} \in \mathbb{C}$, die nicht Elemente von $M \subset \mathbb{R}$ sind.

Definition. Für eine algebraische Körpererweiterung $K \subset L$ ist *eine normale Hülle* eine algebraische Körpererweiterung $L \subset L'$, so dass

(1) $K \subset L'$ normal ist, und
(2) es keinen echten Teilkörper $L \subset L'' \subsetneq L'$ mit $K \subset L''$ normal gibt.

Satz 3.16. *Sei $K \subset L$ eine algebraische Körpererweiterung. Dann gilt*

(1) *L/K hat eine normale Hülle, die bis auf Isomorphie eindeutig bestimmt ist.*
(2) *Falls L/K endlich ist, ist die normale Hülle von L/K endlich über K.*
(3) *Wenn $L \subset M$ eine algebraische Körpererweiterung ist und $K \subset M$ normal ist, gibt es eine normale Hülle L' von L/K, die durch*

$$L \subset L' = K(\{\varphi(l) : l \in L, \varphi \in \mathrm{Hom}_K(L, M)\}) \subset M$$

definiert wird. Ferner ist L' als Teilkörper von M eindeutig bestimmt.

Beweisidee. Es gibt eine Familie $\mathcal{A} = \{\alpha_i : i \in I\} \subset L$ von algebraischen Elementen über K mit $L = K(\mathcal{A})$, da L/K algebraisch ist. Sei $m_i \in K[t]$ das Minimalpolynom von α_i und $\mathcal{F} = \{m_i : i \in I\}$. Sei $L \subset M$ eine algebraische Körpererweiterung, so dass jedes m_i in Linearfaktoren über M zerfällt (z.B. $M = \overline{L}$ oder M ist eine algebraische Erweiterung von L, so dass M/K normal ist). Seien $\beta_{i,1}, \ldots, \beta_{i,d_i} \in M$ die Nullstellen von m_i und sei $\mathcal{B} = \{\beta_{i,j} : i \in I, 1 \leq j \leq d_i\} \subset M$ die Nullstellen aller m_i für $i \in I$.

Für die Existenz bei (1) behaupten wir, dass $K(\mathcal{B})$ eine normale Hülle von L/K ist. Aus $\mathcal{A} \subset \mathcal{B}$ folgt $L = K(\mathcal{A}) \subset K(\mathcal{B}) \subset M$. Die Körpererweiterung $K \subset K(\mathcal{B})$ ist normal, weil

$K(\mathcal{B})$ ein Zerfällungskörper von $\mathcal{F}$ ist (Satz 3.15). Ferner gibt es zu jedem echten Teilkörper $L \subset L' \subsetneq K(\mathcal{B})$ ein Element $\beta_{i,j} \in \mathcal{B}$ mit $\beta_{i,j} \notin \mathcal{B}$. Dann hat m_i eine Nullstelle $\alpha_i \in L'$ aber nicht alle Nullstellen liegen in L' (da $\beta_{i,j} \notin L'$). Deshalb ist L'/K nicht normal und es folgt, dass $K(\mathcal{B})$ eine normale Hülle von L/K ist.

Für die Eindeutigkeit bis auf Isomorphie bei (1): seien L_1 und L_2 zwei normale Hülle von L/K. Dann sind L_i Zerfällungskörper von $\mathcal{F}$ über K und auch über L. Nach dem Korollar vom Satz 3.14 gibt es einen L-Isomorphismus $L_1 \cong L_2$.

Für (2): wenn L/K endlich ist, kann man $\mathcal{A}$ endlich nehmen und dann ist $\mathcal{B}$ auch endlich. Deshalb ist $K(\mathcal{B})/K$ endlich.

Für (3): Sei $L \subset M$ eine algebraishce Körpererweiterung mit M/K normal. Nach dem Existenzbeweis von (1) gilt $\mathcal{B} \subset M$ und $K(\mathcal{B}) \subset M$. Sei

$$L' := K(\{\varphi(l) : l \in L, \varphi \in \mathrm{Hom}_K(L, M)\}) = K(\varphi(\alpha_i) : \alpha_i \in \mathcal{A}, \varphi \in \mathrm{Hom}_K(L, M)\}).$$

Dann behaupten wir, dass $K(\mathcal{B}) = L'$. Für jeden $\varphi \in \mathrm{Hom}_K(L, M)$ gilt $m_i^\varphi = m_i \in M[t]$, $\varphi|_K = \mathrm{Id}_K$. Wenn $\gamma \in L$ eine Nullstelle von m_i ist, dann ist $\varphi(\gamma)$ eine Nullstelle von $m_i^\varphi = m_i$. Deshalb ist $\varphi(\alpha_i) \in \mathcal{B}$ für jeden $\varphi \in \mathrm{Hom}_K(L, M)$ und $\alpha_i \in \mathcal{A}$ und es gilt $L' \subset K(\mathcal{B})$. Für die andere inklusion sei $\beta_{i,j} \in \mathcal{B}$. Nach dem Lemma vor dem Satz 3.11 gibt es $\sigma \in \mathrm{Hom}_K(K(\alpha_i), K(\mathcal{B}))$ mit $\sigma(\alpha_i) = \beta_{i,j}$ und $\sigma|_K$ ist die Inklusion $K \hookrightarrow K(\mathcal{B})$. Nach dem Satz 3.11 gibt es eine Erweiterung $\sigma' \in \mathrm{Aut}_K(\overline{K(\mathcal{B})})$, so dass $\sigma'|_{K(\alpha_i)} = \sigma$. Für jedes $\alpha_{i'} \in \mathcal{A}$ ist $\sigma'(\alpha_{i'})$ eine Nullstelle von $m_{i'}^{\sigma'} = m_{i'}$ und daher gilt $\sigma'(L) \subset K(\mathcal{B}) \subset M$. Insbesondre ist $\varphi := \sigma'|_L \in \mathrm{Hom}_K(L, M)$ und es gilt $\varphi(\alpha_i) = \sigma(\alpha_i) = \beta_{i,j}$. Deshalb folgt $K(\mathcal{B}) \subset L'$ auch und daraus $L' = K(\mathcal{B})$. Jede normale Hülle $L'' \subset M$ von L/K ist ein Zerfällungskörper von $\mathcal{F}$ und deshalb folgt $L'' = L'$ wie in dem Beweis, dass $K(\mathcal{B}) = L'$. Insbesondere ist die normale Hülle eindeutig bestimmt als Teilkörper von M. □

Definition. Sei $f \in K[t]$ ein Polynom. [13.12.18]

(1) Die *Vielfachheit* einer Nullstelle $\alpha \in \overline{K}$ von f ist

$$\mu(f, \alpha) := \max\{r : (t-\alpha)^r | f \in \overline{K}[t]\}.$$

Dann heißt α *einfache (bzw. mehrfache) Nullstelle* von f, wenn $\mu(f, \alpha) = 1$ (bzw. $\mu(f, \alpha) > 1$).

(2) f heißt *separable*, wenn alle Nullstellen von f (in $\overline{K}$) einfach sind.

Bemerkung. Es gibt eine *Derivation* $D : K[t] \to k[t]$, die durch $f(t) = \sum_{i=0}^n a_i t^i \mapsto D(f(t)) := f'(t) = \sum_{i=1}^n i a_i t^{i-1}$ definiert wird. Für $f, g \in K[t]$ und $a, b \in K$ gilt

(1) $D(af+bg) = aD(f)+bD(g)$ (d.h. D ist eine lineare Abbildung zwischen K-Vektorräumen).

(2) $D(fg) = D(f)g + fD(g)$ (d.h. D ist keine Ringhomomorphismus).

Übung. Sei $K \subset L$ eine Körpererweiterung. Für $f, g \in K[t] \setminus \{0\}$ beweisen Sie, dass der größte gemeinsame Teiler $\mathrm{ggT}_K(f, g)$ von $f, g \in K[t]$ gleich der größte gemeinsame Teiler $\mathrm{ggT}_L(f, g)$ von $f, g \in L[t]$ ist.

Lemma. Für eine Nullstelle $\alpha \in \overline{K}$ von $f \in K[t]$ ist äquivalent:

(1) α ist eine mehrfache Nullstelle von f,

(2) α ist eine Nullstelle von f',

(3) α ist eine Nullstelle von $\mathrm{ggT}(f, f')$.

Beweisidee. Nach der Übung ist es hinreichend, die Aussage für $K = \overline{K}$ einen algebraischen abgeschlossenen Körper. Für 1) $\implies$ 2): Falls $f(t) = (t-\alpha)^r g(t)$ mit $r \geq 2$ gilt $f'(t) = r(t-\alpha)^{r-1} g(t) + (t-\alpha)^r g'(t)$ und deshalb folgt $f'(\alpha) = 0$. Die Implikation 2) $\implies$ 3) folgt, da $\mathrm{ggT}(f, f')$ eine Linearkombination von f und f' ist. Für 1) $\implies$ 2): aus $(t-\alpha) | \mathrm{ggT}(f, f')$ folgt $(t-\alpha) | f, f'$. Daher gilt $f(t) = (t-\alpha)g(t)$ und $(t-\alpha) | f'(t) = (t-\alpha)g'(t) + g(t)$ impliziert, dass

$(t-\alpha)|g(t)$, d.h. $(t-\alpha)^2|f(t)$. □

Satz 3.17. *Ein nicht-konstantes Polynom f ist genau dann separabel, wenn* $\mathrm{ggT}(f,f')=1$.

Beweisidee. Nach dem Lemma ist f genau dann separabel, wenn $\mathrm{ggT}(f,f')$ keine Nullstelle hat (d.h. $\mathrm{ggT}(f,f')=1$[5].) □

Bemerkung.

