Algebra I
Wintersemester 2020/21

Prof. Dr. Alexander Schmidt

Ziel: Gruppen, Ringe, Körper
Anwendung:
- warum kann man das 17-Eck konstruieren, aber nicht das 19-Eck?
- warum kann man „den Kreis nicht quadrieren“?
- warum kann man Gleichungen 5ten und höheren Grades nicht auflösen?

Literatur: Bosch: „Algebra“.

Inhaltsverzeichnis

1 Gruppentheorie **2**
1.1 Definitionen . . . 2
1.2 Nebenklassen, Normalteiler, Faktorgruppen . . . 4
1.3 Zyklische Gruppen . . . 8

2 Ringe und Polynome **10**
2.1 Ringe, Polynomringe in einer Variablen . . . 10
2.2 Faktorielle Ringe . . . 13
2.3 Der Satz von Gauß . . . 15
2.4 Irreduzibilitätskriterien . . . 20
2.5 Verallgemeinerte Polynomringe . . . 22

3 Algebraische Körpererweiterungen **25**
3.1 Charakteristik . . . 25
3.2 Endliche und algebraische Körpererweiterungen . . . 27
3.3 Algebraischer Abschluss . . . 32
3.4 Ganze Ringerweiterungen . . . 35
3.5 Zerfällungskörper . . . 39
3.6 Separable Erweiterungen . . . 43
3.7 Endliche Körper . . . 48
3.8 Rein inseparable Erweiterungen . . . 50
3.9 Der Satz vom primitiven Element . . . 52

1 Gruppentheorie

1.1 Definitionen

Definition 1.1. Eine Menge M zusammen mit einer Verknüpfung $M \times M \to M$, $(a, b) \to ab$ heißt **Monoid**, wenn die folgenden Eigenschaften erfüllt sind:

(i) Assoziativität: $(ab)c = a(bc), \quad \forall a, b, c \in M$
(ii) neutrales Element: es existiert ein $e \in M$ mit $em = m = me$ für alle $m \in M$.

Bemerkung 1.2. 1) e ist eindeutig bestimmt. Ist e' ein weiteres neutrales Element, so gilt $e = e \cdot e' = e'$.
2) Wegen (i) kann man Klammerung weglassen und für $m_1, \ldots, m_n \in M$ vom Produkt $m_1 \cdots m_n \in M$ sprechen. Für $a \in M$ und $n \in \mathbb{N}$ setzt man

$$a^n = \underbrace{a \cdots a}_{n\text{-mal}}$$

Per Konvention ist $a^0 = e$.

Definition 1.3. Sei $(M, \cdot)$ ein Monoid und $a \in M$. Ein $b \in M$ heißt **invers** zu a, wenn $ab = e = ba$ gilt.

Bemerkung 1.4. b ist, wenn es existiert, eindeutig durch a bestimmt: Ist b' auch Inverses, so gilt $b = eb = b'ab = b'e = b'$.

Definition 1.5. Ein Monoid $(G, \cdot)$ heißt **Gruppe**, wenn jedes Element ein Inverses hat.

Bemerkung 1.6. Man kann dies abschwächen zu:
- Assoziativität,
- Existenz eines linksneutralen Elements,
- Existenz von Linksinversen,

und dann zeigen, dass das linksneutrale Element auch rechtsneutral und ein Linksinverses auch rechtsinvers ist (siehe LA I-Vorlesung).

Definition 1.7. Ein Monoid (eine Gruppe) heißt **kommutativ**, wenn $ab = ba$ für beliebige a, b gilt.

Beispiele 1.8. • $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ mit "+" sind kommutative Gruppen.
• $(\mathbb{Z}, \cdot)$ und $(\mathbb{N}_0, +)$ sind kommutative Monoide.
• $\mathfrak{S}_n$ ist eine Gruppe, nicht kommutativ für $n \geq 3$
• Ist k ein Körper, so sind $\mathrm{Gl}_n(k)$ und $\mathrm{Sl}_n(k)$ Gruppen, die für $n > 1$ nicht-kommutativ sind.

Definition 1.9. Sei G ein Monoid. Eine Teilmenge $H \subset G$ heißt **Untermonoid**, falls

(i) $e \in H$.

(ii) $a, b \in H \Rightarrow ab \in H$.

Ist G eine Gruppe, so heißt H **Untergruppe** wenn zusätzlich gilt

(iii) $a \in H \Rightarrow a^{-1} \in H$.

Definition 1.10. Seien G, G' Monoide mit neutralen Elementen e, e'. Eine Abbildung $\varphi : G \to G'$ heißt **Monoidhomomorphismus** wenn

(i) $\varphi(e) = e'$.

(ii) $\varphi(ab) = \varphi(a)\varphi(b) \qquad \forall\, a, b \in G.$

Bemerkung 1.11. Sind G und G' Gruppen, so folgt (i) schon aus (ii) wegen $\varphi(e) = \varphi(e \cdot e) = \varphi(e)\varphi(e)$, also $e' = \varphi(e)^{-1}\varphi(e) = \varphi(e)^{-1}\varphi(e)\varphi(e) = \varphi(e)$.

Bemerkung 1.12. Ist M ein Monoid und $x \in M$, so definiert

$$\begin{array}{rcl} \varphi : \mathbb{N}_0 & \longrightarrow & M \\ n & \longmapsto & x^n \end{array}$$

einen Monoidhomomomorphismus. Ist G eine Gruppe und $x \in G$ so erhält man einen Gruppenhomomorphismus

$$\begin{array}{rcl} \varphi : \mathbb{Z} & \longrightarrow & G \\ n & \longmapsto & x^n \end{array}$$

wobei man für $n < 0$ setzt: $x^n = (x^{-n})^{-1}$.

Satz 1.13. *(Satz von Cayley). Sei G eine endliche Gruppe mit n Elementen. Dann gibt es einen injektiven Gruppenhomomorphismus $\varphi : G \hookrightarrow \mathfrak{S}_n$.*

Beweis. Wir nummerieren die Elemente

$$G = \{g_1, \ldots, g_n\}.$$

Für $g \in G$ definieren wir $\pi_g : \{1, \ldots, n\} \to \{1, \ldots, n\}$ durch $gg_i = g_{\pi_g(i)}$.
Behauptung: π_g ist bijektiv, also $\pi_g \in \mathfrak{S}_n$.
Injektivität: ist $\pi_g(i) = \pi_g(j)$, so gilt $gg_i = gg_j \Rightarrow g_i = g_j \Rightarrow i = j$.
Surjektivität: folgt aus Injektivität und Endlichkeit.

Nun definiere $\varphi : G \to \mathfrak{S}_n$ durch $\varphi(g) = \pi_g$.

Behauptung: $\varphi : G \to \mathfrak{S}_n$ ist ein Gruppenhomomorphismus.
Nach Definition gilt $(hh')g_i = g_{\varphi(hh')(i)}$, es gilt aber auch

$$\begin{array}{rcl} (hh')g_i = h(h'g_i) & = & hg_{\varphi(h')(i)} \\ & = & g_{\varphi(h)(\varphi(h')(i))} = g_{(\varphi(h)\varphi(h'))(i)}. \end{array}$$

Also $\varphi(hh') = \varphi(h)\varphi(h')$, was die Behauptung zeigt.
Behauptung: $\varphi : G \to \mathfrak{S}_n$ ist injektiv.
Sei $\varphi(g) = \mathrm{id}$. Dann gilt $gh = h$ für alle $h \in G$, insbesondere $g = ge = e$. □

Bemerkung 1.14. Sei G eine kommutative Gruppe und $n \in \mathbb{N}$. Dann ist $G \to G$, $g \mapsto g^n$, ein Gruppenhomomorphismus.

Bemerkung 1.15. Sei G eine Gruppe und $a \in G$. Dann ist $\varphi_a : G \to G$, $g \mapsto aga^{-1}$, ein Gruppenhomomorphismus. Man nennt φ_a **inneren Automorphismus**. Die Abbildung

$$G \longrightarrow \mathrm{Aut}(G),\ a \longmapsto \varphi_a,$$

ist ein Gruppenhomomorphismus. Dieser ist genau dann trivial (d.h. konstant $= \mathrm{id}_G$), wenn G kommutativ ist.

1.2 Nebenklassen, Normalteiler, Faktorgruppen

Definition 1.16. Sei G eine Gruppe und $H \subset G$ eine Untergruppe. Eine **Linksnebenklasse** von H in G ist eine Teilmenge der Gestalt $aH := \{ah \mid h \in H\}$.

Satz 1.17. *Je zwei Linksnebenklassen von H in G sind gleichmächtig, verschiedene Linksnebenklassen von H in G sind disjunkt. Insbesondere ist G disjunkte Vereinigung der Linksnebenklassen von H.*

Beweis. Für jedes $a \in G$ ist die Abbildung

$$eH = H \longrightarrow aH,\ h \longmapsto ah,$$

bijektiv, also sind alle Linksnebenklassen gleichmächtig. Die zweite Behauptung folgt aus dem nächsten Lemma. □

Lemma 1.18. *Seien aH, bH zwei Linksnebenklassen in G. Dann sind äquivalent*

(i) $aH = bH$.
(ii) $aH \cap bH \neq \varnothing$.
(iii) $a \in bH$.
(iv) $b^{-1}a \in H$.

Beweis. (i) $\Rightarrow$ (ii) ist trivial wegen $H \neq \varnothing$.
(ii) $\Rightarrow$ (iii) Sei $c \in aH \cap bH$, $c = ah_1 = bh_2$. Dann gilt $a = bh_2h_1^{-1} \in bH$.
(iii) $\Rightarrow$ (iv) $a \in bH \Rightarrow a = bh, h \in H$, also $b^{-1}a = h \in H$.
(iv) $\Rightarrow$ (i) $b^{-1}a = h \in H$, also $a = bh$ und daher $aH \subset bH$. Nun ist H Untergruppe, also gilt auch $a^{-1}b = (b^{-1}a)^{-1} \in H$ und wir erhalten analog $bH \subset aH$. □

Bemerkung 1.19. • Die Linksnebenklassen von H in G sind die Äquivalenzklassen bzgl. der Relation $a \sim_H b \iff b^{-1}a \in H$.
• die Elemente der Linksnebenklasse aH heißen ihre **Repräsentanten**. Ist a' ein Repräsentant von aH, so folgt aus dem Lemma, dass $aH = a'H$.
• Die Menge der Linksnebenklassen wird mit G/H bezeichnet.
• In analoger Weise definiert man die Menge $H\backslash G$ der Rechtsnebenklassen von H in G, d.h. der Teilmengen der Gestalt

$$Ha := \{ha \mid h \in H\},\ a \in G.$$

Lemma 1.20. *Die bijektive Abbildung $G \to G$, $a \mapsto a^{-1}$ definiert eine Bijektion*

$$G/H \xrightarrow{\sim} H\backslash G$$

Beweis. $ah \mapsto h^{-1}a^{-1}$, also bildet sich die Linksnebenklasse aH bijektiv auf die Rechtsnebenklasse Ha^{-1} ab. □

Definition 1.21. Der **Index** von H in G ist die Anzahl der Links (Rechts)-nebenklassen von H in G. Bezeichnung: $(G : H)$. Die **Ordnung** von G ist die Anzahl der Elemente von G. Bezeichnung: $\mathrm{ord}(G)$. (Sowohl Index als auch Ordnung können ∞ sein.)

Mit den üblichen Konventionen für das Rechnen mit ∞ ergibt sich aus Satz 1.17 sofort

Satz 1.22 (Satz von Lagrange). *Ist $H \subset G$ eine Untergruppe, so gilt*

$$\mathrm{ord}(G) = \mathrm{ord}(H)(G : H).$$

Definition 1.23. Eine Untergruppe $H \subset G$ heißt **Normalteiler**, wenn $aH = Ha$ für alle $a \in G$ gilt. In diesem Fall bezeichnet man dieNebenklasse $aH = Ha$ als die **Restklasse** von a modulo H.

Lemma 1.24. *Die folgenden Aussagen sind äquivalent*
(i) $H \subset G$ ist Normalteiler.
(ii) $aHa^{-1} = H \quad \forall\, a \in G$.
(iii) $aHa^{-1} \subset H \quad \forall\, a \in G$.

Beweis. (i) $\Leftrightarrow$ (ii) ist trivial, genauso (ii) $\Rightarrow$ (iii). Sei nun $aHa^{-1} \subset H$, also $aH \subset Ha$. Es gilt aber auch $a^{-1}Ha \subset H$, also $Ha \subset aH$, also $aH = Ha$. □

Notation: $H \lhd G$ bedeutet H ist Normalteiler in G.

Bemerkung 1.25. Die Untergruppen $\{1\}$ und G sind aus trivialen Gründen stets Normalteiler in G.

Lemma 1.26. *Jede Untergruppe $H \subset G$ vom Index 2 ist Normalteiler.*

Beweis. Zu zeigen: $aH = Ha$ für beliebiges $a \in G$. Für $a \in H$ gilt $aH = H = Ha$. Für $a \notin H$ folgt $G = H \dot\cup aH$ und $G = H \dot\cup Ha$. Wir erhalten $aH = G - H = Ha$. □

Lemma 1.27. *Ist $f : G \to G'$ ein Gruppenhomomorphismus, so ist* $\mathrm{Kern}(f) \subset G$ *ein Normalteiler.*

Beweis. Ist $a \in G$, $h \in \mathrm{Kern}(f)$ so gilt

$$f(aha^{-1}) = f(a) \cdot e' \cdot f(a^{-1}) = f(aa^{-1}) = f(e) = e',$$

also $aha^{-1} \in \mathrm{Kern}\, f$. □

Bemerkung 1.28. Bild$(f) \subset G'$ ist eine Untergruppe aber i.A. kein Normalteiler.

Definition 1.29. Sei $H \lhd G$. Dann heißt G/H mit der Verknüpfung

$$(aH)(a'H) = aa'H$$

die **Faktorgruppe** von G nach H.

Verifikation:
• Die Verknüpfung ist wohldefiniert: Sei $a_1 = a_2h$, $a_1' = a_2'h'$, $h, h' \in H$. Dann gilt $a_1a_1' = a_2ha_2'h' = a_2a_2' \cdot \underbrace{(a_2')^{-1}ha_2'}_{\in H} h'$, also $a_1a_1'H = a_2a_2'H$.
(Hier haben wir $H \lhd G$ benutzt!)
• neutrales Element: eH.
• Inverses zu aH ist $a^{-1}H$.

Bemerkung 1.30. Die kanonische Projektion $G \to G/H$, $g \mapsto gH$ ist ein Gruppenhomomorphismus mit Kern H. Daher sind die Normalteiler genau die Untergruppen, die als Kerne von Gruppenhomomorphismen auftreten.

Satz 1.31. *Sei $H \lhd G$ und $\phi : G \to G/H$ die kanonische Projektion. Dann induziert die Zuordnung $U \mapsto \varphi^{-1}(U)$ eine inklusionserhaltende Bijektion*

$$\left\{ \begin{array}{c} \text{Untergruppen} \\ \text{in } G/H \end{array} \right\} \xrightarrow{\sim} \left\{ \begin{array}{c} \text{Untergruppen} \\ \text{in } G \text{ die } H \\ \text{enthalten} \end{array} \right\}$$

U ist genau dann Normalteiler in G/H, wenn $\phi^{-1}(U)$ Normalteiler in G ist.

Beweis. 1) $\phi^{-1}(U)$ ist Untergruppe in G und $\phi^{-1}(U) \supset \text{Kern}(\phi) = H$.
2) Die Zuordnung ist surjektiv. Sei $W \subset G$ mit $W \supset H$. Setze $U = \phi(W)$.
Behauptung: $W = \phi^{-1}(U)$.
Klar ist $W \subset \phi^{-1}(U) = \phi^{-1}(\phi(W))$. Sei nun $w \in \phi^{-1}(U)$, d.h. $\phi(w) \in U = \phi(W)$. Dann existiert ein $w' \in W$ mit $\phi(w) = \phi(w')$. Es folgt $w(w')^{-1} \in \text{Kern}(\phi) = H$ und wegen $H \subset W$ folgt $w = w(w')^{-1} \cdot w' \in W$.
3) Die Zuordnung ist injektiv. Wegen der Surjektivität von ϕ gilt $U = U' \iff \phi^{-1}(U) = \phi^{-1}(U')$.

Letztens: Ist $U \lhd G/H$, so gilt

$$g\phi^{-1}(U)g^{-1} \subset \phi^{-1}(\phi(g)U\phi(g)^{-1}) = \phi^{-1}(U),$$

also ist $\phi^{-1}(U)$ Normalteiler.
Ist umgekehrt $\phi^{-1}(U) \lhd G$ und $u \in U$, $g \in G/H$ und wählen wir $u', g' \in G$ mit $\phi(u') = u$, $\phi(g') = g$,
so gilt

$$gug^{-1} = \phi(\underbrace{g'u'(g')^{-1}}_{\in \phi^{-1}(U)}) \in \phi(\phi^{-1}(U)) = U. \qquad \square$$

Satz 1.32 (**Homomorphiesatz**). *Sei $f : G \to G'$ ein Gruppenhomomorphismus. Dann faktorisiert f in eindeutiger Weise in der Form*

$$G \xrightarrow{p} G/\operatorname{Kern}(f) \xrightarrow[F]{\sim} \operatorname{Bild}(f) \xhookrightarrow{i} G'.$$

Hierbei ist p die kanonische Projektion, i die kanonische Inklusion und F ist durch $F(a \operatorname{Kern}(f)) = f(a)$ definiert. F ist ein Isomorphismus.

Beweis. Genau der gleiche wie der für kommutative Gruppen, den wir in der LA gesehen haben. □

Definition 1.33. Sind $H_1, H_2 \subset G$ Untergruppen, so bezeichnet H_1H_2 die Menge

$$H_1H_2 = \{h_1h_2 \mid h_1 \in H_1,\ h_2 \in H_2\}.$$

Lemma 1.34. *Ist eine der Untergruppen H_1, H_2 Normalteiler, so ist H_1H_2 eine Untergruppe. Sind beide Normalteiler, so auch H_1H_2.*

Beweis. Sei H_1 Normalteiler. Dann liegt für $h_1, h_1' \in H_1$, $h_2, h_2' \in H_2$:

$$(h_1h_2)(h_1'h_2') = h_1 \underbrace{(h_2h_1'h_2^{-1})}_{\in H_1} h_2h_2'$$

wieder in H_1H_2. Mit h_1h_2 liegt auch $(h_1h_2)^{-1} = h_2^{-1}h_1^{-1} = \underbrace{h_2^{-1}h_1^{-1}h_2}_{\in H_1} h_2^{-1}$ in H_1H_2. Der Fall $H_2 \lhd G$ läuft analog. Schließlich gilt falls $H_1, H_2 \lhd G$, dass

$$gH_1H_2g^{-1} = (gH_1g^{-1})(gH_2g^{-1}) = H_1H_2.$$ □

Lemma 1.35. *Ist $N \lhd G$ Normalteiler und $H \subset G$ eine Untergruppe, so ist N Normalteiler in HN und $H \cap N$ Normalteiler in H.*

Beweis. • $(hn)n'(hn)^{-1} \in N$ wegen $hn \in G$
• Ist $n \in H \cap N$ so gilt $hnh^{-1} \in H \cap N$. □

Satz 1.36 (**1. Isomorphiesatz**). *Sei G eine Gruppe, $H \subset G$ eine Untergruppe und $N \lhd G$ ein Normalteiler. Dann induziert die natürliche Inklusion $H \hookrightarrow HN$ einen Isomorphismus*

$$H/H \cap N \xrightarrow{\sim} HN/N.$$

Beweis. Wir betrachten die Komposition

$$f : H \longrightarrow HN \longrightarrow HN/N.$$

Wegen $hnN = hN$ ist f surjektiv. Außerdem gilt $f(h) = e \iff hN = eN \iff h \in N$, also $\operatorname{Kern}(f) = H \cap N$. Der Homomorphiesatz impliziert einen natürlichen Isomorphismus $H/\operatorname{Kern}(f) \xrightarrow{\sim} \operatorname{Bild}(f)$, also genau

$$H/H \cap N \xrightarrow{\sim} HN/N.$$ □

Satz 1.37 (2. Isomorphiesatz). *Sei G eine Gruppe und $N, H \triangleleft G$ mit $N \subset H$. Dann gibt es einen natürlichen Isomorphismus*

$$(G/N)/(H/N) \xrightarrow{\sim} G/H.$$

Beweis. Zunächst induziert die Inklusion $H \hookrightarrow G$ eine Injektion $H/N \hookrightarrow G/N$, also ist H/N Untergruppe von G/N. Dies ist genau die Menge der Nebenklassen hN mit $h \in H$. Nun betrachten wir die kanonische Projektion $p : G \to G/H$. Es gilt $N \subset \mathrm{Kern}(p) = H$. Daher erhalten wir einen induzierten surjektiven Homomorphismus $\pi : G/N \to G/H$ mit $\mathrm{Kern}(\pi) = H/N$. Der Homomorphiesatz impliziert das Resultat. □

1.3 Zyklische Gruppen

Für $n \in \mathbb{N}$ bezeichne $n\mathbb{Z} \subset \mathbb{Z}$ die Untergruppe der durch n teilbaren ganzen Zahlen.

