

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	5
1.3	Zyklische Gruppen	9
2	Ringe und Polynome	11
2.1	Ringe, Polynomringe in einer Variablen	11
2.2	Faktorielle Ringe	13
2.3	Der Satz von Gauß	16
2.4	Irreduzibilitätskriterien	21
2.5	Verallgemeinerte Polynomringe	23
3	Algebraische Körpererweiterungen	26
3.1	Charakteristik	26
3.2	Endliche und algebraische Körpererweiterungen	27
3.3	Algebraischer Abschluss	33
3.4	Ganze Ringerweiterungen	37
3.5	Zerfällungskörper	40
3.6	Separable Erweiterungen	44
3.7	Endliche Körper	49
3.8	Rein inseparable Erweiterungen	51
3.9	Der Satz vom primitiven Element	54

4	Galoistheorie	55
4.1	Galois-Erweiterungen	55
4.2	Die Galoisgruppe einer Gleichung	61
4.3	Die allgemeine Gleichung über einem Körper	66
4.4	Symmetrische Polynome	68
4.5	Einheitswurzelkörper	70
4.6	Lineare Unabhängigkeit von Charakteren	74
4.7	Norm und Spur	76
4.8	Zyklische Erweiterungen	79
5	Mehr Gruppentheorie	80
5.1	Gruppenoperationen	80
5.2	p -Gruppen	84
5.3	Sylow-Gruppen	85
5.4	Auflösbare Gruppen	88
6	Anwendungen der Galoistheorie	90
6.1	Auflösbarkeit von Gleichungen	90
6.2	Konstruktionen mit Zirkel und Lineal	93
6.3	Die Cardanosche Formel	95
6.4	Die Transzendenz von π	98
6.5	Der Fundamentalsatz der Algebra	101
7	Transzendente Erweiterungen	103
7.1	Transzendenzbasen	103
7.2	Rein transzendente Erweiterungen	106
7.3	Der Satz von Lüroth	107

1 Gruppentheorie

1.1 Definitionen

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

- (i) Assoziativität: $(ab)c = a(bc)$, $\forall a, b, c \in M$
- (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 $m_1, \dots, m_n \in M$ 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 $\text{Gl}_n(k)$ und $\text{Sl}_n(k)$ 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 $\varphi : G \rightarrow G'$ heißt **Monoidhomomorphismus** wenn

- (i) $\varphi(e) = e'$.
- (ii) $\varphi(ab) = \varphi(a)\varphi(b) \quad \forall a, b \in G$.

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

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

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

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

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

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

Für $g \in G$ definieren wir $\pi_g : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ 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 $\varphi : G \rightarrow \mathfrak{S}_n$ durch $\varphi(g) = \pi_g$.

Behauptung: $\varphi : G \rightarrow \mathfrak{S}_n$ ist ein Gruppenhomomorphismus.

Nach Definition gilt $(hh')g_i = g_{\varphi(hh')(i)}$, es gilt aber auch

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

Also $\varphi(hh') = \varphi(h)\varphi(h')$, was die Behauptung zeigt.

Behauptung: $\varphi : G \rightarrow \mathfrak{S}_n$ ist injektiv.

Sei $\varphi(g) = \text{id}$. 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 $G \rightarrow G$, $g \mapsto g^n$, ein Gruppenhomomorphismus.

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

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

ist ein Gruppenhomomorphismus. Dieser ist genau dann trivial (d.h. konstant $= \text{id}_G$), 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. \square

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

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

Beweis. (i) \Rightarrow (ii) ist trivial wegen $H \neq \emptyset$.

(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 $bH \subset aH$. \square

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 $G \rightarrow G$, $a \mapsto a^{-1}$ 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. \square

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: $\text{ord}(G)$. (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*

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

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

Notation: $H \triangleleft G$ 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 $aH = G - H = Ha$. \square

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

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

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

also $aha^{-1} \in \text{Kern } f$. \square

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

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

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

die **Faktorgruppe** von G nach H .

Verifikation:

- Die Verknüpfung ist wohldefiniert: Sei $a_1 = a_2h$, $a'_1 = a'_2h'$, $h, h' \in H$. Dann gilt $a_1a'_1 = a_2ha'_2h' = a_2a'_2 \cdot \underbrace{(a'_2)^{-1}ha'_2}_{\in H} h'$, also $a_1a'_1H = a_2a'_2H$.

(Hier haben wir $H \triangleleft G$ benutzt!)

- neutrales Element: eH .
- Inverses zu aH ist $a^{-1}H$.

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

Satz 1.31. Sei $H \triangleleft G$ und $\phi: G \rightarrow G/H$ die kanonische Projektion. Dann induziert die Zuordnung $U \mapsto \phi^{-1}(U)$ 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 $U \triangleleft G/H$, 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 $\phi^{-1}(U) \triangleleft G$ und $u \in U$, $g \in G/H$ und wählen wir $u', g' \in G$ mit $\phi(u') = u$, $\phi(g') = g$,

so gilt

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

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

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

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

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

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

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

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

Beweis. Sei H_1 Normalteiler. Dann liegt für $h_1, h'_1 \in H_1, h_2, h'_2 \in H_2$:

$$(h_1 h_2)(h'_1 h'_2) = h_1 \underbrace{(h_2 h'_1 h_2^{-1})}_{\in H_1} h_2 h'_2$$

wieder in $H_1 H_2$. Mit $h_1 h_2$ liegt auch $(h_1 h_2)^{-1} = h_2^{-1} h_1^{-1} = \underbrace{h_2^{-1} h_1^{-1} h_2}_{\in H_1} h_2^{-1}$ in $H_1 H_2$.

Der Fall $H_2 \triangleleft G$ läuft analog. Schließlich gilt falls $H_1, H_2 \triangleleft G$, dass

$$g H_1 H_2 g^{-1} = (g H_1 g^{-1})(g H_2 g^{-1}) = H_1 H_2. \quad \square$$

Lemma 1.35. Ist $N \triangleleft G$ 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 $hnh^{-1} \in H \cap N$. \square

Satz 1.36 (1. Isomorphiesatz). Sei G eine Gruppe, $H \subset G$ eine Untergruppe und $N \triangleleft G$ 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 $\text{Kern}(f) = H \cap N$. Der Homomorphiesatz impliziert einen natürlichen Isomorphismus $H/\text{Kern}(f) \xrightarrow{\sim} \text{Bild}(f)$, also genau

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

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 $p : G \rightarrow G/H$. Es gilt $N \subset \text{Kern}(p) = H$. Daher erhalten wir einen induzierten surjektiven Homomorphismus $\pi : G/N \rightarrow G/H$ mit $\text{Kern}(\pi) = H/N$. Der Homomorphiesatz impliziert das Resultat. \square

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 $\underbrace{n + \dots + n}_{m\text{-mal}} \in H$, also $nm \in H$ für alle $m \in \mathbb{N}$. Das gleiche gilt für $-nm$, also:

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

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 $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}$, $a \mapsto na$. Es gilt: $\text{Kern}(\varphi) = 0$, $\text{Bild}(\varphi) = n\mathbb{Z}$. Nach dem Homomorphiesatz induziert φ einen Isomorphismus $\mathbb{Z} \xrightarrow{\sim} n\mathbb{Z}$. \square

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

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

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. \square

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. Das folgt aus Lemma 1.40 mit $X = \{x\}$. \square

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

Korollar 1.44. Sei G eine zyklische Gruppe. Dann gilt

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

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

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

Der Homomorphiesatz liefert nun das Ergebnis. \square

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

Beweis. Faktorgruppe: Sei $\varphi : \mathbb{Z} \rightarrow G$ 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 $\varphi : \mathbb{Z} \rightarrow G$ 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. \square

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

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

Lemma 1.47.

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

Beweis. Es gilt

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

und falls $\text{ord}(a) = \infty$ 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 $\text{ord}(a) = \infty$.

Nun sei $\text{ord}(a) = n \in \mathbb{N}$. Dann sind (benutze das gleiche Argument) die Elemente $\{a, a^2, \dots, a^n = e\}$ paarweise verschieden und diese bilden die Gruppe $\langle a \rangle$. \square

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

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

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

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

für alle $a \in G$.

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

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

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

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

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

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 $f : R \rightarrow R'$ 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 $\phi: R \rightarrow R/\mathfrak{a}$, $a \mapsto a + \mathfrak{a}$ ist ein surjektiver Ringhomomorphismus.

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

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

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 $f: R \rightarrow S$ 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 $f: R \rightarrow S$ ein Ringhomomorphismus mit $S \neq 0$. Wegen $0 \neq 1$ in S ist $\text{Kern}(f) \subset R$ ein Ideal $\neq R \Rightarrow \text{Kern}(f) = 0$.

(iii) \Rightarrow (i). Sei $x \in R$ keine Einheit. Dann ist $(x) \neq R$, also $S = R/(x)$ nicht der Nullring. Es gilt $x \in \text{Kern}(\phi: R \rightarrow R/(x))$, also $x = 0$. Daher ist R Körper. \square

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) $xy \in \mathfrak{p} \iff \overline{xy} = 0$ 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. \square

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

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

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 $\Rightarrow (x) \subsetneq R$. \square

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 $\iff (\pi)$ ist Primideal

irreduzibel \iff 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: $a \hat{=} b$.

Lemma 2.15. Für $a, b \in R$ sind äquivalent:

- (i) $a \hat{=} b$.
- (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 $\bar{a}\bar{b} = 0$ im nullteilerfreien Faktoring $R/(\pi)$. Also $\bar{a} = 0$ oder $\bar{b} = 0$. Sei OE $\bar{a} = 0$, 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 $p_i \hat{=} q_i$, $i = 1, \dots, r$.

Beweis. Da p_1 prim ist folgt aus $p_1 \mid a = q_1 \cdots q_s$, 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

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

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 $q_{r+1} \cdots q_s$ 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 $\pi \hat{=} a_i$ für ein i oder $\pi \hat{=} b_j$ 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. \square

Beispiele faktorieller Ringe

Definition 2.21. Ein nullteilerfreier Ring R heißt **euklidischer Ring**, wenn es eine Abbildung $v : R \setminus \{0\} \rightarrow \mathbb{N}_0$ 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. \square

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 $a = \varepsilon_a \prod_{i \in I} p_i^{v_i(a)}$ 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

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

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

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

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

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

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

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

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 Hauptidealringe 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 $f = a_r T^r + \dots + a_0$, $g = b_s T^s + \dots + b_0$ 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 $\deg(fg) = r + s$. \square

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

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

Quotientenkörper: Sei R ein nullteilerfreier Ring. Wir orientieren uns am Übergang $\mathbb{Z} \leadsto \mathbb{Q}$ 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:

$$\begin{aligned} b_2 a_3 b_1 = b_3 a_2 b_1 &= b_3 b_2 a_1 \\ &= b_2 a_1 b_3 \\ \text{Kürzen gibt: } a_3 b_1 &= a_1 b_3. \end{aligned}$$

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)

$$(a_1b_2 + a_2b_1, b_1b_2) \sim (a'_1b_2 + a_2b'_1, b'_1b_2)$$

wegen

$$\begin{aligned} b'_1b_2(a_1b_2 + a_2b_1) &= b'_1a_1b_2^2 + b_1b'_1b_2a_2 \\ &= b_1a'_1b_2^2 + b_1b'_1b_2a_2 = b_1b_2(a'_1b_2 + a_2b'_1) \end{aligned}$$

• $Q(R)$ 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

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

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 höchstens $\deg f$ viele Nullstellen (siehe LA1) und die natürliche Abbildung $R \rightarrow Q(R)$ ist injektiv. \square

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 der nullteilerfreie Ring R eingebettet werden kann. In der Sprache der Universaleigenschaften:

Satz 2.33. Sei R ein nullteilerfreier Ring und $f : R \rightarrow K$ 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

$$\begin{array}{ccc} R & \xrightarrow{f} & K \\ \text{kan} \downarrow & \nearrow \phi & \\ Q(R) & & \end{array}$$

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 Assoziiiertheit, 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: $\frac{a}{b} \in R \subset Q(R) \iff v_i\left(\frac{a}{b}\right) \geq 0$ 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 $p_i \hat{=} p$. 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:

$$v_3\left(\frac{2}{9}\right) = -2, \quad v_2\left(\frac{2}{9}\right) = 1, \quad v_p\left(\frac{2}{9}\right) = 0 \text{ für jede Primzahl } p \neq 2, 3.$$

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

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

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

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

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

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 $fg \notin \text{Kern}(\phi)$, $v_p(fg) = 0$. \square

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 $f, g \in R[T]$. \square

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 $i \in I$. \square

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 $p \in R$:

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

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 $p \in R$:

$$\begin{array}{rclclcl} v_p(\tilde{f}) & = & v_p(c) + & v_p(\tilde{f}_1) & + \dots + & v_p(\tilde{f}_r) \\ \parallel & & & \parallel & & \parallel \\ 0 & & & 0 & & 0 \end{array}$$

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

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. \square

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 $f = a_n T^n + \dots + a_0 \in R[T]$ primitiv vom Grad > 0 . Sei $p \in R$ ein Primelement mit

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

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

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

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

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

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

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

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

irreduzibel in $\mathbb{Q}[T]$:

Offenbar ist $f = f(T)$ dann und nur dann irreduzibel, wenn $f(T+1)$ irreduzibel ist. Nun gilt

$$\begin{aligned} f(T+1) &= \frac{(T+1)^p - 1}{(T+1) - 1} \\ &= \frac{T^p + \binom{p}{1}T^{p-1} + \dots + \binom{p}{p-1}T + 1 - 1}{T} \\ &= T^{p-1} + \binom{p}{1}T^{p-2} + \dots + \binom{p}{p-1}. \end{aligned}$$

Nun gilt: $p^2 \nmid \binom{p}{p-1} = p$ und $p \mid \binom{p}{i}$ für $i = 1, \dots, p-1$. 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:

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

Dann ist $R/(p) = k[T_1, \dots, T_{n-1}]$ 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 nichttriviale Zerlegung $f = gh$ in $R[T]$ und wegen der Primitivität von f gilt $\deg(g) > 0$, $\deg(h) > 0$. 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 $Q(R)[T]$. \square

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:

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

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

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

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

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

durch

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

• Noch allgemeiner: Sei I eine (Index)Menge und $M = (\mathbb{N}_0)^{(I)} = \{\phi_i : I \rightarrow \mathbb{N}_0, \phi(i) = 0 \text{ f. a. } i\}$.

Wir ordnen formal jedem $i \in I$ eine Variable X_i zu. Dann gilt

$$R[(\mathbb{N}_0)^{(I)}] \xrightarrow{\sim} R[(X_i)_{i \in I}]$$

$$(r_a)_{a \in \mathbb{N}_0^{(I)}} \longrightarrow \sum_{a \in \mathbb{N}_0^{(I)}} r_a \prod_{i \in I} X_i^{a_i},$$

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 $\phi : R \rightarrow R'$ ein Ringhomomorphismus und $\sigma : M \rightarrow (R', \cdot)$ ein Monoidhomomorphismus. Dann gibt es einen eindeutig bestimmten Ringhomomorphismus $\Phi : R[M] \rightarrow R'$ 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

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

Umgekehrt kann man diese Gleichung zur Definition machen.

Nachzuprüfen: Φ ist Ringhomomorphismus. Dies folgt, weil ϕ Ring- und σ Monoidhomomorphismus ist. \square

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

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

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

zurückbekommen. \square

Definition 2.53. Es sei $R \subset R'$ eine Ringerweiterung (d.h. ein injektiver Ringhomomorphismus) und (x_1, \dots, 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

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

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 $\Phi : \mathbb{Q}[X] \rightarrow \mathbb{C}$, $X \mapsto \sqrt{2}$, gilt $X^2 - 2 \in \text{Kern}(\Phi)$.
- Die Eulersche Zahl $e = \lim_{n \rightarrow \infty} \left(1 + \frac{1}{n}\right)^n$ ist transzendent (Hermite).

- Das System (e, e^2) ist nicht transzendent.
Grund: Der Homomorphismus $\Phi : \mathbb{Q}[X, Y] \rightarrow \mathbb{C}$, $X \mapsto e$, $Y \mapsto e^2$, 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 $\varphi : \mathbb{Z} \rightarrow R$ mit $n \mapsto n \cdot 1_R$ der kanonische Homomorphismus. Ist R nullteilerfrei, so ist das Nullideal in R prim und somit ist auch $\text{Kern}(\varphi) = \varphi^{-1}(0) \subset \mathbb{Z}$ ein Primideal. Nach Satz 1.38 folgt

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

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

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

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

- es gilt für jeden nullteilerfreien Ring R

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

- Ist $R \xrightarrow{i} S$ ein Teilring, so gilt $\text{char}(R) = \text{char}(S)$.

[Grund: $\varphi_S = i \circ \varphi_R$. Weil i injektiv ist, folgt $\text{Kern}(\varphi_S) = \text{Kern} \varphi_R$.]

Lemma 3.3. Sind K, L Körper und $\text{char}(K) \neq \text{char}(L)$, 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 $\text{char}(K) = \text{char}(L)$. \square

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

$$\text{char}(K) = 0 \iff P \cong \mathbb{Q}$$

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

Beweis. Die \Leftarrow Implikationen sind trivial. Wegen $P \ni 1$, faktorisiert $\varphi : \mathbb{Z} \rightarrow K$ über P .

1. Fall: $\text{char}(K) = 0$: $\mathbb{Z} \cong \text{Bild}(\varphi) \subset P$ folglich ist $Q(\text{Bild}(\varphi)) \cong \mathbb{Q}$ ein Teilkörper von P und deshalb $= P$.

2. Fall: $\text{char}(K) = p > 0$: dann gilt $\mathbb{F}_p \cong \text{Bild}(\varphi) \subset P$. Dies ist ein Teilkörper, also $P = \text{Bild}(\varphi)$. \square

Definition 3.7. Sei K ein Körper mit $\text{char}(K) = p > 0$. Dann heißt der Körperhomomorphismus

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

der **Frobeniushomomorphismus** von K .