(1) Ein irreduzible Polynom $f\in K[t]$ hat genau dann eine mehrfache Nullstelle, wenn $f'=0$ (das Nullpolynom). Für die nicht-trivial Implikation: wenn α eine Nullstelle von f ist, dann ist das Minimalpolynom m_α gleich λf für $\lambda\in K^\times$ (da f irreduzibel ist). Falls α eine mehrfache Nullstelle von f ist, gilt $f'(\alpha)=0$. Aber $\mathrm{grad}(f')<\mathrm{grad}(f)=\mathrm{grad}(m_\alpha)$ und nach der Minimalität von m_α folgt $f'=0$.
(2) In Charakteristik Null ist jedes irreduzible Polynom separabel, da für jedes nicht-konstante Polynom f die Ableitung nicht das Nullpolynom ist.
(3) In Charakteristik $p>0$ gibt es nicht-konstante Polynome mit $f'=0$. z.B. $f(t)=t^p-a$ für $a\in K^\times$ und deshalb ist f nicht separabel.

Satz 3.18. *Sei $f\in K[t]$ irreduzibel.*

(1) Falls $\mathrm{Char}(K)=0$ *ist f separable.*
(2) Falls $\mathrm{Char}(K)=p>0$ *sei* $r:=\max\{s\in\mathbb{N}:\exists h\in K[t]$ *mit* $f(t)=h(t^{p^s})\}$. *Sei $g\in K[t]$ mit $f(t)=g(t^{p^r})$. Dann gilt*
a) f ist genau dann separabel, wenn $r=0$.
b) g ist irreduzibel und separabel.
c) Die Nullstellen von f haben Vielfachheiten p^r.
d) Die Nullstellen von f sind p^r-Wurzeln der Nullstellen von g.

Beweisidee. Wir haben schon Aussage 1) in der Bemerkung bewiesen. Für 2) *a*) schreiben wir $f(t)=\sum_{i=0}^n a_it^i$ und $f'(t)=\sum_{i=1}^n ia_it^{i-1}$. Nach der Bemerkung ist f genau dann nicht separable, wenn $f'=0$. Es gilt $f'=0$ genau dann, wenn $p|a_i=0$ für alle $i=1,\dots,n$ mit $a_i\neq 0$ (d.h. $f(t)=h(t^p)$ für $h\in K[t]$, also $r>0$). Für *b*) folgt die Irreduzibilität von g aus f. Nach der Maximalität von r gilt $g'\neq 0$ (das Nullpolynom) und daher ist g separabel. Für *c*) und *d*) schreiben wir $g(t)=\prod_{i=1}^m(t-\alpha_i)\in\overline{K}[t]$ mit $\alpha_1,\dots,\alpha_m$ paarweise verschieden. Sei $\beta_i\in\overline{K}$ eine p^r-Wurzel von α, also $\beta_i^{p^r}=\alpha_i$. Dann gilt

$$f(t)=g(t^{p^r})=\prod_{i=1}^m(t^{p^r}-\beta_i^{p^r})=\prod_{i=1}^m(t-\beta_i)^{p^r}$$

und $\beta_1,\dots,\beta_m$ sind die Nullstelle von f mit Vielfachheiten $\mu(f,\beta_i)=p^r$. □

Definition. Sei $K\subset L$ eine algebraische Körpererweiterung.

(1) $\alpha\in L$ heißt *separabel über K*, wenn das Minimalpolynom $m_\alpha\in K[t]$ separabel ist.
(2) Die Körpererweiterung $K\subset L$ heißt *separabel*, wenn jedes Element $\alpha\in L$ separabel über K ist.
(3) Ein Körper K heißt *perfekt*, wenn jede algebraische Körpererweiterung von K separabel ist.

Korollar. (Satz 3.18) In Charakteristik 0 ist jede algebraische Körpererweiterung separabel. Deshalb ist jeder Körper der Charakteristik 0 perfekt.

Beispiel. Sie $\mathbb{F}_p(t)=Q(\mathbb{F}_p[t])$. Dann ist $x^p-t\in\mathbb{F}_p(t)[x]$ irreduzibel nach Eisenstein. Die Körpererweiterung $\mathbb{F}_p(t)\subset\mathbb{F}_p(t)[x]/(x^p-t)$ ist nicht separabel: sei $\alpha\in\mathbb{F}_p(t)[x]/(x^p-t)$ eine

[5]Der ggT ist nur bis auf Assoziiertheit wohldefiniert.

Nullstell von $x^p - t$, dann ist $m_\alpha(x) = x^p - t$ nicht separabel ($m'_\alpha(x) = 0$).

Definition. Sei $K \subset L$ eine algebraische Körpererweiterung. Der Separabilitätsgrad von L/K ist

$$[L : K]_s := |\operatorname{Hom}_K(L, \overline{K})|$$

für einen algebraischen Abschluss $\overline{K}$ von K.[6]

Lemma. Sei $K \subset L = K(\alpha)$ eine einfache algebraische Körpererweiterung und $m_\alpha \in K[t]$ das Minimalpolynom von α. Dann gilt [18.12.18]

i) $[L : K]_s$ ist die Anzahl der verschiedenen Nullstelle von m_α (in $\overline{K}$).
ii) α ist genau dann separabel, wenn $[L : K]_s = [L : K]$.
iii) Wenn $\operatorname{Char}(K) = p > 0$ und $\mu(m_\alpha, \alpha) = p^r$ (Satz 3.18), dann gilt $[L : K] = p^r[L : K]_s$.

Beweisidee. Teil i) folgt aus dem Lemma vor dem Satz 3.11. Für ii) ist α genau dann separabel, wenn m_α genau $\operatorname{grad}(m_\alpha)$ verschiedene Nullstellen hat. Ferner gilt $[L : K] = \operatorname{grad}(m_\alpha)$ nach dem Satz 3.3. Teil iii) folgt aus i) und Satz 3.18. □

Satz 3.19. *Seien $K \subset L \subset M$ eine Kette von algebraischen Körpererweiterungen. Dann gilt*

$$[M : K]_s = [M : L]_s[L : K]_s.$$

Beweisidee. Sei $\overline{K}$ ein algebraischer Abschluss von K. Dann ist $\overline{K}$ auch ein algebraische Abschluss von L und M (da $\overline{K}$ keine echte algebraische Körpererweiterungen hat). Wir schreiben

$$\operatorname{Hom}_K(L, \overline{K}) = \{\sigma_i : i \in I\} \quad \text{und} \quad \operatorname{Hom}_L(M, \overline{K}) = \{\tau_j : j \in J\}.$$

Dann gilt $[L : K]_s = |I|$ und $[M : L]_s = |J|$ und wir müssen zeigen, dass $[M : K]_s = |I||J|$. Nach dem Satz 3.11 hat jeder K-Homomorphismus $\sigma_i : L \to \overline{K}$ eine Erweiterung $\tilde{\sigma}_i \in \operatorname{Aut}_K(\overline{K})$ mit $\tilde{\sigma}_i|_L = \sigma_i$. Wir behaupten:

a) Der K-Homomorphismen $\tilde{\sigma}_i \circ \tau_j : M \to \overline{K}$ sind paarweise verschieden.
b) $\operatorname{Hom}_K(M, \overline{K}) = \{\tilde{\sigma}_i \circ \tau_j : i \in I, j \in J\}$ (und deshalb gilt $[M : K]_s = |I||J|$).

Für a): aus $\tilde{\sigma}_i \circ \tau_j = \tilde{\sigma}_{i'} \circ \tau_{j'}$ folgt

$$\sigma_i = \tilde{\sigma}_i|_L = (\tilde{\sigma}_i \circ \tau_j)|_L = (\tilde{\sigma}_{i'} \circ \tau_{j'})|_L = \tilde{\sigma}_{i'}|_L = \sigma_{i'}$$

da $\tau_j|_L = \tau_{j'}|_L = \operatorname{Id}_L$. Deshalb gilt $i = i'$ und da $\tilde{\sigma}_i = \tilde{\sigma}_{i'}$ invertierbar ist, folgt $\tau_j = \tau_{j'}$ und $j = j'$.

Für b): sei $\varphi \in \operatorname{Hom}_K(M, \overline{K})$. Dann gilt $\varphi|_L \in \operatorname{Hom}_K(L, \overline{K})$, also $\varphi|_L = \sigma_i$ für ein Element $i \in I$. Dann folgt $\tilde{\sigma}_i^{-1} \circ \varphi \in \operatorname{Hom}_L(M, \overline{K})$, also $\tilde{\sigma}_i^{-1} \circ \varphi = \tau_j$ für ein Element $j \in J$. □

Satz 3.20. *Sei $K \subset L$ eine endliche Körpererweiterung.*

(1) Falls $\operatorname{Char}(K) = 0$ gilt $[L : K]_s = [L : K]$.
(2) Falls $\operatorname{Char}(K) = p > 0$ existiert $r \in \mathbb{N}$ mit $[L : K] = p^r[L : K]_s$.

Beweisidee. Man schreibt $K \subset L$ als eine Kette von einfachen Körpererweiterungen und dann benutzt Satz 3.19 und das obige Lemma. □

Satz 3.21. *Für eine endliche Körpererweiterung $K \subset L$ ist äquivalent:*

(1) L/K ist separabel,
(2) Es gibt separable Elemente $\alpha_1, \cdots, \alpha_n \in L$ (über K) mit $L = K(\alpha_1, \ldots, \alpha_n)$,
(3) $[L : K]_s = [L : K]$.

Beweisidee. (1) $\implies$ (2) ist trivial.
(2) $\implies$ (3): Man betrachtet die Kette

$$K = K_0 \subset K_1 = K(\alpha_1) \subset K_2 = K(\alpha_1, \alpha_2) \subset \cdots \subset K_n = K(\alpha_1, \ldots, \alpha_n) = L.$$

Da jede $\alpha_i \in K_i$ ist separabel über K_{i-1} verwenden wir das obige Lemma und Satz 3.19.

[6]Die Definition ist unabhängig der Wahl von $\overline{K}$ nach der Eindeutigkeit von $\overline{K}$ bis auf Isomorphie.