Satz 1.38. *Die Untergruppen von $\mathbb{Z}$ sind genau die folgenden: $\{0\}$, $n\mathbb{Z}$, $n \in \mathbb{N}$. Für $n \in \mathbb{N}$ ist $n\mathbb{Z}$ isomorph zu $\mathbb{Z}$.*

Beweis. Sei $H \subset \mathbb{Z}$ eine Untergruppe $H \neq 0$. Sei

$$n = \min\{a \in \mathbb{N},\ a \in H\}.$$

Da mit a auch $-a$ in H liegt, ist die obige Menge nichtleer und n eine wohldefinierte natürliche Zahl. Wegen $n \in H$ folgt $\underbrace{n + \cdots + n}_{m\text{-mal}} \in H$, also $nm \in H$ für alle $m \in \mathbb{N}$. Das gleiche gilt für $-nm$, also:

$$na \in H \text{ für } \forall\, a \in \mathbb{Z} \quad \Longrightarrow \quad n\mathbb{Z} = H.$$

Angenommen es gäbe ein $a \in H$, $a \notin n\mathbb{Z}$. Dann existierte ein $b \in \mathbb{Z}$ mit

$$0 < a - nb < n.$$

Wegen $a \in H$ und $nb \in H$ folgt $a - nb \in H$ im Widerspruch zur Definition von n. Daher gilt $n\mathbb{Z} \subset H$.

Für $n \in \mathbb{N}$ betrachten wir den injektiven Gruppenhomomorphismus $\varphi : \mathbb{Z} \to \mathbb{Z}$, $a \mapsto na$. Es gilt: $\mathrm{Kern}(\varphi) = 0$, $\mathrm{Bild}(\varphi) = n\mathbb{Z}$. Nach dem Homomorphiesatz induziert φ einen Isomorphismus $\mathbb{Z} \xrightarrow{\sim} n\mathbb{Z}$. □

Sei G eine Gruppe und $X \subset G$ eine Teilmenge.

Definition 1.39. Der Durchschnitt aller Untergruppen $H \subset G$ mit $X \subset H$ heißt die **von X erzeugte Untergruppe**. Bezeichnung $\langle X \rangle$. Diese ist die kleinste Untergruppe von G die X enthält. Man sagt G werde von X erzeugt, wenn $\langle X \rangle = G$ gilt.

Lemma 1.40. *$\langle X \rangle$ ist die Teilmenge aller Elemente von G der Form*

$$x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n} \quad \textit{mit} \quad n \in \mathbb{N}_0, \quad \varepsilon_i \in \{\pm 1\},$$

und $x_1, \dots, x_n \in X$.

Beweis. Diese Teilmenge ist offenbar eine Untergruppe und jede Untergruppe $H \subset G$ mit $X \subset H$ enthält alle diese Elemente. □

Bemerkung 1.41. Ist $X = \{x_1, \dots, x_r\}$ endlich, so schreibt man auch $\langle x_1, \dots, x_r \rangle$ anstelle von $\langle \{x_1, \dots, x_r\} \rangle$.

Lemma 1.42. *Sei $x \in G$. Dann ist $\langle x \rangle$ das Bild des Gruppenhomomorphismus*

$$\mathbb{Z} \longrightarrow G, \quad n \longmapsto x^n.$$

Beweis. Klar. □

Definition 1.43. Eine Gruppe G heißt **zyklisch**, wenn sie von einem Element erzeugt wird. Äquivalent: Es gibt einen surjektiven Gruppenhomomorphismus $\mathbb{Z} \to G$.

Korollar 1.44. *Sei G eine zyklische Gruppe. Dann gilt*

$$G \cong \begin{cases} \mathbb{Z} & \textit{falls} \quad \operatorname{ord} G = \infty \\ \mathbb{Z}/n\mathbb{Z} & \textit{falls} \quad \operatorname{ord} G = n \in \mathbb{N}. \end{cases}$$

Beweis. Sei $\varphi : \mathbb{Z} \to G$ ein surjektiver Gruppenhomomorphismus. Nach Satz 1.38 gilt

$$\operatorname{Kern}(\varphi) = \begin{cases} 0 & \text{oder} \\ n\mathbb{Z} & \text{mit } n \in \mathbb{N}. \end{cases}$$

Der Homomorphiesatz liefert nun das Ergebnis. □

Satz 1.45. *Ist G eine zyklische Gruppe, so ist jede Untergruppe und jede Faktorgruppe von G wieder zyklisch.*

Beweis. Faktorgruppe: Sei $\varphi : \mathbb{Z} \to G$ surjektiv. Dann ist für jeden Normalteiler $N \triangleleft G$ auch $\mathbb{Z} \xrightarrow{\varphi} G \xrightarrow{p} G/N$ surjektiv, also G/N ist zyklisch.
Untergruppe: Sei $H \subset G$ eine Untergruppe und $\varphi : \mathbb{Z} \to G$ surjektiv. Dann ist $\varphi^{-1}(H) \subset \mathbb{Z}$ eine Untergruppe die sich surjektiv auf H abbildet. Nach dem ersten Teil des Beweises genügt es zu zeigen, dass $\varphi^{-1}(H)$ zyklisch ist. Nun ist nach Satz 1.38

$$\varphi^{-1}(H) = \begin{cases} 0 & \text{oder} \\ n\mathbb{Z} & n \in \mathbb{N} \end{cases}$$

Die triviale Gruppe ist zyklisch und $n\mathbb{Z}$ ist nach Satz 1.38 isomorph zu $\mathbb{Z}$, also zyklisch. □

Sei G eine Gruppe und $a \in G$.

Definition 1.46. Die **Ordnung** $\mathrm{ord}(a)$ von a ist die kleinste natürliche Zahl so dass $a^{\mathrm{ord}(a)} = e$ gilt. Existiert eine solche Zahl nicht, so setzt man $\mathrm{ord}(a) = \infty$.

Lemma 1.47.

$$\mathrm{ord}(a) = \mathrm{ord}(\langle a \rangle)$$

Beweis. Es gilt

$$\langle a \rangle = \{\dots, a^{-2}, a^{-1}, e, a, a^2, \dots\}$$

und falls $\mathrm{ord}(a) = \infty$ gilt, so sind alle diese Elemente verschieden. Würde nämlich $a^\alpha = a^\beta$ mit $\beta > \alpha \in \mathbb{Z}$ gelten, so folgt $a^{\beta-\alpha} = e$ und $\beta - \alpha \in \mathbb{N}$ im Widerspruch zu $\mathrm{ord}(a) = \infty$.
Nun sei $\mathrm{ord}(a) = n \in \mathbb{N}$. Dann sind (benutze das gleiche Argument) die Elemente $\{a, a^2, \dots, a^n = e\}$ paarweise verschieden und diese bilden die Gruppe $\langle a \rangle$. □

Korollar 1.48. *Für $a \in G$ gilt* $\mathrm{ord}(a) \mid \mathrm{ord}(G)$.

Beweis. Es gilt nach dem Satz von Lagrange: $\mathrm{ord}(G) = (G : \langle a \rangle) \cdot \mathrm{ord}(a)$. □

Satz 1.49 (Kleiner Fermatscher Satz)**.** *Ist G eine endliche Gruppe, so gilt*

$$a^{\mathrm{ord}(G)} = e$$

für alle $a \in G$.

Beweis. Beweis: $\mathrm{ord}(a) \mid \mathrm{ord}(G)$ und $a^{\mathrm{ord}(a)} = e$. □

Satz 1.50. *Sei G eine endliche Gruppe von Primzahlordnung, d.h.* $\mathrm{ord}(G) = p$, *p Primzahl. Dann ist G zyklisch und $G \cong \mathbb{Z}/p\mathbb{Z}$.*

Beweis. Sei $a \in G$, $a \neq e$. Dann gilt $\mathrm{ord}(a) > 1$ und $\mathrm{ord}(a) \mid \mathrm{ord}(G) = p$. Also $\mathrm{ord}(a) = p$ und daher $G = \langle a \rangle$. □

2 Ringe und Polynome

2.1 Ringe, Polynomringe in einer Variablen

Definition 2.1. Ein **Ring** (mit 1) ist eine Menge R mit zwei binären Operatoren „$+$“ und „$\cdot$“ und Elementen $0, 1 \in R$, so dass

(i) $(R, +, 0)$ ist eine kommutative Gruppe
(ii) $(R, \cdot, 1)$ ist ein Monoid
(iii) es gilt

$$(a + b)c = ac + bc,\ c(a + b) = ca + cb$$

für alle $a, b, c \in R$.
R heißt **kommutativ**, wenn die Multiplikation kommutativ ist.

Eine Teilmenge $S \subset R$ heißt **Unterring**, wenn $(S, +)$ eine Untergruppe in $(R, +)$ und $(S, \cdot)$ ein **Untermonoid** in $(R, \cdot)$ ist.
Eine Abbildung $f : R \to R'$ heißt **Ringhomomorphismus** wenn $f(a + b) = f(a) + f(b)$, $f(ab) = f(a)f(b)$ und $f(1) = 1$ gilt.

Aus der Definition sieht man direkt: $0a = (0 + 0)a = 0a + 0a$, woraus $0a = 0$ für alle $a \in R$ folgt.

Beispiel 2.2. • $R = K$ ein Körper.
• $R = \mathbb{Z}$.
• Ist R ein Ring, so auch der Ring der Polynome $R[T]$.
• Der Nullring 0, d.h. eine einelementige Menge mit den einzig möglichen Operationen ist ein Ring. In diesem gilt $0 = 1$. Bis auf Isomorphie gibt es nur einen Ring mit $0 = 1$, nämlich den Nullring. Grund: Ist $0 = 1$, so gilt für jedes $a \in R$:

$$a = 1 \cdot a = 0 \cdot a = 0.$$

Wir betrachten im folgenden nur kommutative Ringe, d.h. ohne das extra nochmals zu sagen wird im folgenden von jedem Ring angenommen, dass er kommutativ ist!

Definition 2.3. Ein **Ideal** $\mathfrak{a}$ in einem Ring R ist eine Teilmenge $\mathfrak{a} \subset R$ so dass
(i) $(\mathfrak{a}, +) \subset (R, +)$ ist Untergruppe
(ii) $r \in R$, $a \in \mathfrak{a} \Rightarrow ra \in \mathfrak{a}$.

Beispiel 2.4. • $\mathfrak{a} = R$ und $\mathfrak{a} = \{0\}$ sind stets Ideale.
• die Untergruppen von $\mathbb{Z}$ (d.h. 0 und $n\mathbb{Z}$, $n \in \mathbb{N}$) sind sämtlich Ideale.

Ist R ein Ring und $\mathfrak{a} \subset R$ ein Ideal, so wird die Faktorgruppe $R/\mathfrak{a}$ mit der Multiplikation

$$(a + \mathfrak{a})(b + \mathfrak{a}) = ab + \mathfrak{a}$$

wieder ein Ring. Die kanonische Projektion $\phi : R \to R/\mathfrak{a}$, $a \mapsto a + \mathfrak{a}$ ist ein surjektiver Ringhomomorphismus.

Satz 2.5. *Die Zuordnung $\mathfrak{b} \mapsto \phi^{-1}(\mathfrak{b})$ definiert eine inklusionserhaltende Bijektion*

$$\left\{ \begin{array}{c} \textit{Ideale in} \\ R/\mathfrak{a} \end{array} \right\} \xrightarrow{\sim} \left\{ \begin{array}{c} \textit{Ideale in } R \textit{ die} \\ \mathfrak{a} \textit{ enthalten} \end{array} \right\}$$

Beweis. Analog wie 1.31. Siehe auch die LA II-Vorlesung. □

Definition 2.6. $x \in R$ heißt **Nullteiler**, wenn ein $y \in R$, $y \neq 0$ mit $xy = 0$ existiert. R heißt nullteilerfrei, wenn $R \neq 0$ und $0 \in R$ der einzige Nullteiler ist. $x \in R$ heißt **Einheit** wenn ein $y \in R$ mit $xy = 1$ existiert.

Die Menge $R^\times$ der Einheiten von R bildet eine abelsche Gruppe bzgl. Multiplikation.

Jedes Element $x \in R$ definiert ein **Hauptideal** $(x) = Rx = \{rx \mid r \in R\}$. $x \in R$ ist Einheit $\iff (x) = R$.
Ein Ideal $\mathfrak{a} \subset R$ heißt Hauptideal, wenn $\mathfrak{a} = (x)$ für ein $x \in R$.
R heißt **Hauptidealring**, wenn R nullteilerfrei ist und jedes Ideal in R Hauptideal ist.

Beispiel 2.7. $\mathbb{Z}$ ist ein Hauptidealring.

Definition 2.8. R heißt **Körper**, wenn $R^\times = R \setminus \{0\}$ (insbesondere ist $R = 0$ *kein* Körper).

Satz 2.9. *Sei R ein Ring $\neq 0$. Dann sind äquivalent*
(i) *R ist Körper.*
(ii) *(0) und (1) sind die einzigen Ideale in R.*
(iii) *jeder Homomorphismus $f : R \to S$ in einen Ring $S \neq 0$ ist injektiv.*

Beweis. (i) $\Rightarrow$ (ii). Sei $\mathfrak{a} \subset R$ ein Ideal $\neq 0$. Dann existiert ein $0 \neq x \in \mathfrak{a}$. Daher gilt $1 = x^{-1}x \in \mathfrak{a}$, folglich $R = (1) \subseteq \mathfrak{a} \subseteq R$.
(ii) $\Rightarrow$ (iii). Sei $f: R \to S$ ein Ringhomomorphismus mit $S \neq 0$. Wegen $0 \neq 1$ in S ist $\mathrm{Kern}(f) \subset R$ ein Ideal $\neq R \Rightarrow \mathrm{Kern}(f) = 0$.
(iii) $\Rightarrow$ (i). Sei $x \in R$ keine Einheit. Dann ist $(x) \neq R$, also $S = R/(x)$ nicht der Nullring. Es gilt $x \in \mathrm{Kern}(\phi : R \to R/(x))$, also $x = 0$. Daher ist R Körper. □

Definition 2.10. Ein Ideal $\mathfrak{p} \subset R$ heißt **Primideal** wenn $\mathfrak{p} \neq R$ und $xy \in \mathfrak{p} \Rightarrow x \in \mathfrak{p}$ oder $y \in \mathfrak{p}$. Ein Ideal heißt **Maximalideal**, wenn $\mathfrak{m} \neq R$ und es gibt kein Ideal $\mathfrak{a}$ mit $\mathfrak{m} \subsetneq \mathfrak{a} \subsetneq R$.

Satz 2.11. (i) *$\mathfrak{p}$ ist Primideal $\iff R/\mathfrak{p}$ ist nullteilerfrei.*
(ii) *$\mathfrak{m}$ ist Maximalideal $\iff R/\mathfrak{m}$ ist Körper.*
Insbesondere sind Maximalideale prim.

Beweis. (i) $xy \in \mathfrak{p} \Leftrightarrow \overline{xy} = 0$ in $R/\mathfrak{p}$.
(ii) Nach 2.5 entsprechen die Ideale $\mathfrak{a}$ mit $\mathfrak{m} \subsetneq \mathfrak{a} \subsetneq R$ den Idealen $\neq 0, (1)$ in $R/\mathfrak{m}$. Nach 2.9 ist $R/\mathfrak{m}$ genau dann ein Körper, wenn es solche Ideale nicht gibt. □

Satz 2.12. *Jeder Ring $\neq 0$ enthält ein Maximalideal.*

Beweis. Mit Hilfe des Zornschen Lemmas. Lassen wir weg. Siehe LA II. □

Korollar 2.13. (i) *Jedes Ideal $\mathfrak{a} \subsetneq R$ ist in einem Maximalideal enthalten.*
(ii) *jede Nichteinheit ist in einem Maximalideal enthalten.*

Beweis. (i) $\mathfrak{a} \subsetneq R \Rightarrow R/\mathfrak{a} \neq 0$. Nach Satz 2.12 erhalten wir ein Maximalideal in $R/\mathfrak{a}$ dessen Urbild in R nach Satz 2.5 ein Maximalideal ist, das $\mathfrak{a}$ umfasst.
(ii) x Nichteinheit $\Rightarrow (x) \subsetneq R$. □

2.2 Faktorielle Ringe

Im ganzen Abschnitt sind Ringe stets kommutativ und *nullteilerfrei*. Dann kann man „kürzen“, d.h. ist $a \neq 0$ und $ab = ac$ so folgt $b = c$.
Begründung: Es gilt $a(b-c) = 0$, also $b - c = 0$.

Definition 2.14. Ein Element $0 \neq \pi \in R \setminus R^\times$ heißt

Primelement $\Longleftrightarrow$ (π) ist Primideal
irreduzibel $\Longleftrightarrow$ aus $ab = \pi$ folgt $a \in R^\times$ oder $b \in R^\times$.

Wir sagen $a \mid b$ in R wenn ein $c \in R$ mit $ac = b$ existiert.
Also: π ist Primelement falls $\pi \mid ab \Rightarrow \pi \mid a$ oder $\pi \mid b$.
Elemente $a, b \in R$ heißen **assoziiert**, wenn $a \mid b$ und $b \mid a$. Notation: $a \mathrel{\hat{=}} b$.

Lemma 2.15. *Für $a, b \in R$ sind äquivalent:*
(i) $a \mathrel{\hat{=}} b$.
(ii) $a = be$ *mit* $e \in R^\times$.
(iii) $(a) = (b)$.

Beweis. (i) $\Rightarrow$ (ii) $a = b \cdot e$, $b = a \cdot c$, also $b = b(ec)$. Ist $b \neq 0$ folgt $ec = 1$, also e Einheit. Ist $b = 0$, so auch $a = be = 0$. Nun gilt $0 = 0 \cdot 1$.
(ii) $\Rightarrow$ (iii) $a = be$ mit $e \in R \Rightarrow (a) \subset (b)$. Ist $e \in R^\times$ so existiert $e^{-1} \in R$ und $b = ae^{-1}$. Also gilt $(b) \subset (a)$.
(iii) $\Rightarrow$ (i) $b \in (a) \Rightarrow a \mid b$
$a \in (b) \Rightarrow b \mid a$. □

Lemma 2.16. *Primelemente sind irreduzibel.*

Beweis. Sei π prim und $ab = \pi$. Dann gilt $\overline{a}\overline{b} = 0$ im nullteilerfreien Faktorring $R/(\pi)$. Also $\overline{a} = 0$ oder $\overline{b} = 0$. Sei OE $\overline{a} = 0$, also $a = a'\pi$, $a' \in R$. Dann gilt $\pi = ab = \pi a' b$. Kürzen liefert $1 = a'b$, also $b \in R^\times$. □

Erinnerung: R nullteilerfrei im ganzen Abschnitt.

Lemma 2.17. *Ein Element $a \in R$ habe Zerlegungen*

$$a = p_1 \cdots p_r = q_1 \cdots q_s$$

in Primelemente p_i und irreduzible Elemente q_j. Dann gilt $r = s$ und nach Umnummerierung ist $p_i \mathrel{\hat{=}} q_i$, $i = 1, \ldots, r$.

Beweis. Da p_1 prim ist folgt aus $p_1 \mid a = q_1 \ldots q_s$, dass $p_1 \mid q_j$ für ein j (insbesondere gilt $s \geq 1$). Nach Umnummerierung sei dies q_1. Also gilt $q_1 = \varepsilon_1 p_1$. Da q_1 irreduzibel ist, muß ε_1 Einheit sein. Durch Kürzen erhalten wir

$$p_2 \ldots p_r = \varepsilon_1 q_2 \ldots q_s.$$

Induktiv erhalten wir das Ergebnis. (Letzter Schritt: $1 = \varepsilon_1 \cdots \varepsilon_r \cdot q_{r+1} \cdots q_s$, woraus $s = r$ folgt, da ansonsten $q_{r+1} \ldots q_s$ Einheiten wären). □

Satz 2.18. *Sei R ein nullteilerfreier Ring. Dann sind äquivalent:*

(i) *Jedes $a \in R \setminus R^\times$, $a \neq 0$, läßt sich eindeutig (bis auf Reihenfolge und Assoziiertheit) als Produkt irreduzibler Elemente schreiben.*

(ii) *Jedes $a \in R \setminus R^\times$, $a \neq 0$, läßt sich als Produkt von Primelementen schreiben.*

Definition 2.19. Ein nullteilerfreier Ring, der die äquivalenten Bedingungen von Satz 2.18 erfüllt heißt **faktoriell**.

Satz 2.20. *In einem faktoriellen Ring ist jedes irreduzible Element Primelement.*

Beweis der Sätze 2.20 und 2.18. Sei Satz 2.18 (i) erfüllt. Wir zeigen dass jedes irreduzible Element schon prim ist. Sei π irreduzibel und $a, b \in R$ mit $\pi \mid ab$. Z.z. $\pi \mid a$ oder $\pi \mid b$. Wir können annehmen, dass $a, b \in R \setminus (R^\times \cup \{0\})$. Seien $a = a_1 \cdots a_r$, $b = b_1 \cdots b_s$ Zerlegungen in irreduzible Elemente. Wegen $\pi \mid ab$ taucht π als einer der Faktoren in einer Zerlegung in irreduzible Elemente von $ab = a_1 \cdots a_r \cdot b_1 \cdots b_s$ auf. Die Eindeutigkeitsaussage von Satz 2.18(i) impliziert $\pi \mathrel{\hat{=}} a_i$ für ein i oder $\pi \mathrel{\hat{=}} b_j$ für ein j. Also $\pi \mid a$ oder $\pi \mid b$.
Dies zeigt (i) $\Rightarrow$ (ii) und Satz 2.20. Die Implikation (ii)$\Rightarrow$(i) folgt aus Lemma 2.17. □

Beispiele faktorieller Ringe

Definition 2.21. Ein nullteilerfreier Ring R heißt **euklidischer Ring**, wenn es eine Abbildung $v : R \setminus \{0\} \to \mathbb{N}_0$ gibt, so dass gilt: zu $f, g \in R$, $g \neq 0$ gibt es stets Elemente $q, r \in R$ mit $f = qg + r$ mit $v(r) < v(g)$ oder $r = 0$.