Bemerkung 3.8. σ ist Homomorphismus wegen

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

Da K nullteilerfrei ist, ist σ injektiv.

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. \square

Lemma 3.10. Sei $\text{char}(K) = p > 0$ 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 $a^p - a = 0$. \square

3.2 Endliche und algebraische Körpererweiterungen

Seien $K \subset L$ Körper. Sprechweise: L ist Erweiterungskörper von K .

Vermittels: $K \times L \rightarrow L, (x, y) \mapsto xy$, 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 $[M : K] = \infty$. \square

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 $[L : K] = 1$. \square

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 $1, t, t^2, \dots$ sind linear unabhängig).

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

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

mit $c_0, \dots, c_{n-1} \in K$ 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 $\text{Kern}(\varphi) = (f)$ 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. $g(\alpha) = 0 \iff g \in \text{Kern}(\varphi)$. $\text{Kern}(\varphi)$ ist ein Primideal $\neq (0)$ im Hauptidealring $K[X]$, also von der Form (f) mit einem eindeutig bestimmten normierten irreduziblen Polynom f . \square

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 α über K erzeugte Teilring von 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 α über K erzeugte Teilkörper von 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 $\varphi : K[X] \rightarrow L, g \mapsto g(\alpha)$, 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

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

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 $1, X, \dots, X^{\deg(f)-1}$ eine K -Basis von $K[X]/(f)$. \square

Zum Vertrautwerden: Wie findet man $\alpha^{-1} \in K[\alpha]$?

Sei $f = X^n + c_{n-1}X^{n-1} + \dots + c_0$ das Minimalpolynom von $\alpha \neq 0$. Es gilt $n \geq 1$ und $c_0 \neq 0$ weil f irreduzibel ist. Es folgt $0 = \alpha^{-1}(\alpha^n + c_{n-1}\alpha^{n-1} + \dots + c_0)$ also $(-c_0)\alpha^{-1} = \alpha^{n-1} + c_{n-1}\alpha^{n-2} + \dots + c_1$ 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

$$1, \alpha, \dots, \alpha^n$$

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

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. \square

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 $S = \{\alpha_1, \dots, \alpha_n\}$ endlich, so schreiben wir

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

$K[\alpha_1, \dots, \alpha_n]$ 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

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

Ist S unendlich, so gilt

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

Begründung: Für $T \subset S$ gilt $K(T) \subset K(S)$, daher ist die rechte Seite in der linken enthalten. Jedes Element $s \in S$ liegt bereits in einer endlichen Teilmenge von S (z.B. in $\{s\}$). Daher liegen alle Elemente aus S in der rechten Seite und es verbleibt zu zeigen, dass diese ein Körper ist. Zunächst hat jedes Element ungleich 0 ein Inverses, weil alle $K(T)$ Körper sind. Für $a_1 \in K(T_1)$ und $a_2 \in K(T_2)$ liegen $a_1 a_2$ und $a_1 + a_2$ in $K(T_1 \cup T_2)$. Daher ist die rechte Seite ein Ring und somit ein Körper.

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

$$[L : K] =$$

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

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 .

Sei $S \subset L$ ein Erzeugendensystem der Körpererweiterung L/K (so etwas gibt es stets, z.B. $S = L$). In der Darstellung eines beliebigen Elements aus L kommen stets nur endlich viele Elemente aus S vor. Daher gilt:

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

Sind alle Elemente aus S algebraisch über K , so ist L Vereinigung endlicher und damit 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 (relativen) **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 $\alpha\beta, \alpha^{-1}$. □

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/L algebraisch sind.

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

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

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 $f \in \text{Kern}(p)$. \square

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 $n = \deg f$, $c \in K^\times$, $\alpha_1, \dots, \alpha_n \in K$, 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 . \square

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

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 $f_1, \dots, f_n \in I$ und $g_1, \dots, g_n \in K[\mathfrak{X}]$. Nach n -maliger Anwendung von Satz 3.33 finden wir eine Erweiterung K'/K , so dass für $i = 1, \dots, n$ das Polynom f_i eine Nullstelle $\alpha_i \in K'$ besitzt. Wir betrachten den nach Universaleigenschaft eindeutigen Ringhomomorphismus $\phi: K[\mathfrak{X}] \rightarrow K'$ mit

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

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

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

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

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.

$$K \subset L_1 \subset L_2 \subset \dots$$

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. \square

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 $\alpha \in \overline{K}$. \square

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

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

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

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 $\sigma : K \rightarrow L$ ein Körperhomomorphismus.*

- (i) *Ist $\sigma' : K' \rightarrow L$ 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 $\sigma' : K' \rightarrow L$ 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 $\sigma' : K' \rightarrow L$ 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 $\sigma' : K' \rightarrow L$ von σ mit $\sigma'(\alpha) = \beta$.

Der Kern des Homomorphismus $\phi : K[X] \rightarrow L$, $X \mapsto \beta$, $\phi|_K = \sigma$ 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

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

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

$$\begin{array}{ccccc} & & K & & \\ & \swarrow \text{kan} & \downarrow \text{kan} & \searrow \sigma & \\ K' & \xleftarrow[\xi]{\sim} & K[X]/(f) & \xrightarrow{\psi} & L \end{array}$$

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

Satz 3.41. Sei $K \subset K'$ eine algebraische Körpererweiterung und $\sigma : K \rightarrow L$ ein Körperhomomorphismus. Sei L algebraisch abgeschlossen. Dann besitzt σ eine Fortsetzung $\sigma' : K' \rightarrow L$. 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 $\tau : F \rightarrow L$ 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 $\alpha \in K' \setminus F$, man könnte nach Lemma 3.40 τ von F auf $F(\alpha)$ fortsetzen und (F, τ) wäre nicht maximal. Dies zeigt die Existenz von $\sigma' : K' \rightarrow L$. 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 $\Rightarrow \sigma' : K' \rightarrow L$ ist Isomorphismus. \square

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

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

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 $\phi : A \rightarrow B$ 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 $\psi : A[X] \rightarrow B$, $\psi|_A = \phi$, $\psi(X) = b$) ist als A -Modul endlich erzeugt.
- (iii) Es existiert ein endlich erzeugter A -Untermodule $M \subset B$ mit $1 \in M$ und $b \cdot M \subset M$.

Beweis. (i) \Rightarrow (ii) Es gelte $f(b) = 0$ mit $f = X^n + a_{n-1}X^{n-1} + \dots + a_0$. Dann gilt $b^n = -\phi(a_{n-1})b^{n-1} - \dots - \phi(a_0)$. Sei $M = \langle 1, b, \dots, b^{n-1} \rangle \subset B$ der von $1, \dots, b^{n-1}$ erzeugte A -Untermodule. 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 $M = \langle m_1, \dots, m_n \rangle \subset B$ ein endlich erzeugter A -Untermodule mit $1 \in M$ und $bM \subset M$. Dann existieren Gleichungen

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

M.a.W.

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

mit $Q = (b\delta_{ij} - \phi(a_{ij}))_{i,j} \in M_{n,n}(B)$. 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. $\det(Q)m_i = 0$, $i = 1, \dots, n$.

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

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

mit $c_0, \dots, c_{n-1} \in A$. □

Definition 3.46. Sei $\phi : A \rightarrow B$ 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 $A \rightarrow B$ und $B \rightarrow C$ endliche Ringhomomorphismen, so auch ihre Komposition $A \rightarrow C$.

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

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

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

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

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

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

□

Korollar 3.50. Sei $\phi : A \rightarrow B$ 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

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

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

Korollar 3.51. Sei $\phi : A \rightarrow B$ 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. \square

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

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

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

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

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 $(Y, X^2 - Y^3) \neq (Y, X^2) \nmid X$. Also ist A nicht ganzabgeschlossen.

Satz 3.56. *Jeder faktorielle Ring ist ganzabgeschlossen.*

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

$$a^n + c_{n-1}ba^{n-1} + \dots + c_0b^n = 0.$$

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 $\alpha \in A$. \square

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 und daher nach 3.56 ganzabgeschlossen. \square

3.5 Zerfällungskörper

Notation: Sind L/K und L'/K zwei Körpererweiterungen und ist $\sigma : L \rightarrow L'$ 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, \dots, a_n die Nullstellen von f in \overline{K} . Dann ist $L = K(a_1, \dots, a_n)$ 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 $\mathcal{F} = (f_1, \dots, f_n)$ 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 $\overline{\sigma} : L_1 \rightarrow \overline{L}_2$ 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 $\overline{\sigma} : L_1 \rightarrow \overline{L}_2$ fort. Nach Satz 3.62 erhalten wir einen Isomorphismus $\sigma : L_1 \xrightarrow{\sim} L_2$ \square

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, \dots, a_n die Nullstellen (mit Vielfachheiten) von f in L_1 und b_1, \dots, 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 $b_i = \overline{\sigma}(a_i)$, $i = 1, \dots, n$, und

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

2. Schritt: \mathcal{F} ist endliche Familie (f_1, \dots, f_n) . Ersetze \mathcal{F} durch die einelementige Familie $f_1 \cdots f_n$ 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} . \square

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

- (i) *Jeder K -Homomorphismus $L \rightarrow \overline{L}$ 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 $L \rightarrow \overline{L}$ 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

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

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) \Rightarrow (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 $\sigma : K(a) \rightarrow \overline{L}$ mit $\sigma(a) = b$. Nach Satz 3.41 finden wir eine Fortsetzung $\sigma' : L \rightarrow \overline{L}$. 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 $\sigma : L \rightarrow \overline{L}$ 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 $L = \sigma(L)$. \square

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. \square

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 . \square

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 $L \subsetneq M \subsetneq L'$ 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 $\sigma : L \rightarrow M$ 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 $L \rightarrow M$. Nach Lemma 3.40 finden wir einen K -Homomorphismus $\bar{\sigma} : K(a_i) \rightarrow L'$ mit $\bar{\sigma}(a_i) = \alpha_i$.

Bild:

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

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

3.6 Separable Erweiterungen

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

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

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: $h_2 \mid h_1$. \square

Wir setzen die Konvention $\text{ggT}_{K[X]}(f, 0) = f$ für beliebiges $f \in K[X]$.

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 $f = a_n X^n + \dots + a_0 \in K[X]$. Wir nennen das Polynom

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

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 $\text{ggT}(f, f')$.
- (ii) Ist f irreduzibel, so hat f genau dann Mehrfachnullstellen wenn $f' = 0$ gilt.

Beweis. (i) OE $K = \overline{K}$ und f normiert. Dann gilt $f = (X - a_1) \cdots (X - a_n)$ und die Produktregel liefert

$$f' = \sum_{i=1}^n (X - a_1) \cdots (\widehat{X - a_i}) \cdots (X - a_n),$$

und damit die Aussage.

(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 $f \mid f'$ und wegen $\deg f' < \deg f$ folgt $f' = 0$. Ist $f' = 0$ so folgt aus (i) dass jede Nullstelle Mehrfachnullstelle ist. \square

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

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

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

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 aus einem Element. Ist $\text{char}(K) = p > 0$, 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 $\text{char } K = p > 0$ 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

$$\begin{aligned} f' = 0 &\iff i c_i = 0, \quad i = 1, \dots, n \iff c_i = 0 \text{ für alle } i \text{ mit } (p, i) = 1 \\ &\iff f(X) = h(X^p) \text{ für ein } h \in K[X]. \end{aligned}$$

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 , daher ist g irreduzibel und separabel. Seien OE f und g normiert und a_i die Nullstellen von g in \overline{K} , d.h.

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

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 . \square

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 $\mathbb{F}_p(t)[X]/(X^p - t)/\mathbb{F}_p(t)$ 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

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

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) $[L : K]_s = \text{Anzahl der verschiedenen Nullstellen von } f \text{ in } \overline{K}$.
- (ii) α separabel über $K \iff [L : K] = [L : K]_s$.
- (iii) Gilt $\text{char}(K) = p > 0$ 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 $\stackrel{(i)}{\iff} n = [L : K]_s$. Nach Satz 3.20 gilt aber $n = [L : K]$.

(iii) Dies folgt aus Satz 3.81 und aus (i). \square

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

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

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

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

Zu (1): Sei $\bar{\sigma}_i \circ \tau_j = \bar{\sigma}_{i'} \circ \tau_{j'}$. Wegen $\tau_j|_L = \text{id}_L = \tau_{j'}|_L$ gilt $\sigma_i = (\bar{\sigma}_i \circ \tau_j)|_L = (\bar{\sigma}_{i'} \circ \tau_{j'})|_L = \sigma_{i'}$, also $i = i'$. Also gilt $\bar{\sigma}_i = \bar{\sigma}_{i'}$ und folglich $\tau_j = \tau_{j'}$.

Zu (2): Sei nun $\tau : M \rightarrow \bar{K}$ ein K -Homomorphismus. Es gilt $\tau|_L \in \text{Hom}_K(L, \bar{K})$ also $\tau|_L = \sigma_i$ für ein $i \in I$. Dann ist $\bar{\sigma}_i^{-1} \circ \tau \in \text{Hom}_L(M, \bar{K})$, d.h. es existiert ein $j \in J$ mit $\bar{\sigma}_i^{-1} \circ \tau = \tau_j$. Dann gilt $\tau = \bar{\sigma}_i \circ \tau_j$. Bild:

$$\begin{array}{ccccc}
 & & \bar{K} & \xrightarrow{\bar{\sigma}_i^{-1}} & \bar{K} \\
 & \nearrow \tau & & & \nearrow \\
 \bar{K} & & & & \\
 \downarrow & & & & \\
 M & & & & M \\
 \downarrow & \nearrow \tau|_L = \sigma_i & & \searrow & \\
 L & \xrightarrow{\text{id}_L} & L & & \\
 \downarrow & & & & \\
 K & & & &
 \end{array}$$

□

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

- (i) Falls $\text{char}(K) = 0$, so gilt $[L : K] = [L : K]_s$.
- (ii) Falls $\text{char}(K) = p > 0$, 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 $L = K(a)/K$ einfach, so folgt dies aus Lemma 3.87. Der allgemeine Fall $L = K(a_1, \dots, a_n)/K$ folgt hieraus per Induktion nach n 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, \dots, a_n mit $L = K(a_1, \dots, a_n)$.
- (iii) $[L : K]_s = [L : K]$.

Beweis. (i) \Rightarrow (ii) ist trivial.

(ii) \Rightarrow (iii) $K \subset K(a_1) \subset K(a_1, a_2) \subset \dots \subset K(a_1, \dots, a_n) = L$ sind jeweils einfache Erweiterungen und für alle i ist a_i separabel über $K(a_1, \dots, a_{i-1})$. Wir erhalten die Gleichung in (iii) aus Lemma 3.87 und den Gradformeln Satz 3.13, Satz 3.88.

(iii) \Rightarrow (i). Sei $a \in L$ beliebig. Z.z. a separabel $/K$. OE sei $\text{char}(K) = p > 0$. 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 $r = 0$. \square

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

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

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 $K(a_{i_1}, \dots, a_{i_n})$ für gewisse $i_1, \dots, i_n \in I$. 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 $[L : K]_s = \infty$. \square

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 $f = X^n + c_{n-1}X^{n-1} + \dots + c_0 \in L[X]$ das Minimalpolynom von a über L . Sei $L' = K(c_0, \dots, c_{n-1})$. 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

$$\begin{aligned} [L'(a) : K] &= [L'(a) : L'] \cdot [L' : K] \\ &= [L'(a) : L']_s \cdot [L' : K]_s = [L'(a) : K]_s. \end{aligned}$$

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

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 ein Zerfällungskörper der Familie der separablen Polynome über K und nach Korollar 3.63 eindeutig bis auf K -Isomorphie. \square

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

3.7 Endliche Körper

Lemma 3.98. Sei \mathbb{F} ein endlicher Körper. Dann gilt $\text{char}(\mathbb{F}) = p > 0$ 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 (siehe Lemma 3.6). \mathbb{F} endlich $\Rightarrow [\mathbb{F} : \mathbb{F}_p] =: n < \infty$. Es ist \mathbb{F} 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 . \square

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 $f = X^q - X \in \mathbb{F}_p[X]$. 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. Genauso gilt $(ab)^q = a^q b^q = ab$ und für $b \neq 0$ ist mit b auch b^{-1} Nullstelle von f . Daher bilden die q vielen Nullstellen von f einen Teilkörper in $\overline{\mathbb{F}}_p$, den in $\overline{\mathbb{F}}_p$ gebildeten Zerfällungskörper von $X^q - X$. Die Eindeutigkeitsaussagen folgen aus Lemma 3.98. \square

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!

Nun wählen wir einen algebraischen Abschluss $\overline{\mathbb{F}}_p$ von \mathbb{F}_p und betten die Körper \mathbb{F}_q , $q = p^n$, $n \in \mathbb{N}$, in $\overline{\mathbb{F}}_p$ ein. Das Bild von \mathbb{F}_q in $\overline{\mathbb{F}}_p$ ist unabhängig von der Wahl der Einbettung, weil nach Lemma 3.98 die \mathbb{F}_q normal über \mathbb{F}_p sind. So fassen wir die \mathbb{F}_q als Teilkörper von $\overline{\mathbb{F}}_p$ auf.

Korollar 3.100. *Es ist $\mathbb{F}_q \subset \mathbb{F}_{q'}$ 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 $\mathbb{F} \rightarrow \overline{\mathbb{F}}_p$ und diese dann wieder zu einer Inklusion $\mathbb{F}' \subset \overline{\mathbb{F}}_p$ fortsetzen und ist im betrachteten Fall. \square

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. \square

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 : $\sigma^r : K \rightarrow K$, $a \mapsto a^q$.

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 $\text{Aut}_{\mathbb{F}_q}(\mathbb{F})$ eine zyklische Gruppe der Ordnung n und wird vom relativen Frobeniusautomorphismus $\sigma^r : \mathbb{F} \rightarrow \mathbb{F}$, $a \mapsto a^q$, erzeugt.*

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

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

Wegen $a^q = a$ für alle $a \in \mathbb{F}_q$ gilt $\sigma^r \in \text{Aut}_{\mathbb{F}_q}(\mathbb{F})$. Es genügt daher zu zeigen, dass die Ordnung $\text{ord}(\sigma^r)$ in $\text{Aut}_{\mathbb{F}_q}(\mathbb{F})$ gleich n ist. Nach Korollar 1.48 gilt $\text{ord}(\sigma^r) \mid n$. Wäre nun $\text{ord}(\sigma^r) < n$, 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. \square

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 durchlaufen.