(3) $\implies$ (1): Sei $\alpha \in L$ und $m_\alpha \in K[t]$ das Minimalpolynom von α. In Charakteristik 0 gilt (1), da jede endliche Körpererweiterung separabel ist. Deshalb nehmen wir an, dass $\mathrm{Char}(K) = p > 0$. Nach dem Satz 3.20 gibt es $r \in \mathbb{N}$ mit $[K(\alpha) : K] = p^r[K(\alpha) : K]_s$ und jede Nullstelle von m_α hat Vielfachheit p^r. Es gilt

$$[L : K] = [L : K(\alpha)][K(\alpha) : K] \geq [L : K(\alpha)]_s p^r [K(\alpha) : K]_s = p^r [L : K]_s.$$

Aus $[L : K]_s = [L : K]$ folgt $r = 0$, d.h. jede Nullstelle von m_α hat Vielfachheit $1 = p^0$ und deshalb ist α separabel. □

Satz 3.22. *Sei $K \subset L = K(\mathcal{A})$ eine algebraische Körpererweiterung, wobei $\mathcal{A} = \{\alpha_i : i \in I\}$ eine Familie von Elementen aus L ist. Dann ist äquivalent:*

(1) L/K ist separabel,
(2) Jedes $\alpha_i \in \mathcal{A}$ ist separabel (über K),

Wenn diese äquivalente Bedingungen gelten, folgt $[L : K]_s = [L : K]$.

Beweisidee. Die Äquivalenz (1) $\iff$ (2) folgt aus dem Satz 3.21, da zu jedem Element $\alpha \in L$ es $\alpha_{i_1}, \ldots, \alpha_{i_n}$ mit $\alpha \in K(\alpha_{i_1}, \ldots, \alpha_{i_n})$ gibt. Wenn K/L separabel und endlich ist, folgt die Gleichheit $[L : K]_s = [L : K]$ aus dem Satz 3.21. Wenn K/L separabel und unendlich ist, dann gilt für alle Zwischenkörper $K \subset L' \subset L$ mit $[L' : K] < \infty$ die Gliechheit $[L' : K]_s = [L' : K]$ (da L'/K auch separabel ist). Ferner gilt

$$[L : K]_s = [L : L']_s [L' : K]_s \geq [L' : K].$$

Zu jeder Zahl $n \in N$ gibt es einen Zwischenkörper $K \subset L'_n \subset L$ mit $[L'_n : K] \geq n$ (da $[L : K] = \infty$) und deshalb folgt $[L : K]_s = \infty$. □

Korollar. Seien $K \subset L \subset M$ eine Kette von algebraischen Körpererweiterungen. Dann ist M/K genau dann separabel, wenn M/L und L/K separabel sind.

Beweisidee. $\implies$ ist trivial. Für die andere Implikation: sei $\alpha \in M$ mit $m_\alpha = \sum_{i=0}^n a_i t^i \in L[t]$ das Minimalpolynom über L. Wir haben eine Kette $K \subset L' := K(a_0, \ldots, a_n) \subset L$ mit L/K separabel und deshalb ist L'/K separabel. Wir haben eine Kette $L' \subset L'(\alpha) \subset M$, wobei $L'(\alpha)/L'$ separabel ist (da $m_\alpha \in L[t]$ separabel ist und $m_\alpha \in L'[t] \subset L[t]$ nach der Definition von L'). Dann folgt

$$[L'(\alpha) : K]_s = [L'(\alpha) : L']_s [L' : K]_s = [L'(\alpha) : L'][L' : K] = [L'(\alpha) : K]$$

weil beide $L'(\alpha)/L'$ und L'/K endlich und separabel sind. Die endliche Körpererweiterung $K \subset L'(\alpha)$ ist dann separable nach dem Satz 3.21 und insbesondere ist $\alpha \in L'(\alpha)$ separabel über K. □

Übung. Sei H eine endliche Untergruppe der multiplikativen Gruppe $K^\times$ eines Körpers K. Dann ist H zyklisch.

Satz 3.23 (Satz von primitiven Element)**.** *Sei $K \subset L = K(\alpha_1, \ldots, \alpha_n)$ eine algebraische Körpererweiterung, so dass $\alpha_2, \ldots, \alpha_n$ separabel über K sind. Dann ist die Körpererweiterung einfach: es gibt ein* primitives *Element $\beta \in L$ mit $L = K(\beta)$.*

Beweisidee. Falls K endlich ist, dann ist auch L endlich (da $[L : K] < \infty$) und $L^\times$ ist eine endliche zyklische Gruppe nach der obigen Übung. Deshalb gibt es $\beta \in L^\times$ mit $L^\times =< \beta >$ und dann folgt $L = K(\beta)$.

Falls K unendlich ist, dann beweisen wir die Aussage durch Induktion nach n. Für den Induktionsanfang ($n = 2$) sei $L = K(\alpha_1, \alpha_2)$ und $m := [L : K]_s$ und seien $\mathrm{Hom}_K(L, \overline{K}) = \{\sigma_1, \ldots, \sigma_m\}$. Das Polynom

$$P(t) := \prod_{i \neq j} (\sigma(\alpha_1) - \sigma_j(\alpha_1) + t(\sigma_i(\alpha_2) - \sigma_j(\alpha_2))) \in \overline{K}[t]$$

ist nicht das Nullpolynom, weil $\sigma_i(\alpha_1) = \sigma_j(\alpha_1)$ und $\sigma_i(\alpha_1) = \sigma_j(\alpha_1) \implies i = j$. Deshalb hat P nur endliche viele Nullstellen in $\overline{K}$. Da K unendlich ist, gibt es $c \in K$ mit $P(c) \neq 0$. Sei

$\beta = \alpha_1 + c\alpha_2$. Dann sind $\sigma_i(\beta) = \sigma_i(\alpha_1) + c\sigma_i(\alpha_2)$ für $1 \leq i \leq m$ paarweise verschieden. Sei [20.12.18]
$L' := K(\beta) \subset L$. Dann folgt $[L' : K]_s \geq m = [L : K]_s$, da $\sigma_1|_{L'}, \ldots, \sigma_m|_{L'} \in \mathrm{Hom}_K(L', \overline{K})$ paarweise verschieden sind. Aus $L' \subset L$ folgt, $[L' : K]_s \leq [L : K]_s = m$ und deshalb gilt $[L' : K]_s = [L : K]_s$ und

$$[L : K]_s \geq [L'(\alpha_2) : K]_s = [L'(\alpha_2) : L']_s[L' : K]_s = [L'(\alpha_2) : L'][L : K]_s$$

weil $L'(\alpha_2)/L'$ separabel ist (wegen der Separabilität von α_2 über K). Daher gilt $[L'(\alpha_2) : L'] = 1$ und insbesondere sind α_2 und $\alpha_1 = \beta - c\alpha_2$ Elemente von L', also $L' := K(\beta) = K(\alpha_1, \alpha_2) = L$. Für den Induktionsschritt betrachten wir die Kette

$$K \subset K(\alpha_1, \ldots, \alpha_{n-1}) = L' \subset K(\alpha_1, \ldots, \alpha_n) = L$$

und nach der Induktionsvoraussetzung gilt $L' = K(\beta')$ und deshalb folgt $L = K(\beta', \alpha_n)$ und dann verwenden wir das obige Argument. □

Korollar. Jede endliche separable Körpererweiterung ist einfach. Insbesondere ist jede endliche Körpererweiterung in Charakteristik 0 einfach.

3.7. **Endliche Körper.** Für jede Primzahl p gibt es ein Körper $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ mit p Elementen. In diesem Abschnitt werden wir zeigen, dass für jede Primzahl p und $n \in \mathbb{N}_{>0}$ gibt es einen Körper $\mathbb{F}_{p^n}$ mit p^n Elementen.

Lemma. Sei K ein endlicher Körper. Dann gilt $\mathrm{Char}(K) = p > 0$ und der Primkörper von K ist isomorph zu $\mathbb{F}_p$. Ferner hat K genau p^n Elementen, wobei $n = [K : \mathbb{F}_p]$, und K ist ein Zerfällungskörper von $t^{p^n} - t \in \mathbb{F}_p[t]$. Daher ist $K/\mathbb{F}_p$ normal.

Beweisidee. Nach der Klassifizierung von Primkörper ist der Primkörper P isomorph zu $\mathbb{Q}$ oder $\mathbb{F}_p$. Wegen die Endlichkeit von K ist $P \cong \mathbb{F}_p$ und $\mathrm{Char}(K) = \mathrm{Char}(P) = p$. Aus der Endlichkeit von K folgt $[K : P] < \infty$. Sei $n = [K : P]$. Dann gibt es einen Isomorphismus $K \to (\mathbb{F}_p)^n$ zwischen $\mathbb{F}_p$-Vektorräume und daher gilt $|K| = p^n$. Der Multiplikative Gruppe $K^\times$ hat Ordnung $p^n - 1$ und es folgt, dass jedes $\alpha \in K^\times$ eine Nullstelle von $t^{p^n-1} - 1 \in \mathbb{F}_p[t]$ ist. Dann ist jedes $\alpha \in K$ eine Nullstelle von $t^{p^n} - t$, also K ist ein Zerfällungskörper von $t^{p^n} - t \in \mathbb{F}_p[t]$.□

Satz 3.24 (Existenz und Eindeutigkeit von endlichen Körper)**.** *Zu jeder Primzahl p und $n \in \mathbb{N}_{>0}$ gibt es eine normal und separable Körpererweiterung $\mathbb{F}_p \subset \mathbb{F}_{p^n}$ vom Grad n mit $|\mathbb{F}_{p^n}| = p^n$. Der Körper $\mathbb{F}_{p^n}$ ist bis auf Isomorphie eindeutig charakterisiert als Zerfällungskörper von $t^{p^n} - t \in \mathbb{F}_p[t]$. Ferner ist jeder endlich Körper isomorph zu $\mathbb{F}_{p^n}$ für eine Primzahl p und $n \in \mathbb{N}_{>0}$.*

Beweisidee. Für die Existenz sei $f(t) = t^{p^n} - t \in \mathbb{F}_p[t]$. Wegen $f'(t) = -1$ hat f' genau p^n verschiedene Nullstellen in $\overline{\mathbb{F}_p}$ (jede Nullstelle hat Vielfachheit 1). Ferner bilden die Nullstellen ein Körper mit p^n Elemente, die $\mathbb{F}_p$ enthält. Deshalb ist der Zerfällungskörper von f ein Erweiterungskörper von $\mathbb{F}_p$ mit genau p^n Elementen. Die Körpererweiterung $\mathbb{F}_{p^n}/\mathbb{F}_p$ ist normal (da $\mathbb{F}_{p^n}$ ein Zerfällungskörper von f ist) und separabel (da die Nullstellen von f einfach sind). Die andere Aussagen folgen aus dem Lemma. □

Korollar. Man kann die Körper $\mathbb{F}_{p^n}$ als Teilkörper von $\overline{\mathbb{F}_p}$ konstruieren. Dann gilt $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^{n'}}$ genau dann, wenn $n \mid n'$. Ferner sind die Körpererweiterungen bis aud Isomorphie die eindeutige Körpererweiterungen zwischen endlichen Körper.