Beispiel 2.22. • $R = k[T]$, k ein Körper. Setze $v(f) = \deg(f)$
• $R = \mathbb{Z}$. Setze $v(a) = |a|$.

Satz 2.23. *(i) Jeder euklidische Ring ist Hauptidealring.*
(ii) Jeder Hauptidealring ist faktoriell.

Beweis. Siehe LA II. □

In einem faktoriellen Ring haben wir kgV und ggT. Diese sind bis auf Assoziiertheit wohlbestimmt. Ist $(p_i)_{i \in I}$ ein Vertretersystem von Primelementen bis auf Assoziiertheit und $a = \varepsilon_a \prod_{i \subset I} p_i^{v_i(a)}$ wobei $v_i(a) = 0$ für fast alle i und analog $b = \varepsilon_b \prod_{i \in I} p_i^{v_i(b)}$ so setzt man

$$\begin{aligned} \mathrm{ggT}(a,b) &= \prod_{i \in I} p_i^{\min(v_i(a), v_i(b))} \\ \mathrm{kgV}(a,b) &= \prod_{i \in I} p_i^{\max(v_i(a), v_i(b))}. \end{aligned}$$

Sind $\mathfrak{a}, \mathfrak{b} \subset R$ Ideale, so auch $\mathfrak{a} \cap \mathfrak{b}$ und $\mathfrak{a} + \mathfrak{b} = \{a + b \mid a \in \mathfrak{a},\ b \in \mathfrak{b}\}$.

Lemma 2.24. *Ist R ein Hauptidealring, so gelten die folgenden Identitäten von Idealen*

$$\begin{aligned}(a)+(b) &= (ggT(a,b))\\ (a)\cap(b) &= (kgV(a,b))\end{aligned}$$

Beweis. Sei $(d) = (a) + (b)$. Dann gilt $d|a$, $d|b$, also $d|\mathrm{ggT}(a,b)$. Andererseits existieren $x, y \in R$ mit $xa + yb = d \Rightarrow \mathrm{ggT}(a,b)|d$. Folglich $(\mathrm{ggT}(a,b)) = (d)$.

Desweiteren gilt $e \in (a)\cap(b) \Leftrightarrow a|e \wedge b|e \Leftrightarrow \mathrm{kgV}(a,b)|e \Leftrightarrow e \in (\mathrm{kgV}(a,b))$. □

Lemma 2.25. *Ist R ein Hauptidealring, so ist jedes Primideal $\neq (0)$ maximal.*

Beweis. Für $a, b \in R$ gilt $(\mathrm{ggT}(a,b)) = (a) + (b)$. Sei nun $\mathfrak{p} = (p)$ ein Primideal, $\overline{a} \in R/(p)$ und $a \in R$ ein Vertreter. Ist $\overline{a} \neq 0$, so gilt $p \nmid a$, also $\mathrm{ggT}(a,p) = 1$. Wegen $(a) + (p) = R$ finden wir $x, y \in R$ mit $xa + yp = 1$. Es folgt $\overline{x} \cdot \overline{a} = 1$ in $R/(p)$, d.h. $\overline{a}$ ist invertierbar. Folglich ist $R/(p)$ ein Körper, also (p) ein Maximalideal. □

2.3 Der Satz von Gauß

Ziel dieses Abschnitts: R faktoriell $\Rightarrow R[T]$ faktoriell.
So erhalten wir eine große Klasse faktorieller Ringe, die keine Hautpidealringe sind.

Vorbereitungen:

Lemma 2.26. *Ist R nullteilerfrei, so gilt für $f, g \in R[T]$:*

$$\deg(f \cdot g) = \deg(f) + \deg(g).$$

Beweis. Erinnerung: per Konvention gilt $\deg(0) = -\infty$. Das Lemma ist daher richtig, falls einer der Faktoren Null ist. Seien also $f \neq 0$, $g \neq 0$. Dann ist $f = a_r T^r + \cdots + a_0$ $g = b_s T^s + \cdots + b_0$ mit $a_r \neq 0$, $b_s \neq 0$, $r = \deg f$, $s = \deg g$.
Da R nullteilerfrei ist, gilt $a_r b_s \neq 0$. Wegen

$$fg = a_r b_s T^{r+s} + \text{Terme kleineren Grades},$$

folgt $\deg(fg) = r + s$. □

Korollar 2.27. *Ist R nullteilerfrei, so auch $R[T]$.*

Beweis. Dies folgt aus $\deg(fg) = \deg(f) + \deg(g)$. □

Quotientenkörper: Sei R ein nullteilerfreier Ring. Wir orientieren uns am Übergang $\mathbb{Z} \rightsquigarrow \mathbb{Q}$ und definieren Brüche. Wir betrachten die Menge M aller Paare (a,b), $a, b \in R$, $b \neq 0$, (Idee: $(a,b) =$ "$\frac{a}{b}$") und sagen $(a_1, b_1) \sim (a_2, b_2)$ falls $a_1 b_2 = a_2 b_1$.

Bemerkung 2.28. $\sim$ ist eine Äquivalenzrelation.
Reflexivität und Symmetrie sind klar.
Transitivität: $(a_1, b_1) \sim (a_2, b_2)$ und $(a_2, b_2) \sim (a_3, b_3)$.
Dann gilt:

$$\begin{aligned} b_2a_3b_1 = b_3a_2b_1 &= b_3b_2a_1 \\ &= b_2a_1b_3 \\ \text{Kürzen gibt:} \quad a_3b_1 &= a_1b_3. \end{aligned}$$

Man beachte: Wir haben die Nullteilerfreiheit benutzt.

Definition 2.29. Die Menge der Äquivalenzklassen von M bzgl. $\sim$ wird mit $Q(R)$ bezeichnet. $Q(R)$ mit den vertreterweise definierten Operationen

$$(a_1, b_1) + (a_2, b_2) = (a_1b_2 + a_2b_1, b_1b_2)$$

und

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1a_2, b_1b_2)$$

heißt der **Quotientenkörper** von R.
Die Äquivalenzklasse von $(a, b) \in M$ in $Q(R)$ wird mit $\frac{a}{b} \in Q(R)$ bezeichnet.
Die Operationen schreibt man eingänglich in der Form:

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1b_2 + a_2b_1}{b_1b_2} \quad \text{und} \quad \frac{a_1}{b_1} \cdot \frac{a_2}{b_2} = \frac{a_1a_2}{b_1b_2}.$$

Verifikationen: • die Operationen sind wohldefiniert.

Z.B. sei $(a_1, b_1) \sim (a_1', b_1')$, also $a_1b_1' = b_1a_1'$. Dann gilt für jedes Paar (a_2, b_2)

$$(a_1b_2 + a_2b_1, b_1b_2) \sim (a_1'b_2 + a_2b_1', b_1'b_2)$$

wegen

$$\begin{aligned} b_1'b_2(a_1b_2 + a_2b_1) &= b_1'a_1b_2^2 + b_1b_1'b_2a_2 \\ = b_1a_1'b_2^2 + b_1b_1'b_2a_2 &= b_1b_2(a_1'b_2 + a_2b_1') \end{aligned}$$

• $Q(R)$ wird mit diesen Operationen zum Körper:
Ringaxiome: Einselement: $(1, 1)$. Nullelement: $(0, 1)$.
Körper: Sei $(a, b) \in M$, $\frac{a}{b} \in Q(R)$ und $\frac{a}{b} \neq \frac{0}{1}$. Dann gilt $a \neq 0$ und $\frac{b}{a}$ ist ein Inverses.

Bemerkung 2.30. Die natürliche Abbildung

$$R \longrightarrow Q(R),\ x \longmapsto \frac{x}{1},$$

ist ein injektiver Ringhomomorphismus. (Wegen $\frac{a}{1} = \frac{b}{1} \Leftrightarrow a = b$.)

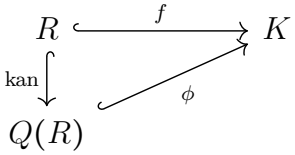
Korollar 2.31. *Es sei R ein nullteilerfreier Ring und $f \in R[T]$, $f \neq 0$, ein Polynom. Dann hat f höchstens* $\deg f$ *viele Nullstellen in R.*

Beweis. Ist $a \in R$ eine Nullstelle, d.h. $f(a) = 0$, so ist $\frac{a}{1}$ eine Nullstelle von f in $Q(R)$. In $Q(R)$ hat f nur endlich viele Nullstellen (siehe LA1) und die natürliche Abbildung $R \to Q(R)$ ist injektiv. □

Beispiel 2.32. Im (nicht nullteilerfreien) Ring $R = \mathbb{Z}/8\mathbb{Z}$ hat das quadratische Polynom $T^2 - 1$ vier Nullstellen: $\bar{1}$, $\bar{3}$, $\bar{5}$, $\bar{7}$.

Philosophie: $Q(R)$ ist der kleinste Körper in den sich der nullteilerfreie Ring R eingebettet werden kann. In der Sprache der Universaleigenschaften:

Satz 2.33. *Sei R ein nullteilerfreier Ring und $f : R \to K$ ein injektiver Ringhomomorphismus von R in einen Körper K. Dann gibt es einen eindeutig bestimmten Körperhomomorphismus $\phi : Q(R) \hookrightarrow K$, so dass das Diagramm*



kommutiert.

Beweis. Sei $\frac{a}{b} \in Q(R)$. Wegen $b \neq 0$ gilt $f(b) \neq 0$. Wir setzen $\phi\left(\frac{a}{b}\right) = f(a)f(b)^{-1} \in K$. Zu verifizieren:
- die Definition von ϕ ist vertreterunabhängig.
- ϕ ist Ringhomomorphismus.
- Eindeutigkeit.

(alles ganz einfach) □

Bemerkung 2.34. Bei nicht nullteilerfreien Ringen ist die Lage komplizierter. Dort macht man folgendes. Ausgehend von einer multiplikativ abgeschlossenen Teilmenge $S \subset R$ (d.h. $1 \in S$ und $s, s' \in S \Rightarrow ss' \in S$) betrachtet man die Menge aller Paare (r, s), $r \in R$, $s \in S$ und man sagt $(r', s') \sim (r'', s'')$ falls ein $s \in S$ mit $sr's'' = sr''s'$ existiert (das zusätzliche s braucht man, damit $\sim$ eine Äquivalenzrelation wird).
Die Menge der Äquivalenzklassen heißt die **Lokalisierung** $(S^{-1}R)$ von R nach S und ist in natürlicher Weise ein Ring. Für nullteilerfreie Ringe haben wir also

$$Q(R) = (R \setminus \{0\})^{-1}R.$$

Ist R nicht nullteilerfrei, so ist $R \setminus \{0\}$ nicht multiplikativ abgeschlossen.

Bemerkung 2.35. Ist R ein faktorieller Ring, und ist $(p_i)_{i \in I}$ ein Repräsentantensystem für die Primelemente bis auf Assoziiertheit, so hat jedes $\frac{a}{b} \in Q(R)$, $\frac{a}{b} \neq 0$, eine eindeutige Darstellung der Form

$$\frac{a}{b} = \varepsilon \cdot \prod_{i \in I} p_i^{v_i\left(\frac{a}{b}\right)}$$

wobei $v_i\left(\frac{a}{b}\right) \in \mathbb{Z}$ für fast alle i gleich 0 ist und $\varepsilon \in R^\times$. Dies folgt aus der eindeutigen Primzerlegung.
Außerdem gilt: $\frac{a}{b} \in R \subset Q(R) \Longleftrightarrow v_i\left(\frac{a}{b}\right) \geq 0$ für alle $i \in I$.
Für ein Primelement $p \in R$ und $x = \frac{a}{b} \in Q(R)$ schreiben wir $v_p(x) = v_i\left(\frac{a}{b}\right)$ wobei $p_i \mathrel{\hat{=}} p$. Das hängt nicht von der Wahl des Repräsentantensystems ab, weil sich beim Wechsel alle Daten nur um Einheiten aus R verändern.

Konvention: $v_p(0) = +\infty$.

Beispiel 2.36. In $\mathbb{Z}$ gilt:
$v_3\left(\frac{2}{9}\right) = -2$, $v_2\left(\frac{2}{9}\right) = 1$, $v_p\left(\frac{2}{9}\right) = 0$ für jede Primzahl $p \neq 2, 3$.

Für ein Polynom $f = a_r T^r + \cdots + a_0 \in Q(R)[T]$ und ein Primelement $p \in R$ setzen wir

$$v_p(f) \stackrel{df}{=} \min_{i=0,\ldots,r} v_p(a_i).$$

Es gilt: $v_p(f) = 0$ für fast alle Primelemente (bis auf $\hat{=}$) und $f \in R[T] \subset Q(R)[T]$ $\Longleftrightarrow v_p(f) \geq 0$ für alle p.

Satz 2.37 (Gauß). *Es sei R ein faktorieller Ring und $p \in R$ ein Primelement. Dann gilt für $f, g \in Q(R)[T]$:*

$$v_p(fg) = v_p(f) + v_p(g).$$

Beweis. 1. Die Gleichung ist richtig, falls f oder g konstant ist (eindeutige Primzerlegung in R).
2. Nach Schritt 1 können wir f und g mit Konstanten $\neq 0$ aus R multiplizieren, also OE $f, g \in R[T]$.
3. Dividiert man f durch den ggT seiner Koeffizienten, erhält man $v_p(f) = 0$. Analog $v_p(g) = 0$.

Also z.z: $f, g \in R[T]$ und $v_p(f) = 0 = v_p(g) \Rightarrow v_p(fg) = 0$.
Wir betrachten den natürlichen Projektionshomomorphismus

$$\phi : R[T] \twoheadrightarrow R/(p)[T]$$

$$\begin{aligned} \operatorname{Kern}(\phi) &= \{\text{Pol. deren Koeff. alle durch } p \text{ teilbar sind}\} \\ &= \{h \in R[T] \mid v_p(h) > 0\}. \end{aligned}$$

Wegen $v_p(f) = 0 = v_p(g)$ gilt $\phi(f) \neq 0$, $\phi(g) \neq 0$. Da p Primelement ist, ist $R/(p)$ nullteilerfrei und nach Korollar 2.27 auch $R/(p)[T]$. Wir erhalten $0 \neq \phi(f)\phi(g) = \phi(fg)$. Also $fg \notin \operatorname{Kern}(\phi)$, $v_p(fg) = 0$. □

Korollar 2.38. *Sei R ein faktorieller Ring und $h \in R[T]$ ein normiertes Polynom. Gilt $h = fg$ mit normierten Polynomen $f, g \in Q(R)[T]$, so gilt $f, g \in R[T]$.*

Beweis. Sei p ein beliebiges Primelement. h normiert und in $R[T] \Rightarrow v_p(h) = 0$. f, g normiert $\Rightarrow v_p(f) \leq 0$, $v_p(g) \leq 0$. Wegen $0 = v_p(h) = v_p(f) + v_p(g)$ folgt $v_p(f) = v_p(g) = 0$. Da p beliebig war, folgt $f, g \in R[T]$. □

Definition 2.39. Sei R faktoriell. Ein Polynom $f \in R[T]$ heißt **primitiv**, wenn der ggT seiner Koeffizienten = 1 ist, d.h. wenn $v_p(f) = 0$ für alle Primelemente $p \in R$ gilt.

Beispiel 2.40. Jedes normierte Polynom ist primitiv.

Lemma 2.41. *Sei $0 \neq f \in Q(R)[T]$. Dann existiert ein $0 \neq a \in Q(R)$ und ein primitives $\tilde{f} \in R[T]$ so dass $f = a\tilde{f}$.*

Beweis. Sei $(p_i)_{i \in I}$ ein Repräsentantensystem der Primelemente bis auf $\hat{=}$. Setze

$$a = \prod_{i \in I} p_i^{v_{p_i}(f)}$$

und $\tilde{f} = a^{-1} \cdot f$.

Es gilt $v_{p_i}(a^{-1}) = -v_{p_i}(f)$ für alle $i \in I$ und daher $v_{p_i}(\tilde{f}) = 0$ für alle $i \in I$. □

Satz 2.42 (Gauß). *Sei R ein faktorieller Ring. Dann ist auch $R[T]$ faktoriell. Ein Polynom $q \in R[T]$ ist genau dann Primelement in $R[T]$ wenn gilt*

(i) *$q \in R$ und q ist Primelement in R, oder*
(ii) *q ist primitiv in $R[T]$ und Primelement in $Q(R)[T]$.*

Beweis. Sei q ein Primelement in R. Dann ist R/Rq und damit auch $(R/Rq)[T] = R[T]/R[T]q$ nullteilerfrei, und deshalb q ein Primelement in $R[T]$. Sei nun $q \in R[T]$ primitiv und prim als Element in $Q(R)[T]$ und $f, g \in R[T]$ mit $q \mid fg$ in $R[T]$. Dann gilt auch $q \mid fg$ in $Q(R)[T]$. OE gelte $q \mid f$ in $Q(R)[T]$, d.h. es existiert ein $h \in Q(R)[T]$ mit $qh = f$ in $Q(R)[T]$. Nun gilt für jedes Primelement $p \in R$:

$$\begin{array}{rcl} 0 \leq v_p(f) & = & v_p(q) + v_p(h). \\ & & \| \leftarrow q \text{ primitiv} \\ & & 0 \end{array}$$

Also $v_p(h) \geq 0$ für alle p und deshalb $h \in R[T]$, d.h. $q \mid f$ in $R[T] \Rightarrow q$ ist Primelement in $R[T]$.
Bleibt z.z.: $R[T]$ ist faktoriell und jedes Primelement ist von der Form (i) oder (ii).
G.z.z.: Jedes $f \in R[T] \setminus (R[T]^\times \cup \{0\})$ zerfällt in ein Produkt von Primelementen der Form (i) und (ii). Wir schreiben

$$f = a\tilde{f}$$

mit $a = \text{ggT}$ (Koeffizienten von f), also $\tilde{f} \in R[T]$ primitiv. a ist entweder Einheit in R oder Produkt von Primelementen vom Typ (i). Wir zeigen: $\tilde{f}$ ist Produkt von Primelementen vom Typ (ii). Sei

$$\tilde{f} = c\tilde{f}_1 \dots \tilde{f}_r$$

eine Primzerlegung in $Q(R)[T]$ und $c \in Q(R)^\times$. Nach geeigneter Wahl von c können wir annehmen, dass alle $\tilde{f}_i$ primitiv und in $R[T]$ sind. Dann gilt nach dem Lemma von Gauß für jedes Primelement $p \in R$:

$$\begin{array}{ccccccc} v_p(\tilde{f}) & = v_p(c) + & v_p(\tilde{f}_1) & + \cdots + & v_p(\tilde{f}_r) \\ \| & & \| & & \| \\ 0 & & 0 & & 0 \end{array}$$

also $v_p(c) = 0$ für alle p. Also auch $v_p(c^{-1}) = 0 \quad \forall\, p$ und deshalb $c, c^{-1} \in R$, $c \in R^\times$. □

Korollar 2.43. *Sei R ein faktorieller Ring. Dann ist der Polynomring in n Variablen ($n \in \mathbb{N}$) $R[T_1, \dots, T_n]$ faktoriell.*

Beweis. Es gilt

$$R[T_1, \dots, T_n] = R[T_1][T_2] \cdots [T_n].$$

Man wende den Satz von Gauß n-mal an. □

Beispiele 2.44. • Ist k ein Körper, so ist $k[T_1 \dots T_n]$ faktoriell.
• $\mathbb{Z}[T_1 \dots T_n]$ ist faktoriell.

2.4 Irreduzibilitätskriterien

Sei R faktoriell und $K = Q(R)$. Sei $f \in K[T]$, $\deg(f) \geq 1$. Wann ist f irreduzibel? Nach Lemma 2.41 findet man ein $c \in K^\times$ so dass $\tilde{f} = c \cdot f$ primitiv und in $R[T]$ ist. Es gilt nach dem Satz von Gauß

$$f \text{ irred. in } K[T] \iff \tilde{f} \text{ irred. in } K[T] \iff \tilde{f} \text{ irred. in } R[T].$$

Satz 2.45 (**Eisensteinsches Irreduzibilitätskriterium**). *Sei R ein faktorieller Ring und $f = a_n f^n + \cdots + a_0 \in R[T]$ primitiv vom Grad > 0. Sei $p \in R$ ein Primelement mit*

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

Dann ist f irreduzibel in $R[T]$ und damit auch in $Q(R)[T]$.