Satz 3.103 folgt als 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 $a_r = h$, $a_1 = \dots = a_{r-1} = 1$, und H ist zyklisch. \square

3.8 Rein inseparable Erweiterungen

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

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 einem algebraischen Abschluss \overline{K} von 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 $(X^{p^n} - c)^m$ 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} . \square

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 $(f_i)_{i \in I}$. \square

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) \Rightarrow (ii) ist trivial.

(ii) \Rightarrow (iii) Es sei \overline{K} ein algebraischer Abschluss von L . Z.z. $\#\text{Hom}_K(L, \overline{K}) = 1$. Da id_L in der Menge liegt, ist also für einen beliebigen K -Homomorphismus $\varphi : L \rightarrow \overline{K}$ zu zeigen, dass $\varphi = \text{id}_L$ gilt. Wegen $L = K((a_i)_{i \in I})$ ist φ schon durch seine Werte auf den a_i festgelegt. Es ist $\varphi(a_i)$ eine Nullstelle des Minimalpolynoms von a_i über K . Nach Voraussetzung hat dieses genau eine Nullstelle, woraus $\varphi(a_i) = a_i$ für alle $i \in I$ folgt. Daher gilt $\varphi = \text{id}_L$.

(iii) \Rightarrow (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 $a^{p^n} = c \in K$.

(iv) \Rightarrow (i) Gilt $a^{p^n} = c \in K$, so folgt $f_a \mid (X^{p^n} - c)$. Also hat f_a genau eine Nullstelle in \overline{K} und a ist rein inseparabel. \square

Bemerkung 3.111. Wegen $[L : K] = p^2[L : K]_s$ 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. Ist L/K sowohl separabel, als auch rein inseparabel, so gilt $[L : K] = [L : K]_s = 1$ nach Satz 3.110(iii). Es folgt $L = K$. \square

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. Nach Satz 3.88 gilt $[M : K]_s = [M : L]_s \cdot [L : K]_s$. Wegen Satz 3.110(iii) folgt hieraus das Ergebnis. \square

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 ein $r \geq 0$, 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. Weil jedes Element aus K'_s separabel über K ist, gilt $K'_s \subset K_s$. Zudem ist K_s/K'_s 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 $K_s = K'_s$ nach Korollar 3.112.

Sei nun L/K normal und $\sigma : K_s \rightarrow \bar{L}$ ein K -Homomorphismus. σ setzt sich zu einem K -Homomorphismus $\sigma' : L \rightarrow \bar{L}$ fort und weil L/K normal ist beschränkt sich σ' zu einem Automorphismus $\sigma' : L \rightarrow L$. Dann ist $L = \sigma'(L)/\sigma'(K_s)$ rein inseparabel und $\sigma'(K_s)/\sigma'(K) = K$ separabel. Wegen der Eindeutigkeit von K_s gilt $\sigma'(K_s) = K_s$. Daher ist K_s/K normal. \square

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. Weil L/K normal ist, gilt $\text{Hom}_K(L, \bar{L}) = \text{Aut}_K(L)$. Setze

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

K_i ist offensichtlich ein Körper. Sei $\sigma : K_i \rightarrow \bar{L}$ ein K -Homomorphismus. Dann setzt sich σ zu $\sigma' : L \rightarrow \bar{L}$ fort und nach Definition von K_i gilt $\sigma = \sigma'|_{K_i} = \text{id}_{K_i}$. Es folgt $\#\text{Hom}_K(K_i, \bar{L}) = 1$ und $[K_i : K]_s = 1$. Daher ist K_i/K rein inseparabel. Ist $K \subset M \subset L$ ein Zwischenkörper mit M/K rein inseparabel, so gilt $\#\text{Hom}_K(M, \bar{L}) = 1$, also $\sigma|_M = \text{id}_M$ für alle $\sigma : L \rightarrow \bar{L}$. Definitionsgemäß folgt $M \subset K_i$. Daher ist K_i die maximale rein inseparable Teilerweiterung von L/K (insbesondere existiert eine solche). Es bleibt zu zeigen, dass L/K_i separabel ist. Sei $a \in L$ beliebig. Für $\sigma \in \text{Aut}_K(L)$ ist $\sigma(a)$ Nullstelle des Minimalpolynoms von a über K , d.h. es existieren nur endlich viele Möglichkeiten. Wir wählen $\sigma_1, \dots, \sigma_r \in \text{Aut}_K(L)$ so, dass $\sigma_1(a), \dots, \sigma_r(a)$ paarweise verschieden sind und r maximal möglich ist. Wegen $\text{id}_L \in \text{Aut}_K(L)$ kommt a unter den $\sigma_i(a)$ vor. Jedes $\sigma \in \text{Aut}_K(L)$ induziert eine bijektive Selbstabbildung auf der Menge $\{\sigma_1(a), \dots, \sigma_r(a)\}$. Sei

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

Dann gilt $\sigma(c_i) = c_i$ für alle $\sigma \in \text{Aut}_K(L)$ und jedes i , $0 \leq i \leq r-1$. Nach Definition von K_i gilt $f \in K_i[X]$. Zudem hat f keine Doppelnulstellen, ist also separabel. Folglich ist a separabel über K_i und weil $a \in L$ beliebig war, ist L/K_i separabel.

Sei nun $K \subset K'_i \subset L$ so, dass L/K'_i separabel und K'_i/K rein inseparabel ist. Zu zeigen: $K'_i = K_i$. Wir haben oben gesehen, dass K_i die maximale rein inseparable Erweiterung von K in L ist. Daher gilt $K'_i \subset K_i$. Als Teilerweiterung von L/K'_i ist K_i/K'_i separabel. Als Teilerweiterung der rein inseparablen Erweiterung K_i/K ist K_i/K'_i auch rein inseparabel. Nach Korollar 3.112 folgt $K_i = K'_i$. \square

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 und nach Satz 3.102 ist L^\times eine endliche zyklische Gruppe. Ist $a \in L^\times$ ein Erzeuger, 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 $\text{Hom}_K(L, \bar{K}) = \{\sigma_1, \dots, \sigma_n\}$. 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 und somit $P \neq 0 \in \overline{K}[X]$. 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 $\sigma_i(a + cb)$, $i = 1, \dots, n$, paarweise verschiedene Nullstellen von f , woraus $\deg f \geq n$ folgt. Wir schließen

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

und folglich $L = K(a + bc)$. □

4 Galoistheorie

Idee: Wir betrachten eine algebraische Gleichung

$$f(X) = 0, \quad f \in K[X].$$

Wir wählen einen algebraischen Abschluss \overline{K} von K und setzen

$$L = K(\text{alle Nullstellen von } f \text{ in } \overline{K}),$$

d.h. L ist Zerfällungskörper von f über K . Ein $\sigma \in \text{Aut}_K(L)$ ist durch seine Werte auf den Nullstellen von f gegeben. Wir studieren die Nullstellen mit Hilfe gruppentheoretischer Eigenschaften von $\text{Aut}_K(L)$.

4.1 Galois-Erweiterungen

Definition 4.1. Eine algebraische Körpererweiterung L/K heißt **galoissch** (oder **Galoiserweiterung**) wenn sie normal und separabel ist. Man bezeichnet dann $\text{Gal}(L/K) := \text{Aut}_K(L)$ als die **Galoisgruppe** der Erweiterung L/K .

Beispiele 4.2. • Ist $f \in K[X]$ ein separables Polynom und L der Zerfällungskörper von f , so ist L/K eine Galoiserweiterung.

• \mathbb{C}/\mathbb{R} ist galoissch und $\text{Gal}(\mathbb{C}/\mathbb{R})$ ist zyklisch von der Ordnung 2. Das nichttriviale Element ist die komplexe Konjugation.

• Jede algebraische Erweiterung \mathbb{F}/\mathbb{F}_q ist galoissch ($q = p^r$, p Primzahl). Ist \mathbb{F}/\mathbb{F}_q eine endliche Erweiterung, so ist $\mathbb{F} = \mathbb{F}_{q^n}$ mit $q^n = q^n$, $n = [\mathbb{F} : \mathbb{F}_q]$, und $\text{Gal}(\mathbb{F}/\mathbb{F}_q)$ ist zyklisch von der Ordnung n . Ein Erzeuger ist der relative Frobeniusautomorphismus $\mathbb{F} \rightarrow \mathbb{F}$, $a \mapsto a^q$ (siehe Abschnitt 3.7).

Lemma 4.3. Sei L/K eine Galoiserweiterung und E ein Zwischenkörper.

- (i) L/E ist galoissch und $\text{Gal}(L/E)$ ist in natürlicher Weise eine Untergruppe von $\text{Gal}(L/K)$.
- (ii) Ist auch E/K galoissch, so beschränkt sich jeder K -Automorphismus von L zu einem K -Automorphismus von E und $\text{Gal}(L/K) \rightarrow \text{Gal}(E/K)$, $\sigma \mapsto \sigma|_E$, ist ein surjektiver Gruppenhomomorphismus mit Kern $\text{Gal}(L/E)$.

Beweis. (i) Wir hatten schon gesehen, dass L/E und E/K separabel sind (Korollar 3.93) und L/E normal (Korollar 3.70). Also ist L/E galoissch. Nun gilt

$$\text{Gal}(L/E) = \text{Aut}_E(L) \subset \text{Aut}_K(L) = \text{Gal}(L/K).$$

- (ii) Ist E/K normal so gilt $\sigma(E) = E$ für jedes $\sigma \in \text{Aut}_K(L)$, also ist

$$\phi : \text{Gal}(L/K) \rightarrow \text{Gal}(E/K), \sigma \mapsto \sigma|_E,$$

wohldefiniert. Es gilt $\sigma|_E = \text{id} \Leftrightarrow \sigma \in \text{Aut}_E(L)$, also $\text{Kern}(\phi) = \text{Gal}(L/E)$. Sei nun $\tau \in \text{Gal}(E/K)$ beliebig. τ setzt sich fort zu einem K -Homomorphismus $\sigma : L \rightarrow \bar{L}$, und wegen L/K normal können wir σ als Element in $\text{Gal}(L/K)$ auffassen. Es gilt $\sigma|_E = \tau$. Daher ist ϕ surjektiv. \square

Sei nun L/K normal und endlich. Dann gilt $\#\text{Aut}_K(L) = [L : K]_s$. Im Fall $\text{char}(K) = 0$ ist L/K automatisch separabel und damit galoissch vom Grad $[L : K]$. Im Fall $\text{char}(K) > 0$ sei $K_i \subset L$ der Zwischenkörper aus Satz 3.115. Dann gilt für jedes $\sigma \in \text{Aut}_K(L)$: $\sigma|_{K_i} = \text{id}_{K_i}$ und $\#\text{Aut}_K(L) = [L : K]_s = [L : K_i] \leq [L : K]$. Wir erhalten

$$\#\text{Aut}_K(L) = [L : K] \iff K = K_i \iff L/K \text{ galoissch}.$$

Satz 4.4. Sei L ein Körper und G eine Untergruppe von $\text{Aut}(L)$. Weiter setze man

$$K = L^G = \{a \in L \mid \sigma(a) = a \text{ für alle } \sigma \in G\}.$$

- (i) Ist G endlich, so ist L/K eine endliche Galoiserweiterung vom Grad $[L : K] = \#G$ mit Galoisgruppe $\text{Gal}(L/K) = G$.
- (ii) Ist G nicht endlich, L/K aber algebraisch, so ist L/K eine unendliche Galoiserweiterung und $\text{Gal}(L/K)$ enthält G als Untergruppe.

Definition 4.5. Man nennt $K = L^G$ den **Fixkörper** von L unter G .

Beweis von Satz 4.4. Zunächst ist $K = L^G$ ein Teilkörper von L . Sei nun G endlich oder L/K algebraisch und $a \in L$ beliebig. Wir wählen, wie im Beweis von Satz 3.115 $\sigma_1, \dots, \sigma_r \in G$, so dass $\sigma_1(a), \dots, \sigma_r(a)$ paarweise verschieden und r maximal ist. Nun betrachten wir das Polynom

$$f_a = \prod_{i=1}^r (X - \sigma_i(a)),$$

welches Koeffizienten in $K = L^G$ hat (jedes Element $\sigma \in G$ definiert eine Permutation die Menge $\{\sigma_1(a), \dots, \sigma_r(a)\}$, vertauscht daher nur die Faktoren und lässt f_a fest). Es ist a ist Nullstelle des separablen Polynoms f_a und da $a \in L$ beliebig war, ist L/K separabel. Nach Konstruktion liegen alle anderen Nullstellen von f_a auch in L , also ist L Zerfällungskörper der Familie aller Polynome f_a , $a \in L$. Daher ist L/K normal und separabel, also galoissch.

Wir haben eine natürliche Inklusion $G \hookrightarrow \text{Aut}_K(L) = \text{Gal}(L/K)$. Ist G unendlich, so auch $\text{Gal}(L/K)$, also hat L/K unendlichen Grad. Sei G endlich und $n = \#G$. Nach dem obigen Argument hat jedes $a \in L$ ein Minimalpolynom vom Grad $\leq n$. Ist $K \subset E \subset L$ mit E/K endlich, so gilt nach dem Satz über das primitive Element, dass $E = K(a)$ für ein $a \in L$, also $[E : K] \leq n$. Also gilt auch $[L : K] \leq n$. Wir erhalten

$$n = \#G \leq \#\text{Gal}(L/K) = [L : K] \leq n,$$

also sind alle Ungleichungen Gleichungen und die Inklusion $G \hookrightarrow \text{Gal}(L/K)$ ist ein Isomorphismus. \square

Korollar 4.6. *Es sei L/K normal algebraisch und $G = \text{Aut}_K L$. Dann gilt:*

- (i) L/L^G ist eine Galoiserweiterung mit Galoisgruppe G .
- (ii) Ist L/K separabel so gilt $K = L^G$.
- (iii) Ist im Fall $\text{char } K > 0$ die Erweiterung L/K nicht separabel, so ist L^G/K rein inseparabel und die Kette $K \subset L^G \subset L$ stimmt mit der Kette $K \subset K_i \subset L$ aus Satz 3.115 überein.

Beweis. Als Zwischenerweiterung von L/K ist L/L^G algebraisch, also nach Satz 4.4 eine Galoiserweiterung. Wir haben die Inklusionen $G \hookrightarrow \text{Aut}_{L^G}(L) \subset \text{Aut}_K(L) = G$, die weil links und rechts dieselbe Gruppe steht, Gleichheiten sind. Wir zeigen nun: $[L^G : K]_s = 1$. Sei $\sigma : L^G \rightarrow \bar{L}$ ein K -Homomorphismus. Dann setzt sich σ zu einem K -Homomorphismus $\sigma' : L \rightarrow \bar{L}$ fort und σ' beschränkt sich zu einem K -Automorphismus von L . Diese wirken trivial auf L^G (nach Definition), also gilt $\#\text{Hom}_K(L^G, \bar{L}) = 1$. Nach Satz 3.110 ist L^G/K rein inseparabel, und L/L^G ist als Galoiserweiterung insbesondere separabel. Nach der Eindeutigkeitsaussage von Satz 3.115 gilt $L^G = K_i$; und $L^G = K$ falls L/K separabel. \square

Satz 4.7 (Hauptsatz der Galoistheorie). Sei L/K eine endliche Galoiserweiterung mit $G = \text{Gal}(L/K)$ als Galoisgruppe. Dann sind die Zuordnungen

$$\left\{ \begin{array}{c} \text{Untergruppen} \\ \text{von } G \end{array} \right\} \begin{array}{c} \xrightarrow{\Phi} \\ \xleftarrow{\Psi} \end{array} \left\{ \begin{array}{c} \text{Zwischenkörper} \\ \text{von } L/K \end{array} \right\}$$

$$\begin{array}{ccc} H & \longmapsto & L^H \\ \text{Gal}(L/E) & \longleftarrow & E \end{array}$$

bijektiv und zueinander invers.

Es ist L^H genau dann normal, also galoissch über K , wenn H ein Normalteiler in G ist. Ist dies der Fall, so induziert die Einschränkungabbildung $G \rightarrow \text{Gal}(L^H/K)$, $\sigma \mapsto \sigma|_{L^H}$, einen Isomorphismus

$$G/H \xrightarrow{\sim} \text{Gal}(L^H/K).$$

Bemerkung 4.8. Ist L/K unendlich, galoissch, so gilt noch $\Phi \circ \Psi = \text{id}$, d.h. wir erhalten eine Bijektion zwischen der Menge der Zwischenkörper und den Untergruppen in G , die im Bild von Ψ liegen. Dies sind genau die abgeschlossenen Untergruppen von G bzgl. der *Krull-Topologie*.

Beweis von Satz 4.7. Sei L/K eine nicht notwendig endliche Galoiserweiterung und E ein Zwischenkörper. Nach Lemma 4.3 ist L/E galoissch und $\text{Gal}(L/E) \subset G = \text{Gal}(L/K)$. Nach Korollar 4.6 gilt $E = L^{\text{Gal}(L/E)}$, also gilt $\Phi \circ \Psi = \text{id}$.

Sei umgekehrt $H \subset G$ eine Untergruppe. Ist G endlich, so auch H und nach Satz 4.4(i) ist L/L^H eine Galoiserweiterung mit Gruppe H , also $\Psi \circ \Phi = \text{id}$, wenn G endlich. Wir erhalten die behauptete Bijektion. Sei nun $H \subset G$ eine Untergruppe und $\sigma \in G$. Mit $\sigma H \sigma^{-1} = \{\sigma h \sigma^{-1} \mid h \in H\}$ bezeichnet man die konjugierte Untergruppe. Nach Definition von Normalteiler gilt

$$H \triangleleft G \iff \sigma H \sigma^{-1} = H \quad \text{für alle } \sigma \in G.$$

Andererseits gilt: $E := L^H$ ist normal über $K \iff \sigma(E) = E$ für alle $\sigma \in G$.