Beweisidee. Aus $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^{n'}}$ folgt $p^{n'} = |\mathbb{F}_{p^{n'}}| = |\mathbb{F}_{p^n}|^m = p^{nm}$, wobei $m = [\mathbb{F}_{p^{n'}} : \mathbb{F}_{p^n}]$. Deshalb gilt $n \mid n'$. Falls $n \mid n'$ (d.h. $n' = mn$) gilt für $\alpha \in \mathbb{F}_{p^n}$

$$\alpha^{p^{n'}} = (\alpha^{p^n})^{p^{n(m-1)}} = \alpha^{p^{n(m-1)}} = \cdots = \alpha,$$

also gilt $\alpha \in \mathbb{F}_{p^{n'}}$. Die Eindeutigkeitaussage folgt nach dem Satz 3.11. □

Korollar. Jedes algebraische Körpererweiterung eines endlichen Körpers ist normal und separable. Insbesondere sind die endliche Körper perfekt.

Beweisidee. Sei $K \cong \mathbb{F}_{p^n} \subset L$ eine algebraische Körpererweiterung eines endlichen Körper. Wenn L/K endlich ist, dann folgt $L \cong \mathbb{F}_{p^n}$ und $L/\mathbb{F}_p$ ist normal und separabel und es folgt, dass L/K normal und separabel ist (Korollar des Satzes 3.15 und 3.22). Wenn L/K unendlich ist, ist L eine Vereinigung von endlichen Körpererweiterungen von K, die alle normal und separabel sind. Daher ist L/K normal und separabel. □

Bemerkung. Sei $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^{n'}}$ eine Körperweiterung und $m := n'/n = [\mathbb{F}_{p^{n'}} : \mathbb{F}_{p^n}] = [\mathbb{F}_{p^{n'}} : \mathbb{F}_{p^n}]_s$ (da die endliche Körpererweiterung separabel ist). Aus der Normalität von $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^{n'}}$ folgt $\mathrm{Aut}_{\mathbb{F}_{p^n}}(\mathbb{F}_{p^{n'}}) = \mathrm{Hom}_{\mathbb{F}_{p^n}}(\mathbb{F}_{p^{n'}}, \overline{\mathbb{F}_p})$ (Satz 3.15). Daher hat $\mathrm{Aut}_{\mathbb{F}_{p^n}}(\mathbb{F}_{p^{n'}})$ die Ordnung m. Sei $\mathrm{Fr} : \mathbb{F}_{p^{n'}} \to \mathbb{F}_{p^{n'}}$ der Frobenius-Homomorphismus mit $\mathrm{Fr}(\alpha) = \alpha^p$. Dann gilt $\mathrm{Fr}^n \in \mathrm{Aut}_{\mathbb{F}_{p^n}}(\mathbb{F}_{p^{n'}})$ und es folgt, dass $|\mathrm{Fr}^n| \leq m$. Wir nennen den Homomorphismus Fr^n den *relativen Frobenius-Homomorphismus* von $\mathbb{F}_{p^{n'}}/\mathbb{F}_{p^n}$.

Satz 3.25. *Sei $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^{n'}}$ eine Körperweiterung vom Grad m zwischen endlichen Körper. Dann gilt* $\mathrm{Aut}_{\mathbb{F}_{p^n}}(\mathbb{F}_{p^{n'}}) =< \mathrm{Fr}^n > \cong \mathbb{Z}/m\mathbb{Z}$.

Beweisidee. Es ist hinreichend zu zeigen, dass $|\mathrm{Fr}^n| = m$ nach der obigen Bemerkung. Falls $|\mathrm{Fr}^n| < m$ folgt $l = |\mathrm{Fr}| < nm = n'$ und jedes $\alpha \in \mathbb{F}_{p^{n'}}$ ist eine Nullstelle von $t^{p^l} - t$, d.h. $\mathbb{F}_{p^{n'}} \subset \mathbb{F}_{p^l}$, also $n' \mid l$ aber $n' > l$. Daher müss $|\mathrm{Fr}^n| = m$ gelten. □

4. Galois-Theorie

[08.01.19]

4.1. Automorphismen Gruppen und Fixkörper.

Übung. Sei $K \subset L \subset M$ eine Kette von Körpererweiterungen. Dann ist $\mathrm{Aut}_L(M)$ eine Untergruppen von $\mathrm{Aut}_K(M)$.

Bemerkung. Sei $K \subset L$ eine Körpererweiterung. Es gibt eine Gruppenwirkung

$$\mathrm{Aut}_K(L) \times L \to L$$

mit $\varphi \cdot \alpha := \varphi(\alpha)$ für $\varphi \in \mathrm{Aut}_K(L)$ und $\alpha \in L$.

Definition. Sei $K \subset L$ eine Körpererweiterung und $H < \mathrm{Aut}_K(L)$ eine Untergruppe. Wir definieren den Fixkörper von H

$$L^H := \{\alpha \in L : \varphi(\alpha) = \alpha \, \forall \, \varphi \in H\}.$$

Bemerkung. L^H ist die Fixpunktmenge der Gruppenwirkung $H \times L \to L$.

Lemma. Für eine Körpererweiterung $K \subset L$ und eine Untergruppe $H < \mathrm{Aut}_K(L)$ ist L^H ein Teilkörper von L, der K enthält.

Definition. Für eine Körpererweiterung L/K betrachten wir die Menge alle Zwischenkörper

$$\mathrm{ZK}(L/K) := \{M \text{ Körper } : K \subset M \subset L\}$$

und die Menge alle Untergruppe der Automorphismengruppe von L/K

$$\mathrm{UG}(L/K) := \{H : H \subset \mathrm{Aut}_K(L)\}.$$

Wir definieren zwei Abbildungen

$$\Psi : \mathrm{ZK}(L/K) \rightleftarrows \mathrm{UG}(L/K) : \Phi$$

mit $\Psi(M) := \mathrm{Aut}_M(L)$ und $\Phi(H) := L^H$. Die Abbildungen sind wohldefiniert nach dem Lemma und der Übung.

Übung. Für eine Körpererweiterung $K \subset L$ haben die Abbildungen Ψ und Φ die folgende Eigenschaften:

(1) $\Psi(M) \leq \Psi(M')$ für $M, M' \in \mathrm{ZK}(L/K)$ mit $M' \subset M$,
(2) $\Phi(H) \subset \Phi(H')$ für $H, H' \in \mathrm{UG}(L/K)$ mit $H' \leq H$,
(3) $H \leq \Psi(\Phi(H))$ für alle $H \in \mathrm{UG}(L/K)$,
(4) $M \subset \Phi(\Psi(M))$ für alle $M \in \mathrm{ZK}(L/K)$,
(5) $\Phi(H) = \Phi(\Psi(\Phi(H)))$ für alle $H \in \mathrm{UG}(L/K)$,
(6) $\Psi(M) = \Psi(\Phi(\Psi(M)))$ für alle $M \in \mathrm{ZK}(L/K)$.

4.2. **Galois-Erweiterungen.**

Definition. Eine Körpererweiterung $K \subset L$ heißt *galoissch* (oder *eine Galois-Erweiterung*), wenn sie normal und separabel ist. In diesem Fall ist die Galois-Gruppe von L/K

$$\mathrm{Gal}(L/K) := \mathrm{Aut}_K(L).$$

Beispiel.

(1) $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$ ist galoissch, da jede algebraische Körpererweiterung in Charakteristik 0 separable ist und die Normalität folgt aus $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.
(2) Für $n' = nm$ ist $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^{n'}}$ ist eine Galois-Erweiterung mit Galois-Gruppe

$$\mathrm{Gal}(\mathbb{F}_{p^{n'}}/\mathbb{F}_{p^n}) \cong \mathbb{Z}/m\mathbb{Z}$$

nach §**??**.

Bemerkung. Sei $K \subset L$ eine Galois-Erweiterung und $M \in \mathrm{ZK}(L/K)$. Dann gilt

(1) $M \subset L$ ist galoissch und es gilt $\mathrm{Gal}(L/M) \subset \mathrm{Gal}(L/K)$,
(2) Wenn $K \subset M$ galoissch ist, dann beschränkt sich jeder K-Automorphismus von L zu einem K-Automorphismus von M und die induzierte Abbildung $\mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K)$ ist ein surjektiver Gruppenhomomorphismus.

Bemerkung. Wenn L/K eine endliche normale Körpererweiterung ist, dann gilt

$$|\mathrm{Aut}_K(L)| = [L : K]_s \leq [L : K]$$

nach Satz 3.15 und Satz 3.20. Ferner gilt $|\mathrm{Aut}_K(L)| = [L : K]$ genau dann, wenn L/K auch separabel ist (Satz 3.21).

Lemma. Für eine endliche Körpererweiterung $K \subset L$ gilt $|\mathrm{Aut}_K(L)| \leq [L : K]$ und insbesondere ist die Automorphismen Gruppe $\mathrm{Aut}_K(L)$ endlich.