Beweis. Angenommen f ist reduzibel in $R[T]$, $f = gh$ mit

$$g = b_r T^r + \cdots + b_0,\ h = c_s T^s + \cdots + c_0$$

mit $r+s=n$, $r>0$, $s>0$. Es folgt: $a_n = b_r c_s$, $p \nmid b_r$, $p \nmid c_s$, $a_0 = b_0 c_0$, $p \mid b_0 c_0$, $p^2 \nmid b_0 c_0$.
Es gelte OE $p \mid b_0$, $p \nmid c_0$. Sei nun $t \leq r-1$ maximal mit $p \mid b_i$ für $0 \leq i \leq t$. Mit der Konvention $b_i = 0$ für $i > r$ und $c_i = 0$ für $i > s$ gilt

$$a_{t+1} = b_0 c_{t+1} + \cdots + b_{t+1} c_0.$$

Es folgt $p \nmid a_{t+1}$, da $p \mid b_0 c_{t+1}$, $p \mid b_1 c_t$, $\ldots$, $p \mid b_t c_1$, $p \nmid b_{t+1} c_0$. Wegen $p \mid a_i$, $i < n$ folgt $t+1 = n$, also $n = t+1 \leq r = n-s$ im Widerspruch zu $s > 0$. □

Beispiele 2.46. • Sei k ein Körper und $K := k(t)$ der Quotientenkörper von $k[t]$ ("der rationale Funktionenkörper über k"). Wir betrachten für $n \in \mathbb{N}$ das Polynom

$$f = T^n - t \in K[T].$$

Nun gilt $f \in k[t][T]$ und $k[t]$ ist faktoriell. Eisenstein mit $p = t$ liefert die Irreduzibilität von f.
• $f(T) = T^3 + 5T^2 + 5$ ist irreduzibel in $\mathbb{Q}[T]$ ($p = 5$).
• Sei p eine Primzahl. Dann ist

$$f(T) = T^{p-1} + T^{p-2} + \cdots + 1 \left(= \frac{T^p - 1}{T - 1} \right)$$

irreduzibel in $\mathbb{Q}[T]$:
Offenbar ist $f = f(T)$ dann und nur dann irreduzibel, wenn $f(T+1)$ irreduzibel ist. Nun gilt

$$f(T+1) = \frac{(T+1)^p - 1}{(T+1) - 1}$$

$$= \frac{T^p + \binom{p}{1} T^{p-1} + \cdots + \binom{p}{p-1} T + 1 - 1}{T}$$

$$= T^{p-1} + \binom{p}{1} T^{p-2} + \cdots + \binom{p}{p-1}.$$

Nun gilt: $p^2 \nmid \binom{p}{p-1} = p$ und $p \mid \binom{p}{i}$ für $i = 1, \ldots, p-1$. Eisenstein: $f(T+1)$ ist irreduzibel $\Rightarrow f(T)$ ist irreduzibel.

Satz 2.47 (**Reduktionskriterium**). *Sei R ein faktorieller Ring, $p \in R$ ein Primelement und $f \in R[T]$ ein Polynom dessen Leitkoeffizient nicht durch p teilbar ist. Wir betrachten die Projektion*

$$\phi : R[T] \longrightarrow R/(p)[T].$$

Dann gilt: Ist $\phi(f)$ irreduzibel in $R/(p)[T]$, so ist f irreduzibel in $Q(R)[T]$. Ist f zusätzlich primitiv, so ist f irreduzibel in $R[T]$.

Bemerkung 2.48. Dieses Kriterium wendet sich vor allem an, wenn R ein Hauptidealring ist. Dann ist $R/(p)$ ein Körper nach 2.25. Im allgemeinen ist $R/(p)$ nullteilerfrei aber nicht notwendig faktoriell.

Anderes Anwendungsbeispiel:

$$R = k[T_1, \ldots, T_n] \quad \text{und} \quad p = T_n.$$

Dann ist $R/(p) = k[T_1, \ldots, T_{n-1}]$ wieder faktoriell und wir haben das Problem um eine Variable vereinfacht.

Beweis von Satz 2.47. Sei zunächst $f \in R[T]$ primitiv. Ist f reduzibel, so gibt es eine Zerlegung $f = gh$ und wegen der Primitivität gilt mit $\deg(g) > 0$, $\deg(h) > 0$. Weil p nicht den Leitkoeffizienten von f teilt, gilt das gleiche auch für g und h. Also gilt $\phi(f) = \phi(g) \cdot \phi(h)$ und $\deg(\phi(g)) > 0$, $\deg(\phi(h)) > 0$. Also: f primitiv und $\phi(f)$ irreduzibel $\Rightarrow$ f irreduzibel.

Im allgemeinen Fall gilt $f = c\tilde{f}$ mit $c \in R$ und $\tilde{f} \in R[T]$ primitiv. Da p nicht den Leitkoeffizienten von f teilt, teilt p nicht c und nicht den Leitkoeffizienten von $\tilde{f}$. Aus $\phi(f) = \phi(c) \cdot \phi(\tilde{f})$ und $\phi(c) \neq 0$ folgt: $\phi(f)$ irreduzibel $\Rightarrow$ $\phi(\tilde{f})$ irreduzibel. Nach dem ersten Teil des Beweises folgt $\tilde{f}$ irreduzibel in $R[T]$, also $\tilde{f}$ irreduzibel in $Q(R)[T]$ und somit f irreduzibel in $Q(R)[T]$. □

Anwendungsbeispiele:
1) $f = X^3 + 3X^2 - 4X - 1$ ist irreduzibel in $\mathbb{Q}[X]$. Grund: $f \in \mathbb{Z}[X]$ und f ist primitiv. Betrachte $p = 3$.

$$\phi(f) = X^3 - X - 1 \in \mathbb{Z}/3\mathbb{Z}[X]$$

ist irreduzibel (einer der Teiler müßte vom Grad 1 sein und es gibt keine Nullstelle in $\mathbb{Z}/3\mathbb{Z}$).
2) $f = X^4 + 3X^3 + 5XY^2 + Y + 3 \in \mathbb{Q}[X, Y]$ ist irreduzibel.

Setze $R = \mathbb{Q}[Y]$, $p = Y$. Dann gilt $\phi(f) = X^4 + 3X^3 + 3$ in $\mathbb{Q}[Y]/(Y)[X] = \mathbb{Q}[X]$ und $\phi(f)$ ist irreduzibel nach Eisenstein $(p = 3)$.

2.5 Verallgemeinerte Polynomringe

Zum Warmwerden:

$$R[T] = R^{(\mathbb{N}_0)} = \{(r_i)_{i \in \mathbb{N}_0},\ r_i = 0 \quad \text{f. f. a. } i\}$$

mit folgenden Operationen

$$(r_i)_{i \in \mathbb{N}_0} + (s_i)_{i \in \mathbb{N}_0} = (r_i + s_i)_{i \in \mathbb{N}_0} \text{ und}$$

$$(r_i)_{i \in \mathbb{N}_0} \cdot (s_i)_{i \in \mathbb{N}_0} = (t_i)_{i \in \mathbb{N}_0} \text{ mit } t_n = \sum_{i+j=n} r_i s_j.$$

Definition 2.49. Sei R ein Ring und M ein kommutatives Monoid dessen Operator wir als „+“ schreiben. Dann nennt man

$$R[M] = R^{(M)} = \{(r_m)_{m\in M} \mid r_m = 0 \quad \text{f. f. a. } m \in M\}$$

mit den Operationen

$$(r_m)_{m\in M} + (s_m)_{m\in M} = (r_m + s_m)_{m\in M}$$

und

$$(r_m)_{m\in M} \cdot (s_m)_{m\in M} = (t_m)_{m\in M}, \quad t_m = \sum_{m_1+m_2=m} r_{m_1} \cdot s_{m_2}$$

den **Polynomring über M mit Koeffizienten in R**.

Nullelement $(r_m)_{m\in M}$ mit $r_m = 0$ für alle $m \in M$.

Einselement $(r_m)_{m\in M}$, $r_m = \begin{cases} 1 & m = 0 \in M \\ 0 & \text{sonst.} \end{cases}$

Beispiel 2.50. • $M = \mathbb{N}_0$. Wir erhalten

$$R[\mathbb{N}_0] \xrightarrow{\sim} R[T],\ (r_i)_{i\in\mathbb{N}_0} \xrightarrow{\sim} \sum_{i=0}^{\infty} r_i T^i.$$

• Allgemeiner: für $M = (\mathbb{N}_0)^n$ erhalten wir einen Isomorphismus

$$R[(\mathbb{N}_0)^n] \xrightarrow{\sim} R[X_1, \ldots, X_n]$$

durch

$$(r_{(a_1,\ldots,a_n)})_{(a_1,\ldots,a_n)\in\mathbb{N}_0^n} \longmapsto \sum_{(a_1,\ldots,a_n)\in\mathbb{N}_0^n} r_{(a_1,\ldots,a_n)} X_1^{a_1} \ldots X_n^{a_n}.$$

• Noch allgemeiner: Sei I eine (Index)Menge und $M = (\mathbb{N}_0)^{(I)} = \{\phi_i : I \to \mathbb{N}_0, \phi(i) = 0 \text{ f. f. a. } i\}$.
Wir ordnen formal jedem $i \in I$ eine Variable X_i zu. Dann gilt

$$\begin{aligned} R[(\mathbb{N}_0)^{(I)}] &\xrightarrow{\sim} R[(X_i)_{i\in I}] \\ (r_a)_{a\in\mathbb{N}_0^{(I)}} &\longrightarrow \sum_{a\in\mathbb{N}_0^{(I)}} r_a \prod_{i\in I} X_i^{a_i}, \end{aligned}$$

wobei wir $X_i^0 = 1$ setzen und weglassen. $R[(X_i)_{i\in I}]$ ist der Ring der Polynome in den unabhängigen Variablen $(X_i)_{i\in I}$.

• Ist G eine abelsche Gruppe so heißt $R[G]$ der **Gruppenring** von G über R.

Um für allgemeine Monoide M intuitiv arbeiten zu können führen wir die folgende Notation ein:

Für $m \in M$ sei das Element $X^m \in R[M]$ definiert durch

$$X^m = (r_n)_{n \in M},\ r_n = \begin{cases} 1 & \text{für } n = m \\ 0 & \text{sonst.} \end{cases}$$

Es gilt $X^{m_1} \cdot X^{m_2} = X^{m_1+m_2}$.
Die Familie $(X^m)_{m \in M}$ ist eine R-Modulbasis von $R[M]$: Jedes $f \in R[M]$ hat eine eindeutige Darstellung der Form

$$f = \sum_{m \in M} r_m \cdot X^m$$

mit $r_m = 0$ für fast alle m. Es gelten die üblichen Rechenregeln für Polynome.

Wir fassen R als Teilring von $R[M]$ auf durch $r \mapsto rX^0$ (X^0 ist die 1 in $R[M]$).

Satz 2.51 (**Universelle Eigenschaft des Polynomrings).** *Es sei $\phi : R \to R'$ ein Ringhomomorphismus und $\sigma : M \to (R', \cdot)$ ein Monoidhomomorphismus. Dann gibt es einen eindeutig bestimmten Ringhomomorphismus $\Phi : R[M] \to R'$ mit $\Phi_{|R} = \phi$ und $\Phi(X^m) = \sigma(m)$ für alle $m \in M$.*

Beweis. Zum Nachweis der Eindeutigkeit betrachte man ein Element

$$\sum_{m \in M} r_m X^m \in R[M].$$

Falls Φ existiert, so gilt notwendig

$$\Phi(\sum r_m X^m) = \sum \Phi(r_m X^m) = \sum \phi(r_m) \cdot \sigma(m).$$

Umgekehrt kann man diese Gleichung zur Definition machen.
Nachzuprüfen: Φ ist Ringhomomorphismus. Dies folgt, weil ϕ ist Ring- und σ Monoidhomomorphismus ist. □

Korollar 2.52. *Gegeben sei ein Ringhomomorphismus $\phi : R \to R'$ sowie n Elemente $x_1, \ldots, x_n \in R'$. Dann gibt es einen eindeutig bestimmten Ringhomomorphismus $\Phi : R[X_1, \ldots, X_n] \to R$ mit $\Phi_{|R} = \phi$ und $\Phi(X_i) = x_i$, $i = 1, \ldots, n$.*

Beweis. Wir erhalten einen Monoidhomomorphismus $\sigma : (\mathbb{N}_0)^n \to (R', \cdot)$ durch $\sigma((0, \ldots, 1, \ldots, 0)) = x_i$. Die Existenz von Φ folgt nun aus Satz 2.51. Eindeutigkeit gilt, weil wir aus Φ den Monoidhomomorphismus $\sigma : (\mathbb{N}_0)^n \to (R', \cdot)$ durch die Regel

$$\sigma((a_1, \ldots, a_n)) = x_1^{a_1} \ldots x_n^{a_n}$$

zurückbekommen. □

Definition 2.53. Es sei $R \subset R'$ eine Ringerweiterung (d.h. ein injektiver Ringhomomorphismus) und $(x_1, \ldots, x_n)$ ein System von Elementen aus R'. Dieses System heißt **algebraisch unabhängig** oder **transzendent** über R, wenn der nach Korollar 2.52 assoziierte Ringhomomorphismus

$$\begin{array}{rcl} R[X_1 \ldots X_n] & \longrightarrow & R' \\ X_i & \longmapsto & x_i \end{array}$$

injektiv ist. Ansonsten heißt das System **algebraisch abhängig**.

Beispiel 2.54. Wir betrachten $R = \mathbb{Q} \subset R' = \mathbb{C}$

- das einelementige System $(\sqrt{2})$ ist nicht transzendent (sprich: $\sqrt{2}$ ist nicht transzendent). Grund:
  Für $\Phi : \mathbb{Q}[X] \to \mathbb{C}$, $X \mapsto \sqrt{2}$, gilt $X^2 - 2 \in \mathrm{Kern}(\Phi)$.
- Die Eulersche Zahl $e = \lim\limits_{n\to\infty} \left(1 + \frac{1}{n}\right)^n$ ist transzendent (Hermite).
- Das System (e, e^2) ist nicht transzendent.
  Grund: Der Homomorphismus $\Phi : \mathbb{Q}[X, Y] \to \mathbb{C}$, $X \mapsto e$, $Y \mapsto e^2$, schickt das Polynom $X^2 - Y$ auf 0.
- Die Zahl π ist transzendent (Lindemann).
- Frage: Ist das System (e, π) transzendent? (ungelöst).

3 Algebraische Körpererweiterungen

3.1 Charakteristik

Sei R ein Ring und $\varphi : \mathbb{Z} \to R$ mit $n \mapsto n \cdot 1_R$ der kanonische Homomorphismus. Ist R nullteilerfrei, so ist das Nullideal in R prim und somit ist auch $\mathrm{Kern}(\varphi) = \varphi^{-1}(0) \subset \mathbb{Z}$ ein Primideal. Nach Satz 1.38 folgt

$$\mathrm{Kern}(\varphi) = \begin{cases} (0) & \text{oder} \\ (p) & \text{für eine Primzahl } p. \end{cases}$$

Definition 3.1. Sei R ein nullteilerfreier Ring. Das eindeutig bestimmte Element $n \in \mathbb{N}_0$ mit $(n) = \mathrm{Kern}(\varphi)$ heißt die **Charakteristik** von R. Bezeichnung: $\mathrm{char}(R)$.

Beispiel 3.2. • $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ haben Charakteristik 0.
• p Primzahl: $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ und $\mathbb{F}_p[T]$ haben Charakteristik p.
• für jeden Körper k gilt

$$\mathrm{char}(k) = \mathrm{char}(k[T]) = \mathrm{char}(k(T)).$$

- es gilt für jeden nullteilerfreien Ring R

$$\operatorname{char}(R) = \operatorname{char}(Q(R)).$$

- Ist $R \overset{i}{\hookrightarrow} S$ ein Teilring, so gilt $\operatorname{char}(R) = \operatorname{char}(S)$.
  [Grund: $\varphi_S = i \circ \varphi_R$. Weil i injektiv ist, folgt $\operatorname{Kern}(\varphi_S) = \operatorname{Kern}\varphi_R$.]

Lemma 3.3. *Sind K, L Körper und $\operatorname{char}(K) \neq \operatorname{char}(L)$, so gibt es keinen Körperhomomorphismus von K nach L.*

Beweis. Gäbe es einen solchen Homomorphismus, so wäre dieser injektiv und K wäre isomorph zu einem Teilkörper von L. Also $\operatorname{char}(K) = \operatorname{char}(L)$. □

Definition 3.4. Sei K ein Körper. Der Durchschnitt aller Teilkörper von K heißt der **Primkörper** von K.

Bemerkung 3.5. Der Primkörper ist der kleinste Teilkörper von K.

Lemma 3.6. *Sei K ein Körper und $P \subset K$ sein Primkörper. Dann gilt*

$\operatorname{char}(K) = 0 \Longleftrightarrow P \cong \mathbb{Q}$

$\operatorname{char}(K) = p > 0 \Longleftrightarrow P \cong \mathbb{F}_p$.

Beweis. Die $\Leftarrow$ Implikationen sind trivial. Wegen $P \ni 1$, faktorisiert $\varphi : \mathbb{Z} \to K$ über P.
1. Fall: $\operatorname{char}(K) = 0$: $\mathbb{Z} \cong \operatorname{Bild}(\varphi) \subset P$ folglich ist $Q(\operatorname{Bild}(\varphi)) \cong \mathbb{Q}$ ein Teilkörper von P und deshalb $= P$.
2. Fall: $\operatorname{char}(K) = p > 0$: dann gilt $\mathbb{F}_p \cong \operatorname{Bild}(\varphi) \subset P$. Dies ist ein Teilkörper, also $P = \operatorname{Bild}(\varphi)$. □

Definition 3.7. Sei K ein Körper und $0 < p = \operatorname{char}(K)$. Dann heißt der Körperhomomorphismus

$$\sigma : K \to K,\ a \mapsto a^p,$$

der **Frobeniushomomorphismus** von K.

Bemerkung 3.8. σ ist Homomorphismus wegen

$$(a+b)^p = a^p + \underbrace{\binom{p}{1}a^{p-1}b + \cdots + \binom{p}{p-1}ab^{p-1}}_{=0} + b^p$$

Lemma 3.9. *Ist K ein endlicher Körper, so ist der Frobeniushomomorphismus ein Automorphismus.*

Beweis. σ ist injektiv und weil K endlich ist, auch surjektiv. □

Lemma 3.10. *Sei $\operatorname{char}(K) = p > 0$ und $P \subset K$ der Primkörper. Dann gilt*

$$P = \{a \in K \mid \sigma(a) = a\}.$$

Beweis. $P^\times$ ist eine Gruppe der Ordnung $p-1$, also $a^{p-1} = 1$ für jedes $a \in P^\times$. Folglich gilt $a^p = a$ für alle $a \in P$. Gilt nun $a \in K$, $a^p = a$, so ist a Nullstelle des Polynoms $X^p - X$. Dieses hat höchstens p Nullstellen in K. Daher sind die p vielen Elemente von $P \cong \mathbb{F}_p$ genau die Menge der $a \in K$ mit $a^p - a = 0$. □

3.2 Endliche und algebraische Körpererweiterungen

Seien $K \subset L$ Körper. Sprechweise: L ist Erweiterungskörper von K.
Vermittels: $K \times L \to L$, $(x, y) \mapsto xy$, wird L zu einem K-Vektorraum.

Definition 3.11. $\dim_K L$ heißt der **Grad** der Körpererweiterung L über K.

Notation: $[L : K] \in \mathbb{N} \cup \{\infty\}$

Bemerkung 3.12. $[L : K] = 1 \Leftrightarrow L = K$ ($K \subset L$ ist ein 1-dimensionaler K-Untervektorraum).

Satz 3.13 (Gradsatz). *Es seien $K \subset L \subset M$ Körpererweiterungen. Dann gilt*

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

Beweis. Sind M/L und L/K endlich, d.h. von endlichem Grad, so auch M/K und es gilt die Gradformel. Dies sieht man so:

Es ist $M \cong L^{[M:L]}$ als L-Vektorraum , also auch $M \cong L^{[M:L]}$ als K-Vektorraum. Nun gilt $L \cong K^{[L:K]}$ als K-Vektorraum, also

$$M \cong (K^{[L:K]})^{[M:L]} \cong K^{[M:L]\cdot[L:K]}.$$

Ist $[L : K] = \infty$, so existiert ein unendliches System von K-linear unabhängigen Elementen in L, also auch in M, also $[M : K] = \infty$.
Ist $[M : L] = \infty$, so existiert ein unendliches System von L-linear unabhängigen Elementen in M. Dieses System ist auch K-linear unabhängig. Also $[M : K] = \infty$. □

Korollar 3.14. *Sind $K \subset L \subset M$ Körpererweiterungen und $[M : K]$ eine Primzahl, so gilt $L = K$ oder $L = M$.*

Beweis. Aus Satz 3.13 folgt $[M : L] = 1$ oder $[L : K] = 1$. □

Beispiele 3.15. • $[\mathbb{C} : \mathbb{R}] = 2$.
• Sei $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \in \mathbb{C} \mid a, b \in \mathbb{Q}\}$. Dies ist ein Körper und weil $\sqrt{2}$ irrational ist, gilt $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.
• $[\mathbb{R} : \mathbb{Q}] = \infty$ (ein endlichdimensionaler $\mathbb{Q}$-Vektorraum ist abzählbar).
• Für jeden Körper gilt

$$[k(t) : k] = \infty$$

(die Polynome $1, t, t^2, \ldots$ sind linear unabhängig).

(Erinnerung). Sei $K \subset L$ eine Körpererweiterung. Ein Element $\alpha \in L$ heißt **algebraisch** über K, wenn α eine Gleichung

$$\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_0 = 0$$

mit $c_0, \ldots, c_{n-1} \in K$ erfüllt. M.a.W.: α ist algebraisch, wenn der Substitutionshomomorphismus

$$\varphi : K[X] \longrightarrow L,\ f \longmapsto f(\alpha),$$

nicht injektiv ist. Andernfalls heißt α **transzendent**.

Definition 3.16. L heißt **algebraisch** über K, wenn jedes Element von L algebraisch über K ist.

Beispiele 3.17. • $\mathbb{C}/\mathbb{R}$ ist algebraisch. Ist $\alpha = a + bi \in \mathbb{C}$, so gilt $f(\alpha) = 0$ mit $f(X) = X^2 - 2aX + (a^2 + b^2)$.
• Ist k ein Körper, so ist $k(t)/k$ nicht algebraisch, weil $t \in k(t)$ nicht algebraisch ist: Die Abbildung

$$k[X] \longrightarrow k(t),\ f(X) \longmapsto f(t)$$

ist injektiv (ein Isomorphismus auf den Unterring $k[t] \subset k(t)$).