Behauptung. $\sigma(E) = L^{\sigma H \sigma^{-1}}$.

Grund:

$$\begin{aligned} \sigma(E) &= \{\sigma x \mid x \in E\} \\ &= \{y \mid \sigma^{-1} y \in E = L^H\} \\ &= \{y \mid \tau \sigma^{-1} y = \sigma^{-1} y \quad \forall \tau \in H\} \\ &= \{y \mid \sigma \tau \sigma^{-1} y = y \quad \forall \tau \in H\} = L^{\sigma H \sigma^{-1}}. \end{aligned}$$

Wir erhalten L^H/K normal $\iff \sigma(L^H) = L^H \quad \forall \sigma \iff L^H = L^{\sigma H \sigma^{-1}} \quad \forall \sigma$

$$\stackrel{1. \text{ Teil}}{\iff} H = \sigma H \sigma^{-1} \quad \forall \sigma \iff H \triangleleft G.$$

Ist nun L^H/K normal, so erhalten wir aus Lemma 4.3

$$\text{Gal}(L^H/K) \cong \text{Gal}(L/K)/\text{Gal}(L/L^H).$$

Zudem gilt $\text{Gal}(L/K) = G$, $\text{Gal}(L/L^H) = H$. \square

Korollar 4.9. Jede endliche separable Erweiterung hat nur endlich viele Teilerweiterungen.

Beweis. Die normale Hülle einer separablen Erweiterung ist separabel (man kann z.B. die normale Hülle im separablen Abschluss betrachten). Sei L/K endlich, separabel. Durch Übergang zur normalen Hülle können wir annehmen, dass L/K endlich und galoissch ist. Dann korrespondieren die Zwischenerweiterungen bi-jektiv zu den endlich vielen Untergruppen der endlichen Gruppe $\text{Gal}(L/K)$. \square

Bemerkung 4.10. Eine endliche inseparable Erweiterung kann unendlich viele Zwischenkörper haben.

Beispiel 4.11. Wir betrachten die Erweiterung $L = \mathbb{F}_p(X, Y)/K = \mathbb{F}_p(X^p, Y^p)$. Es ist L/K eine rein inseparable Erweiterung vom Grad p^2 . Es gilt $f^p \in \mathbb{F}_p(X^p, Y^p)$ für alle $f \in \mathbb{F}_p(X, Y)$. Daher ist das Minimalpolynom jedes $f \in L$ über K vom Grad $\leq p$; also kann L/K keine einfache Erweiterung sein. Für beliebiges $c \in K$ ist daher $K(X + cY) \subset L$ eine echte Zwischenerweiterung (vom Grad p).

Behauptung: für $c \neq d$ gilt auch $K(X + cY) \neq K(X + dY)$ (insbesondere existieren unendlich viele Zwischenkörper).

Grund: Wäre $X + dY \in K(X + cY)$, so auch $(d - c)Y = (X + dY) - (X + cY)$. Wir schließen $Y \in K(X + cY)$ und somit auch $X = (X + cY) - cY \in K(X + cY)$. Es folgt $L = K(X + cY)$, was aber einen Widerspruch zu $[L : K] = p^2$ darstellt.

Definition 4.12. Seien $E, E' \subset L$ Teilkörper. Das **Kompositum** EE' von E und E' in L ist der kleinste Teilkörper von L der E und E' enthält.

Bemerkung 4.13. Existenz: $EE' = E'(E) = E(E')$.

Korollar 4.14. Es sei L/K eine endliche Galoiserweiterung. Zu Zwischenkörpern E, E' von L/K betrachten wir $H = \text{Gal}(L/E)$ und $H' = \text{Gal}(L/E')$ als Untergruppen von $G = \text{Gal}(L/K)$. Dann gilt:

- (i) $E \subset E' \iff H \supset H'$.
- (ii) $EE' = L^{H \cap H'}$.
- (iii) $E \cap E' = L^{H''}$, wobei $H'' = \langle H, H' \rangle \subset G$.

Beweis. (i) Gilt $E \subset E'$ so ist jeder E' -Automorphismus von L auch ein E -Automorphismus von L , also $H = \text{Gal}(L/E') \supset \text{Gal}(L/E) = H'$. Umgekehrt folgt aus $H \supset H'$, dass $E = L^H \subset L^{H'} = E'$.

(ii) Es gilt trivialerweise $EE' \subset L^{H \cap H'}$ und $\text{Gal}(L/EE') \subset H \cap H'$. Aus der zweiten Aussage folgt mit (i), dass $EE' \supset L^{H \cap H'}$.

(iii) Es gilt $L^{H''} = L^H \cap L^{H'} = E \cap E'$. \square

Definition 4.15. Eine endliche Galoiserweiterung L/K heißt **abelsch** (bzw. **zyklisch**) wenn $\text{Gal}(L/K)$ abelsch (bzw. zyklisch) ist.

Korollar 4.16. Ist L/K eine endliche abelsche (bzw. zyklische) Galoiserweiterung, so sind für jeden Zwischenkörper E von L/K auch L/E und E/K abelsch (bzw. zyklisch).

Beweis. $\text{Gal}(L/E) \subset \text{Gal}(L/K)$ und jede Untergruppe einer abelschen (bzw. zyklischen) Gruppe ist abelsch (bzw. zyklisch). Auch ist in jedem Fall $\text{Gal}(L/E)$ Normalteiler in $\text{Gal}(L/K)$ und deshalb E/K galoissch. Außerdem ist $\text{Gal}(E/K)$ als Faktorgruppe von $\text{Gal}(L/K)$ wieder abelsch (bzw. zyklisch). \square

Satz 4.17. Sei L/K eine endliche Körpererweiterung mit Zwischenkörpern E, E' so dass E/K und E'/K galoissch sind. Dann gilt:

(i) EE' ist endlich und galoissch über K und der Homomorphismus

$$\begin{aligned} \varphi : \text{Gal}(EE'/E) &\longrightarrow \text{Gal}(E'/E \cap E') \\ \sigma &\longmapsto \sigma|_{E'} \end{aligned}$$

ist ein Isomorphismus.

(ii) Der Homomorphismus

$$\begin{aligned} \psi : \text{Gal}(EE'/K) &\longrightarrow \text{Gal}(E/K) \times \text{Gal}(E'/K) \\ \sigma &\longmapsto (\sigma|_E, \sigma|_{E'}) \end{aligned}$$

ist injektiv. Gilt $E \cap E' = K$, so ist ψ auch surjektiv, also ein Isomorphismus.

Beweis. (i) Es ist EE'/K normal, separabel und endlich.

Für jedes $\sigma \in \text{Gal}(EE'/E)$, gilt $\sigma|_E = \text{id}$. Ist zudem $\sigma \in \text{Kern}(\varphi)$, so folgt auch $\sigma|_{E'} = \text{id}$, also $\sigma = \text{id}_{EE'}$. Somit ist φ injektiv. Nun gilt

$$\begin{aligned} (E')^{\text{Bild}(\varphi)} &= (EE')^{\text{Gal}(EE'/E)} \cap E' \\ &= E \cap E'. \end{aligned}$$

Nach Satz 4.4 folgt $\text{Bild}(\varphi) = \text{Gal}(E'/E \cap E')$.

(ii) Die Injektivität von ψ ist klar. Sei nun $E \cap E' = K$ und $(\sigma, \sigma') \in \text{Gal}(E/K) \times \text{Gal}(E'/K)$. Nach (i) lässt sich σ zu einem $\bar{\sigma} \in \text{Gal}(EE'/E)$ fortsetzen und σ' zu einem $\bar{\sigma}' \in \text{Gal}(EE'/E)$ (sogar eindeutig). Nun gilt $\bar{\sigma}' \circ \bar{\sigma} \in \text{Gal}(EE'/K)$ und

$$\begin{aligned} (\bar{\sigma}' \circ \bar{\sigma})|_E &= \sigma \\ (\bar{\sigma}' \circ \bar{\sigma})|_{E'} &= \sigma'. \end{aligned}$$

Also haben wir ein Urbild gefunden. \square

Lemma 4.18. Sei L/K endlich, galoissch, $L = K(\alpha)$ und $H \subset \text{Gal}(L/K)$ eine Untergruppe. Wir betrachten das Polynom

$$f = \prod_{\sigma \in H} (X - \sigma(\alpha)) = \sum_{i=0}^r a_i X^i, \quad r = \#H.$$

Dann gilt $L^H = K(a_0, \dots, a_r)$.

Beweis. Es gilt $f^\sigma = f$ für alle $\sigma \in H$, also $M := K(a_0, \dots, a_r) \subset L^H$. Nun gilt $L = M(\alpha)$ und $f(\alpha) = 0$. Daraus folgt $[L : M] \leq \deg f = r$. Andererseits gilt $[L : L^H] = \#H = r$, also $M = L^H$. \square

4.2 Die Galoisgruppe einer Gleichung

Sei $f \in K[X]$ separabel, nicht-konstant und L/K der Zerfällungskörper von f . Dann ist L/K endlich, galoissch und man nennt $\text{Gal}(L/K)$ die **Galoisgruppe von f über K** , oder auch die Galoisgruppe der Gleichung $f(X) = 0$.

Satz 4.19. Sei $f \in K[X]$ separabel vom Grad $n > 0$ mit Zerfällungskörper L/K . Sind dann $\alpha_1, \dots, \alpha_n \in L$ die (paarweise verschiedenen) Nullstellen von f , so definiert

$$\begin{aligned} \varphi : \text{Gal}(L/K) &\longrightarrow \mathfrak{S}(\{\alpha_1, \dots, \alpha_n\}) = \mathfrak{S}_n \\ \sigma &\longmapsto \sigma|_{\{\alpha_1, \dots, \alpha_n\}} \end{aligned}$$

einen injektiven Gruppenhomomorphismus der Galoisgruppe von L/K in die Gruppe der Permutationen von $\alpha_1, \dots, \alpha_n$ bzw. in die Gruppe \mathfrak{S}_n der Permutationen von n Elementen. Insbesondere ist $[L : K] = \#\text{Gal}(L/K)$ ein Teiler von $\#\mathfrak{S}_n = n!$. Das Polynom f ist genau dann irreduzibel, wenn $\text{Gal}(L/K)$ transitiv auf der Menge der Nullstellen $\{\alpha_1, \dots, \alpha_n\}$ operiert, d.h. wenn es zu beliebigen $1 \leq i, j \leq n$ ein $\sigma \in \text{Gal}(L/K)$ mit $\sigma(\alpha_i) = \alpha_j$ gibt. Insbesondere ist dies der Fall für $[L : K] = n!$ bzw. $\text{Gal}(L/K) = \mathfrak{S}_n$.

Beweis. Sei $\sigma \in \text{Gal}(L/K)$. Weil σ die Koeffizienten von f fest lässt, bildet es die Nullstellen auf Nullstellen ab. Da σ injektiv und $\{\alpha_1, \dots, \alpha_n\}$ endlich ist, induziert σ eine Bijektion dieser Menge auf sich. Da $L = K(\alpha_1, \dots, \alpha_n)$ gilt, ist σ durch seine Werte auf den α_i bestimmt, also ist ϕ injektiv. Ist nun f irreduzibel, so existiert nach Lemma 3.40 für beliebige i, j ein K -Homomorphismus $\sigma : K(\alpha_i) \rightarrow L$ mit $\sigma(\alpha_i) = \alpha_j$. Dieser setzt sich zu einem K -Automorphismus von L , d.h. zu einem Element in $\text{Gal}(L/K)$ fort. Also wirkt $\text{Gal}(L/K)$ transitiv. Ist nun f reduzibel, d.h. $f = g \cdot h$, so überführt $\text{Gal}(L/K)$ die Nullstellen von g in Nullstellen von g und Nullstellen von h in Nullstellen von h . Da f separabel ist, hat es keine Mehrfach-Nullstellen, d.h. die Menge der Nullstellen von g und die Menge der Nullstellen von h sind disjunkt. Also kann eine Nullstelle von g nicht in eine Nullstelle von h überführt werden und umgekehrt. Daher kann $\text{Gal}(L/K)$ nicht transitiv wirken. \square

Korollar 4.20. Sei L/K eine endliche Galoiserweiterung vom Grad n . Dann gibt es eine endliche Menge $\{\alpha_1, \dots, \alpha_n\} \subset L$ die durch $\text{Gal}(L/K)$ in sich überführt wird und $\text{Gal}(L/K)$ kann als Untergruppe von $\mathfrak{S}(\{\alpha_1, \dots, \alpha_n\})$ aufgefasst werden.

Beweis. Da L/K separabel ist, existiert ein $\alpha \in L$ mit $L = K(\alpha)$ und L ist Zerfällungskörper des Minimalpolynoms f von α über K . Man wähle als $\{\alpha_1, \dots, \alpha_n\}$ die Menge der Nullstellen von f . \square

Grad 2:

Wir betrachten $f = X^2 + aX + b \in K[X]$ und nehmen an, dass f keine Nullstellen in K hat. Dann ist f irreduzibel. Falls $\text{char } K \neq 2$ oder $a \neq 0$, so gilt $f' = 2X + a \neq 0$ und f ist nach 3.76(ii) separabel. Nehmen wir $\text{char } K \neq 2$ an. Adjungiert man eine Nullstelle α von f so zerfällt f über $L = K(\alpha)$ in Linearfaktoren. Daher ist L/K normal, also galoissch und $\text{Gal}(L/K)$ ist zyklisch von der Ordnung 2. Substituiert man die Variable X durch $X - \frac{a}{2}$, so erhält man ein Polynom der Form $X^2 - c$ mit gleichem Zerfällungskörper L . Ist γ eine Quadratwurzel von c in L , so ist das nicht-triviale Element $\text{id} \neq \sigma \in \text{Gal}(L/K)$ durch $\sigma(\gamma) = -\gamma$ gegeben.

Grad 3:

Es sei $\text{char}(K) \neq 2, 3$ und $f = X^3 + aX + b$. (Jedes andere normierte Polynom $X^3 + c_2X^2 + c_1X + c_0$ lässt sich mit der Substitution $X \mapsto X - \frac{c_2}{3}$ auf diese Form bringen.) Wir nehmen an, dass f keine Nullstellen hat. Dann ist f irreduzibel. Es gilt $f' = 3X^2 + a \neq 0$, also ist f separabel nach Lemma 3.76(ii).

Sei L/K ein Zerfällungskörper von f und $\alpha \in L$ eine Nullstelle von f . Es gilt $K \subset K(\alpha) \subset L$ und $[K(\alpha) : K] = 3$, $[L : K] \mid 3! = 6$.

Also bleiben die Möglichkeiten:

$$\#[L : K] = \begin{cases} 3 \\ 6 \end{cases} \quad \text{also } \text{Gal}(L/K) = \begin{cases} \text{zyklisch Ordnung 3} \\ \cong \mathfrak{S}_3. \end{cases}$$

In \mathfrak{S}_3 gibt es:

- 1 Element der Ordnung 1, die Identität,
- 3 Elemente der Ordnung 2: (12) , (23) , (31) ,
- 2 Elemente der Ordnung 3: (123) , (132) .

Die Elemente der Ordnung $\neq 2$ sind genau die mit $\text{sgn} = +1$, also gibt es genau eine Untergruppe der Ordnung 3 in \mathfrak{S}_3 , nämlich $\mathfrak{A}_3 = \{\sigma \in \mathfrak{S}_3 \mid \text{sgn } \sigma = 1\}$.

Daher gilt

$$\text{Gal}(L/K) = \begin{cases} \mathfrak{A}_3 \\ \mathfrak{S}_3 \end{cases}.$$

Wann tritt welcher Fall auf?

Seien $\alpha_1, \alpha_2, \alpha_3$ die Nullstellen von f in L . Setze

$$\delta = (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1).$$

Man nennt $\Delta = \delta^2$ die **Diskriminante** des Polynoms f . Beachte: $\Delta \neq 0$. Es gilt

$$\sigma(\delta) = \begin{cases} \delta & \text{wenn } \text{sgn}(\sigma) = 1 \\ -\delta & \text{wenn } \text{sgn}(\sigma) = -1 \end{cases}$$

und deshalb $\sigma(\Delta) = \Delta$ für alle $\sigma \in \text{Gal}(L/K)$. Daher gilt $\Delta \in K$ und

$$\delta \in K \iff \text{Gal}(L/K) \cong \mathfrak{A}_3.$$

Also:

$$\text{Gal}(L/K) \cong \begin{cases} \mathfrak{A}_3 & \Delta \text{ hat Quadratwurzel in } K, \\ \mathfrak{S}_3 & \text{sonst.} \end{cases}$$

Berechnung von Δ in den Koeffizienten von f :

Es gilt $\Delta = -4a^3 - 27b^2$.

Das kann man unter Beachtung von $\alpha_1 + \alpha_2 + \alpha_3 = 0$ direkt ausrechnen.

Beispiele 4.21. 1.) $f = X^3 - X + 1 \in \mathbb{Q}[X]$ ist irreduzibel.

Grund: Wenn reduzibel über \mathbb{Q} , so auch über \mathbb{Z} :

$$(X^3 - X + 1) = (X + a)(X^2 + bX + c)$$

$\Rightarrow ac = 1 \Rightarrow a \in \{\pm 1\}$ aber $f(1) = 1$, $f(-1) = 1$, also ist f irreduzibel. Es gilt $\Delta = -4(-1)^3 - 27 \cdot 1^2 = -23$ (kein Quadrat in \mathbb{Q}).

Also: Die Galoisgruppe des Zerfällungskörpers von f ist \mathfrak{S}_3 .

2.) Wir betrachten $f = X^3 + X^2 - 2X - 1$.

$f(1) = -1$, $f(-1) = 1$ also irreduzibel nach gleichem Argument.