Beweisidee. Zuerst zeigen wir, dass $\mathrm{Aut}_K(L)$ endlich ist. Seien $\alpha_1, \cdots, \alpha_n$ eine K-Basis von L. Für jeden Automorphismus $\varphi \in \mathrm{Aut}_K(L)$ und jedes Element $\alpha = \sum_{i=1}^n \lambda_i \alpha_i \in L$ mit $\lambda_i \in K$ gilt

$$\varphi(\alpha) = \sum_{i=1}^{n} \lambda_i \varphi(\alpha_i)$$

und $\varphi(\alpha_i)$ ist eine Nullstelle von m_{α_i} nach dem Lemma vor Satz 3.11. Insbesondere gibt es nur endliche Möglichkeiten für φ.

Wir schreiben $\mathrm{Aut}_K(L) = \{\varphi_1, \ldots, \varphi_m\}$ und $n = [L : K]$. Falls $m > n$ betrachten wir ein homogenes lineares Gleichungssystem in m Variablen $x_1, \ldots, x_m$ mit L-Koeffizienten und n Gleichungen:

$$\begin{aligned} \varphi_1(\alpha_1)x_1 + \cdots \varphi_m(\alpha_1)x_n = 0 \quad (\star)_1 \\ \vdots \\ \varphi_1(\alpha_n)x_1 + \cdots \varphi_m(\alpha_n)x_n = 0 \quad (\star)_n \end{aligned}$$

Wegen $m > n$ gibt es eine nicht-triviale Lösung $(x_1, \cdots, x_n) \in L^m \setminus \{0\}$. Für alle $\alpha = \sum_{i=1}^n \lambda_i \alpha_i \in L$ mit $\lambda_i \in K$ gilt $\varphi_j(\alpha) = \sum_{i=1}^n \lambda_i \varphi_j(\alpha_i)$. Es gilt

$$\sum_{i=1}^n \lambda_i \cdot (\star)_i \quad : \quad \sum_{i=1}^n \sum_{j=1}^m x_j \lambda_i \varphi_j(\alpha_i) = \sum_{j=1}^m x_j \varphi_j(\alpha) = 0,$$

also $\sum_{j=1}^m x_j \varphi_j(\alpha) = 0$ für jedes $\alpha \in L$. Aber die Automorphismen $\varphi_1, \ldots, \varphi_m$ sind lineare unabhängig über L (Übung) und deshalb muss $m \leq n$ gelten. □

Satz 4.1. *Sei L ein Körper und $H \subset \mathrm{Aut}(L)$ eine endliche Untergruppe. Dann ist $K := L^H \subset L$ eine Galois-Erweiterung vom Grad $[L : L^H] = |H|$ mit Galois-Gruppe H.*

[10.01.19] *Beweisidee.* Sei $\alpha \in L$ und seien $\varphi_1, \ldots, \varphi_r \in H$ ein maximale System von Elementen von H, so dass $\varphi_1(\alpha), \ldots, \varphi_r(\alpha)$ paarweise verschieden sind. Wir schreiben $H = \{\varphi_1, \ldots, \varphi_m\}$ mit $m \geq r$. Für jedes $\varphi_k \in H$ gilt $\{\varphi_k \circ \varphi_1, \ldots, \varphi_k \circ \varphi_m\} = \{\varphi_1, \ldots, \varphi_m\}$. Wegen $\{\varphi_1(\alpha), \ldots, \varphi_m(\alpha)\} = \{\varphi_1(\alpha), \ldots, \varphi_r(\alpha)\}$ gibt es eine Bijektion

$$\varphi_k : \{\varphi_1(\alpha), \ldots, \varphi_r(\alpha)\} \to \{\varphi_1(\alpha), \ldots, \varphi_r(\alpha)\}.$$

Sei $f_\alpha(t) = \prod_{i=1}^r (t - \varphi_i(\alpha)) \in L[t]$. Aus $f_\alpha^{\varphi_k} = f_\alpha$ für alle $\varphi_k \in H$ folgt $f_\alpha(t) \in K[t]$, weil $K := L^H$. Ferner ist $f_\alpha \in K[t]$ separabel und es folgt, dass α separabel ist, weil $\alpha \in \{\varphi_1(\alpha), \ldots, \varphi_m(\alpha)\} = \{\varphi_1(\alpha), \ldots, \varphi_r(\alpha)\}$ eine Nullstelle des separablen Polynom f_α ist. Daher ist L/K separable. Ferner ist L/K normal, weil L ein Zerfällungskörper der Familie $\{f_\alpha \in K[t] : \alpha \in L\}$ ist. Insbesondere ist L/K galoissch.

Wir behaupten dass $[L : K] \leq |H|$ und damit ist L/K endlich. Sei $H = \{\varphi_1, \ldots, \varphi_m\}$. Es ist hinreichend zu zeigen, dass jede K-linear unabhängige Teilmenge von L höchstens m Elemente enthält. Falls es $n > m$ mit $\alpha_1, \ldots, \alpha_n \in L$ linear unabhängig über K gibt, werden wir einen Widerspruch finden. Wir betrachten das homogene lineare Gleichungssystem in Variablen $x_1, \ldots, x_n$ mit L-Koeffizienten und m Gleichungen

$$\begin{aligned} \varphi_1(\alpha_1)x_1 + \cdots \varphi_1(\alpha_n)x_n = 0 \quad (\star)_1 \\ \vdots \\ \varphi_m(\alpha_1)x_1 + \cdots \varphi_m(\alpha_n)x_n = 0 \quad (\star)_m \end{aligned}$$

Wegen $n > m$ gibt es eine nicht-triviale Lösung $(x_1, \ldots, x_n) \in L^n \setminus \{0\}$. Sei $x = (x_1, \ldots, x_n)$ eine nicht-trivial Lösung, so dass $r := |\{i : x_i \neq 0\}|$ minimal ist. Wir können die α_i neu ordnen, so dass $x = (x_1, \ldots, x_r, 0, \ldots, 0)$. Ferner können wir x mit $\lambda \in L^\times$ multiplizieren und dann ist λx auch eine nicht-triviale Lösung. Deshalb können wir annehmen, dass $x_r = 1$. Falls $r = 1$, gilt $\varphi_1(\alpha_1) = 0$ nach $(\star)_1$ aber dann folgt $\alpha_1 = 0$, was einen Widerspruch zu der linearen Unabhängigkeit liefert. Daher gilt $r > 1$. Falls $x_1, \ldots, x_r \in K \subset L$ folgt $\varphi_i(x_j) = x_j$ für alle $1 \leq i \leq m$ und $1 \leq j \leq n$. Aus $(\star)_1$ folgt $\varphi_1(\alpha_1 x_1 + \cdots \alpha_{r-1}x_{r-1} + \alpha_r) = 0$ und damit $\alpha_1 x_1 + \cdots \alpha_{r-1}x_{r-1} + \alpha_r$ mit Koeffizienten $x_i \in K$, aber dann wäre $\alpha_1, \ldots, \alpha_n$ linear abhängig über K. Deshalb gibt es $1 \leq i < r$ mit $x_i \notin K$. Ohne Einschränkung der Allgemeinheit $i = 1$ und $x_1 \notin K$, also gibt es $\varphi_k \in H$ mit $\varphi_k(x_1) \neq x_1$. Wir betrachten die Bilder der Gleichungen $(\star)_i$ under φ_k und nach einer Permutation der m Gleichungen erhalten wir

$$\begin{aligned} \varphi_1(\alpha_1)\varphi_k(x_1) + \cdots \varphi_1(\alpha_{r-1})\varphi_k(x_{r-1}) + \varphi_1(\alpha_r) = 0 \quad (\dagger)_1 \\ \vdots \\ \varphi_m(\alpha_1)\varphi_k(x_1) + \cdots \varphi_m(\alpha_{r-1})\varphi_k(x_{r-1}) + \varphi_1(\alpha_r) = 0 \quad (\dagger)_m \end{aligned}$$

Die Gleichungen $(\star)_i - (\dagger)_i$ liefern $\sum_{j=1}^{r-1} \varphi_i(\alpha_j)(x_j - \varphi_k(x_j))$ für alle $1 \leq i \leq m$. Deshalb ist $x' := (x_1 - \varphi_k(x_1), \ldots, x_{r-1} - \varphi_k(x_{r-1}), 0, \ldots, 0) \in L^n$ eine Lösung zu $(\star)$, die nicht-trivial ist $(x_1 \neq \varphi_k(x_1))$, was einen Widerspruch zu der Minimalität von r ist. Deshalb gilt $n \leq m$ und $[L : K] \leq m := |H|$.

Es gilt $H \subset \mathrm{Aut}_K(L)$ und nach der Behauptung und dem obigen Lemma haben wir

$$|H| \leq |\mathrm{Aut}_K(L)| \leq [L : K] \leq |H|.$$

Daher folgt $|H| = |\operatorname{Aut}_K(L)| = [L : K]$ und $H = \operatorname{Aut}_K(L) = \operatorname{Gal}(L/K)$. □

Bemerkung. Wenn $H < \operatorname{Aut}(L)$ unendlich ist und $L^H \subset L$ algebraisch ist, dann ist $L^H \subset L$ eine unendliche Galois-Erweiterung mit Galois-Gruppe $\operatorname{Gal}(L/L^H)$, die H enthält.

Satz 4.2. *Für eine endliche Körpererweiterung $K \subset L$ ist äquivalent:*

(1) L/K ist galoissch,
(2) L ist ein Zerfällungskörper eines separablen Polynoms $f \in K[t]$,
(3) $L^{\operatorname{Aut}_K(L)} = K$.

Beweisidee. (1) $\implies$ (2) : Jede endliche separable Körpererweiterung ist einfach nach dem Satz von primitiven Element (Satz **??**) und daher gilt $L = K(\alpha)$. Sei $m_\alpha(t) \in K[t]$ das Minimalpolynom von α über K. Wegen der Normalität von L/K liegen alle Nullstellen von m_α in L und wegen der Separabilität von L/K ist m_α separable. Dann ist L ein Zerfällungskörper eines separablen Polynoms $m_\alpha \in K[t]$.