Definition/Lemma 3.18. *Sei $K \subset L$ eine Körpererweiterung und $\alpha \in L$ algebraisch über K. Dann existiert ein eindeutig bestimmtes normiertes Polynom kleinsten Grades $f \in K[X]$ mit $f(\alpha) = 0$. Es gilt* $\mathrm{Kern}(\varphi) = (f)$ *für den Substitutionshomomorphismus*

$$\varphi : K[X] \longrightarrow L,\ g \longmapsto g(\alpha),$$

Insbesondere ist (f) ein Primideal, also f irreduzibel. Man nennt f das **Minimalpolynom** *von α.*

Beweis. $g(\alpha) = 0 \iff g \in \mathrm{Kern}(\varphi)$. $\mathrm{Kern}(\varphi)$ ist ein Primideal $\neq (0)$ im Hauptidealring $K[X]$, also von der Form (f) mit einem eindeutig bestimmten normierten irreduziblen Polynom f. □

Definition 3.19. Sei $K \subset L$ eine Körpererweiterung und $\alpha \in L$. Der Teilring

$$K[\alpha] = \{c_0 + c_1\alpha + \cdots + c_n\alpha^n \mid n \in \mathbb{N}_0,\ c_i \in K\}$$

ist der kleinste Teilring von L der K und α umfasst und heißt der **von $\boldsymbol{\alpha}$ über $\boldsymbol{K}$ erzeugte Teilring von $\boldsymbol{L}$**. Der Quotientenkörper $K(\alpha) = Q(K[\alpha]) \subset L$ ist der kleinste Teilkörper von L der K und α umfasst und heißt der **von $\boldsymbol{\alpha}$ über $\boldsymbol{K}$ erzeugte Teilkörper von $\boldsymbol{L}$** (man liest $K(\alpha)$ als „K adjungiert α“).

Satz 3.20. *Sei $K \subset L$ eine Körpererweiterung und $\alpha \in L$ algebraisch. Dann ist $K[\alpha]$ schon ein Körper, d.h. es gilt*

$$K[\alpha] = K(\alpha).$$

Der Homomorphismus $\varphi : K[X] \to L,\ g \mapsto g(\alpha)$, induziert einen natürlichen Isomorphismus

$$K[X]/(f) \xrightarrow{\sim} K(\alpha),$$

wobei f das Minimalpolynom von α über K ist. Es gilt

$$[K(\alpha) : K] = \deg(f),$$

insbesondere ist $K(\alpha)/K$ eine endliche Körpererweiterung.

Beweis. Nach dem Homomorphiesatz induziert φ einen Isomorphismus

$$K[X]/(f) \tilde{\to} K[\alpha].$$

Wegen $f \neq 0$ und f prim folgt nach Lemma 2.25, dass $K[X]/(f)$ Körper ist. Also gilt $K[\alpha] = Q(K[\alpha]) = K(\alpha)$. Schließlich bilden die Restklassen von $1, X, \ldots, X^{\deg(f)-1}$ eine K-Basis von $K[X]/(f)$. □

Zum Vertrautwerden: Wie findet man $\alpha^{-1} \in K[\alpha]$?
Sei $f = X^n + c_{n-1}X^{n-1} + \cdots + c_0$ das Minimalpolynom von $\alpha \neq 0$. Es gilt $n \geq 1$ und $c_0 \neq 0$ weil f irreduzibel ist. Es folgt $0 = \alpha^{-1}(\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_0)$ also $(-c_0)\alpha^{-1} = \alpha^{n-1} + c_{n-1}\alpha^{n-2} + \cdots + c_1$ und somit $\alpha^{-1} \in K[\alpha]$.

Verbindung zur linearen Algebra.
Sei $[L : K] < \infty$. Wir betrachten den K-Vektorraum-Endomorphismus

$$h_\alpha : L \longrightarrow L,\ b \longmapsto \alpha b.$$

Wegen $h_\alpha(1) = \alpha$ gilt $\alpha = 0 \iff h_\alpha = 0$ und allgemeiner für ein Polynom f

$$f(\alpha) = 0 \iff f(h_\alpha) = 0.$$

Also ist das Minimalpolynom von α gleich $\chi_{\min}(h_\alpha)$.

Satz 3.21. *Jede endliche Körpererweiterung ist algebraisch.*

Beweis. Sei $\alpha \in L$ beliebig und $n = [L : K]$. Dann sind die $n + 1$ vielen Elemente

$$1, \alpha, \ldots, \alpha^n$$

linear abhängig über K und wir finden eine Gleichung für α. □

Bemerkung 3.22. Es gibt unendliche algebraische Erweiterungen.

Korollar 3.23. *Sei $K \subset L$ und $\alpha \in L$ algebraisch über K. Dann ist die Körpererweiterung $K(\alpha)/K$ algebraisch.*

Beweis. $[K(\alpha) : K] < \infty$ nach Satz 3.20. □

Verallgemeinerte Terminologie: Sei $K \subset L$ und $S \subset L$ eine Teilmenge. Wir bezeichnen den kleinsten Teilkörper von L der K und S umfasst mit $K(S)$, den kleinsten Teilring mit $K[S]$. Ist $S = \{\alpha_1, \ldots, \alpha_n\}$ endlich, so schreiben wir

$$\begin{aligned} K(S) &= K(\alpha_1, \ldots, \alpha_n) \\ K[S] &= K[\alpha_1, \ldots, \alpha_n]. \end{aligned}$$

$K[\alpha_1,\dots,\alpha_n]$ ist der Teilring in L aller Elemente der Form $f(\alpha_1,\dots,\alpha_n)$, $f \in K[X_1,\dots,X_n]$ und $k(\alpha_1,\dots,\alpha_n)$ besteht aus allen Elementen der Form

$$\frac{f(\alpha_1,\dots,\alpha_n)}{g(\alpha_1,\dots,\alpha_n)},\ f,g \in K[X_1,\dots,X_n],\ g(\alpha_1,\dots,\alpha_n) \neq 0.$$

Ist S unendlich, so gilt

$$K(S) = \bigcup_{\substack{T \subset S \\ T \text{ endl}}} K(T) \subset L.$$

Definition 3.24. Sei $K \subset L$ und $\alpha \in L$. Der Grad $[K(\alpha) : K]$ heißt der **Grad** von α über K (= Grad des Minimalpolynoms). L/K heißt **einfach**, wenn es ein $\alpha \in L$ mit $L = K(\alpha)$ gibt.
L/K heißt **endlich erzeugt**, wenn es endlich viele Elemente $\alpha_1,\dots,\alpha_n \in L$ mit $L = K(\alpha_1,\dots,\alpha_n)$ gibt.

Beispiele 3.25. • $\mathbb{C}/\mathbb{R}$ ist einfach, wegen $\mathbb{C} = \mathbb{R}(i)$.
• $k(t)/k$ ist einfach.
• $k(X,Y) = Q(k[X,Y])/k$ ist endlich erzeugt, aber nicht einfach (Beweis später).

Satz 3.26. *Es sei $L = K(\alpha_1,\dots,\alpha_n)$ eine endlich erzeugte Körpererweiterung von K. Sind $\alpha_1,\dots,\alpha_n$ algebraisch, so gilt:*

(i) $L = K(\alpha_1,\dots,\alpha_n) = K[\alpha_1,\dots,\alpha_n]$.
(ii) *L/K ist endlich, insbesondere algebraisch.*

Beweis. Per Induktion nach n. Anfang: $n = 1$ war Satz 3.20 und Korollar 3.23.
Schritt: Wir wissen, dass $K(\alpha_1,\dots,\alpha_{n-1}) = K[\alpha_1,\dots,\alpha_{n-1}]$ endlich über K ist. Nach Satz 3.20 angewendet auf $K[\alpha_1,\dots,\alpha_{n-1}]$ und $\alpha_n \in L$ gilt:
$K[\alpha_1,\dots,\alpha_n] = K[\alpha_1,\dots,\alpha_{n-1}][\alpha_n]$ ist Körper (also gleich $L = K(\alpha_1,\dots,\alpha_n)$) und

$$(K(\alpha_1,\dots,\alpha_n) : K(\alpha_1,\dots,\alpha_{n-1})) < \infty.$$

Die Gradformel liefert

$$[L : K] =$$

$$[K(\alpha_1,\dots,\alpha_n) : K(\alpha_1,\dots,\alpha_{n-1})] \cdot [K(\alpha_1,\dots,\alpha_{n-1}) : K] < \infty. \qquad \square$$

Korollar 3.27. *Sei $K \subset L$ eine Körpererweiterung. Dann sind äquivalent*

(i) *L/K ist endlich.*
(ii) *L wird über K von endlich vielen algebraischen Elementen erzeugt.*
(iii) *L ist endlich erzeugte algebraische Körpererweiterung von K.*

Ist $S \subset L$ ein Erzeugendensystem einer Körpererweiterung L/K (so etwas gibt es stets, z.B. $S = L$), so gilt

$$L = \bigcup_{\substack{T \subset S \\ \text{endl}}} K(T).$$

Sind alle Elemente aus S algebraisch über K, so ist L Vereinigung algebraischer Erweiterungen, also algebraisch. Wir erhalten

Korollar 3.28. *Sei $K \subset L$ eine Körpererweiterung. Dann sind äquivalent*

(i) *L/K ist algebraisch.*
(ii) *L/K wird von algebraischen Elementen erzeugt.*

Korollar 3.29. *Sei $K \subset L$ eine Körpererweiterung. Dann ist die Menge*

$$\{\alpha \in L \mid \alpha \text{ algebraisch über } K\}$$

ein Unterkörper von L.

Definition 3.30. Man nennt diesen Körper den **algebraischen Abschluss** von K in L.

Beweis von Korollar 3.29. Sei M diese Menge. Es gilt für $\alpha, \beta \in M$: $\alpha + \beta \in K(\alpha, \beta)$.
Wegen $K(\alpha, \beta)/K$ algebraisch folgt $\alpha + \beta \in M$.
Analog für $\alpha\beta$, α^{-1}. □

Satz 3.31. *Es seien $K \subset L \subset M$ Körpererweiterungen. Ist $\alpha \in M$ algebraisch über L und ist L/K algebraisch, so ist α algebraisch über K. Insbesondere ist M/K genau dann algebraisch, wenn L/K und M/K algebraisch sind.*

Beweis. Sei $f = X^n + c_{n-1}X^{n-1} + \cdots + c_0$ das Minimalpolynom von α über L. Dann ist α schon algebraisch über dem Körper $K(c_0, \ldots, c_{n-1}) \subset L$. Nach Satz 3.20 folgt: $[K(\alpha, c_0, \ldots, c_{n-1}) : K(c_0, \ldots, c_{n-1})] < \infty$ und wegen $[K(c_0, \ldots, c_{n-1}) : K) < \infty$ ist $K(\alpha, c_0, \ldots, c_{n-1})/K$ endlich, also algebraisch $\Rightarrow \alpha$ algebraisch über K. Wir erhalten: M/K algebraisch, falls M/L algebraisch und L/K algebraisch.

Die Umkehrung ist trivial. □

Beispiel 3.32. Wir betrachten $\mathbb{Q} \subset \mathbb{C}$.
• Jedes normierte, irreduzible Polynom mit Koeffizienten in $\mathbb{Q}$ taucht als Minimalpolynom eines algebraischen Elements in $\mathbb{C}$ auf.
Grund: f hat eine Nullstelle α in $\mathbb{C}$ und wegen der Irreduzibilität ist f das Minimalpolynom von α.
• Sei $\mathbb{Q}^{\text{alg}} \subset \mathbb{C}$ der Körper der algebraischen Elemente in $\mathbb{C}$. $\mathbb{Q}^{\text{alg}}/\mathbb{Q}$ ist algebraisch. Ist $f \in \mathbb{Q}[X]$ irreduzibel vom Grad n und $f(\alpha) = 0$, so gilt $\mathbb{Q}(\alpha) \subset \mathbb{Q}^{\text{alg}}$ und $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$ und folglich $[\mathbb{Q}^{\text{alg}} : \mathbb{Q}] \geq n$.
Da es über $\mathbb{Q}$ irreduzible Polynome beliebig hohen Grades gibt (benutze Eisenstein) folgt $[\mathbb{Q}^{\text{alg}} : \mathbb{Q}] = \infty$.
• die Menge der normierten, irreduziblen Polynome über $\mathbb{Q}$ ist abzählbar. Jedes Polynom hat nur endlich viele Nullstellen, also ist $\mathbb{Q}^{\text{alg}}$ abzählbar. Da $\mathbb{C}$ überabzählbar ist, erhalten wir:

Es gibt überabzählbar viele transzendente Elemente in $\mathbb{C}$.

3.3 Algebraischer Abschluss

Satz 3.33. *Sei K ein Körper und $f \in K[X]$ ein Polynom vom Grad ≥ 1. Dann existiert eine endliche (algebraische) Körpererweiterung L/K so dass f eine Nullstelle in L besitzt.*

Beweis. OE sei f irreduzibel. Setze $L = K[X]/(f)$ und betrachte die kanonische Abbildung

$$K \to K[X] \xrightarrow{p} K[X]/(f) = L.$$

Diese ist injektiv (weil Körperhomomorphismus) und so wird L zum Erweiterungskörper von K vom Grad $= \deg f$.
Sei α das Bild von $X \in K[X]$ in L. Dann gilt $f(\alpha) = 0$ weil $f(\alpha) = p(f(X)) = 0$ wegen $f \in \mathrm{Kern}(p)$. □

Definition 3.34. Ein Körper K heißt **algebraisch abgeschlossen**, wenn jedes $f \in K[X]$, $\deg f \geq 1$, eine Nullstelle in K besitzt.

Bemerkung 3.35. Sukzessives Abspalten von Nullstellen ergibt, dass jedes $0 \neq f \in K[X]$ von der Form

$$f = c(X - \alpha_1) \dots (X - \alpha_n)$$

mit $n = \deg f$, $c \in K^\times$, $\alpha_1, \cdots, \alpha_n \in K$, ist. Insbesondere ist jedes irreduzible Polynom linear, d.h. vom Grad 1.

Lemma 3.36. *K ist genau dann algebraisch abgeschlossen, wenn es keine echte (d.h. $L \neq K$) endliche Erweiterung L/K gibt.*

Beweis. Sei K algebraisch abgeschlossen. Sei L/K eine endliche Erweiterung und $\alpha \in L$. Sei f das Minimalpolynom von α über K. K algebraisch abgeschlossen und f irreduzibel $\Rightarrow \deg f = 1 \Rightarrow \alpha \in K \Rightarrow L = K$.
Nun nehmen wir an, dass K keine echte algebraische Erweiterung besitzt. Sei $f \in K[X]$. Z.z. f hat Nullstelle in K. OE sei f irreduzibel. Dann ist $L = K[X]/(f)$ eine algebraische Erweiterung vom Grad $= \deg f \Rightarrow \deg f = 1 \Rightarrow f$ hat Nullstelle in K. □

Theorem 3.37. *Zu jedem Körper K gibt es einen algebraisch abgeschlossenen Erweiterungskörper L.*

Beweis. Wir betrachten die Menge $I = \{f \in K[X], \deg f \geq 1\}$ und den Polynomring

$$K[\mathbb{N}_0^{(I)}] = \text{Polynomring in den Variablen } (X_f)_{f \in I}$$

und bezeichnen diesen Ring mit $K[\mathfrak{X}]$. Wir betrachten das Ideal

$$\mathfrak{a} = (f(X_f), f \in I)$$

welches von der Familie der Polynome $f(X_f)$ in $K[\mathfrak{X}]$ erzeugt wird.

Behauptung: $\mathfrak{a} \subsetneqq K[\mathfrak{X}]$.

Angenommen $1 \in \mathfrak{a}$. Dann gibt es eine Gleichung in $K[\mathfrak{X}]$ der Form

$$1 = \sum_{i=1}^{n} g_i f_i(X_{f_i})$$

mit $f_1, \ldots, f_n \in I$ und $g_1, \ldots, g_n \in K[\mathfrak{X}]$. Nach n-maliger Anwendung von Satz 3.3 finden wir eine Erweiterung K'/K, so dass für $i = 1, \ldots, n$ das Polynom f_i eine Nullstelle $\alpha_i \in K'$ besitzt. Wir betrachten den nach Universaleigenschaft eindeutigen Ringhomomorphismus $\phi : K[\mathfrak{X}] \to K'$ mit

$\phi|_K$ = die gegebene Einbettung $K \hookrightarrow K'$

$$\phi(X_f) = \begin{cases} \alpha_i & \text{wenn} \quad f = f_i \\ 0 & \text{wenn} \quad f \notin \{f_1, \ldots, f_n\}. \end{cases}$$

Dann gilt

$$\begin{aligned} 1 &= \phi(1) = \phi\left(\sum_{i=1}^{n} g_i f_i(X_{f_i})\right) \\ &= \sum_{i=1}^{n} \phi(g_i)\phi(f_i(X_{f_i})). \end{aligned}$$

Nun gilt aber

$$\phi(f_i(X_{f_i})) = f_i(\phi(X_{f_i})) = f_i(\alpha_i) = 0.$$

Wir erhalten $1 = 0$, Widerspruch.
Also existiert ein Maximalideal $\mathfrak{m} \subset K[\mathfrak{X}]$ mit $\mathfrak{a} \subseteq \mathfrak{m}$. Wir setzen

$$L_1 = K[\mathfrak{X}]/\mathfrak{m} \quad \text{(Erweiterungskörper von } K\text{)}.$$

Ist $f \in I$, so ist das Bild von X_f in L_1 eine Nullstelle von f in L_1, wegen $f(X_f) \in \mathfrak{a} \subseteq \mathfrak{m}$. Also: Jedes nichtkonstante Polynom mit Koeffizienten in K hat eine Nullstelle in L_1.
Jetzt wenden wir diesen Prozess auf L_1 anstelle von K an, erhalten L_2 u.s.w.

$$K \subset L_1 \subset L_2 \subset \ldots \ .$$

Setze $L = \bigcup_{i=1}^{\infty} L_i$. Sei $f \in L[X]$, $\deg f \geq 1$. Dann gibt es ein $n \in \mathbb{N}$, so dass alle Koeffizienten von f schon in L_n liegen. Also hat f eine Nullstelle in L_{n+1} und damit auch in L. Daher ist L algebraisch abgeschlossen. □

Korollar 3.38. *Sei K ein Körper. Dann gibt es einen algebraisch abgeschlossenen Erweiterungskörper $\overline{K}$ von K so dass $\overline{K}/K$ algebraisch ist. Man nennt $\overline{K}$ einen* ***algebraischen Abschluss*** *von K.*

Beweis. 1. Variante: Man überprüfe, dass der im Beweis von Theorem 3.37 konstruierte Körper L algebraisch über K ist.
2. Sei L/K irgendeine Erweiterung mit L algebraisch abgeschlossen (existiert nach Theorem 3.37). Sei

$$\overline{K} = \{\alpha \in L \mid \alpha \text{ algebraisch über } K\}$$

der algebraische Abschluss von K in L (siehe Korollar 3.29).

Behauptung: $\overline{K}$ ist algebraisch abgeschlossen.

Beweis der Behauptung: Sei $f \in \overline{K}[X]$, $\deg f \geq 1$. Dann hat f eine Nullstelle α in L. Das Element α ist algebraisch über $\overline{K}$, also nach Satz 3.31 algebraisch über K, also $\alpha \in \overline{K}$. □

Beispiel 3.39. Der am Ende von Abschnitt 3.2 konstruierte Körper $\overline{\mathbb{Q}} \subset \mathbb{C}$ ist ein algebraischer Abschluss von $\mathbb{Q}$.

Nächstes Ziel: „zwei algebraische Abschlüsse von K sind stets isomorph".

Wir führen die folgende Notation ein. Sei $\sigma : K \to L$ ein Körperhomomorphismus und $f = a_n X^n + \cdots + a_0 \in K[X]$. Wir setzen $f^\sigma = \sigma(a_n)X^n + \cdots + \sigma(a_0) \in L[X]$.

Lemma 3.40. *Sei K ein Körper und $K' = K(\alpha)$ eine einfache algebraische Körpererweiterung mit Minimalpolynom $f \in K[X]$ zu α. Weiter sei $\sigma : K \to L$ ein Körperhomomorphismus.*

(i) *Ist $\sigma' : K' \to L$ ein Körperhomomorphismus, der σ fortsetzt (d.h. $\sigma'|_K = \sigma$), so ist $\sigma'(\alpha)$ eine Nullstelle von $f^\sigma \in L[X]$.*

(ii) *Umgekehrt gibt es zu jeder Nullstelle $\beta \in L$ von $f^\sigma \in L[X]$ genau eine Fortsetzung $\sigma' : K' \to L$ von σ mit $\sigma'(\alpha) = \beta$.*

Daher ist die Anzahl der verschiedenen Fortsetzungen σ' von σ auf K' gleich der Anzahl der Nullstellen von f^σ in L, insbesondere endlich und $\leq \deg f$.