Substitution:

$$(X - \frac{1}{3})^3 + (X - \frac{1}{3})^2 - 2(X - \frac{1}{3}) - 1 = X^3 - \frac{7}{3}X - \frac{7}{27}.$$

Wir erhalten $\Delta = 4\left(\frac{7}{3}\right)^3 - 27\left(-\frac{7}{27}\right)^2 = \frac{1372-49}{27} = \frac{1323}{27} = 49$. Da 49 eine Quadratzahl ist, hat der Zerfällungskörper die Galoisgruppe \mathfrak{A}_3 .

Wie kommt man auf dieses Beispiel? Sei $\zeta_7 = e^{2\pi i/7}$. Das Minimalpolynom von ζ_7 über \mathbb{Q} ist

$$\frac{X^7 - 1}{X - 1} = X^6 + X^5 + \dots + 1$$

(das Polynom ist nach Beispiele 2.46 irreduzibel). Die Nullstellen sind ζ_7^i , $i = 1, \dots, 6$. Also hat $\xi := \zeta_7 + \zeta_7^{-1}$ die Galoisconjugierte $\zeta_7^2 + \zeta_7^{-2}$ und $\zeta_7^3 + \zeta_7^{-3}$.

Nun berechnet man das Minimalpolynom von ξ und erhält f .

Grad 4 (in Spezialfällen)

Beispiele 4.22. 1.) Sei $f \in \mathbb{Q}[X]$ irreduzibel von der Form $X^4 + cX^2 + d$. Durch Substitution bringen wir f auf die Form

$$f = (X^2 - a)^2 - b.$$

Wir setzen voraus: $b > a^2$ (z.B. $X^4 - 2$, $X^4 - 4X^2 - 6$). Die Nullstellen von f in \mathbb{C} sind

$$\alpha = \sqrt{a + \sqrt{b}}, -\alpha, \beta = \sqrt{a - \sqrt{b}}, -\beta.$$

Nach Voraussetzung ist $a + \sqrt{b} > 0$, d.h. α ist eine reelle Quadratwurzel, die wir ohne Einschränkung positiv wählen können. Wieder nach Voraussetzung ist $a - \sqrt{b} < 0$, d.h. β ist eine rein imaginäre Quadratwurzel aus $a - \sqrt{b}$ (z.B. $i\sqrt{|a - \sqrt{b}|}$) und $-\beta$ ist die andere.

Es ist $L = \mathbb{Q}(\alpha, \beta) \subset \mathbb{C}$ der Zerfällungskörper von f . Wir haben $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg f = 4$.

Außerdem gilt $\beta^2 = a - \sqrt{b} = 2a - (a + \sqrt{b}) = 2a - \alpha^2 \in K(\alpha)$. Also gilt $[K(\alpha, \beta) : K(\alpha)] \leq 2$.

Nun ist aber $\alpha \in \mathbb{R}$, also $\mathbb{Q}(\alpha) \subset \mathbb{R}$ und $\beta \notin \mathbb{R}$, also $\beta \notin \mathbb{Q}(\alpha)$, folglich gilt

$$[L : \mathbb{Q}(\alpha)] = 2 \text{ und } [L : \mathbb{Q}] = 8.$$

$\text{Gal}(L/\mathbb{Q})$ ist eine Untergruppe in $\mathfrak{S}_4 = \mathfrak{S}(\{\alpha, -\alpha, \beta, -\beta\})$ und es gilt $\#\mathfrak{S}_4 = 4! = 24$. Für jedes $\sigma \in G = \text{Gal}(L/\mathbb{Q}) \subset \mathfrak{S}_4$ gilt $\sigma(-\alpha) = -\sigma(\alpha)$ und $\sigma(-\beta) = -\sigma(\beta)$.

Es gibt genau 8 Elemente in $S(\{\alpha, -\alpha, \beta, -\beta\})$, die diese Bedingung erfüllen: Für $\sigma(\alpha)$ gibt es 4 Möglichkeiten. Dann für $\sigma(-\alpha)$ genau eine. Für $\sigma(\beta)$ verbleiben 2 Möglichkeiten und $\sigma(-\beta)$ ist dann festgelegt. Da $[L : \mathbb{Q}]$ den Grad 8 hat, sind dies genau die Elemente in $G := \text{Gal}(L/\mathbb{Q})$. Betrachte $\sigma, \tau \in G \subset \mathfrak{S}_4$ die durch

$$\begin{aligned} \sigma : \alpha &\mapsto \beta, & \beta &\mapsto -\alpha \\ \tau : \alpha &\mapsto -\alpha, & \beta &\mapsto \beta \end{aligned}$$

gegeben sind. Die Untergruppe $\langle \sigma \rangle \subset G$ ist zyklisch von der Ordnung 4, also vom Index 2 in G (also Normalteiler). τ hat die Ordnung 2. Wegen $\tau \notin \langle \sigma \rangle$ gilt (Nebenklassenzerlegung)

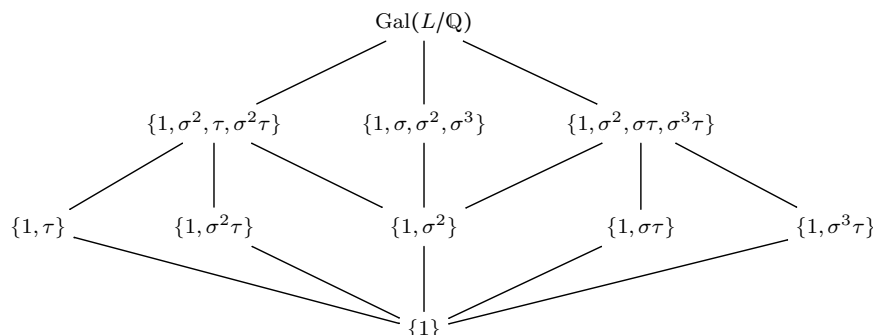
$$G = \langle \sigma, \tau \rangle = \langle \sigma \rangle \sqcup \tau \langle \sigma \rangle = \langle \sigma \rangle \sqcup \langle \sigma \rangle \tau$$

explizit: $G = \{1, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}$.

Man rechnet nach: $\tau\sigma = \sigma^3\tau$. So erhält man die Gruppenstruktur, z.B.

$$\begin{aligned} \sigma^3(\sigma^2\tau) &= \sigma^5\tau = \sigma^4\sigma\tau = \sigma\tau \\ (\sigma^2\tau)(\sigma^3) &= \sigma^2\tau\sigma\sigma\sigma \\ &= \sigma^2\sigma^3\tau\sigma\sigma \\ &= \sigma^2\sigma^3\sigma^3\tau\sigma \\ &= \sigma^2\sigma^3\sigma^3\sigma^3\tau \\ &= \sigma^{11}\tau = \sigma^3\tau. \end{aligned}$$

Insbesondere ist G nicht kommutativ. Mittels Probieren findet man dann alle Untergruppen und bekommt folgendes Bild.



Identifiziert man mit Reihenfolge $\{\alpha, \beta, -\alpha, \beta\}$ mit $\{1, 2, 3, 4\}$ so ist $\text{Gal}(L/\mathbb{Q}) \subset \mathfrak{S}_4$ die von $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ und $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$ erzeugte Untergruppe. Diese nennt man D_4 (Diedergruppe).

2.)

$$\begin{aligned} f &= X^4 - 4X^2 + 16 \in \mathbb{Q}[X] \\ &= (X^2 - 2)^2 + 12. \end{aligned}$$

Suchen Nullstellen:

$$\begin{aligned} (X^2 - 2)^2 &= -12 \Rightarrow X^2 - 2 = 2\sqrt{-3} \\ \Rightarrow X^2 &= 4\left(\frac{1}{2} + \frac{1}{2}\sqrt{-3}\right) = 4e^{2\pi i/6}. \end{aligned}$$

Wir sehen, dass $x = 2\zeta$, $\zeta = e^{2\pi i/12}$, eine Nullstelle ist.

Durch Einsetzen sieht man, dass die anderen Nullstellen $2\zeta^5$, $2\zeta^7$ und $2\zeta^{11}$ sind. Irreduzibilität des Polynoms: Nach Satz 2.42 genügt es zu zeigen, dass f irreduzibel in $\mathbb{Z}[X]$ ist. Zunächst hat f keine Nullstellen in \mathbb{Z} (weil nicht in \mathbb{R}). Sei

$$\begin{aligned} f &= (X^2 + aX + b)(X^2 + cX + d), a, b, c, d \in \mathbb{Z} \\ &= X^4 + (a + c)X^3 + (b + d + ac)X^2 + (ad + bc)X + bd \end{aligned}$$

$$\leadsto c = -a \text{ und } a(d - b) = 0.$$

$a = 0$ führt auf $b + d = -4$, $bd = 16$; hat keine Lösung in \mathbb{Z} .

$a \neq 0$ führt auf $d = b \Rightarrow b^2 = 16$ und $2b - a^2 = -4 \leadsto a^2 = 2b + 4 = -4$ oder 12 , Widerspruch.

Also ist f irreduzibel und hat die Nullstellen 2ζ , $2\zeta^5$, $2\zeta^7$, $2\zeta^{11}$. Es folgt $L = \mathbb{Q}(2\zeta) = \mathbb{Q}(\zeta)$. Dieser Körper hat Grad 4 über \mathbb{Q} und ist der Zerfällungskörper von f . Jedes $\sigma \in \text{Gal}(L/\mathbb{Q})$ ist schon durch $\sigma(\zeta)$ bestimmt. Also gilt

$$\text{Gal}(L/\mathbb{Q}) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$$

mit $\sigma_1 : \zeta \mapsto \zeta$, $\sigma_2 : \zeta \rightarrow \zeta^5$, $\sigma_3 : \zeta \rightarrow \zeta^7$, $\sigma_4 : \zeta \rightarrow \zeta^{11}$.

Es gilt $(\zeta^a)^b = (\zeta^{a+b}) = (\zeta^b)^a$, also gilt $\sigma_i \circ \sigma_j = \sigma_j \circ \sigma_i$ für $i, j \in \{1, 2, 3, 4\}$. Daher ist $G = \text{Gal}(L/\mathbb{Q})$ kommutativ. Außerdem gilt $\sigma_1 = \text{id}$, $\sigma_2^2 = \sigma_3^2 = \sigma_4^2 = \text{id}$ und $\sigma_4 = \sigma_2 \circ \sigma_3$. Daher ist die Abbildung

$$G \rightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$$

$$\sigma_1 \mapsto (0, 0), \sigma_2 \mapsto (1, 0), \sigma_3 \mapsto (0, 1), \sigma_4 \mapsto (1, 1),$$

ein Gruppenisomorphismus. Der Körper $L = \mathbb{Q}(\zeta)$ heißt der **12. Kreisteilungskörper**.

4.3 Die allgemeine Gleichung über einem Körper

Seien T_1, \dots, T_n Variablen und

$$L = k(T_1, \dots, T_n) = Q(k[T_1, \dots, T_n]).$$

Jede Permutation $\pi \in \mathfrak{S}_n$ induziert einen Automorphismus von L , indem man π auf die Indizes der Variablen anwendet:

$$\frac{g(T_1, \dots, T_n)}{h(T_1, \dots, T_n)} \mapsto \frac{g(T_{\pi(1)}, \dots, T_{\pi(n)})}{h(T_{\pi(1)}, \dots, T_{\pi(n)})}.$$

Dies gibt uns eine natürliche Inklusion

$$\mathfrak{S}_n \subset \text{Aut}(L).$$

Definition 4.23. Der Fixkörper $K = L^{\mathfrak{S}_n}$ heißt der Körper der **symmetrischen rationalen Funktionen** mit Koeffizienten in k .

Nach Satz 4.4 ist L/K eine Galoiserweiterung und $\text{Gal}(L/K) \cong \mathfrak{S}_n$, insbesondere gilt $[L : K] = n!$.

Wir suchen eine Gleichung für L/K , d.h. ein Polynom in $K[X]$ mit L als Zerfällungskörper. Ansatz:

$$\begin{aligned} f(X) &= \prod_{i=1}^n (X - T_i) \\ &= \sum_{j=0}^n (-1)^j s_j(T_1, \dots, T_n) X^{n-j} \in k[T_1, \dots, T_n][X]. \end{aligned}$$

Definition 4.24. Das Polynom $s_j, j = 0, \dots, n$, heißt das **j -te elementarsymmetrische Polynom** (auch **elementarsymmetrische Funktion**) in T_1, \dots, T_n . Explizit:

$$\begin{aligned} s_0 &= 1 \\ s_1 &= T_1 + \dots + T_n \\ s_2 &= T_1 T_2 + T_1 T_3 + \dots + T_{n-1} T_n \\ &\vdots \\ s_n &= T_1 \dots T_n \end{aligned}$$

Beachte: $s_j \in K$, $j = 1, \dots, n$, also $k(s_1, \dots, s_n) \subset K$ und $f \in k(s_1, \dots, s_n)[X] \subset K[X]$. L ist Zerfällungskörper von f über $k(s_1, \dots, s_n)$, also auch über K . Es gilt $\deg f = n$, $[L : K] = n!$, also ist f irreduzibel über K .

Satz 4.25. *Jede symmetrische rationale Funktion lässt sich auf genau eine Weise als rationale Funktion in den elementarsymmetrischen Funktionen darstellen, d.h.*

$$(i) \quad k(s_1, \dots, s_n) = K,$$

(ii) s_1, \dots, s_n sind algebraisch unabhängig über k .

Beweis. (i) L ist Zerfällungskörper von f über $k(s_1, \dots, s_n)$, daher gilt $[L : k(s_1, \dots, s_n)] \leq n!$. Aber es gilt $[L : K] = n!$ und daher $[K : k(s_1, \dots, s_n)] = 1$.

(ii) Wir betrachten den Polynomring $k[S_1, \dots, S_n]$ wobei S_1, \dots, S_n Variablen sind. Um zu zeigen, dass s_1, \dots, s_n algebraisch unabhängig über k sind, ist nach Definition zu zeigen, dass der durch die universelle Eigenschaft des Polynomrings gegebene Ringhomomorphismus

$$k[S_1, \dots, S_n] \rightarrow K, \quad S_i \mapsto s_i$$

injektiv ist. Wir betrachten den Zerfällungskörper \tilde{L} über $k(S_1, \dots, S_n)$ des Polynoms

$$\tilde{f} = \sum_{j=0}^n (-1)^j S_j X^{n-j} \in k(S_1, \dots, S_n)[X],$$

wobei formal $S_0 = 1$ gesetzt sei. Seien t_1, \dots, t_n die Nullstellen von \tilde{f} in \tilde{L} (evtl. mit Vielfachheiten). Dann gilt (die S_j sind Polynome in den t_j)

$$\tilde{L} = k(S_1, \dots, S_n)(t_1, \dots, t_n) = k(t_1, \dots, t_n).$$

Bild:

$$\begin{array}{ccc} L = k(T_1, \dots, T_n) & & \tilde{L} = k(t_1, \dots, t_n) \\ \downarrow & & \downarrow \\ k(s_1, \dots, s_n) & & k(S_1, \dots, S_n) \\ \downarrow & & \downarrow \\ k & \xlongequal{\quad\quad\quad} & k. \end{array}$$

Nun betrachten wir den durch die Universaleigenschaft des Polynomrings gegebenen Homomorphismus

$$k[T_1, \dots, T_n] \longrightarrow k[t_1, \dots, t_n], \quad T_i \longrightarrow t_i.$$

Dieser bildet die elementarsymmetrischen Funktionen in den T_i auf die elementarsymmetrischen Funktionen in den t_i ab, also geht s_j auf S_j für $j = 1, \dots, n$, d.h. wir erhalten einen surjektiven Homomorphismus

$$k[s_1, \dots, s_n] \longrightarrow k[S_1, \dots, S_n], \quad s_i \longmapsto S_i.$$

Nun geht ein $x = h(s_1, \dots, s_n) \in k[s_1, \dots, s_n]$ genau dann auf 0 in $k[S_1, \dots, S_n]$ wenn $h = 0$, also wenn $x = 0$. Der Homomorphismus ist daher ein Isomorphismus. Insbesondere existiert der inverse Homomorphismus und ist wieder bijektiv. Die Komposition dieses inversen Homomorphismus mit der Einbettung $k[s_1, \dots, s_n] \hookrightarrow k(s_1, \dots, s_n) = K$ ist somit injektiv. Dieser ist aber gerade der Homomorphismus, der nach Universaleigenschaft durch $S_i \mapsto s_i$, $i = 1, \dots, n$ gegeben ist. Daher sind s_1, \dots, s_n algebraisch unabhängig über k . \square

Bemerkung 4.26. Wir erhalten einen Isomorphismus

$$\begin{array}{ccc} k(T_1, \dots, T_n) & \xrightarrow{\sim} & k(t_1, \dots, t_n) \\ | & & | \\ k(s_1, \dots, s_n) & \xrightarrow{\sim} & k(S_1, \dots, S_n) \end{array}$$

von Galoiserweiterungen mit Galoisgruppe \mathfrak{S}_n .

Definition 4.27. Seien S_1, \dots, S_n Variablen und k ein Körper. Das Polynom

$$p(X) = X^n + S_1 X^{n-1} + \dots + S_n \in k(S_1, \dots, S_n)[X]$$

heißt das **allgemeine Polynom n -ten Grades über k** . Die Gleichung $p(X) = 0$ heißt die **allgemeine Gleichung n -ten Grades über k** .

Satz 4.28. Das allgemeine Polynom n -ten Grades $p(X) \in k(S_1, \dots, S_n)$ ist separabel und irreduzibel. Es besitzt die symmetrische Gruppe \mathfrak{S}_n als Galoisgruppe.