(3) $\implies$ (1) : Wir nehmen an, dass $L^{\operatorname{Aut}_K(L)} = K$. Nach dem Lemma haben wir $|\operatorname{Aut}_K(L)| \leq [L : K] < \infty$ und nach dem Satz 4.1 für $H := \operatorname{Aut}_K(L) \subset \operatorname{Aut}(L)$ ist $L^H = K \subset L$ galoissch.

(2) $\implies$ (3) : Wir beweisen diese Implikation durch Induktion nach $n = [L : K]$. Für den Induktionsanfang $n = 1$ haben wir $L = K$ und $\operatorname{Aut}_K(L) = \{\mathrm{Id}\}$ und $L^{\operatorname{Aut}_K(L)} = K$. Für den Induktionsschritt: seien $n > 1$ und L ein Zerfällungskörper eines separablen Polynoms $f \in K[t]$. Wenn f in Linearfaktoren über K zerfällt, gilt $L = K$ und $L^{\operatorname{Aut}_K(L)} = K$. Daher nehmen wir an, dass f ein irreduzibler Faktor g vom Grad $m \geq 2$ hat. Seien $\alpha_1, \ldots, \alpha_m$ die paarweise verschiedene Nullstellen von g (wegen $g \mid f$ ist g auch separabel). Dann gilt

$$[L : K] = [L : K(\alpha_1)][K(\alpha_1) : K] = [L : K(\alpha_1)]m$$

und $[L : K(\alpha_1)] = [L : K]/m < [L : K]$. Ferner ist L der Zerfällungskörper von f über $K(\alpha_1)$. Nach der Induktionsvoraussetzung folgt $L^{\operatorname{Aut}_{K(\alpha_1)}(L)} = K(\alpha_1)$. Seien $G = \operatorname{Aut}_K(L)$ und $H = \operatorname{Aut}_{K(\alpha_1)}(L) \leq G$. Es folgt, dass $L^G \subset L^H = K(\alpha_1)$ und wir müssen zeigen, dass $L^G = K$. Für $\beta \in L^G \subset K(\alpha_1)$ schreiben wir $\beta = \lambda_0 + \lambda_1\alpha_1 + \cdots + \lambda_{m-1}\alpha_1^{m-1}$ mit $\lambda_i \in K$. Bis auf Skalarmultiplikation ist g das Minimalpolynom von α_1 und nach dem Lemma vor Satz 3.11 gibt es für jede Nullstelle α_i von g einen K-Automorphismus $\varphi \in \operatorname{Aut}_K(L)$ mit $\varphi_i(\alpha_1) = \alpha_i$. Aus $\beta \in L^G$ und $\varphi_i \in G$ folgt $\varphi_i(\beta) = \beta$ für $1 \leq i \leq m$, d.h. $\beta = \varphi(\beta) = \lambda_0 + \lambda_1\alpha_i + \cdots + \lambda_{m-1}\alpha_i^{m-1}$. Das Polynom $f(t) = \lambda_{m-1}t^{m-1} + \cdots + \lambda_1 t + \lambda_0 - \beta \in L^G[t]$ hat m paarweise verschiedene Nullstellen $\alpha_1, \ldots, \alpha_m$, aber $\operatorname{grad}(f) \leq m-1$. Daher gilt $f = 0$ und insbesondere ist $\beta = \lambda_0 \in K$. Dies gilt für jedes $\beta \in L^G$, also haben wir $L^G = K$. □

[15.01.19]

Satz 4.3 (Hauptsazt der Galois-Theorie)**.** *Sei $K \subset L$ eine endliche Galois-Erweiterung mit Galois-Gruppe $G := \operatorname{Gal}(L/K)$. Dann gilt*

(1) Die zwei Abbildungen

$$\Psi : \mathrm{ZK}(L/K) \rightleftarrows \mathrm{UG}(L/K) : \Phi$$

mit $\Psi(M) := \operatorname{Aut}_M(L)$ und $\Phi(H) := L^H$ sind bijektiv mit $\Phi = \Psi^{-1}$.
(2) $|G| = [L : K]$.
(3) Für Zwischenkörper $K \subset M_1 \subset M_2 \subset L$ gilt $\Psi(M_1) \geq \Psi(M_2)$ und für Untergruppen $H_1 \leq H_2 \leq G$ gilt $\Phi(H_1) \supseteq \Phi(H_2)$.
(4) Für $H \leq G$ ist $\Phi(H) = L^H$ genau dann normal über K (und damit galoissch), wenn $H \triangleleft G$ eine normale Untergruppe ist. In diesem Fall gibt es einen surjektiven Gruppenhomomorphismus

$$G = \operatorname{Gal}(L/K) \to \operatorname{Gal}(L^H/K), \quad \varphi \mapsto \varphi|_{L^H}$$

mit dem Kern H. Deshalb gibt es einen Gruppenisomorphismus $G/H \cong \operatorname{Gal}(L^H/K)$.

Bemerkung. Für eine unendliche Galois-Erweiterung L/K gilt nur $\Phi \circ \Psi = \mathrm{Id}$, also Φ ist surjektiv und Ψ ist injektiv.

Beispiel. Die Körpererweiterung $\mathbb{Q} \subset L = \mathbb{Q}(\sqrt{p}, \sqrt{q})$ für Primzahlen $p \neq q$ ist galoissch vom Grad $[L : \mathbb{Q}] = 4$. Ein Automorphismus $\varphi \in G := \mathrm{Gal}(L/K)$ wird von der Werten $\varphi(\sqrt{p})$ und $\varphi(\sqrt{q})$ bestimmt. Ferner gilt $\varphi(\sqrt{p}) \in \{\pm\sqrt{p}\} = \{$ Nullstellen von $m_{\sqrt{p}}(t)\}$ und ebenso $\varphi(\sqrt{q}) \in \{\pm\sqrt{q}\}$. Alle 4 Möglichkeiten existieren, weil $|\mathrm{Gal}(L/\mathbb{Q})| = [L : K] = 4$. Jeder Automorphismus $\varphi \neq \mathrm{Id}$ hat Ordnung 2 und dehalb folgt $G =< \sigma, \tau > \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, wobei $\sigma(\sqrt{p}) = -\sqrt{p}$ und $\sigma(\sqrt{q}) = \sqrt{q}$, und $\tau(\sqrt{q}) = -\sqrt{q}$ und $\tau(\sqrt{p}) = \sqrt{p}$. Die echte Untergruppen von G sind $H_1 =< \sigma >$ und $H_2 =< \tau >$ und $H_3 =< \sigma \circ \tau >$. Übung: Was sind die entsprechende Zwischenkörper von L/K?

Korollar. Sei $K \subset L$ eine endliche Galois-Erweiterung mit Galois-Gruppe $G = \mathrm{Gal}(L/K)$. Für einen Zwischenkörper $K \subset M \subset L$ ist äquivalent:

(1) M/K ist normal (und damit galoissch),
(2) $\Psi(M)$ ist eine normale Untergruppe von G,
(3) Für jeden Automorphismus $\varphi \in G$ gilt $\varphi(M) = M$.

Korollar. Jede endliche separable Körpererweiterung besitzt nur endlich viele Zwischenkörper.

[17.01.19]

Korollar. Sei L/K eine endliche Galois-Erweiterung und $M_1, M_2 \in \mathrm{ZK}(L/K)$ mit $H_i = \Psi(M_i) \leq G := \mathrm{Gal}(L/K)$. Dann gilt

(1) $M_1 \cdot M_2 = L^{H_1 \cap H_2}$,
(2) $M_1 \cap M_2 = L^{<H_1 . H_2>}$.

Definition. Eine Galois-Erweiterung L/K heißt abelsch (bzw. zyklisch), wenn $\mathrm{Gal}(L/K)$ abelsch (bzw. zyklisch) ist.

Beispiel. $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^{n'}}$ mit $n \mid n'$ ist eine zyklische Galois-Erweiterung.

Bemerkung. Sei L/K eine endliche abelsche (bzw. zyklische) Galois-Erweiterung. Für jeden Zwischenkörper $K \subset M \subset L$ ist dann M/K auch abelsch (bzw. zyklisch).

Satz 4.4. *Sei $K \subset M$ eine Körpererweiterung und $K \subset M_i \subset L$ ein Zwischenkörper für $i = 1, 2$. Dann gilt*

(1) $M_1 \cdot M_2/K$ ist endlich und galoissch,
(2) $M_1 \cdot M_2/M_i$ und $M_i/M_1 \cap M_2$ sind endlich und galoissch,
(3) Die Abbildung $f : \mathrm{Gal}(M_1 \cdot M_2/M_1) \to \mathrm{Gal}(M_2/M_1 \cap M_2)$ mit $f(\varphi) = \varphi|_{M_2}$ ist ein Gruppenisomorphismus.
(4) Die Abbildung $\rho : \mathrm{Gal}(M_1 \cdot M_2/K) \to \mathrm{Gal}(M_1/K) \times \mathrm{Gal}(M_2/K)$ mit $\rho(\varphi) = (\varphi|_{M_1}, \varphi|_{M_2})$ ist ein injektiver Gruppenhomomorphismus. Falls $M_1 \cap M_2 = K$ ist ρ auch surjektiv und damit ein Gruppenisomorphismus.

4.3. **Die Galois-Gruppe einer Gleichung.**

Bemerkung. Sei $f \in K[t]$ ein nicht-konstantes Polynom und L ein Zerfällungskörper von f über K. Dann ist L/K normal und falls f separabel über K ist, dann ist L/K separabel (und damit galoissch).

Notation. Für ein separables Polynom $f \in K[t]$ ist die *Galois-Gruppe von f* (oder die *Galois-Gruppe der Glechung $f(t) = 0$*) die Galois-Gruppe $\mathrm{Gal}(f) := \mathrm{Gal}(L/K)$ eines Zerfällungskörper L von f über K.