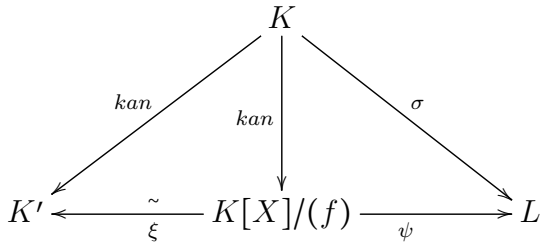
Beweis. Für jede Fortsetzung $\sigma' : K' \to L$ von σ folgt aus $f(\alpha) = 0$, dass $f^\sigma(\sigma'(\alpha)) = \sigma'(f(\alpha)) = 0$.
Außerdem gilt nach Satz 3.20: $K' = K[\alpha]$, also ist σ' schon durch $\sigma'(\alpha)$ eindeutig bestimmt. Bleibt z.z.: Zu gegebener Nullstelle $\beta \in L$ von f^σ existiert eine Fortsetzung $\sigma' : K' \to L$ von σ mit $\sigma'(\alpha) = \beta$.
Der Kern des Homomorphismus $\phi : K[X] \to L$, $X \mapsto \beta$, $\phi_{|K} = \sigma$ enthält f. Grund:

$$\begin{aligned} \phi(f) = \phi(f(X)) &= f^\sigma(\phi(X)) \\ &= f^\sigma(\beta) = 0. \end{aligned}$$

Wir erhalten einen induzierten Homomorphismus

$$\psi : K[X]/(f) \to L, \quad \psi(X + (f)) = \beta.$$

Wir erinnern uns an den Isomorphismus $\xi : K[X]/(f) \xrightarrow{\sim} K'$, $X + (f) \mapsto \alpha$, und erhalten das kommutative Diagramm



Nun setzen wir $\sigma' = \psi \circ \xi^{-1}$. □

Satz 3.41. *Sei $K \subset K'$ eine algebraische Körpererweiterung und $\sigma : K \to L$ ein Körperhomomorphismus. Sei L algebraisch abgeschlossen. Dann besitzt σ eine Fortsetzung $\sigma' : K' \to L$. Ist K' algebraisch abgeschlossen und L algebraisch über $\sigma(K)$, so ist jede Fortsetzung σ' ein Isomorphismus.*

Beweis. Wir wenden das Zornsche Lemma an. Sei Σ die Menge aller Paare (F, τ) mit einem Zwischenkörper $K \subset F \subset K'$ und einer Fortsetzung $\tau : F \to L$ von σ. Wir setzen $(F, \tau) \leq (F', \tau')$ wenn $F \subset F'$ und $\tau'_{|F} = \tau$ gilt. Dann ist Σ halbgeordnet. Wegen $(K, \sigma) \in \Sigma$ ist Σ nichtleer. Jede Kette in Σ hat eine obere Schranke (man vereinige die Körper in der Kette). Nach Zorn existiert ein maximales Element $(F, \tau) \in \Sigma$. Dann gilt $F = K'$: Ansonsten gäbe es ein $\alpha \in K' \setminus F$, so könnte man nach Lemma 3.40 τ auf $F(\alpha)$ fortsetzen und (F, τ) wäre nicht maximal. Dies zeigt die Existenz von $\sigma' : K' \to L$. Ist nun K' algebraisch abgeschlossen, so auch $\sigma'(K') \subset L$. Ist L algebraisch über $\sigma(K)$, so auch über $\sigma'(K')$ und deshalb $L = \sigma'(K')$. Körperhomomorphismen sind stets injektiv $\Rightarrow \sigma : K' \to L$ ist Isomorphismus. □

Korollar 3.42. *Es seien $\overline{K}_1$ und $\overline{K}_2$ zwei algebraische Abschlüsse von K. Dann existiert ein Isomorphismus $\overline{K}_1 \xrightarrow{\sim} \overline{K}_2$, der die Identität von K fortsetzt.*

Bemerkung 3.43. Dieser Isomorphismus existiert, es gibt aber keine kanonische Wahl, d.h. $\overline{K}_1$ und $\overline{K}_2$ sind *unkanonisch* isomorph.

3.4 Ganze Ringerweiterungen

Sei $\phi : A \to B$ ein Ringhomomorphismus. Erinnerung: Man nennt B eine A-Algebra. B wird zum A-Modul durch

$$a \cdot b \overset{df}{=} \phi(a) \cdot b.$$

Insbesondere ist für $f \in A[X]$ und $b \in B$ das Element $f(b) \in B$ definiert.

Definition 3.44. ϕ heißt **endlich** (und B **endliche A-Algebra**) wenn B als A-Modul endlich erzeugt ist.

Satz 3.45. *Sei $\phi : A \to B$ ein Ringhomomorphismus und $b \in B$. Dann sind äquivalent:*

(i) *Es existiert ein normiertes Polynom $f \in A[X]$ so dass $f(b) = 0$ gilt.*

(ii) *Der Unterring $A[b] \subset B$ (d.h. das Bild des kanonischen Homomorphismus $\psi : A[X] \to B$, $\psi|_A = \phi$, $\psi(X) = b$) ist als A-Modul endlich erzeugt.*

(iii) *Es existiert ein endlich erzeugter A-Untermodul $M \subset B$ mit $1 \in M$ und $b \cdot M \subset M$.*

Beweis. (i) $\Rightarrow$ (ii) Es gelte $f(b) = 0$ mit $f = X^n + a_{n-1}X^{n-1} + \cdots + a_0$. Dann gilt $b^n = -\phi(a_{n-1})b^{n-1} - \cdots - \phi(a_0)$. Sei $M = \langle 1, b, \ldots, b^{n-1}\rangle \subset B$ der von $1, \ldots, b^{n-1}$ erzeugte A-Untermodul. Dann gilt $b^n \in M$ und per Induktion $b^m \in M$ für alle $m \in \mathbb{N}$. Also $A[b] \subset M$, folglich $A[b] = M$.
(ii) $\Rightarrow$ (iii) Man wähle $M = A[b]$.
(iii) $\Rightarrow$ (i). Sei $M = \langle m_1, \ldots, m_n\rangle \subset B$ ein endlich erzeugter A-Untermodul mit $1 \in M$ und $bM \subset M$. Dann existieren Gleichungen

$$\begin{array}{ccc} bm_1 & = & a_{11}m_1 + \cdots + a_{1n}m_n \\ \vdots & \vdots & \vdots \\ bm_n & = & a_{n1}m_1 + \cdots + a_{nn}m_n \end{array} .$$

M.a.W.

$$Q\begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0$$

mit $Q = (b\delta_{ij} - a_{ij})_{i,j} \in M_{n,n}(B)$. Sei Q^{ad} die Adjunkte zu Q, d.h. $Q^{ad}Q = \det(Q) \cdot E_n$. Dann gilt:

$$(\det(Q) \cdot E_n) \cdot \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = Q^{ad}Q \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0,$$

d.h. $\det(Q)m_i = 0$, $i = 1, \ldots, n$.

Hieraus folgt $\det(Q) \cdot m = 0 \ \forall\, m \in M$ und wegen $1 \in M$: $\det(Q) = 0$. Die Leibniz-Regel für det gibt uns eine Gleichung der Form

$$b^n + c_{n-1}b^{n-1} + \cdots + c_0 = 0$$

mit $c_0, \ldots, c_{n-1} \in A$. □

Definition 3.46. Sei $\phi : A \to B$ ein Ringhomomorphismus. Ein Element $b \in B$ heißt **ganz über A** (bzgl. ϕ) wenn b die äquivalenten Bedingungen von Satz 3.45 erfüllt. Man sagt **B ist ganz über A** (bzw. ϕ sei ganz), wenn jedes $b \in B$ ganz über A ist.

Korollar 3.47. *Jeder endliche Ringhomomorphismus ϕ ist ganz.*

Beweis. Man setze $M = B$ in Satz 3.45 (iii). □

Bemerkung 3.48. Sei $\phi : K \subset L$ eine Körpererweiterung. Dann gilt

ϕ endlich $\iff L/K$ endlich,

ϕ ganz $\iff L/K$ algebraisch.

Lemma 3.49. *Sind $A \to B$ und $B \to C$ endliche Ringhomomorphismen, so auch ihre Komposition $A \to C$.*

Beweis. Ist C als B-Modul durch $c_1, \dots, c_n$ erzeugt und B als A-Modul durch $b_1, \dots, b_m$, so ist C als A-Modul durch die $n \cdot m$ Produkte $(b_i c_j)_{\substack{i=1,\dots,m \\ j=1,\dots,n}}$ erzeugt.

Grund: Sei $c \in C$ beliebig $\Rightarrow$ ex. $\beta_1, \dots, \beta_n \in B$ mit

$$c = \beta_1 c_1 + \cdots + \beta_n c_n.$$

Nun existieren zu jedem β_i Elemente $a_{ij} \in A$ mit

$$\beta_i = a_{i1} b_1 + \cdots + a_{im} b_m.$$

Benennen wir $A \xrightarrow{\phi} B \xrightarrow{\psi} C$, so gilt

$$\begin{aligned} c = \beta_1 c_1 + \cdots + \beta_n c_n \quad &\overset{df}{=} \quad \psi(\beta_1) c_1 + \cdots + \psi(\beta_n) c_n \\ &= \quad \psi(\phi(a_{11}) b_1) c_1 + \cdots + \psi(\phi(a_{1m}) b_m) c_1 \\ &\qquad\qquad \vdots \\ &\qquad \psi(\phi(a_{n1}) b_1) c_n + \cdots + \psi(\phi(a_{nm}) b_m) c_n. \end{aligned}$$

□

Korollar 3.50. *Sei $\phi : A \to B$ ein Ringhomomorphismus und $b_1, \dots, b_n \in B$ so dass $B = A[b_1, \dots, b_n]$. Sind dann $b_1, \dots, b_n$ ganz über A so ist B endliche A-Algebra, insbesondere ist ϕ ganz.*

Beweis. Wir betrachten die Kette von Ringerweiterungen

$$\phi(A) \subset \phi(A)[b_1] \subset \phi(A)[b_1, b_2] \subset \cdots \subset \phi(A)[b_1, \dots, b_n] = B.$$

Nach Satz 3.45 ist jede Teilerweiterung endlich und nach Lemma 3.49 auch die Komposition. □

Korollar 3.51. *Sei $\phi : A \to B$ ein Ringhomomorphismus und $b_1, b_2 \in B$ ganz über A. Dann sind auch $b_1 + b_2$ und $b_1 b_2$ ganz über A.*

Beweis. $b_1 b_2, b_1 + b_2 \in A[b_1, b_2]$ und dies ist eine endliche, also ganze A-Algebra. □

Korollar 3.52. *Sind $A \to B$ und $B \to C$ ganz, so auch die Komposition $A \to C$.*

Beweis. Sei $c \in C$ beliebig. Es ist c ganz über B, also existieren $b_0, \ldots, b_{n-1} \in B$ mit

$$c^n + b_{n-1}c^{n-1} + \cdots + b_0 = 0.$$

Also ist c auch schon ganz über der endlichen A-Algebra $A[b_0, \ldots, b_{n-1}] \subset B$, d.h. die $A[b_0, \ldots, b_{n-1}]$-Algebra $A[b_0, \ldots, b_{n-1}][c] \subset C$ ist endlich. Diese ist nach Lemma 3.49 also eine endliche A-Algebra und c deshalb ganz über A. □

Sei nun A nullteilerfrei und $K = Q(A)$. Sei L/K eine Körpererweiterung.

Definition 3.53. Die Menge

$$A_L = \{c \in L \mid c \text{ ist ganz über } A\}$$

heißt der **GanzAbschluss** von A in L. A heißt **ganzabgeschlossen**, wenn $A = A_K$ gilt.

Bemerkung 3.54. Nach Korollar 3.51 ist A_L ein Ring.

Beispiel 3.55 (eines nicht ganzabgeschlossenen Ringes). Sei $f = X^2 - Y^3 \in \mathbb{C}[X, Y]$ und $A = \mathbb{C}[X, Y]/(f)$. A ist nullteilerfrei weil f irreduzibel ist.

Sei x das Bild von X in A; wegen $f \nmid X$ gilt $x \neq 0$. Analog sei y das Bild von Y in A; wegen $f \nmid Y$ gilt $y \neq 0$. Es gilt $x^2 = y^3$ in A. Daher gilt

$$\left(\frac{x}{y}\right)^2 - y = \frac{x^2}{y^2} - y = y - y = 0.$$

Also ist $\frac{x}{y} \in Q(A)$ ganz über A. Aber $\frac{x}{y} \notin A$. Ansonsten wäre nämlich $x = y \cdot \frac{x}{y} \in Ay$ und somit $X \in (Y, X^2 - Y^3)$. Aber $(Y, X^2 - Y^3) = (Y, X^2) \not\ni X$. Also ist A nicht ganzabgeschlossen.

Satz 3.56. *Jeder faktorielle Ring ist ganzabgeschlossen.*

Beweis. Sei $K = Q(A)$ und $\alpha \in K$ mit $\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_0 = 0$, wobei $c_0, \ldots, c_{n-1} \in A$. Z.z.: $\alpha \in A$. Sei $\alpha = \frac{a}{b}$, $a, b \in A$, $\mathrm{ggT}(a, b) = 1$. Dann gilt

$$a^n + c_{n-1}ba^{n-1} + \cdots + c_0 b^n = 0.$$

Ist nun $p \in A$ ein Primelement mit $p \mid b$, so folgt $p \mid a^n$, also $p \mid a$, Widerspruch. Also existiert so ein p nicht und es gilt $b \in A^\times$. Folglich gilt $\alpha \in A$. □

Bemerkung 3.57. Wir sehen somit, dass $\mathbb{C}[X,Y]/(X^2-Y^3)$ ein nullteilerfreier, nicht faktorieller Ring ist.

Wir brauchen den folgenden Spezialfall:

Definition 3.58. $\mathcal{O} = \{\alpha \in \mathbb{C} \mid \alpha \text{ ganz über } \mathbb{Z}\}$ heißt der Ring der **ganz-algebraischen Zahlen**.

Korollar 3.59. $\mathcal{O} \cap \mathbb{Q} = \mathbb{Z}$.

Beweis. $\mathbb{Z}$ ist faktoriell. □

3.5 Zerfällungskörper

Notation: Sind L/K und L'/K zwei Körpererweiterungen und ist $\sigma : L \to L'$ ein Homomorphismus, so nennen wir σ einen K-Homomorphismus wenn σ die Identität von K fortsetzt.

Definition 3.60. Sei $\mathcal{F} = (f_i)_{i\in I}$ eine Familie nichtkonstanter Polynome über einem Körper K. Ein Erweiterungskörper L/K heißt **Zerfällungskörper** (über K) der Familie $\mathcal{F}$ wenn gilt

(i) Jedes f_i zerfällt über L vollständig in Linearfaktoren.
(ii) L/K wird von den Nullstellen der f_i erzeugt.

Beispiele 3.61. • Sei $\mathcal{F}$ die einelementige Familie, bestehend aus einem $f \in K[X]$. Sei $\overline{K}/K$ ein algebraischer Abschluss und $a_1, \ldots, a_n$ die Nullstellen von f in $\overline{K}$. Dann ist $L = K(a_1, \ldots, a_n)$ ein Zerfällungskörper für f.
• Für eine beliebige Familie $(f_i)_{i\in I}$ erhält man einen Zerfällungskörper, indem man in einem gewählten algebraischen Abschluss von K die Nullstellen der f_i adjungiert.
• Ist $\mathcal{F} = (f_1, \ldots, f_n)$ eine endliche Familie so ist jeder Zerfällungskörper des Produktes $f_1 \cdots f_n$ auch Zerfällungskörper von $\mathcal{F}$ und umgekehrt.

Satz 3.62. *Seien L_1, L_2 zwei Zerfällungskörper der Familie $\mathcal{F} = (f_i)_{i\in I}$ von Polynomen über K. Dann beschränkt sich jeder K-Homomorphismus $\overline{\sigma} : L_1 \to \overline{L}_2$ in einen algebraischen Abschluss $\overline{L}_2$ von L_2 zu einem Isomorphismus $\sigma : L_1 \xrightarrow{\sim} L_2$.*

Korollar 3.63. *Je zwei Zerfällungskörper von $\mathcal{F}$ sind (unkanonisch) K-isomorph.*

Beweis. Nach Satz 3.41 setzt sich die Inklusion $K \hookrightarrow \overline{L}_2$ zu einem K-Homomorphismus $\overline{\sigma} : L_1 \to \overline{L}_2$ fort. Nach Satz 3.62 erhalten wir einen Isomorphismus $\sigma : L_1 \xrightarrow{\sim} L_2$ □

Beweis von Satz 3.62. 1. Schritt: $\mathcal{F} = (f)$ (einelementige Familie). OE f normiert. Weil f Koeffizienten in K hat, gilt $f^{\overline{\sigma}} = f$. Sind $a_1, \ldots, a_n$ die Nullstellen (mit Vielfachheiten) von f in L_1 und $b_1, \ldots, b_n$ die Nullstellen von f in $L_2 \subset \overline{L}_2$

so folgt $f^{\overline{\sigma}} = \prod(X - \overline{\sigma}(a_i))$. Wegen $f = \prod(X - b_i)$ folgt nach Umnummerierung $b_i = \overline{\sigma}(a_i)$, $i = 1, \ldots, n$, und

$$L_2 = K(b_1, \ldots, b_n) = K(\overline{\sigma}(a_1), \ldots, \overline{\sigma}(a_n)) = \overline{\sigma}(L_1)$$

2. Schritt: $\mathcal{F}$ ist endliche Familie $(f_1, \ldots, f_n)$. Ersetze $\mathcal{F}$ durch die einelementige Familie $f_1 \cdots f_r$ und wende Schritt 1 an.

3. Schritt: $\mathcal{F}$ beliebige Familie. L_1 und L_2 sind Vereinigung von Zerfällungskörpern zu den endlichen Teilfamilien von $\mathcal{F}$. □

Satz 3.64. *Es sei L/K eine algebraische Körpererweiterung. Dann sind äquivalent:*

(i) *Jeder K-Homomorphismus $L \to \overline{L}$ in einen algebraischen Abschluss $\overline{L}$ von L beschränkt sich zu einem Automorphismus von L.*

(ii) *L ist Zerfällungskörper einer Familie von Polynomen über K.*

(iii) *Jedes irreduzible Polynom aus $K[X]$, das in L eine Nullstelle hat, zerfällt über L vollständig in Linearfaktoren.*

Bemerkung 3.65 (zu Satz 3.64 (i))**.** Ein algebraischer Abschluss $\overline{L}/L$ ist eine Körpererweiterung, d.h. es gibt eine vorgegebene Einbettung $L \hookrightarrow \overline{L}$. Es gibt aber i.A. noch mehr K-Homomorphismen $L \to \overline{L}$ als diesen einen.

Beispiel 3.66. Sei $\alpha = \sqrt[3]{2} \in \mathbb{R}$ die eindeutig bestimmte *reelle* Zahl α mit $\alpha^3 = 2$ und sei $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}^{\text{alg}} (\subset \mathbb{C})$ die natürliche Inklusion. Die Abbildung

$$\begin{array}{rcl} \varphi : \mathbb{Q}(\sqrt[3]{2}) & \longrightarrow & \mathbb{Q}^{\text{alg}} \\ a_1 + a_2\alpha + a_3\alpha^2 & \longmapsto & a_1 + a_2\alpha e^{2\pi i/3} + a_3\alpha^2 e^{4\pi i/3} \end{array}$$

ist ein $\mathbb{Q}$-Homomorphismus. $\varphi(\alpha)$ ist die komplexe Nullstelle $\alpha e^{2\pi i/3}$ des Polynoms $X^3 - 2$. Daher ist $\varphi(\mathbb{Q}(\sqrt[3]{2}))$ nicht in $\mathbb{R}$ enthalten und insbesondere ungleich $\mathbb{Q}(\sqrt[3]{2})$. Die Erweiterung $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ erfüllt daher nicht die Bedingung (i) von Satz 3.64.

Definition 3.67. Eine algebraische Körpererweiterung L/K heißt **normal**, wenn sie die äquivalenten Bedingung von Satz 3.64 erfüllt.

Beispiel 3.68. $\overline{K}/K$ ist normal.

Beweis von Satz 3.64. (i) ⇒ (iii). Sei $f \in K[X]$ irreduzibel und $a \in L$ eine Nullstelle. Wir betrachten den Teilkörper $K(a) \subset L$. Sei b eine weitere Nullstelle von f in $\overline{L}$. Z.z.. $b \in L$. Nach Lemma 3.40 finden wir einen K-Homomorphismus $\sigma : K(a) \to \overline{L}$ mit $\sigma(a) = b$. Nach Satz 3.41 finden wir eine Fortsetzung $\sigma' : L \to \overline{L}$. Nach Voraussetzung gilt $\sigma(L) = L$, also $b = \sigma(a) \in \sigma(L) = L$.