Beweis. Wir betrachten $L = k(T_1, \dots, T_n)$ und $K = L^{\mathfrak{S}_n} = k(s_1, \dots, s_n)$. Nach Satz 4.25 sind s_1, \dots, s_n algebraisch unabhängig über k , also definiert die Regel $S_j \mapsto (-1)^j s_j$ einen Körperisomorphismus

$$k(S_1, \dots, S_n) \xrightarrow{\sim} k(s_1, \dots, s_n),$$

wobei S_1, \dots, S_n Variablen sind. Bezüglich dieser Identifizierung wird p zu dem Polynom \tilde{f} aus dem Beweis von Satz 4.25 und \tilde{f} ist separabel, irreduzibel mit \mathfrak{S}_n als Galoisgruppe des Zerfällungskörpers. \square

4.4 Symmetrische Polynome

Sei A ein Ring (kommutativ mit 1). Die symmetrische Gruppe \mathfrak{S}_n wirkt auf dem Ring $A[T_1, \dots, T_n]$ durch

$$\pi(f(T_1, \dots, T_n)) = f(T_{\pi(1)}, \dots, T_{\pi(n)}).$$

Definition 4.29. Ein Polynom $f \in A[T_1, \dots, T_n]$ heißt **symmetrisch** wenn $\pi(f) = f$ für alle $\pi \in \mathfrak{S}_n$ gilt.

Beispiel 4.30. Die elementarsymmetrischen Polynome

$$\begin{aligned}s_0 &= 1 \\ s_1 &= T_1 + \cdots + T_n \\ s_2 &= T_1 T_2 + T_1 T_3 + \cdots + T_{n-1} T_n \\ &\vdots \\ s_n &= T_1 \cdots T_n\end{aligned}$$

sind symmetrisch.

Bemerkung 4.31. Die Anzahl der Variablen müsste eigentlich mit in die Notation. Setzt man für $i = 0, \dots, n$

$$(s_i)_0(T_1, \dots, T_{n-1}) = s_i(T_1, \dots, T_{n-1}, 0),$$

so ist $(s_n)_0 = 0$ und für $i = 0, \dots, n-1$ ist $(s_i)_0$ das i -te elementarsymmetrische Polynom in $n-1$ Variablen.

Satz 4.32. Jedes symmetrische Polynom $f \in A[T_1, \dots, T_n]$ lässt sich als Polynom in den elementarsymmetrischen Polynomen schreiben, d.h. es existiert ein $g \in A[T_1, \dots, T_n]$ mit

$$f(T_1, \dots, T_n) = g(s_1, \dots, s_n).$$

Beispiel 4.33.

$$\begin{aligned}T_1^2 + T_2^2 &= (T_1 + T_2)^2 - 2T_1 T_2 \\ &= s_1^2 - 2s_2.\end{aligned}$$

Bemerkungen 4.34. 1) Man kann zeigen, dass g eindeutig bestimmt ist. Ist A nullteilerfrei, so folgt dies aus Satz 4.25. Es gilt nämlich

$$f(T_1, \dots, T_n) = g(s_1, \dots, s_n)$$

in $Q(A)(T_1, \dots, T_n)$ und deshalb ist g eindeutig in $Q(A)(T_1, \dots, T_n)$. Aber die natürliche Abbildung $A[T_1, \dots, T_n] \rightarrow Q(A)(T_1, \dots, T_n)$ ist injektiv.

2) Das eindeutig bestimmte Polynom $N_r \in \mathbb{Z}[T_1, \dots, T_n]$ mit

$$N_r(s_1, \dots, s_n) = T_1^r + \cdots + T_n^r$$

heißt **r -tes Newton-Polynom**. Beispiel: $N_2(s_1, s_2) = s_1^2 - 2s_2$. Für $r \leq n$ ist N_r unabhängig von der Anzahl der Variablen n .

Beweis von Satz 4.32. Für $n = 1$ gilt $s_1 = T_1$ und die Aussage ist trivial. Wir wollen den allgemeinen Fall per Induktion nach n behandeln. Damit die Induktion durchläuft, verschärfen wir die Aussage leicht. Dafür definieren für $f \in A[T_1, \dots, T_n]$ wir den **Grad** $\deg f$ und das **Gewicht** $\gamma(f)$ wie folgt:

Wir setzen für ein Monom $M = aT_1^{i_1} \dots T_n^{i_n}$ mit $a \neq 0$, $\deg M = i_1 + \dots + i_n$ und $\gamma(M) = i_1 + 2i_2 + \dots + ni_n$. Für $f = \sum M_i$ setzen wir

$$\deg(f) := \max \deg(M_i), \gamma(f) := \max \gamma(M_i).$$

Wir beweisen nun die verschärfte Aussage: *Für jedes symmetrische Polynom $f \in A[T_1, \dots, T_n]$ vom Grad d existiert ein $g \in A[T_1, \dots, T_n]$ vom Gewicht $\leq d$ mit $f(T_1, \dots, T_n) = g(s_1, \dots, s_n)$.*

Die Aussage ist trivial für $n = 1$. Sei nun $n > 1$ und der Satz für symmetrische Polynome in weniger als n Variablen schon bewiesen.

Sei $f \in A[T_1, \dots, T_n]$ symmetrisch vom Grad d . Nach Induktionsvoraussetzung gilt

$$f(T_1, \dots, T_{n-1}, 0) = \phi((s_1)_0, \dots, (s_{n-1})_0)$$

für ein $\phi \in A[T_1, \dots, T_{n-1}]$ mit $\gamma(\phi) \leq d$

(Beachte: $\deg f(T_1, \dots, T_{n-1}, 0) \leq \deg f(T_1, \dots, T_{n-1}, T_n) = d$).

Setze

$$h(T_1, \dots, T_n) = f(T_1, \dots, T_n) - \phi(s_1, \dots, s_{n-1}).$$

Dann ist h symmetrisch. Im Fall $h = 0$ sind wir fertig. Sei $h \neq 0$. Wegen $\deg s_i = i$ ist der Grad von $\phi(s_1, \dots, s_{n-1})$ als Polynom in den T_i 's höchstens $\gamma(\phi) \leq d$. Daher gilt $\deg h \leq d$. Nach Konstruktion gilt $h(T_1, \dots, T_{n-1}, 0) = 0$. Daher taucht T_n in jedem Monom von h auf, und wegen der Symmetrie auch T_1, \dots, T_{n-1} . Folglich gilt

$$h = s_n \cdot f_1$$

mit f_1 symmetrisch und $\deg f_1 = \deg(h) - n \leq d - n$. Wir erhalten

$$f = \phi(s_1, \dots, s_{n-1}) + s_n \cdot f_1.$$

Jetzt machen wir mit f_1 weiter und erhalten mit der gleichen Methode

$$f_1 = \phi_1(s_1, \dots, s_{n-1}) + s_n f_2$$

mit $\gamma(\phi_1) \leq d - n$ und $\deg f_2 \leq d - 2n$. Einsetzen ergibt

$$f = \phi(s_1, \dots, s_{n-1}) + s_n \phi_1(s_1, \dots, s_{n-1}) + s_n f_2.$$

Wir beachten, dass $\gamma(X_n \phi_1(X_1, \dots, X_{n-1})) = \gamma(\phi_1) + n \leq d$ gilt. Nun machen wir mit f_2 weiter. Der Grad wird jedes mal kleiner, daher bricht der Prozess ab. \square

4.5 Einheitswurzelkörper

Lemma 4.35. *Für $n \in \mathbb{N}$ ist das Polynom $X^n - 1 \in K[X]$ genau dann separabel, wenn $\text{char}(K) \nmid n$.*

Beweis. $f' = nX^{n-1}$ ist 0 wenn $\text{char}(K) \mid n$ und wenn $\text{char}(K) \nmid n$ gilt $1 = \frac{1}{n}f' \cdot X - f$, also $(f, f') = 1$. \square

Definition 4.36. Sei $n \in \mathbb{N}$ und $\text{char}(K) \nmid n$. Ein $\zeta \in \overline{K}$ heißt **n -te Einheitswurzel**, wenn $\zeta^n = 1$ gilt.

Die Menge $\mu_n \subset \overline{K}^\times$ der n -ten Einheitswurzeln ist offenbar eine Untergruppe.

Satz 4.37. Sei $n \in \mathbb{N}$, $\text{char } K \nmid n$. Die Gruppe μ_n der n -ten Einheitswurzeln in \overline{K} ist zyklisch von der Ordnung n .

Beweis. Nach Lemma 4.35 ist $X^n - 1$ separabel, also $\#\mu_n = n$. Nach Satz 3.105 ist μ_n zyklisch. \square

Definition 4.38. $\zeta \in \mu_n$ heißt **primitive n -te Einheitswurzel**, wenn es ein Erzeuger der Gruppe μ_n ist.

Beispiel 4.39. $K = \mathbb{C}$: $\zeta_n := e^{2\pi i/n}$ ist eine primitive n -te Einheitswurzel.

Die **Eulersche φ -Funktion** ist auf natürlichen Zahlen definiert durch

$$\varphi(n) = \#\{r \mid 1 \leq r \leq n \text{ und } (n, r) = 1\} = \#(\mathbb{Z}/n\mathbb{Z})^\times.$$

Nun ist $r \in \mathbb{Z}/n\mathbb{Z}$ genau dann eine Einheit, wenn $1 + n\mathbb{Z}$ und damit jedes Element von $\mathbb{Z}/n\mathbb{Z}$ ein Vielfaches von r ist. Daher ist $(\mathbb{Z}/n\mathbb{Z})^\times$ gleich der Menge der Erzeuger der Gruppe $\mathbb{Z}/n\mathbb{Z}$. Da jede zyklische Gruppe der Ordnung n zu $\mathbb{Z}/n\mathbb{Z}$ isomorph ist, gilt

$\varphi(n)$ = Anzahl der Erzeuger einer (jeder) zyklischen Gruppe der Ordnung n .

Lemma 4.40. Es gibt genau $\varphi(n)$ primitive n -te Einheitswurzeln in \overline{K} .

Beweis. Nach Satz 4.37 ist μ_n zyklisch von der Ordnung n . \square

Bemerkung 4.41. Wie berechnet man $\varphi(n)$?

1) Für $(n, m) = 1$ gilt (Chinesischer Restsatz) $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/nm\mathbb{Z}$. Also $(\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times \cong (\mathbb{Z}/nm\mathbb{Z})^\times$, d.h. $\varphi(nm) = \varphi(n)\varphi(m)$.

Damit ist das Problem auf den Fall $n = p^r$, p Primzahl reduziert.

2) $a \in (\mathbb{Z}/p^r\mathbb{Z})^\times \iff (a, p^r) = 1 \iff (a, p) = 1$. D.h. genau die p^{r-1} Klassen $p, 2p, \dots, p^{r-1}p$ sind nicht prim. Daher gilt $\varphi(p^r) = p^r - p^{r-1} = (p-1)p^{r-1}$.

Lemma 4.42. Sei $\text{char}(K) \nmid n$ und $\zeta \in \mu_n$ eine primitive n -te Einheitswurzel. Dann ist $K(\mu_n) = K(\zeta)/K$ eine endliche Galoiserweiterung.

Beweis. $K(\zeta)/K$ ist separabel, weil das Minimalpolynom von ζ ein Teiler von $X^n - 1$ ist. $K(\mu_n)/K$ ist normal, weil Zerfällungskörper des Polynoms $X^n - 1$. Schließlich gilt $K(\mu_n) = K(\zeta)$ weil ζ primitiv. \square

Wir kommen jetzt zum Fall $K = \mathbb{Q}$.

Definition 4.43. Der Körper $\mathbb{Q}(\zeta_n) \subset \mathbb{C}$ heißt der **n -te Kreisteilungskörper**. Das Polynom

$$\Phi_n(X) = \prod_{\substack{\zeta \text{ primitive } n\text{-te} \\ \text{Einheitswurzel in } \mathbb{C}}} (X - \zeta)$$

heißt das **n -te Kreisteilungspolynom**.

Beispiel 4.44. $\Phi_1 = X - 1$, $\Phi_2 = X + 1$, $\Phi_3 = X^2 + X + 1$, $\Phi_4(X) = X^2 + 1$, $\Phi_5(X) = X^4 + X^3 + X^2 + X + 1$.

Bemerkung 4.45. Für p Primzahl ist jede p -te Einheitswurzel $\neq 1$ primitiv. Also gilt

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + \dots + 1.$$

In Beispiele 2.46 haben wir bereits gezeigt, dass $\Phi_p(X)$ irreduzibel ist.

Lemma 4.46. Es gilt $\Phi_n(X) \in \mathbb{Z}[X]$ und $\deg \Phi_n = \varphi(n)$.

Beweis. Die Aussage über den Grad folgt aus Lemma 4.40. Wir zeigen auf zwei Weisen, dass die Koeffizienten von Φ_n in \mathbb{Z} liegen.

Variante 1. Jedes $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ permutiert die primitiven Einheitswurzeln. Daher gilt $\Phi_n^\sigma = \Phi_n$ für alle σ und daher $\Phi_n \in \mathbb{Q}[X]$.

Die Koeffizienten von Φ_n sind ganzzahlige Polynome in Einheitswurzeln, also ganz über \mathbb{Z} und in \mathbb{Q} . Da \mathbb{Z} faktoriell, also ganzabgeschlossen ist, folgt $\Phi_n \in \mathbb{Z}[X]$.

Variante 2 (klassisch). Jede n -te Einheitswurzel ist primitive d -te Einheitswurzel für genau einen Teiler d von n . Daher gilt

$$X^n - 1 = \prod_{d|n} \Phi_d(X).$$

(nebenbei folgt hieraus durch Übergang zu den Graden die klassische Formel $n = \sum_{d|n} \varphi(d)$).

Nun argumentieren wir per Induktion über n . Der Fall $n = 1$ ist trivial. Sei $n > 1$. Dann gilt

$$X^n - 1 = \Phi_n(X) \cdot \underbrace{\left(\prod_{\substack{d|n \\ d < n}} \Phi_d(X) \right)}_{\in \mathbb{Z}[X]}$$

Da \mathbb{Z} faktoriell ist, folgt nach Korollar 2.38, dass $\Phi_n \in \mathbb{Z}[X]$. □

Satz 4.47. $\Phi_n(X) \in \mathbb{Z}[X]$ ist irreduzibel. Es gilt $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.

Beweis. Es genügt zu zeigen, dass Φ_n irreduzibel ist, weil dann $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg \Phi_n = \varphi(n)$ folgt. Sei $\Phi_n = fg$, $f, g \in \mathbb{Z}[X]$, normiert, f irreduzibel.

Behauptung: Gilt $f(\zeta) = 0$, so auch $f(\zeta^p) = 0$ für jede Primzahl $p \nmid n$.

Beweis der Behauptung: Wegen $(p, n) = 1$ ist ζ^p primitiv, also $\Phi_n(\zeta^p) = 0$. Angenommen $f(\zeta^p) \neq 0$. Dann gilt $g(\zeta^p) = 0$, d.h. ζ ist Nullstelle von $g(X^p)$. Da f das Minimalpolynom von ζ ist, folgt $f \mid g(X^p)$, also $g(X^p) = h \cdot f$ mit $h \in \mathbb{Z}[X]$ normiert. Für die Bilder in $\mathbb{Z}/p\mathbb{Z}[X]$ gilt nun

$$\bar{h} \cdot \bar{f} = \bar{g}(X^p) = \bar{g}(X)^p.$$

Also sind \bar{f} und \bar{g} nicht teilerfremd in $\mathbb{Z}/p\mathbb{Z}[X] \simeq \overline{\Phi}_n = \bar{f} \cdot \bar{g}$ ist nicht separabel in $\mathbb{Z}/p\mathbb{Z}[X]$. Aber $\overline{\Phi}_n$ teilt das nach Lemma 4.35 separable Polynom $X^n - 1 \in \mathbb{Z}/p\mathbb{Z}[X]$. Dieser Widerspruch zeigt die Behauptung.

Nun sei ζ eine Nullstelle von f . Ist ζ' irgendeine andere primitive n -te Einheitswurzel, so gilt $\zeta' = \zeta^k$ mit $(k, n) = 1$, also $k = p_1 \dots p_r$, $p_i \nmid n$. $\xRightarrow{\text{induktiv}} f(\zeta') = 0$. Daher sind alle primitiven n -ten Einheitswurzeln Nullstellen von f , woraus $g = 1$ folgt. \square

Wir kommen jetzt wieder zu einem allgemeinen Körper K , $\text{char}(K) \nmid n$.

Satz 4.48. Sei $\zeta_n \in \overline{K}$ eine primitive n -te Einheitswurzel.

- (i) Es ist $K(\zeta_n)/K$ eine endliche, abelsche Galoiserweiterung vom Grad $\leq \varphi(n)$.
- (ii) Es existiert ein injektiver Gruppenhomomorphismus

$$\chi : \text{Gal}(K(\zeta_n)/K) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times,$$

so dass für jede n -te Einheitswurzel $\zeta \in K(\zeta_n)$ und jedes $\sigma \in \text{Gal}(K(\zeta_n)/K)$ gilt:

$$\sigma(\zeta) = \zeta^{\chi(\sigma)}.$$

Für $K = \mathbb{Q}$ ist χ ein Isomorphismus.

Bemerkung 4.49. 1. Wegen $\zeta^n = 1$ hängt ζ^a nur von $a \bmod n$ ab, daher ist $\zeta^{\chi(\sigma)}$ wohldefiniert.

2. χ heißt der **zyklotomische Charakter**.

Beweis. Wir wissen schon, dass $K(\zeta_n)/K$ endlich, galoissch ist. Aussage (i) folgt aus (ii) wegen $\#(\mathbb{Z}/n\mathbb{Z})^\times = \varphi(n)$ und weil Untergruppen abelscher Gruppen abelsch sind.

Zu (ii). Da ζ_n primitiv ist, gilt $\sigma(\zeta_n) = \zeta_n^a$ für ein eindeutig bestimmtes $a \in \mathbb{Z}/n\mathbb{Z}$. Außerdem ist $\sigma(\zeta_n)$ wieder primitiv, also $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. Setze $\chi(\sigma) = a$. Wir müssen nachweisen:

- 1) χ ist Gruppenhomomorphismus.

2) χ ist injektiv.

3) $\sigma(\zeta) = \zeta^{\chi(\sigma)}$ für jede n -te Einheitswurzel ζ .