Satz 4.5. *Sei $f \in K[t]$ ein separables Polynom vom Grad $n > 0$ mit Zerfällungskörper L über K. Wenn $\alpha_1, \ldots, \alpha_n \in L$ die Nullstellen von f sind, gibt es einen injektiven Gruppenhomomorphismus*

$$\rho : \mathrm{Gal}(L/K) \to S_n \cong \mathrm{Isom}(\{\alpha_1, \ldots, \alpha_n\}), \quad \varphi \mapsto \varphi|_{\{\alpha_1, \ldots, \alpha_n\}}.$$

Insbesondere gilt $|\operatorname{Gal}(L/K)| \mid n! = |S_n|$. *Ferner ist* $f \in K[t]$ *genau dann irreduzibel, wenn* $\operatorname{Gal}(L/K)$ *transitiv auf* $\{\alpha_1, \dots, \alpha_n\}$ *operiert (d.h. für alle* α_i, α_j *gibt es* $\varphi \in \operatorname{Gal}(L/K)$ *mit* $\varphi(\alpha_1) = \alpha_2$*). Dies ist der Fall, wenn* ρ *surjektiv ist (so dass* $\operatorname{Gal}(L/K) \cong S_n$*).*

Korollar. Sei L/K eine endliche Galois-Erweiterung vom Grad n. Dann kann man $\operatorname{Gal}(L/K)$ als Untergruppe von S_n betrachten.

Bemerkung. Für eine Galois-Erweiterung L/K vom Grad n ist $\operatorname{Gal}(L/K)$ eine echte Untergruppe von S_n in allgemeinen.

Beispiel. Sei $f(t) = t^2 + at + b \in K[t]$ ein Polynom vom Grad 2 mit keine Nullstelle in K. Dann ist f irreduzibel und wenn α eine Nullstelle von f ist, dann ist $L := K(\alpha)$ ein Zefällungskörper von f. Wenn f auch separabel ist (z.B. Falls $\operatorname{Char}(K) \neq 2$ oder $a \neq 0$), dann ist L/K eine Galois-Erweiterung vom Grad 2 mit Galois-Gruppe $\operatorname{Gal}(L/K) \cong \mathbb{Z}/2\mathbb{Z}$.

Beispiel. (Die Diskriminante eines Polynoms vom Grad 3) Sei K ein Körper mit $\operatorname{Char}(K) \neq 2, 3$ und $f(t) = t^3 + at + b \in K[t]$[7], so dass f keine Nullstelle in K hat. Wegen der Annahme $\operatorname{Char}(K) \neq 2, 3$ ist f separabel. Seien α, β, γ die Nullstellen von f und $L = K(\alpha, \beta, \gamma)$ ein Zerfällungskörper von f. Deshalb ist L/K eine Galois-Erweiterung mit $\operatorname{Gal}(L/K) < S_3$. Es gilt $[K(\alpha) : K] = \operatorname{grad}(m_\alpha) = \operatorname{grad}(f) = 3$ und [22.01.19]

$$[L : K] = [L : K(\alpha)][K(\alpha) : K] = \begin{cases} 3 & \text{Falls } L = K(\alpha) \\ 6 & \text{Falls } L \neq K(\alpha). \end{cases}$$

Falls $L = K(\alpha)$ folgt $\operatorname{Gal}(L/K) \cong \mathbb{Z}/3\mathbb{Z}$ und diese Untergruppe wird von einer Permuation vom Ordnung 3 erzeugt. Falls $L \neq K(\alpha)$ folgt $\operatorname{Gal}(L/K) \cong S_3$. Um die Galois-Gruppe zu finden kann man die *Diskriminante* Δ von f benutzen, wobei $\Delta := \delta^2$ und

$$\delta := (\alpha - \beta)(\alpha - \gamma)(\beta - \gamma) \in L.$$

Für jedes $\varphi \in \operatorname{Gal}(L/K)$ gilt $f(\{\alpha, \beta, \gamma\}) = \{\alpha, \beta, \gamma\}$ und deshalb folgt $\varphi(\delta) = \pm\delta$ und $\varphi(\Delta) = \Delta$. Insbesondere gilt $\Delta \in L^{\operatorname{Gal}(L/K)} = K$. Ferner man hat $\varphi(\delta) = \operatorname{sgn}(\varphi)\delta$, wobei $\operatorname{sgn} : S_n \to \mathbb{Z}/2\mathbb{Z}$ ist der Gruppenhomomorphismus mit $\operatorname{sgn}(\tau_{ij}) = -1$ für jede Transposition $\tau_{ij} \in S_n$. Die Permutationen mit $\operatorname{sgn}(\sigma) = 1$ (bzw. -1) heißen gerade (bzw. ungerade) Permutationen und *die alternierende Gruppe* $A_n = \ker(\operatorname{sgn})$ ist die Untergruppe aller geraden Permutationen. Für $n \geq 2$ ist sgn surjektiv und $[S_n : A_n] = |S_n/A_n| = |\mathbb{Z}/2\mathbb{Z}| = 2$. Deshalb gilt $|A_n| = n!/2$. Für $n = 3$ ist A_3 die einzige Untergruppe von S_3 mit Ordnung 3. Für die Galois-Erweiterung L/K ist äquivalent:

(1) $|\operatorname{Gal}(L/K)| = 3$,
(2) $\operatorname{Gal}(L/K) \cong A_3 < S_3$,
(3) $\delta \in K$,
(4) Δ besitzt eine Quadratwurzel in K.

Beispiel. Sei $f(t) = (t^2 - a)^2 - b \in \mathbb{Q}[t]$ irreduzibel mit $b > a^2$. Die Nullstellen von f sind $\pm\alpha, \pm\beta$, wobei $\alpha = \sqrt{a + \sqrt{b}}$ und $\beta = \sqrt{a - \sqrt{b}}$, und $L = K(\alpha, \beta)$ ist ein Zerfällungskörper von f. Aus $b > a^2$ folgt $\alpha \in \mathbb{R}$ und $\beta \in \mathbb{C} \setminus \mathbb{R}$ und beide sind nicht Null. Deshalb ist f separabel und L/K ist eine Galois-Erweiterung. Man hat

$$[L : K] = [L : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \cdot 4 = 8,$$

weil das Minimalpolynom von α über $\mathbb{Q}$ gleich f ist und $L \neq \mathbb{Q}(\alpha)$ (da $\beta \notin \mathbb{R}$) und β eine Nullstelle von $t^2 - (2a - \alpha^2) = t^2 - (a - \sqrt{b}) \in \mathbb{Q}(\alpha)[t]$ ist. Für jeden Körperisomorphismus $\varphi \in \operatorname{Gal}(L/K)$ gilt $\varphi(-\alpha) = -\varphi(\alpha)$ und $\varphi(-\beta) = -\beta$. Es gibt genau 8 Permutationen $\sigma \in S_4 \cong \operatorname{Isom}(\{\pm\alpha, \pm\beta\})$ mit $\sigma(-\alpha) = -\alpha$ und $\sigma(\beta) = -\beta$. Deshalb hat $\operatorname{Gal}(L/K)$ die folgende Beschreibung als Untergruppen von S_4

$$\operatorname{Gal}(L/K) \cong \{\sigma \in \operatorname{Isom}(\{\pm\alpha, \pm\beta\}) : \sigma(-\alpha) = -\alpha,\ \sigma(\beta) = -\beta\} < S_4.$$

[7]Nach einer Substitution $t \mapsto t + c$ kann man jedes normierte Polynom vom Grad 3 in dieser Form bringen.

Ferner gilt $\mathrm{Gal}(L/K) =< \sigma, \tau >$, wobei $\sigma(\alpha) = \beta, \sigma(\beta) = -\alpha$ und $\tau(\alpha) = -\alpha, \tau(\beta) = \beta$.

4.4. **Symmetrische Polynome.** Sei R ein kommutativer Ring mit Eins. Dann gibt es eine Gruppenwirkung der symmetrischen Gruppen S_n auf dem Polynomring $R[t_1, \dots, t_n]$. Die Gruppenwirkung wird durch die Abbildung $S_n \times R[t_1, \dots, t_n] \to R[t_1, \dots, t_n]$ definiert mit

$$(\sigma, f(t_1, \dots, t_n)) \mapsto \sigma \cdot f := f(t_{\sigma(1)}, \dots, t_{\sigma(n)}).$$

Definition. Ein symmetrische Polynom ist ein Element f der Fixpunktmenge $R[t_1, \dots, t_n]^{S_n}$ (d.h. $\sigma \cdot f = f$ für alle $\sigma \in S_n$). Die Elementarsymmetrische Polynome sind

$$\begin{aligned}
s_1 &= t_1 + \cdots + t_n = \sum_{1 \le i \le n} t_i \\
s_2 &= t_1 t_2 + \cdots t_{n-1} t_n = \sum_{1 \le i \le j \le n} t_i t_j \\
&\vdots \\
s_k &= t_1 \cdots t_k + \cdots + t_{n-k+1} \cdots t_n = \sum_{1 \le i_1 < i_2 \cdots < i_k \le n} \prod_{j=1}^{n} t_{i_j} \\
&\vdots \\
s_n &= t_1 \cdots t_n = \prod_{j=1}^{n} t_j
\end{aligned}$$

[22.01.19] **Übung.** Die Elementarsymmetrische Polynome sind symmetrische Polynome.

Satz 4.6 (Hauptsatz über symmetrische Polynome)**.** *Es gilt*

$$R[t_1, \dots t_n]^{S_n} = R[s_1, \dots, s_n].$$

Beispiel. $f(t_1, \dots, t_n) := \sum_{i=1}^{n} t_i^2 = s_1^2 - 2s_2$.