(iii) $\Rightarrow$ (ii) Sei $(a_i)_{i\in I}$ eine Familie von Elementen aus L so dass $L = K((a_i)_{i\in I})$. Sei f_i das Minimalpolynom von a_i über K. Nach Voraussetzung zerfallen alle f_i über L in Linearfaktoren, also ist L Zerfällungskörper der Familie $(f_i)_{i\in I}$.
(ii) $\Rightarrow$ (i) Sei L Zerfällungskörper der Familie $(f_i)_{i\in I}$ und $\sigma : L \to \overline{L}$ ein K-Homomorphismus. Dann ist auch $\sigma(L) \subset \overline{L}$ Zerfällungskörper der Familie (f_i) (beide Körper sind K-isomorph). Aber L und $\sigma(L)$ sind beide Teilkörper in $\overline{L}$ und entstehen durch Adjunktion der Nullstellen der f_i. Also $L = \sigma(L)$. □

Korollar 3.69. *Jede Körpererweiterung vom Grad 2 ist normal.*

Beweis. Sei $[L : K] = 2$. Sei $f \in K[X]$ irreduzibel und $\alpha \in L$ eine Nullstelle. Das Minimalpolynom von α über K hat Grad ≤ 2 und teilt f. Also $\deg f \leq 2$. f spaltet über L den Linearfaktor $X - \alpha$ ab und zerfällt deshalb in Linearfaktoren. □

Korollar 3.70. *Sind $M/L/K$ Körpererweiterungen und M/K normal, so auch M/L.*

Beweis. M ist Zerfällungskörper über K einer Familie $\mathcal{F}$ von Polynomen über K. Fassen wir $\mathcal{F}$ als Familie von Polynomen über L auf, so ist M auch Zerfällungskörper von $\mathcal{F}$ über L. □

Bemerkung 3.71. (Normalität ist nicht transitiv). Sei α die eindeutig bestimmte positive reelle Zahl mit $\alpha^4 = 2$. Die Erweiterungen $\mathbb{Q}(\alpha)/\mathbb{Q}(\alpha^2)$ und $\mathbb{Q}(\alpha^2)/\mathbb{Q}$ haben Grad 2 und sind daher normal. Aber $\mathbb{Q}(\alpha)/\mathbb{Q}$ ist nicht normal. In der Tat hat das Polynom $f(X) = X^4 - 2$ die Nullstelle α, zerfällt aber über $\mathbb{Q}(\alpha)$ nicht in Linearfaktoren, wegen $\mathbb{Q}(\alpha) \subset \mathbb{R}$ und weil f die nicht-reelle Nullstelle $i\alpha$ hat.

Definition 3.72. Sei L/K algebraisch. Eine Körpererweiterung L'/L heißt **normale Hülle** von L/K, wenn

(i) L'/K ist normal.
(ii) kein echter Teilkörper $L \subseteq M \subsetneq L'$ ist normal über K.

Man sagt auch: L'/K ist eine normale Hülle von L/K.

Satz 3.73. *Sei L/K eine algebraische Körpererweiterung.*

(i) *Zu L/K gibt es eine normale Hülle L'/K. Diese ist bis auf (unkanonischen) Isomorphismus über L eindeutig bestimmt.*

(ii) *Ist L/K endlich, so auch L'/K.*

(iii) *Ist M/L algebraisch und M/K normal, so kann man $L \subset L' \subset M$ wählen. Als Teilkörper von M ist L' eindeutig bestimmt. Ist $(\sigma_j)_{j\in J}$ das System aller K-Homomorphismen von L nach M, so gilt*

$$L' = K((\sigma_j(L))_{j\in J}).$$

Man bezeichnet den Körper $L' \subset M$ in (iii) als die **normale Hülle von L in M**.

Beweis. Sei $L = K((a_i)_{i\in I})$ wobei $(a_i)_{i\in I}$ eine Familie von Elementen aus L sei. Sei $f_i \in K[X]$ das Minimalpolynom von a_i über K. Sei M/L ein algebraischer Erweiterungskörper der normal über K ist (z.B. ein algebraischer Abschluss von L, der auch algebraischer Abschluss von K ist). Die f_i haben eine Nullstelle in L also in M und zerfallen daher in $M[X]$ in Linearfaktoren. Sei L' der von den Nullstellen der f_i in M über K erzeugte Teilkörper von K. Es gilt $K \subset L \subset L' \subset M$ und L' ist eine normale Hülle von L über K. Ist nun $L'' \subset M$ eine weitere normale Hülle von L in M, so enthält L'' alle Nullstellen der f_i. Also gilt $L' \subset L''$ und wegen der Minimalität gilt $L' = L''$.

Wir haben somit den ersten Teil von (iii), die Existenzaussage von (i) und die Implikation „Eindeutigkeit in (i) $\Rightarrow$ (ii)“ gezeigt.

Eindeutigkeit in (i): Seien L_1'/L, L_2'/L zwei normale Hüllen von L/K. Dann sind L_1', L_2' Zerfällungskörper der Familie $(f_i)_{i\in I}$ über K, also auch über L. Aus Korollar 3.63 folgt die Existenz eines L-Isomorphismus $L_1' \xrightarrow{\sim} L_2'$.

Zweiter Teil von (iii). Sei also M/L mit M/K normal gegeben und L' die eindeutig bestimmte normale Hülle von L in M.
Z.z. $L' = K(\sigma_j(L)_{j\in J}) \subset M$ wobei σ_j die K-Homomorphismen von L nach M durchläuft. Sei $\sigma : L \to M$ ein K-Homomorphismus. Dieser überführt die Nullstellen der f_i wieder in Nullstellen der f_i. Da L über K von den a_i erzeugt wird und L' von *allen* Nullstellen der f_i, gilt also $\sigma(L) \subset L'$. So erhalten wir $L' \supset K(\sigma_j(L)_{j\in J})$. Sei nun α_i eine beliebige Nullstelle von f_i. Z.z.: $\alpha_i \in \sigma(L)$ für einen K-Homomorphismus $L \to M$. Nach Lemma 3.40 finden wir einen K-Homomorphismus $\bar\sigma : K(a_i) \to L'$ mit $\bar\sigma(a) = \alpha_i$.

Bild:

$$\begin{array}{lccc}
\sigma': & L' & \dashrightarrow & \overline{L'} \\
 & \cup & & \cup \\
 & L & & \\
 & \cup & & \\
\bar\sigma: & K(a_i) & \longrightarrow & L' \\
 & \cup & & \cup \\
 & K & = & K
\end{array}$$

Nach Satz 3.41 finden wir eine Fortsetzung $\sigma' : L' \to \overline{L'}$ von $\bar\sigma$. Nach Satz 3.64(i) gilt $\sigma'(L') = L'$. Die Einschränkung von σ' auf L gibt den gewünschten K-Homomorphismus $\sigma : L \to L' \subset M$ mit $\alpha_i \in \sigma(L)$. □

3.6 Separable Erweiterungen

Erinnerung aus der Linearen Algebra: Seien $f, g \in K[X]$ und L/K ein Erweiterungskörper. Dann gilt

$$\begin{array}{ccc} \mathrm{ggT}_{K[X]}(f,g) & = & \mathrm{ggT}_{L[X]}(f,g) \\ \| & & \| \\ h_1 & & h_2 \end{array}$$

Grund: Es existieren $F_1, G_1 \in K[X]$ mit $F_1 f + G_1 g = h_1$ und $F_2, G_2 \in L[X]$ mit $F_2 f + G_2 g = h_2$. Wegen $h_1 \mid f$ und $h_1 \mid g$ (in $K[X]$ also auch in $L[X]$) gilt $h_1 \mid h_2$ in $L[X]$. Analog: $h_2 \mid h_1$. □

Für $f \in K[X]$ betrachten wir die Nullstellen von f in einem algebraischen Abschluss $\overline{K}$ von K und müssen darauf achten, dass alle Aussagen unabhängig von der Auswahl von $\overline{K}$ sind. Beachte: $\overline{K}$ ist eindeutig bis auf unkanonische Isomorphie. Z.B. ist es sinnvoll zu sagen, dass f nur einfache oder dass f mehrfache Nullstellen in $\overline{K}$ hat.

Definition 3.74. Sei $f = a_n X^n + \cdots + a_0 \in K[X]$. Wir nennen das Polynom

$$f' = n a_n X^{n-1} + \cdots + a_1 \in K[X]$$

die **Ableitung von** f.

Bemerkung 3.75. Es gelten die üblichen Rechenregeln aus der Analysis, z.B. gilt die Produktregel

$$(fg)' = f'g + fg'$$

(einfach nachzurechnen).

Lemma 3.76. *Sei $f \in K[X]$ nicht-konstant.*

(i) *Die mehrfachen Nullstellen von f (in einem algebraischen Abschluss $\overline{K}$ von K) sind genau die gemeinsamen Nullstellen von f und f' d.h. die Nullstellen von* $\mathrm{ggT}(f, f')$.

(ii) *Ist f irreduzibel, so hat f genau dann Mehrfachnullstellen wenn $f' = 0$ gilt.*

Beweis. (i) OE $K = \overline{K}$. Dann gilt $f = (X - a_1) \cdots (X - a_n)$ und die Produktregel liefert das Ergebnis.
(ii) (hier *nicht* OE $K = \overline{K}$). Sei f irreduzibel über K und $a \in \overline{K}$ eine Nullstelle von f. Dann ist f das Minimalpolynom von a über K. Ist a auch Nullstelle von f' so gilt wegen $\deg f' < \deg f$ dass $f' = 0$ gilt. Ist $f' = 0$ so folgt aus (i) dass jede Nullstelle Mehrfachnullstelle ist. □

Definition 3.77. $f \in K[X]$ heißt **separabel**, wenn es keine Mehrfachnullstelle hat.

Korollar 3.78. *Ist* $\mathrm{char}(K) = 0$*, so ist jedes irreduzible Polynom separabel.*

Beweis. Ist $\mathrm{char}(K) = 0$ und $\deg f \geq 1$, so gilt $\deg f' = \deg f - 1$, insbesondere $f' \neq 0$. □

Beispiel 3.79. Über $\mathbb{F}_p(t)$ ist das Polynom $f(X) = X^p - t$ irreduzibel, aber nicht separabel, wegen $f'(X) = pX^{p-1} = 0$.

Bemerkung 3.80. In Charakteristik 0 gibt es bis zu n viele verschiedene n-te Wurzeln. Ist $\mathrm{char}(K) = p > 0$, so existiert zu jedem $a \in K$ höchstens eine p^r-te Wurzel, und genau eine p^r-te Wurzel aus a in $\overline{K}$.

Grund: Gilt $\alpha_1^{p^r} = a = \alpha_2^{p^r}$, so folgt $0 = \alpha_1^{p^r} - \alpha_2^{p^r} = (\alpha_1 - \alpha_2)^{p^r}$, also $\alpha_1 = \alpha_2$.

Satz 3.81. *Sei char* $K = p > 0$ *und* $f \in K[X]$ *irreduzibel. Sei* $r \in \mathbb{N}_0$ *maximal mit der Eigenschaft, dass* f *ein Polynom in* X^{p^r} *ist, d.h. dass es ein* $g \in K[X]$ *mit* $f(X) = g(X^{p^r})$ *gibt. Dann hat jede Nullstelle von* f *die Vielfachheit* p^r *und* g *ist ein irreduzibles separables Polynom. Die Nullstellen von* f *sind genau die* p^r*-ten Wurzeln der Nullstellen von* g*.*

Beweis. Sei $f = \sum_{i=0}^{n} c_i X^i$, $f' = \sum_{i=1}^{n} i c_i X^{i-1}$. Dann gilt

$f' = 0 \iff ic_i = 0,\ i = 1, \ldots, n \iff c_i = 0$ für alle i mit $(p, i) = 1$
$\iff f(X) = h(X^p)$ für ein $h \in K[X]$.

Sei nun g wie im Satz. Dann gilt (obige Überlegung auf g anwenden) $g' \neq 0$ wegen der Maximalität von r. Wäre g reduzibel, so auch $f \Rightarrow g$ irreduzibel und separabel. Seien OE f und g normiert und a_i die Nullstellen von g in $\overline{K}$, d.h.

$$g(X) = \prod_i (X - a_i) \qquad a_i \in \overline{K}.$$

Ist dann $b_i^{p^r} = a_i$ in $\overline{K}$ so gilt

$$f(X) = \prod_i (X^{p^r} - b_i^{p^r}) = \prod_i (X - b_i)^{p^r}.$$

Also haben die Nullstellen von f alle die Vielfachheit p^r und sind genau die p^r-ten Wurzeln der Nullstellen von g. □

Definition 3.82. Sei L/K eine algebraische Körpererweiterung. Ein Element $a \in L$ heißt **separabel über** K, wenn es Nullstelle eines separablen Polynoms über K ist ($\iff$ das Minimalpolynom von a über K ist separabel). L/K heißt **separable Körpererweiterung**, wenn jedes $a \in L$ separabel über K ist. K heißt **vollkommen** (oder perfekt) wenn jede algebraische Erweiterung von K separabel ist.

Korollar 3.83. *Jeder Körper der Charakteristik 0 ist vollkommen.*

Beispiel 3.84. Die Erweiterung $\mathbb{F}_p(t)[X]/(X^p - t)\big/\mathbb{F}_p(t)$ ist nicht separabel.

Definition 3.85. Sei L/K eine algebraische Körpererweiterung und $\overline{K}/K$ ein algebraischer Abschluss. Der **Separabilitätsgrad $[L : K]_s$** von L über K ist durch die Gleichung

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

gegeben.

Bemerkung 3.86. Da zwei algebraische Abschlüsse von K stets K-isomorph sind, hängt die Definition von $[L : K]_s$ nicht von der Auswahl von $\overline{K}$ ab.

Lemma 3.87. *Sei $K \subset K(\alpha) = L$ eine einfache, algebraische Körpererweiterung und $f \in K[X]$ das Minimalpolynom von α über K. Dann gilt*

(i) $[L : K]_s$ = *Anzahl der verschiedenen Nullstellen von f in $\overline{K}$.*

(ii) *α separabel über K* $\iff [L : K] = [L : K]_s$.

(iii) *Gilt* $\mathrm{char}(K) = p > 0$ *und ist p^r die Vielfachheit der Nullstelle α von f, so folgt* $[L : K] = p^r[L : K]_s$.

Beweis. (i) ist eine Umformulierung von Lemma 3.40.
(ii) α separabel $\iff$ f hat keine Mehrfachnullstelle $\iff$ f hat genau $n = \deg f$ Nullstellen $\overset{(i)}{\iff}$ $n = [L : K]_s$. Nach Satz 3.20 gilt aber $n = [L : K]$.
(iii) Dies folgt aus Satz 3.81. □

Satz 3.88. *Für $M/L/K$ (algebraisch) gilt*

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

Beweis. Sei $\overline{K}$ ein algebraischer Abschluss von M. ($\overline{K}$ ist auch algebraischer Abschluss von L und von K). Es gelte

$$\mathrm{Hom}_K(L, \overline{K}) = \{\sigma_i \mid i \in I\},\ \mathrm{Hom}_L(M, \overline{K}) = \{\tau_j \mid j \in J\}.$$

Für jedes $i \in I$ wählen wir gemäß Satz 3.41 einen K-Homomorphismus $\overline{\sigma}_i : \overline{K} \to \overline{K}$, der σ_i fortsetzt. Nach Satz 3.64 sind die $\overline{\sigma}_i$ K-Automorphismen von $\bar{K}$. Es genügt nun, die folgenden Aussagen zu zeigen.

(1) Die Abbildungen $\overline{\sigma}_i \circ \tau_j : M \to \overline{K}$, $i \in I$, $j \in J$, sind paarweise verschieden.
(2) $\mathrm{Hom}_K(M, \overline{K}) = \{\overline{\sigma}_i \circ \tau_j \mid i \in I,\ j \in J\}$.

Zu (1): Sei $\overline{\sigma}_i \circ \tau_j = \overline{\sigma_{i'}} \circ \tau_{j'}$. Wegen $\tau_j|_L = id_L = \tau_{j'}|_L$ gilt $\sigma_i = (\overline{\sigma}_i \circ \tau_j)_{|L} = (\overline{\sigma_{i'}} \circ \tau_{j'})_{|L} = \sigma_{i'}$, also $i = i'$. Also gilt $\overline{\sigma}_i = \overline{\sigma_{i'}}$ und folglich $\tau_j = \tau_{j'}$.
Zu (2): Sei nun $\tau : M \to \overline{K}$ ein K-Homomorphismus. Es gilt $\tau|_L \in \mathrm{Hom}_K(L, \overline{K})$ also $\tau|_L = \sigma_i$ für ein $i \in I$. Dann ist $\overline{\sigma}_i^{-1} \circ \tau \in \mathrm{Hom}_L(M, \overline{K})$, d.h. es existiert ein $j \in J$ mit $\overline{\sigma}_i^{-1} \circ \tau = \tau_j$. Dann gilt $\tau = \overline{\sigma}_i \circ \tau_j$. □

Satz 3.89. *Es sei $K \subset L$ eine endliche Körpererweiterung.*

(i) *Falls* $\mathrm{char}(K) = 0$, *so gilt* $[L : K] = [L : K]_s$.
(ii) *Falls* $\mathrm{char}(K) = p > 0$, *so existiert ein* $r \in \mathbb{N}_0$ *mit* $[L : K] = p^r [L : K]_s$.

Insbesondere teilt $[L : K_s]$ *stets* $[L : K]$.

Beweis. Ist L/K einfach, so folgt dies aus Lemma 3.87. Der allgemeine Fall folgt hieraus mithilfe der Gradformeln Satz 3.88 und Satz 3.13. □

Satz 3.90. *Sei L/K endlich. Dann sind äquivalent*

(i) *L/K ist separabel.*
(ii) *Es gibt über K separable Elemente $a_1, \ldots, a_n$ mit $L = K(a_1, \ldots, a_n)$.*
(iii) $[L : K]_s = [L : K]$.

Beweis. (i) ⇒ (ii) ist trivial.
(ii) ⇒ (iii) $K \subset K(a_1) \subset K(a_1, a_2) \subset \cdots \subset K(a_1, \ldots, a_n) = L$ sind jeweils einfache Erweiterungen und für alle $i \geq 2$ ist a_i ist separabel über $K(a_1, \ldots, a_{i-1})$. Wir erhalten die Gleichung in (iii) aus Lemma 3.87 und den Gradformeln.
(iii) ⇒ (i). Sei $a \in L$ beliebig. Z.z. a separabel $/K$. OE sei $\mathrm{char}(K) = p > 0$. Sei $f \in K[X]$ das Minimalpolynom von a. Nach Satz 3.81 existiert ein $r \in \mathbb{N}_0$ so dass jede Nullstelle von f die Vielfachheit p^r hat. Z.z. $r = 0$. Es gilt nach Lemma 3.87

$$[K(a) : K] = p^r [K(a) : K]_s$$

Wir erhalten

$$\begin{aligned} [L : K]_s = [L : K] &= [L : K(a)][K(a) : K] \\ &\geq [L : K(a)]_s \cdot p^r \cdot [K(a) : K]_s = p^r [L : K]_s, \end{aligned}$$

und es folgt $r = 0$. □

Korollar 3.91. *Sei* $\mathrm{char}(K) = p > 0$ *und* $[L : K]$ *endlich und nicht durch p teilbar. Dann ist L/K separabel.*

Beweis. $[L : K] = p^r [L : K]_s$, also $r = 0$. □

Korollar 3.92. *Sei L/K algebraisch, $(a_i)_{i \in I}$ eine Familie von Elementen aus L und $L = K((a_i)_{i \in I})$. Dann sind äquivalent:*

(i) *L/K ist separabel.*

(ii) *a_i ist separabel über K für alle i.*

Sind die Bedingungen erfüllt, so gilt $[L : K] = [L : K]_s$.

Beweis. Jedes $a \in L$ liegt schon in $K(a_{i_1}, \ldots, a_{i_n})$ für gewisse $i_1, \ldots, i_n \in I$. Daher gilt (i) $\Leftrightarrow$ (ii).

Im Fall $[L : K] < \infty$ folgt $[L : K] = [L : K]_s$. Sei $[L : K] = \infty$, und $E \subset L$ ein Teilkörper mit $[E : K] < \infty$. Dann ist auch E/K separabel, also folgt

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

Da wir E mit beliebig großem Grad $[E : K]$ wählen können, folgt $[L : K]_s = \infty$. □

Korollar 3.93. *Es seien $M/L/K$ algebraische Körpererweiterungen. Dann ist M/K genau dann separabel, wenn M/L und L/K separabel sind.*

Beweis. Die Implikation „M/K separabel $\Rightarrow$ M/L separabel + L/K separabel“ ist offensichtlich. Seien nun M/L und L/K separabel. Sei $a \in M$ beliebig und $f = X^n + c_{n-1}X^{n-1} \cdots + c_0 \in L[X]$ das Minimalpolynom von a über L. Sei $L' = K(c_0, \ldots, c_{n-1})$. Da M/L separabel ist, ist f separabel. Also ist $L'(a)/L'$ separabel und wegen $L' \subset L$ ist auch L'/K separabel. Beide Erweiterungen $L'(a)/L'$ und L'/K sind endlich. Es folgt

$$[L'(a) : K] = [L'(a) : L'] \cdot [L' : K]$$

$$= [L'(a) : L']_s \cdot [L' : K]_s = [L'(a) : K]_s.$$

Also ist $L'(a)/K$ separabel, insbesondere ist a separabel über K. □

Definition 3.94. Ein Körper K heißt **separabel abgeschlossen** wenn es keine nicht-triviale algebraische separable Erweiterung von K gibt.

Beispiel 3.95. Ein algebraisch abgeschlossener Körper ist separabel abgeschlossen.

Satz 3.96. *Sei K ein Körper. Dann gibt es einen separabel abgeschlossenen Erweiterungskörper K^{sep} von K, so dass K^{sep}/K algebraisch und separabel ist. Man nennt K^{sep} einen* **separablen Abschluss** *von K. K^{sep} ist bis auf (unkanonische) K-Isomorphie eindeutig bestimmt.*

Beweis. Sei $\overline{K}$ ein algebraischer Abschluss von K und

$$K^{\text{sep}} = \{a \in \overline{K} \mid a \text{ separabel über } K\}.$$

K^{sep} ist ein Körper (adjungiere alle separablen Elemente aus $\overline{K}$ zu K), algebraisch und separabel über K und besitzt keine separable Erweiterung.
Eindeutigkeit: K^{sep} ist der Zerfällungskörper der Familie der separablen Polynome über K und nach Korollar 3.63 eindeutig bis auf K-Isomorphie. □

Bemerkung 3.97. K vollkommen (z.B. char $K = 0$) $\Rightarrow K^{\text{sep}} = \overline{K}$.