Zu 1) Es gilt $\sigma\tau(\zeta_n) = \sigma(\zeta_n^{\chi(\tau)}) = (\sigma(\zeta_n))^{\chi(\tau)} = (\zeta_n^{\chi(\sigma)})^{\chi(\tau)} = \zeta_n^{\chi(\sigma)\chi(\tau)}$.

Also $\chi(\sigma\tau) = \chi(\sigma)\chi(\tau)$.

Zu 2) $\sigma \in \text{Gal}(K(\zeta_n)/K)$ ist durch $\sigma(\zeta_n) = \zeta_n^{\chi(\sigma)}$ eindeutig bestimmt. Daher folgt aus $\chi(\sigma) = 1 = \chi(\text{id})$ dass $\sigma = \text{id}$.

Zu 3) Ist ζ irgendeine n -te Einheitswurzel, so gilt $\zeta = \zeta_n^a$, $a \in \mathbb{Z}/n\mathbb{Z}$. Also $\sigma(\zeta) = \sigma(\zeta_n^a) = \sigma(\zeta_n)^a = (\zeta_n^{\chi(\sigma)})^a = (\zeta_n^a)^{\chi(\sigma)} = \zeta^{\chi(\sigma)}$.

Schließlich gilt nach Satz 4.47: $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$, also ist für $K = \mathbb{Q}$ der injektive Homomorphismus χ ein Isomorphismus. \square

Satz 4.50. Sei q eine Primpotenz und sei $(q, n) = 1$. Sei $\zeta_n \in \bar{\mathbb{F}}_q$ eine primitive n -te Einheitswurzel.

- (i) Der zyklotomische Charakter $\chi : \text{Gal}(\mathbb{F}_q(\zeta_n)/\mathbb{F}_q) \rightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ bildet den relativen Frobeniusautomorphismus von $\mathbb{F}_q(\zeta_n)/\mathbb{F}_q$ auf die Restklasse \bar{q} von q in $(\mathbb{Z}/n\mathbb{Z})^\times$ ab. Insbesondere definiert χ einen Isomorphismus zwischen $\text{Gal}(\mathbb{F}_q(\zeta_n)/\mathbb{F}_q)$ und der durch \bar{q} in $(\mathbb{Z}/n\mathbb{Z})^\times$ erzeugten Untergruppe.
- (ii) Der Grad $[\mathbb{F}_q(\zeta_n) : \mathbb{F}_q]$ ist gleich der Ordnung von \bar{q} in $(\mathbb{Z}/n\mathbb{Z})^\times$ (d.h. die kleinste natürliche Zahl N mit $q^N \equiv 1 \pmod{n}$).
- (iii) Φ_n ist genau dann irreduzibel in $\mathbb{F}_q[X]$, wenn \bar{q} die Gruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ erzeugt.

Bemerkung 4.51. Damit (iii) gelten kann, ist es notwendig, dass $(\mathbb{Z}/n\mathbb{Z})^\times$ zyklisch ist. Dies ist z.B. richtig für $n = \text{Primzahl}$.

Beweis. Nach Satz 3.102 ist $\text{Gal}(\mathbb{F}_q(\zeta_n)/\mathbb{F}_q)$ zyklisch und erzeugt vom relativen Frobenius $\sigma(x) = x^q$. Insbesondere gilt $\sigma(\zeta_n) = \zeta_n^q$ also $\chi(\sigma) = \bar{q} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Somit folgt (i) und (ii) folgt wegen $[\mathbb{F}_q(\zeta_n) : \mathbb{F}_q] = \#\text{Gal}(\mathbb{F}_q(\zeta_n)/\mathbb{F}_q) = \#\langle \bar{q} \rangle = \text{ord}_{(\mathbb{Z}/n\mathbb{Z})^\times}(\bar{q})$.

(iii) Φ_n irreduzibel in $\mathbb{F}_q[X] \iff [\mathbb{F}_q(\zeta_n) : \mathbb{F}_q] = \varphi(n) \iff \text{ord}_{(\mathbb{Z}/n\mathbb{Z})^\times}(\bar{q}) = \varphi(n) \iff \bar{q} \text{ erzeugt } (\mathbb{Z}/n\mathbb{Z})^\times. \square$

4.6 Lineare Unabhängigkeit von Charakteren

Definition 4.52. Sei G eine Gruppe und K ein Körper. Ein Homomorphismus $\chi : G \rightarrow K^\times$ heißt K -wertiger **Charakter** von G .

Die Menge der Abbildungen $\text{Abb}(G, K)$ wird zum K -Vektorraum durch wertweise Addition und Skalarmultiplikation, d.h.

$$(a_1\phi_1 + a_2\phi_2)(g) := a_1\phi_1(g) + a_2\phi_2(g),$$

$$\phi_1, \phi_2 \in \text{Abb}(G, K), \quad a_1, a_2 \in K, \quad g \in G.$$

Satz 4.53. *Verschiedene Charaktere χ_1, \dots, χ_n einer Gruppe G mit Werten in einem Körper K sind linear unabhängig als Elemente im K -Vektorraum $\text{Abb}(G, K)$.*

Beweis. Angenommen der Satz wäre falsch. Dann gibt ein minimales $n \in \mathbb{N}$, so dass n linear abhängige Charaktere χ_1, \dots, χ_n existieren. Da ein Charakter $\neq 0$ ist, gilt $n \geq 2$. Sei nun

$$a_1\chi_1 + \dots + a_n\chi_n = 0, \quad a_i \in K,$$

eine nichttriviale Relation in $\text{Abb}(G, K)$. Wegen n minimal, gilt $a_i \neq 0$, $i = 1, \dots, n$. Wir wählen $g \in G$ mit $\chi_1(g) \neq \chi_2(g)$ und betrachten für variierendes h die Gleichung

$$\begin{aligned} 0 &= a_1\chi_1(gh) + \dots + a_n\chi_n(gh) \\ &= a_1\chi_1(g)\chi_1(h) + \dots + a_n\chi_n(g)\chi_n(h). \end{aligned}$$

Also ist auch

$$a_1\chi_1(g)\chi_1 + \dots + a_n\chi_n(g)\chi_n = 0$$

eine Relation. Abzug von $0 = \chi_1(g)(a_1\chi_1 + \dots + a_n\chi_n)$ ergibt

$$a_2(\chi_1(g) - \chi_2(g))\chi_2 + \dots + a_n(\chi_1(g) - \chi_n(g))\chi_n = 0.$$

Dies ist eine neue nicht-triviale Relation mit (höchstens) $n - 1$ Charakteren im Widerspruch zur Minimalität von n . \square

Es sei nun K ein Körper und L/K und M/K Körpererweiterungen. Die Menge $\text{Hom}_K(L, M)$ (Körperhomomorphismen) ist eine Teilmenge des K -Vektorraums $\text{Hom}_{K\text{-VR}}(L, M)$ (K -Vektorraumhomomorphismen). Die K -Vektorraumstruktur setzt sich zu einer M -Vektorraumstruktur fort durch

$$(\alpha\phi)(x) = \alpha\phi(x), \quad \alpha \in M, \quad x \in L, \quad \phi \in \text{Hom}_{K\text{-VR}}(L, M).$$

Auf diese Weise wird $\text{Hom}_{K\text{-VR}}(L, M)$ ein M -Untervektorraum von $\text{Abb}(L, M)$. Da ein Homomorphismus die Null auf die Null schickt, wird $\text{Hom}_{K\text{-VR}}(L, M)$ auch zu einem M -Untervektorraum von $\text{Abb}(L^\times, M)$:

$$\begin{array}{ccc} \text{Hom}_K(L, M) & & \\ \downarrow & \searrow |_{L^\times} & \\ \text{Hom}_{K\text{-VR}}(L, M) & & \text{Hom}(L^\times, M^\times) \\ \downarrow & \searrow |_{L^\times} & \downarrow \\ \text{Abb}(L, M) & \xrightarrow{|_{L^\times}} & \text{Abb}(L^\times, M). \end{array}$$

Satz 4.54. *Es seien L/K und M/K Körpererweiterungen. Dann ist $\text{Hom}_K(L, M)$ eine linear unabhängige Menge von Vektoren im M -Vektorraum $\text{Abb}(L, M)$.*

Beweis. Es seien $\sigma_1, \dots, \sigma_n \in \text{Hom}_K(L, M)$ linear abhängig in $\text{Abb}(L, M)$. Dann sind sie auch linear abhängig im M -Untervektorraum $\text{Hom}_{K\text{-VR}}(L, M)$ und daher auch in $\text{Abb}(L^\times, M)$. Als Elemente im letzteren sind sie durch $\sigma_i|_{L^\times} : L^\times \rightarrow M^\times$, $i = 1, \dots, n$, gegeben. Dies sind M -wertige Charaktere der Gruppe L^\times , also linear unabhängig nach Satz 4.53. Widerspruch. \square

4.7 Norm und Spur

Definition 4.55. Sei L/K eine endliche Körpererweiterung. Für $a \in L$ betrachtet man

$$\varphi_a : L \longrightarrow L, \quad x \longmapsto ax,$$

als K -Vektorraum-Endomorphismus und nennt

$$\text{Sp}_{L/K}(a) := \text{Sp}(\varphi_a), \quad N_{L/K}(a) := \det \varphi_a.$$

die **Spur** bzw. die **Norm** von a bzgl. L/K .

Bemerkung 4.56. Für $a, b \in L$ gilt $\varphi_{a+b} = \varphi_a + \varphi_b$, also

$$\text{Sp}_{L/K}(a+b) = \text{Sp}_{L/K}(a) + \text{Sp}_{L/K}(b).$$

Mit anderen Worten: $\text{Sp}_{L/K} : L^+ \rightarrow K^+$ ist ein Homomorphismus. Zudem gilt für $a \in K$, $b \in L$: $\varphi_{ab} = a\varphi_b$, also $\text{Sp}_{L/K}(ab) = a\text{Sp}_{L/K}(b)$. D.h.:

$$\text{Sp}_{L/K} : L \longrightarrow K, \quad b \mapsto \text{Sp}_{L/K}(b)$$

ist ein K -Vektorraumhomomorphismus.

Analog: $\varphi_{ab} = \varphi_a \circ \varphi_b$, also gilt

$$N_{L/K}(ab) = N_{L/K}(a)N_{L/K}(b).$$

Für $a \neq 0$ ist φ_a ein Automorphismus und daher $N_{L/K}(a) = \det \varphi_a \neq 0$. Durch Einschränkung erhalten wir daher einen Homomorphismus $N_{L/K} : L^\times \rightarrow K^\times$.

Beispiel 4.57. \mathbb{C}/\mathbb{R} : $\text{Sp}_{\mathbb{C}/\mathbb{R}}(z) = z + \bar{z}$, $N_{\mathbb{C}/\mathbb{R}}(z) = z\bar{z} = |z|^2$.

Grund: Betrachte die Basis $(1, i)$ von \mathbb{C} als \mathbb{R} -Vektorraum. Für $z = a + bi$, $a, b \in \mathbb{R}$ wird φ_z durch die Matrix $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ dargestellt. Wir erhalten: $\text{Sp}(z) = 2a = (a + bi) + (a - bi)$ und $N(z) = a^2 + b^2 = (a + bi)(a - bi)$.

Lemma 4.58. Sei $n = [L : K]$. Dann gilt für $a \in K$

$$\text{Sp}_{L/K}(a) = na, \quad N_{L/K}(a) = a^n.$$

Beweis. $\varphi_a = a \cdot \text{id}_L$. \square

Lemma 4.59. Sei $L = K(a)$ und $f = X^n + c_{n-1}X^{n-1} + \dots + c_0$ das Minimalpolynom von a über K . Dann gilt

$$\mathrm{Sp}_{L/K}(a) = -c_{n-1}, \quad N_{L/K}(a) = (-1)^n c_0.$$

Beweis. Es gilt $n = [L : K]$ und $f = \chi^{\min}(\varphi_a) \stackrel{\text{Gradgründe}}{=} \chi^{\mathrm{char}}(\varphi_a)$. An $\chi^{\mathrm{char}}(\varphi_a)$ liest man $\mathrm{Sp}(\varphi_a)$ und $\det(\varphi_a)$ in gewohnter Weise ab. \square

Lemma 4.60. Sei L/K endlich, $a \in L$ und $s = [L : K(a)]$. Dann gilt

$$\mathrm{Sp}_{L/K}(a) = s \cdot \mathrm{Sp}_{K(a)/K}(a), \quad N_{L/K}(a) = (N_{K(a)/K}(a))^s.$$

Beweis. Man wähle eine K -Basis x_1, \dots, x_r von $K(a)$ und eine $K(a)$ -Basis y_1, \dots, y_s von L . Dann ist $x_i y_j$ eine K -Basis von L . Sei nun $A \in M_{r,r}(K)$ die Matrix die bzgl. x_1, \dots, x_r den Endomorphismus φ_a von $K(a)$ darstellt. Dann wird der Endomorphismus φ_a von L bzgl. der Basis $x_i y_j$ durch

$$s \text{ Kästchen } \left\{ \left(\begin{array}{c|c|c} A & & \\ \hline & A & \\ \hline & & \ddots \end{array} \right) =: B \right.$$

dargestellt. Also

$$\begin{aligned} \det(B) &= \det(A)^s \\ \mathrm{Sp}(B) &= s \cdot \mathrm{Sp}(A) \end{aligned}$$

\square

Satz 4.61. Sei L/K endlich mit $[L : K] = q \cdot [L : K]_s = q \cdot r$. Sei \overline{K} ein algebraischer Abschluss von K und $\mathrm{Hom}_K(L, \overline{K}) = \{\sigma_1, \dots, \sigma_r\}$. Dann gilt

$$\mathrm{Sp}_{L/K}(a) = q \cdot \sum_{i=1}^r \sigma_i(a), \quad N_{L/K}(a) = \left(\prod_{i=1}^r \sigma_i(a) \right)^q.$$

Beweis. Spezialfall: $L = K(a)$.

Ist f das Minimalpolynom von a über K , $f = X^n + c_{n-1}X^{n-1} + \dots + c_0$, so gilt

$$f = \left(\prod_{i=1}^r X - \sigma_i(a) \right)^q$$

und die Aussage folgt aus Lemma 4.59. Sei nun L allgemein und sei

$$[L : K(a)] = q_1 [L : K(a)]_s = q_1 r_1$$

$$[K(a) : K] = q_2 [K(a) : K]_s = q_2 r_2$$

Dann gilt nach Lemma 4.60

$$\begin{aligned}\mathrm{Sp}_{L/K}(a) &= q_1 r_1 \mathrm{Sp}_{K(a)/K}(a) \\ &= q_1 \cdot r_1 \cdot q_2 \cdot \sum_{\sigma \in \mathrm{Hom}_K(K(a), \overline{K})} \sigma(a)\end{aligned}$$

Nach Definition des Separabilitätsgrades hat jedes $\sigma \in \mathrm{Hom}_K(K(a), \overline{K})$ genau r_1 viele verschiedene Fortsetzungen in $\mathrm{Hom}_K(L, \overline{K})$. Wir erhalten

$$\mathrm{Sp}_{L/K}(a) = \underbrace{q_1 \cdot q_2}_{=q} \sum_{\sigma \in \mathrm{Hom}_K(L, \overline{K})} \sigma(a).$$

Das Argument für die Norm ist das Gleiche. \square

Korollar 4.62. *Sind $M/L/K$ endliche Körpererweiterungen und $a \in M$, so gilt*

$$\begin{aligned}N_{M/K}(a) &= N_{L/K}(N_{M/L}(a)), \\ \mathrm{Sp}_{M/K}(a) &= \mathrm{Sp}_{L/K}(\mathrm{Sp}_{M/L}(a)).\end{aligned}$$

Beweis. Im Beweis des Gradsatzes Satz 3.88 für $[\ : \]_s$ haben wir gesehen: Mit $\mathrm{Hom}_K(L, \overline{K}) = \{\sigma_1, \dots, \sigma_{r_1}\}$, $\mathrm{Hom}_L(M, \overline{K}) = \{\tau_1, \dots, \tau_{r_2}\}$ und beliebig aber fest gewählten Fortsetzungen σ'_i von σ_i nach $\mathrm{Hom}_K(\overline{K}, \overline{K})$ gilt

$$\mathrm{Hom}_K(M, \overline{K}) = \{\sigma'_i \circ \tau_j \mid i = 1, \dots, r_1, j = 1, \dots, r_2\}.$$

Nun sei

$$\begin{aligned}[L : K] &= q_1 \cdot [L : K]_s = q_1 r_1, \\ [M : L] &= q_2 \cdot [M : L]_s = q_2 r_2.\end{aligned}$$

Dann gilt:

$$\begin{aligned}\mathrm{Sp}_{M/K}(a) &= q_1 q_2 \cdot \sum_{\sigma \in \mathrm{Hom}_K(M, \overline{K})} \sigma(a) \\ &= q_1 q_2 \sum_{i,j} \sigma'_i \circ \tau_j(a) \\ &= q_1 \sum_i \sigma'_i \left(q_2 \sum_j \tau_j(a) \right) \\ &= q_1 \sum_i \sigma'_i(\mathrm{Sp}_{M/L}(a)) \\ &= q_1 \sum_i \sigma_i(\mathrm{Sp}_{M/L}(a)) \\ &= \mathrm{Sp}_{L/K}(\mathrm{Sp}_{M/L}(a)).\end{aligned}$$

Das Argument für die Norm ist das Gleiche. \square

Korollar 4.63. *Sei L/K endlich galoissch. Dann gilt für $a \in L$, $\sigma \in \mathrm{Gal}(L/K)$*

$$N_{L/K}(a) = N_{L/K}(\sigma(a)), \quad \mathrm{Sp}_{L/K}(a) = \mathrm{Sp}_{L/K}(\sigma(a)).$$

Beweis. Die Formeln aus Satz 4.61 ergeben für a und für $\sigma(a)$ das Gleiche. \square

Satz 4.64. Eine endliche Körpererweiterung L/K ist genau dann separabel, wenn die K -lineare Abbildung $\text{Sp}_{L/K} : L \rightarrow K$ nicht-trivial und damit surjektiv ist. Ist L/K separabel, so ist die symmetrische Bilinearform („Spurform“)

$$\text{Sp} : L \times L \longrightarrow K, (x, y) \longmapsto \text{Sp}_{L/K}(xy)$$

nicht-ausgeartet.