Bemerkung. Sei k ein Körper und

$$L = k(t_1, \dots, t_n) = Q(k[t_1, \dots, t_n]) = \left\{ \frac{f(t_1, \dots, t_n)}{g(t_1, \dots, t_n)} : f, g \in k[t_1, \dots, t_n] \text{ mit } g \neq 0 \right\}$$

der Körper aller rationalen Funktionen mit k-Koeffizienten. Dann gibt es auch eine Gruppenwirkung von S_n auf L und deshalb ist $S_n < \mathrm{Aut}(L)$ eine endliche Untergruppe. Nach dem Satz 4.1 ist $K := L^{S_n} \subset L$ eine endlicheGalois-Erweiterung mit $\mathrm{Gal}(L/K) \cong S_n$. Ferner haben wir $K = k(s_1, \dots, s_n)$ ist der Körper der rationalen Elementarsymmetrischen Funktionen s_i, weil $[L : k(s_1, \dots, s_n)] \le n!$ (da L ein Zerfällungskörper von $\prod_{i=1}^{n}(x - t_i) \in k(s_1, \dots, s_n)[x]$ ist) und deshalb folgt $K = k(s_1, \dots, s_n)$.

[24.01.19] 4.5. **Einheitswurzeln.**

Definition. Sei K ein Körper und $\overline{K}$ ein algebraischer Abschluss von K. Für $n \in \mathbb{N}_{>0}$ definieren wir die Menge $U_n \subset \overline{K}$ der *n-ten Einheitswurzeln* als die Menge der Nullstellen in $\overline{K}$ von $t^n - 1 \in K[t]$.

Bemerkung.

(1) U_n ist eine endliche Untergruppe von $\overline{K}^\times$ (mit Multiplikation) und deshalb ist U_n eine zyklische Gruppe (nach einer Übung vor Satz **??**).
(2) Falls $\mathrm{Char}(K) = 0$ oder $\mathrm{Char}(K) \nmid n$ ist $f(t) = t^n - 1$ separabel (weil $f'(t) = nt^{n-1}$). In diesem Fall gilt $|U_n| = n$ und $U_n \cong \mathbb{Z}/n\mathbb{Z}$.
(3) Falls $\mathrm{Char}(K) = p > 0$ und $n = p^r n'$ mit $p \nmid n'$ gilt $t^n - 1 = (t^{n'} - 1)^{p^r}$ und es folgt, dass $U_n = U_{n'} \cong \mathbb{Z}/n'\mathbb{Z}$.

Definition. Eine *primitive n-te Einheitswurzel* ist ein Element von U_n, das U_n erzeugt.

Beispiel. Für $K = \mathbb{Q}$ und $\overline{\mathbb{Q}} \subset \mathbb{C}$ sind die Einheitswurzeln

$$U_n := \{e^{2\pi ik/n} : 1 \leq k \leq n\}.$$

Für $n = 4$ gilt $U_4 = \{\pm 1, \pm i\}$ und $\pm i$ sind primitive Einheitswurzeln.

Definition. Die Eulersche Phi-Funktion $\phi : \mathbb{N}_{>0} \to \mathbb{N}$ wird durch

$$\phi(n) := |\{1 \leq k \leq n : \mathrm{ggT}(k, n) = 1\}|$$

definiert.

Übung. Es gilt

$$\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times| = |\{k + n\mathbb{Z} : \mathbb{Z}/n\mathbb{Z} \text{ wird von } k + n\mathbb{Z} \text{ erzeugt}\}|.$$

Für eine Primzerlegung $n = p_1^{r_1} \cdots p_s^{r_s}$ hat man $\phi(n) = \prod_{j=1}^{s} p_j^{r_j - 1}(p_j - 1)$.

Korollar. Sei K ein Körper und $n \in \mathbb{N}_{>0}$, so dass $\mathrm{Char}(K) = 0$ oder $\mathrm{Char}(K) \nmid n$.

(1) $\phi(n)$ ist die Anzahl von Primitiven n-ten Einheitswurzeln.
(2) Sei ζ eine primitive n-te Einheitswurzel. Dann ist ζ^k genau dann eine primitive n-te Einheitswurzel, wenn $\mathrm{ggT}(k, n) = 1$.

Bemerkung. Sei K ein Körper und $n \in \mathbb{N}_{>0}$, so dass $\mathrm{Char}(K) = 0$ oder $\mathrm{Char}(K) \nmid n$. Sei $\zeta_n \in U_n$ eine primitive n-te Einheitwurzel. Dann ist $K(\zeta_n)$ ein Zerfällungskörper von $t^n - 1$ und weil $t^n - 1 \in K[t]$ separabel ist, ist $K(\zeta_n)/K$ eine endliche Galois-Erweiterung (Satz 4.2). Sei

$$\Phi_n(t) = \prod_{\substack{\alpha \in U_n \\ \text{primitiv}}} (t - \alpha)$$

ein Polynom vom Grad $\phi(n)$, dessen Nullstellen die primitive n-te Einheitswurzeln sind. Das Bild einer primitiven n-ten Einheitswurzel unter $\varphi \in \mathrm{Gal}(K(\zeta_n)/K)$ ist auch eine primitive n-ten Einheitswurzel. Deshalb gilt $\Phi_n^\varphi = \Phi_n$ für alle $\varphi \in \mathrm{Gal}(K(\zeta_n)/K)$ und insbesondere folgt $\Phi_n(t) \in K[t]$, da $K = K(\zeta)^{\mathrm{Gal}(K(\zeta_n)/K)}$. Das Minimalpolynom $m_{\zeta_n}(t)$ von ζ_n über K ist ein Teiler von $\Phi_n(t)$ und deshalb gilt $[K(\zeta_n) : K] | \deg(\Phi_n) = \phi(n)$.

Definition. Für $K = \mathbb{Q}$ heißt $\mathbb{Q}(\zeta_n)$ der *Kreisteilungskörper* und $\Phi_n(t) \in \mathbb{Q}[t]$ das *Kreisteilungspolynom*.

[29.01.19]

Satz 4.7. *Sei K ein Körper und $n \in \mathbb{N}_{>0}$, so dass $\mathrm{Char}(K) = 0$ oder $\mathrm{Char}(K) \nmid n$. Sei $\zeta_n \in U_n$ eine primitive n-te Einheitswurzel. Dann gilt*

(1) $K \subset K(\zeta_n)$ ist eine endliche Galois-Erweiterung,
(2) Man hat $[K(\zeta_n) : K] \mid \phi(n)$ und für $K = \mathbb{Q}$ man hat $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$,
(3) Es gibt einen injektiven Gruppenhomomorphismus $\rho : \mathrm{Gal}(L/K) \to \mathrm{Aut}(U_n)$ und ferner gilt $\mathrm{Aut}(U_n) \cong \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, wobei die Automorphismengruppen hier die Gruppe von Gruppenautomorphismen von $(U_n, \cdot)$ und $(\mathbb{Z}/n\mathbb{Z}, +)$ sind. Für $K = \mathbb{Q}$ haben wir Gruppenisomorphismen

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

Satz 4.8. *Sei K ein Körper und $n \in \mathbb{N}_{>0}$, so dass $\mathrm{Char}(K) = 0$ oder $\mathrm{Char}(K) \nmid n$. Dann gilt*

(1) Φ_n ist ein normiertes separables Polynom in $K[t]$ vom Grad $\phi(n)$,
(2) $t^n - 1 = \prod_{d|n, d>0} \Phi_d(t)$,
(3) Für $K = \mathbb{Q}$ gilt $\Phi_n(t) \in \mathbb{Z}[t]$ und ferner ist Φ_n irreduzibel in $\mathbb{Z}[t]$ und $\mathbb{Q}[t]$.

Beispiel. Für eine Primzahl p gilt

$$\Phi_p(t) = \frac{t^p - 1}{\Phi_1(t)} = \frac{t^p - 1}{t - 1} = t^{p-1} + t^{p-2} + \cdots + 1.$$

Man hat

$$\Phi_6(t) = \frac{t^6 - 1}{\Phi_3(t)\Phi_2(t)\Phi_1(t)} = t^2 - t + 1.$$

Satz 4.9. *Seien $n, m \in \mathbb{N} \setminus \{0\}$ mit $\mathrm{ggT}(n, m) = 1$ und seien $\zeta_n \in U_n$ und $\zeta_m \in U_m$ primitive n-te und m-te Einheitswurzlen. Dann gilt $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}$ und die Abbildung*

$$\begin{array}{ccc} \mathrm{Gal}(\mathbb{Q}(\zeta_n, \zeta_m)/\mathbb{Q}) & \to & \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \\ \varphi & \mapsto & (\varphi|_{\mathbb{Q}(\zeta_n)}, \varphi|_{\mathbb{Q}(\zeta_m)}) \end{array}$$

ist ein Gruppenisomorphismus.

Satz 4.10. *Sei $q = p^r$ eine Primpotenz und $\zeta_n \in \overline{\mathbb{F}_q}$ eine primitive n-te Einheitswurzel, wobei $p \nmid n$. Dann gilt die folgende Aussagen.*

(1) Es gibt einen injektiven Gruppenhomomorphismus

$$\rho : \mathrm{Gal}(\mathbb{F}_q(\zeta_n)/\mathbb{F}_q) \hookrightarrow \mathrm{Aut}(U_n) \cong \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$$

und der relative Frobenius Homomorphismus Fr_{rel}, der ein erzeugendes Element von $\mathrm{Gal}(\mathbb{F}_q(\zeta_n)/\mathbb{F}_q)$ ist und der durch $Fr_{rel}(\alpha) = \alpha^q$ definiert wird, hat Bild unter φ gleich $q + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$, so dass $\mathrm{Gal}(\mathbb{F}_q(\zeta_n)/\mathbb{F}_q) \cong < q + n\mathbb{Z} > < (\mathbb{Z}/n\mathbb{Z})^\times$.

(2) $[\mathbb{F}_q(\zeta_n) : \mathbb{F}_q]$ ist die Ordung von $q + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$.

(3) $\Phi_n(t) \in \mathbb{F}_q(t)$ ist genau dann irreduzibel, wenn $< q + n\mathbb{Z} >= (\mathbb{Z}/n\mathbb{Z})^\times$.

Literatur

- S. Bosch, Algebra (7. Auflage), Springer-Lehrbuch.
- S. Lang, Undergraduate Algebra, Springer Undergraduate Texts in Mathematics.
- J.S. Milne, Fields and Galois Theory.

Freie Universität Berlin, Arnimallee 3, Raum 011, 14195 Berlin, Germany

hoskins@math.fu-berlin.de