3.7 Endliche Körper

Lemma 3.98. *Sei $\mathbb{F}$ ein endlicher Körper. Dann gilt $\mathrm{char}(\mathbb{F}) = p > 0$ für eine Primzahl p. Der Primkörper von $\mathbb{F}$ ist $\mathbb{F}_p$ und $\mathbb{F}$ enthält genau $q = p^n$ Elemente, wobei $n = [\mathbb{F} : \mathbb{F}_p]$. $\mathbb{F}$ ist Zerfällungskörper des Polynoms $X^q - X$ über $\mathbb{F}_p$. Die Erweiterung $\mathbb{F}/\mathbb{F}_p$ ist daher normal.*

Beweis. $\mathbb{F}$ endlich $\Rightarrow P(\mathbb{F})$ endlich $\Rightarrow P(\mathbb{F}) = \mathbb{F}_p$ für eine Primzahl p. $\mathbb{F}$ endlich $\Rightarrow [\mathbb{F} : \mathbb{F}_p] = n < \infty$ und $\mathbb{F}$ ist n-dimensionaler $\mathbb{F}_p$-Vektorraum, also $\#\mathbb{F} = p^n =: q$. Folglich gilt $\#\mathbb{F}^\times = q - 1$, also $a^{q-1} = 1$ für alle $a \in \mathbb{F}^\times$, und $a^q - a = 0$ für alle $a \in \mathbb{F}$. Das Polynom $X^q - X$ hat also über $\mathbb{F}$ genau q verschiedene Nullstellen, d.h. es zerfällt vollständig in Linearfaktoren. Also ist $\mathbb{F}$ ein Zerfällungskörper von $X^q - X$ über $\mathbb{F}_p$. □

Satz 3.99. *Sei p eine Primzahl. Dann existiert zu jedem $n \in \mathbb{N}$ ein Erweiterungskörper $\mathbb{F}_q/\mathbb{F}_p$ mit $q = p^n$ Elementen. $\mathbb{F}_q$ ist als Zerfällungskörper des Polynoms $X^q - X$ bis auf Isomorphie eindeutig bestimmt, $\mathbb{F}_q$ besteht genau aus den (q vielen) Nullstellen von $X^q - X$.*

Jeder endliche Körper der Charakteristik p ist zu genau einem Körper des Typus $\mathbb{F}_q$ isomorph.

Beweis. Sei $f = X^q - X$. Wegen $f' = -1$ hat f keine Mehrfachnullstellen, also genau q Nullstellen in einem algebraischen Abschluss $\overline{\mathbb{F}}_p$ von $\mathbb{F}_p$. Sind dann $a, b \in \overline{\mathbb{F}}_p$ zwei Nullstellen von f, so gilt $(a \pm b)^q = a^q \pm b^q = a \pm b$, so dass $a \pm b$ wieder Nullstelle von f ist. Für $b \neq 0$ gilt $(ab^{-1})^q = a^q(b^q)^{-1} = ab^{-1}$, also bilden die Nullstellen von f in $\overline{\mathbb{F}}_p$ einen Körper mit q Elementen, den in $\overline{\mathbb{F}}_p$ gebildeten Zerfällungskörper von $X^q - X$. Die Eindeutigkeitsaussagen folgen aus Lemma 3.98. □

Warnung: Es gilt zwar $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ aber für $n > 1$ gilt stets

$$\mathbb{F}_{p^n} \neq \mathbb{Z}/p^n\mathbb{Z}.$$

Links steht ein Körper und rechts ein nicht nullteilerfreier Ring!

Korollar 3.100. *Man bette die Körper $\mathbb{F}_q$, $q = p^n$, $n \in \mathbb{N}$, in einen fest gewählten algebraischen Abschluss $\overline{\mathbb{F}}_p$ von $\mathbb{F}_p$ ein. Es ist dann $\mathbb{F}_q \subset \mathbb{F}_{q'}$ für $q = p^n$, $q' = p^{n'}$, äquivalent zu $n \mid n'$. Die Erweiterungen des Typs $\mathbb{F}_q \subset \mathbb{F}_{q'}$ sind bis auf Isomorphie die einzigen Erweiterungen zwischen endlichen Körpern der Charakteristik p.*

Beweis. Es gelte $\mathbb{F}_q \subset \mathbb{F}_{q'}$ und $m = [\mathbb{F}_{q'} : \mathbb{F}_q]$. Dann gilt $p^{n'} = \#\mathbb{F}_{q'} = (\#\mathbb{F}_q)^m = p^{nm}$, also gilt $n \mid n'$. Gilt umgekehrt $n' = n \cdot m$, so folgt für $a \in \overline{\mathbb{F}}_p$ aus $a^q = a$ stets $a^{q'} = a^{q^m} = a$, also $a \in \mathbb{F}_{q'}$, d.h. $\mathbb{F}_q \subset \mathbb{F}_{q'}$.
Ist nun $\mathbb{F}'/\mathbb{F}$ eine Erweiterung endlicher Körper der Charakteristik p, so kann man die Inklusion $\mathbb{F}_p \subset \mathbb{F}$ zuerst zu einer Inklusion $\mathbb{F} \to \overline{\mathbb{F}}_p$ und diese dann wieder zu einer Inklusion $\mathbb{F}' \subset \overline{\mathbb{F}}_p$ fortsetzen und ist im betrachteten Fall. □

Korollar 3.101. *Jede algebraische Erweiterung eines endlichen Körpers ist separabel und normal. Insbesondere sind endliche Körper vollkommen.*

Beweis. Sei $K/\mathbb{F}$ algebraisch. Ist K ebenfalls endlich, $K = \mathbb{F}_q$ mit $q = p^n$, so ist K als Zerfällungskörper des separablen Polynoms $X^q - X$ normal und separabel. Im allgemeinen Fall schöpfen wir K durch endliche Erweiterungen von $\mathbb{F}$ aus. □

Erinnerung: Für jede endliche Erweiterung $K/\mathbb{F}_p$ haben wir den Frobenius-Automorphismus

$$\sigma : K \longrightarrow K,\ a \longmapsto a^p.$$

Analog betrachten wir für jede endliche Erweiterung $K/\mathbb{F}_q$, $q = p^r$, den **relativen Frobenius-Automorphismus** über $\mathbb{F}_q : \sigma^r : K \to K$, $a \mapsto a^q$.

Satz 3.102. *Sei $\mathbb{F}_q$ ein endlicher Körper, $q = p^r$, sowie $\mathbb{F}/\mathbb{F}_q$ eine endliche Körpererweiterung vom Grad n. Dann ist $\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F})$ eine zyklische Gruppe der Ordnung n und wird vom relativen Frobeniusautomorphismus $\sigma^r : \mathbb{F} \to \mathbb{F}$, $a \mapsto a^q$, erzeugt.*

Beweis. Da $\mathbb{F}/\mathbb{F}_q$ normal ist, gilt $\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}) = \mathrm{Hom}_{\mathbb{F}_q}(\mathbb{F}, \overline{\mathbb{F}}_q)$ ($\overline{\mathbb{F}}_q$ ein algebraischer Abschluss von $\mathbb{F}_q$). Da $\mathbb{F}/\mathbb{F}_q$ separabel ist, gilt

$$\#\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}) = [\mathbb{F} : \mathbb{F}_q]_s = [\mathbb{F} : \mathbb{F}_q] = n.$$

Wegen $a^q = a$ für alle $a \in \mathbb{F}_q$ gilt $\sigma^r \in \mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F})$. Es genügt daher zu zeigen, dass die Ordnung $\mathrm{ord}(\sigma^r)$ in $\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F})$ gleich n ist. Nach Korollar 1.48 gilt $\mathrm{ord}(\sigma^r) \mid n$. Wäre nun $\mathrm{ord}(\sigma^r) < n$, so wäre $\sigma^e = 1$ auf $\mathbb{F}$ für ein $e < rn$. Jedes Element von $\mathbb{F}$ wäre somit Nullstelle des Polynoms $X^{p^e} - X$, dieses hat aber nur $p^e < p^{rn} = \#\mathbb{F}$ viele Nullstellen. Widerspruch. □

Schließlich zeigen wir:

Satz 3.103. *Sei $q = p^n$. Die multiplikative Gruppe $\mathbb{F}_q^\times$ von $\mathbb{F}_q$ ist zyklisch (von der Ordnung $q - 1$).*

Bemerkung 3.104. Dieser Satz geht (im Fall $n = 1$) schon auf Gauß zurück und lautet im zahlentheoretischen Gewand: Sei p eine Primzahl. Dann gibt es eine natürliche Zahl n (eine „primitive Wurzel modulo p“), deren Potenzen alle Restklassen $\neq 0$ modulo p durchläuft.

Satz 3.103 folgt aus Spezialfall aus dem folgenden

Satz 3.105. *Sei K ein Körper und $H \subset K^\times$ eine endliche Untergruppe. Dann ist H zyklisch.*

Beweis. Nach dem Hauptsatz über endlich erzeugte abelsche Gruppen gilt

$$H \cong \mathbb{Z}/a_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/a_r\mathbb{Z},$$

mit $a_1 \mid a_2 \mid \cdots \mid a_r$ und $a_1 \cdots a_r = h := \#H$. Insbesondere gilt $x^{a_r} = 1$ für jedes der h vielen Elemente $x \in H$. Da die Gleichung $X^{a_r} - 1 = 0$ in K höchstens a_r viele Nullstellen hat, folgt $h \leq a_r$ und wegen $h = a_1 \cdots a_r$ folgt $a_r = h$, $a_1 = \ldots = a_{r-1} = 1$, und H ist zyklisch. □

3.8 Rein inseparable Erweiterungen

Sei in diesem Abschnitt K stets ein Körper mit $\mathrm{char}(K) = p > 0$.

Definition 3.106. $f \in K[X]$ heißt **rein inseparabel**, wenn es genau eine Nullstelle in $\overline{K}$ hat.

Lemma 3.107. *Ein Polynom ist genau dann rein inseparabel, wenn es bis auf einen Faktor in $K^\times$ eine Potenz eines Polynoms der Form $X^{p^n} - c$, $n \in \mathbb{N}_0$, $c \in K$, ist.*

Beweis. Sei f rein inseparabel. Ohne Einschränkung sei f normiert. Sei α die Nullstelle von f in $\overline{K}$ und f_α das Minimalpolynom von α über K. Dann gilt $f_\alpha \mid f$ und induktiv $f = (f_\alpha)^m$ für ein $m \in \mathbb{N}$. Nach Satz 3.81 ist $f_\alpha(X) = g(X^{p^n})$ für ein separables, irreduzibles Polynom $g \in K[X]$ und die Nullstellen von f_α sind die p^n-ten Wurzeln aus den Nullstellen von g. Weil f_α genau eine Nullstelle hat, gilt dies nach Bemerkung 3.80 auch für g und weil g separabel ist folgt $g = X - c$ für ein $c \in K$. Umgekehrt hat das Polynom $(X^p - c)^m$ für $n \in \mathbb{N}_0$, $m \in \mathbb{N}$, $c \in K$, genau eine Nullstelle, nämlich die eindeutig bestimmte p^n-te Wurzel aus c in $\overline{K}$. □

Definition 3.108. Sei L/K eine algebraische Körpererweiterung. $\alpha \in L$ heißt **rein inseparabel** über K, wenn α Nullstelle eines rein inseparablen Polynoms über K ist; äquivalent: wenn das Minimalpolynom von α die Form $X^{p^n} - c$, $n \in \mathbb{N}_0$, $c \in K$, hat. L/K heißt rein inseparabel, wenn jedes $\alpha \in L$ rein inseparabel über K ist.

Lemma 3.109. *Jede rein inseparable Erweiterung ist normal.*

Beweis. Sei $L = K((a_i)_{i\in I})$ und sei f_i das Minimalpolynom von a_i über K. Da die a_i rein inseparabel sind, sind die f_i von der Form $f_i = (X^{p^{n_i}} - c_i)$. In L gilt daher $f_i = (X - a_i)^{p^{n_i}}$ und f_i zerfällt daher vollständig in Linearfaktoren. Daher ist L Zerfällungskörper der Familie $(f_i)_{i\in I}$. □

Satz 3.110. *Sei L/K algebraisch. Es sind äquivalent:*

(i) *L/K ist rein inseparabel.*
(ii) *$L = K((a_i)_{i\in I})$ mit a_i rein inseparabel über K für alle $i \in I$.*
(iii) $[L : K]_s = 1$.
(iv) *Zu jedem $a \in L$ gibt es ein $n \in \mathbb{N}_0$ mit $a^{p^n} \in K$.*

Beweis. (i) ⇒ (ii) ist trivial.
(ii) ⇒ (iii) Z.z. $\mathrm{Hom}_K(L, \overline{K})$ besteht aus genau einem Element. Sei $\varphi : L \to \overline{K}$ ein K-Homomorphismus. Wegen $L = K((a_i)_{i\in I})$ ist φ schon durch seine Werte auf den a_i festgelegt. Nun gilt $\varphi(a_i)$ ist eine Nullstelle des Minimalpolynoms von a_i über K. Dieses hat aber nur eine Nullstelle, also $\varphi(a_i) = a_i$ für alle $i \in I$. Damit ist φ festgelegt.
(iii) ⇒ (iv) Sei $a \in L$ beliebig. Wegen $1 = [L : K]_s = [L : K(a)]_s \cdot [K(a) : K]_s$ gilt $[K(a) : K]_s = 1$. Also hat das Minimalpolynom von a genau eine Nullstelle in $\overline{K}$,

ist also von der Form $X^{p^n} - c$. Deshalb gilt $a^{p^n} \in K$.
(iv) $\Rightarrow$ (i) Gilt $a^{p^n} = c \in K$, so folgt $f_\alpha \mid (X^{p^n} - c)$. Also hat f_α genau eine Nullstelle in $\overline{K}$ und a ist rein inseparabel. □

Bemerkung 3.111. Wegen $[L : K] = p^?[L : K]_s$ hat eine endliche rein inseparable Erweiterung stets einen p-Potenzgrad.

Korollar 3.112. *Ist L/K sowohl separabel, als auch rein inseparabel, so gilt $L = K$.*

Beweis. $[L : K] = [L : K]_s = 1$ □

Korollar 3.113. *Seien $M/L/K$ algebraische Körpererweiterungen. Dann ist M/K genau dann rein inseparabel wenn M/L und L/K rein inseparabel sind.*

Beweis. $[M : K]_s = [M : L]_s \cdot [L : K]_s$. □

Satz 3.114. *Sei L/K eine algebraische Körpererweiterung. Dann existiert ein eindeutig bestimmter Zwischenkörper $K \subset K_s \subset L$, so dass L/K_s rein inseparabel und K_s/K separabel ist. Es ist K_s/K die separable Hülle von K in L, d.h.*

$$K_s = \{a \in L \mid a \text{ separabel über } K\},$$

und es gilt $[L : K]_s = [K_s : K]$. Ist L/K normal, so auch K_s/K.

Beweis. Setze $K_s = \{a \in L \mid a \text{ separabel über } K\}$. Nach Korollar 3.92 ist für a, b separabel die Erweiterung $K(a, b)/K$ separabel, also $K(a, b) \subset K_s$. Daher ist K_s ein Körper und die maximale separable Teilerweiterung von L/K. Sei nun $a \in L$ und $f \in K_s[X]$ das Minimalpolynom von a über K_s. Nach Satz 3.81 gilt $f(X) = g(X^{p^r})$ für ein separables irreduzibles Polynom $g \in K_s[X]$ und $r \geq 0$ und g ist das Minimalpolynom von $c = a^{p^r}$. Das Element c ist separabel über K_s, also separabel über K, also $c \in K_s$ und wir schließen nach Satz 3.110 dass L/K_s rein inseparabel ist. Wir erhalten

$$\begin{aligned} [L : K]_s &= [L : K_s]_s \cdot [K_s : K]_s \\ &= 1 \cdot [K_s : K]. \end{aligned}$$

Sei nun K_s' ein weiterer Zwischenkörper mit L/K_s' rein inseparabel und K_s'/K separabel. Dann gilt $K_s' \subset K_s$ und K_s/K_s' ist als Teilerweiterung von L/K_s' rein inseparabel. Da K_s/K separabel ist, folgt dass auch K_s/K_s' separabel ist. Wir schließen $K_s = K_s'$.

Sei nun L/K normal. Sei $\sigma : K_s \to \overline{L}$ ein K-Homomorphismus. σ setzt sich zu einem K-Homomorphismus $\sigma' : L \to \overline{L}$ fort und σ' beschränkt sich zu einem Automorphismus $\sigma' : L \to L$. Wegen der Eindeutigkeit von K_s gilt $\sigma'(K_s) = K_s$. □

Satz 3.115. *Sei L/K eine normale algebraische Erweiterung. Dann existiert ein eindeutig bestimmter Zwischenkörper $K \subset K_i \subset L$ so dass L/K_i separabel und K_i/K rein inseparabel ist.*

Beweis. Es gilt $\mathrm{Hom}_K(L, \overline{L}) = \mathrm{Aut}_K(L)$. Setze

$$K_i = \{a \in L \mid \sigma(a) = a \text{ für alle } \sigma \in \mathrm{Aut}_K(L)\}.$$

K_i ist ein Körper (trivial). Sei $\sigma : K_i \to \overline{L}$ ein K-Homomorphismus. Dann setzt sich σ zu $\sigma : L \to \overline{L}$ fort und deshalb gilt $\sigma|_{K_i} = \mathrm{id}_{K_i}$. Folglich $\#\mathrm{Hom}_K(K_i, \overline{L}) = 1$ und $[K_i : K]_s = 1$. Also ist K_i/K rein inseparabel. Ist $K \subset M \subset L$ ein Zwischenkörper mit M/K rein inseparabel, so gilt $\#\mathrm{Hom}_K(M, \overline{L}) = 1$, also $\sigma|_M = \mathrm{id}_M$ für alle $\sigma : L \to L$. Definitionsgemäß folgt $M \subset K_i$ und K_i ist die maximale rein inseparable Teilerweiterung von L/K. Bleibt z.z., dass $[L : K_i]$ separabel ist. Sei $a \in L$. Für $\sigma \in \mathrm{Aut}_K(L)$ ist $\sigma(a)$ Nullstelle des Minimalpolynoms von a über K, d.h. es existieren nur endlich viele Möglichkeiten. Sei $\sigma_1, \ldots, \sigma_r \in \mathrm{Aut}_K(L)$ so dass $\sigma_1(a), \ldots, \sigma_r(a)$ paarweise verschieden sind und r sei maximal möglich gewählt. Wegen $\mathrm{id} \in \mathrm{Aut}_K(L)$ kommt a unter den $\sigma_i(a)$ vor. Jedes $\sigma \in \mathrm{Aut}_K(L)$ induziert eine bijektive Selbstabbildung auf der Menge $\{\sigma_1(a), \ldots, \sigma_r(a)\}$. Sei

$$f = \prod_{i=1}^{r} (X - \sigma_i(a)) = X^r + c_{r-1}X^{r-1} + \cdots + c_0.$$

Dann gilt $\sigma(c_i) = c_i$ für alle $\sigma \in \mathrm{Aut}_K(L)$ und jedes i, $0 \le i \le r-1$. Definitionsgemäß gilt $f \in K_i[X]$ und f ist separabel. Also ist a separabel über $K_i \Rightarrow L/K_i$ separabel. Bleibt die Eindeutigkeit von K_i. Habe K_i' die gleiche Eigenschaft. Dann gilt $K_i' \subset K_i$ und K_i/K_i' ist als Teilerweiterung von L/K_i separabel. Wegen K_i/K rein inseparabel ist auch K_i/K_i' rein inseparabel. Es folgt $K_i = K_i'$. □

3.9 Der Satz vom primitiven Element

Satz 3.116. *Sei L/K eine endliche, separable Erweiterung. Dann existiert ein $a \in L$ mit $L = K(a)$.*

Beweis. 1. Fall. K endlich. Dann ist auch L endlich. Ist $a \in L^\times$ ein Erzeuger dieser zyklischen Gruppe, so erzeugt a auch L über K.
2. Fall. $\#K = \infty$. Per Induktion können wir annehmen, dass L über K durch zwei Elemente erzeugt wird, d.h. $L = K(a, b)$. Sei $n = [L : K] = [L : K]_s$ und sei $\mathrm{Hom}_K(L, \overline{K}) = \{\sigma_1, \ldots, \sigma_n\}$. Wir betrachten das Polynom

$$P = \prod_{i \neq j} [(\sigma_i(a) - \sigma_j(a)) + (\sigma_i(b) - \sigma_j(b))X]$$

Für $i \neq j$ ist $\sigma_i(a) \neq \sigma_j(a)$ oder $\sigma_i(b) \neq \sigma_j(b)$, also ist keiner der Faktoren $0 \Rightarrow P \neq 0 \in \overline{K}[X]$. Wegen $\#K = \infty$ gibt es ein $c \in K$ mit $P(c) \neq 0$. Dann gilt

$$\sigma_i(a) + c\sigma_i(b) \neq \sigma_j(a) + c\sigma_j(b)$$

für $i \neq j$. Beachte: wegen $c \in K$ gilt

$$\sigma_i(a) + c\sigma_i(b) = \sigma_i(a + cb) \in \overline{K}.$$

Sei f das Minimalpolynom von $a + cb$ über K. Dann sind $\sigma_i(a + cb)$, $i = 1, \ldots, n$, paarweise verschiedene Nullstellen von f, also $\deg f \geq n \Rightarrow$

$$[K(a + cb) : K] \geq n = [L : K]$$

und folglich $L = K(a + bc)$. □