Beweis. Der Inseparabilitätsgrad sei $q = p^i$, $p = \text{char}(K)$. Für $i \geq 1$ gilt $\text{Sp}_{L/K}(a) = q \cdot \sum \sigma(\dots) = 0$. Sei also $i = 0$, d.h. L/K separabel und $\text{Hom}_K(L, \overline{K}) = \{\sigma_1, \dots, \sigma_r\}$. Wegen der linearen Unabhängigkeit der σ_i (Satz 4.54) folgt, dass $\text{Sp}_{L/K}$ nicht die Nullabbildung ist. Wir betrachten nun die Spurform. Sei $x \in L$, $x \neq 0$. Dann ist $L \rightarrow L$, $y \mapsto xy$, bijektiv, also existiert ein $y \in L$ so dass $xy \notin \text{Kern}(\text{Sp}_{L/K})$. Mit anderen Worten: $\text{Sp}_{L/K}(xy) = 0 \ \forall y \Rightarrow x = 0$. Das bedeutet aber, dass die Form nicht-ausgeartet ist. \square

4.8 Zyklische Erweiterungen

Satz 4.65 (Hilberts Satz 90). Es sei L/K eine endliche zyklische Galois-Erweiterung und $\sigma \in \text{Gal}(L/K)$ ein Erzeuger. Für $b \in L^\times$ ist äquivalent:

- (i) $N_{L/K}(b) = 1$.
- (ii) es existiert ein $a \in L^\times$ mit $b = a/\sigma(a)$.

Beweis. Für $b = a/\sigma(a)$ gilt $N(b) = N(a)/N(\sigma(a)) = 1$ nach Satz 4.47. Sei nun $N(b) = 1$ und $n = [L : K]$. Die L -wertigen Charaktere $\sigma^0|_{L^\times}, \dots, \sigma^{n-1}|_{L^\times}$ sind linear unabhängig nach Satz 4.53. Insbesondere gilt

$$\sigma^0 + b\sigma^1 + b\sigma(b)\sigma^2 + \dots + b\sigma(b)\dots\sigma^{n-2}(b)\sigma^{n-1} \neq 0.$$

Daher gibt es ein $c \in L^\times$ mit

$$a := c + b\sigma(c) + b\sigma(b)\sigma^2(c) + \dots + b\sigma(b)\dots\sigma^{n-2}(b)\sigma^{n-1}(c) \neq 0.$$

Also gilt

$$\frac{a}{\sigma(a)} = \frac{c + b\sigma(c) + \dots + b\sigma(b)\dots\sigma^{n-2}(b)\sigma^{n-1}(c)}{\sigma(c) + \sigma(b)\sigma^2(c) + \dots + \sigma(b)\dots\sigma^{n-1}(b)\sigma^n(c)}.$$

Der letzte Summand im Nenner ist wegen $N(b) = 1$ und $\sigma^n = \text{id}$ gleich c/b . Es folgt $a/\sigma(a) = b$. \square

Satz 4.66. Es gelte $\text{char}(K) \nmid n$ und K enthalte eine primitive n -te Einheitswurzel. Dann ist jede zyklische Galoiserweiterung L/K vom Grad n von der Form

$$L = K(\sqrt[n]{c}), \quad c \in K^\times,$$

d.h. $L = K(a)$ für ein $a \in L$ mit Minimalpolynom $X^n - c$, $c \in K^\times$.

Beweis. Sei L/K zyklisch, $[L : K] = n$, $\text{Gal}(L/K) = \langle \sigma \rangle$. Sei $\zeta_n \in K$ primitive n -te Einheitswurzel. Dann gilt

$$N_{L/K}(\zeta_n^{-1}) = \zeta_n^{-[L:K]} = 1.$$

Nach Hilberts Satz 90 existiert $a \in L^\times$ mit $\zeta_n^{-1} = a/\sigma(a)$, d.h. $\sigma(a) = \zeta_n a$. Für $i \in \mathbb{N}$ gilt daher:

$$\sigma^i(a) = \zeta_n^i \cdot a.$$

Daher sind $a, \sigma(a), \dots, \sigma^{n-1}(a)$ paarweise verschieden. Insbesondere wird a nur durch das neutrale Element der Galoisgruppe festgelassen, also $L = K(a)$. Außerdem gilt $\sigma(a^n) = \sigma(a)^n = (\zeta_n a)^n = a^n$, also $c = a^n \in K$. Daher gilt $f(a) = 0$ für $f = X^n - c$ und aus Gradgründen ist f das Minimalpolynom von a . \square

5 Mehr Gruppentheorie

5.1 Gruppenoperationen

Definition 5.1. Sei G eine (multiplikativ geschriebene) Gruppe und X eine Menge. Eine Operation (oder auch Wirkung oder Aktion) von G auf X ist eine Abbildung

$$G \times X \longrightarrow X, (g, x) \longmapsto gx,$$

mit

- (i) $1x = x$ für das neutrale Element $1 \in G$ und jedes $x \in X$.
- (ii) $(gh)x = g(hx)$ für $g, h \in G, x \in X$.

Beispiele 5.2. 1) Die Multiplikation

$$G \times G \longrightarrow G, (g, h) \longmapsto gh,$$

definiert eine G -Operation auf G , die **Translation**.

2) Die Konjugation

$$G \times G \longrightarrow G, (g, h) \longmapsto ghg^{-1}$$

definiert eine Operation von G auf G , die **Konjugation**.

3) Sei X eine Menge und $\mathfrak{S}(X)$ die Gruppe der bijektiven Abbildungen $X \rightarrow X$. Sei $G \subset \mathfrak{S}(X)$ eine Untergruppe. Dann definiert

$$G \times X \longrightarrow X, (g, x) \longmapsto g(x),$$

eine G -Wirkung auf X .

Allgemeiner: sei G eine Gruppe und $\varphi : G \rightarrow \mathfrak{S}(X)$ ein Gruppenhomomorphismus. Dann ist $G \times X \rightarrow X, (g, x) \mapsto \varphi(g)(x)$, eine G -Wirkung. Ist umgekehrt $G \times X \rightarrow X$ eine Gruppenwirkung, so liegt für jedes $g \in G$ die *Translation*

$$\tau_g : X \longrightarrow X, x \longmapsto gx,$$

in $\mathfrak{S}(X)$ und $G \rightarrow \mathfrak{S}(X), g \mapsto \tau_g$, ist ein Gruppenhomomorphismus.

Lemma 5.3. *Diese beiden Bildungen sind zueinander invers.*

Beweis. Sei $\varphi : G \rightarrow \mathfrak{S}(X)$ ein Gruppenhomomorphismus. Dann gilt für $g \in G$, $x \in X$ $\tau_g(x) = gx := \varphi(g)(x)$, also $\tau_g = \varphi(g) \in \mathfrak{S}(X)$.

Ist umgekehrt $G \times X \rightarrow X$ eine Gruppenwirkung, so gilt $\tau_g(x) := gx$, also $\varphi(g)(x) = gx$ für alle $g \in G$, $x \in X$. \square

Für $g \in G$ ist

$$\text{int}_g : G \longrightarrow G, h \longmapsto ghg^{-1},$$

die zu g bzgl. der Konjugation assoziierte Bijektion $G \rightarrow G$. Wegen

$$\begin{aligned} \text{int}_g(h_1 h_2) &= gh_1 h_2 g^{-1} = gh_1 g^{-1} gh_2 g^{-1} \\ &= \text{int}_g(h_1) \text{int}_g(h_2) \end{aligned}$$

ist int_g ein Gruppenhomomorphismus, also

$$\text{int}_g \in \text{Aut}(G) \subset \mathfrak{S}(G) = \text{Aut}_{\text{Mengen}}(G).$$

Wegen

$$\begin{aligned} \text{int}_{g_1 g_2}(h) &= g_1 g_2 h g_1^{-1} g_2^{-1} \\ &= \text{int}_{g_1}(\text{int}_{g_2}(h)) \end{aligned}$$

ist die Abbildung

$$\text{int} : G \longrightarrow \text{Aut}(G), g \longmapsto \text{int}_g,$$

ein Gruppenhomomorphismus.

Definition 5.4. Das Bild $\text{int}(G) \subset \text{Aut}(G)$ von int heißt die Gruppe der **inneren Automorphismen von G** . Der Kern von int :

$$\text{Kern}(\text{int}) = \{g \in G \mid gh = hg \quad \forall h \in G\} =: Z(G)$$

heißt das **Zentrum von G** .

Bemerkung 5.5. $Z(G)$ ist ein Normalteiler in G (weil Kern eines Homomorphismus).

Der Homomorphiesatz liefert:

Korollar 5.6. *Es gilt $G/Z(G) \cong \text{int}(G)$.*

Bemerkung 5.7. $\text{int}(G) = 1 \iff G$ ist kommutativ.

Definition 5.8. Sei $G \times X \longrightarrow X$ eine Gruppenoperation.

(a) Für $x \in X$ heißt

$$Gx = \{gx \mid g \in G\}$$

die **Bahn** (oder der Orbit) von x .

(b) Die Untergruppe

$$G_x = \{g \in G \mid gx = x\}$$

heißt die **Stand- (oder Isotropie-)gruppe** von x .

(c) Ein $x \in X$ heißt **Fixpunkt** der Gruppenwirkung, wenn $gx = x$ für alle $g \in G$ gilt. Die Menge aller Fixpunkte wird mit $\text{Fix}_G(X)$ bezeichnet.

Bemerkungen 5.9. 1) $x \in \text{Fix}_G(X) \Leftrightarrow \#Gx = 1 \Leftrightarrow G_x = G$.

2) X ist die disjunkte Vereinigung von Bahnen.

Grund: ist $g'x' = gx$, so gilt $hx' = hg'^{-1}g'x' = hg'^{-1}gx$ und $hx = hg^{-1}gx = hg^{-1}g'x'$ also $Gx \cap Gx' \neq \emptyset \Leftrightarrow Gx = Gx'$.

Lemma 5.10. Für $x \in X$ definiert die Abbildung $G \rightarrow Gx$, $g \mapsto gx$, eine Bijektion

$$G/G_x \xrightarrow{\sim} Gx.$$

Insbesondere gilt $\#Gx = (G : G_x)$.

Beweis. Die Abbildung ist surjektiv nach Definition von Gx . Weiterhin gilt

$$gx = hx \Leftrightarrow h^{-1}gx = x \Leftrightarrow h^{-1}g \in G_x \Leftrightarrow gG_x = hG_x.$$

□

Aus Lemma 5.10 und Bemerkung 5.9 2) erhalten wir unmittelbar den nächsten Satz.

Satz 5.11 (Bahnengleichung). Sei $G \times X \rightarrow X$ eine Gruppenoperation auf einer endlichen Menge X , sowie x_1, \dots, x_n ein Vertretersystem der Bahnen in X . Dann gilt

$$\#X = \sum_{i=1}^n \#Gx_i = \sum_{i=1}^n (G : G_{x_i}).$$

Bemerkung 5.12. Bzgl. der Konjugation gilt $x \in Z(G) \Leftrightarrow \#Gx = 1$ ($\Leftrightarrow gx = xg \quad \forall g \in G$).

Satz 5.13. Sei G eine Gruppe. Ist $G/Z(G)$ zyklisch, so ist G abelsch.

Beweis. Sei $aZ(G)$ ein Erzeuger von $G/Z(G)$. Sei $g \in G$ und $\bar{g} \in G/Z(G)$ das Bild. Dann gilt $\bar{g} = \bar{a}^i$ für ein $i \in \mathbb{Z}$. Folglich gilt $ga^{-i} \in Z(G)$. Also hat jedes $g \in G$ eine Darstellung der Form $g = a^iz$, $i \in \mathbb{Z}$, $z \in Z(G)$. Dann gilt für $g_1, g_2 \in G$ beliebig

$$\begin{aligned} g_1g_2 &= a^{i_1}z_1a^{i_2}z_2 = a^{i_1+i_2}z_1z_2 \\ &= a^{i_2}z_2a^{i_1}z_1 = g_2g_1. \end{aligned}$$

□

Definition 5.14. Sei G eine Gruppe und $S \subset G$ eine Teilmenge.

(a) $Z_S = \{g \in G \mid gs = sg \text{ für alle } s \in S\}$

heißt der **Zentralisator** von S in G .

(b) $N_S = \{g \in G \mid gS = Sg\}$

heißt der **Normalisator** von S in G .

Bemerkung 5.15. $Z(G) = Z_G$.

Lemma 5.16. (i) Z_S und N_S sind Untergruppen in G .

(ii) Ist S eine Untergruppe in G , so ist N_S die größte aller Untergruppen $H \subset G$ mit $S \triangleleft H$.

Beweis. (i) ist klar nach Definition.

(ii) Es gilt $S \triangleleft N_S$ nach Definition. Ist $H \subset G$ so dass $S \triangleleft H$, so gilt $hS = Sh$ für jedes $h \in H$, also $H \subset N_S$. \square

Für eine Untergruppe $H \subset G$ und ein $g \in G$ heißt

$$H^g = gHg^{-1} = \{ghg^{-1} \mid h \in H\}$$

die mittels g zu H **konjugierte** Untergruppe.

Lemma 5.17. Die Anzahl der zu H konjugierten Untergruppen ist gleich dem Index $(G : N_H)$.

Beweis. Es gilt $gHg^{-1} = g'Hg'^{-1} \iff (g')^{-1}gHg^{-1}g' = H \iff (g')^{-1}g \in N_H \iff gN_H = g'N_H$. \square

Lemma 5.18. Sei X die Menge der Untergruppen von G auf der G (und damit auch jede Untergruppe H von G) durch Konjugation wirkt. Seien $H, S \subset G$ Untergruppen. Dann gilt

$$S \in \text{Fix}_H(X) \iff H \subset N_S.$$

Insbesondere gilt $S \in \text{Fix}_G(X) \iff S \triangleleft G$.

Beweis. $S \in \text{Fix}_H(X)$ bedeutet $hSh^{-1} = S$ für alle $h \in H$, was zu $H \subset N_S$ äquivalent ist. \square

Satz 5.19 (Klassengleichung). Sei G eine endliche Gruppe mit Zentrum Z und sei x_1, \dots, x_n ein Vertretersystem der Bahnen in $G - Z$ bzgl. Konjugation. Dann gilt

$$\#G = \#Z + \sum_{i=1}^n (G : Z_{\{x_i\}})$$

Beweis. Es gilt

$$\begin{aligned} \#G &= \#Z + \sum_{i=1}^n \#Gx_i \\ &= \#Z + \sum_{i=1}^n (G : G_{x_i}). \end{aligned}$$

Bzgl. Konjugation gilt $G_x = Z_{\{x\}}$ für jedes $x \in G$. \square

5.2 p -Gruppen

Definition 5.20. Sei p eine Primzahl. Eine endliche Gruppe G heißt **p -Gruppe**, wenn $\#G$ eine p -Potenz ist.

Satz 5.21. Sei G eine p -Gruppe, $\#G = p^k$, $k \geq 1$. Dann gilt $Z(G) \neq 1$, also $\#Z(G) = p^r$, $r \geq 1$.

Beweis. Aus der Klassengleichung Satz 5.19 erhalten wir

$$\#G = \#Z(G) + \sum_{i=1}^n (G : Z_{\{x_i\}})$$

für ein Vertretersystem x_1, \dots, x_n der Bahnen in $G - Z(G)$ bzgl. Konjugation. Nun gilt $x_i \notin Z(G) \Rightarrow Z_{\{x_i\}} \neq G \Rightarrow p \mid (G : Z_{\{x_i\}})$. Folglich gilt $p \mid \#Z(G) \Rightarrow Z(G) \neq 1$. Nun ist $Z(G) \subset G$ eine Untergruppe, also $\#Z(G) = p^r$, $r \geq 1$. \square

Korollar 5.22. Sei p eine Primzahl. Dann ist jede Gruppe der Ordnung p^2 abelsch.

Beweis. 1. Fall: $G = Z(G)$. Hier ist nichts zu zeigen.

2. Fall: $\#Z(G) = p \Rightarrow \#G/Z(G) = p$. Dann ist $G/Z(G)$ zyklisch $\xrightarrow{5.13} G$ abelsch $\Rightarrow G = Z(G)$, Widerspruch.

3. Fall: $\#Z(G) = 1$ nicht möglich nach Satz 5.21. \square

Korollar 5.23. $\#G = p^2 \Rightarrow G \cong \mathbb{Z}/p^2\mathbb{Z}$ oder $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Beweis. Nach Korollar 5.22 ist G abelsch. Die Aussage folgt aus dem Hauptsatz über endlich erzeugte abelsche Gruppen (\mathbb{Z} -Moduln). \square

Satz 5.24. Sei $\#G = p^k$. Dann existieren Untergruppen

$$G = G_k \supset G_{k-1} \supset \dots \supset G_0 = 1$$

mit

$$(i) \quad \#G_i = p^i, \quad i = 0, \dots, k,$$

$$(ii) \quad G_{i-1} \triangleleft G, \quad i = 1, \dots, k.$$

Insbesondere gilt $G_{i-1} \triangleleft G_i$ und $G_i/G_{i-1} \cong \mathbb{Z}/p\mathbb{Z}$.

Beweis. Per Induktion über k . Der Fall $k = 0$ ist trivial.

Sei $k \geq 1$ und sei $a \in Z(G)$, $a \neq 1$. Dann gilt $\text{ord}(a) = p^r$, $r \geq 1$ und nachdem man a durch $a^{(p^{r-1})}$ ersetzt hat, kann man ohne Einschränkung $\text{ord}(a) = p$ annehmen. Sei $G_1 = \langle a \rangle$. Wegen $a \in Z(G)$ ist $G_1 \triangleleft G$. Sei $\overline{G} = G/G_1$ und $\varphi : G \rightarrow \overline{G}$ die kanonische Projektion. Nach Induktionsvoraussetzung existieren

$$1 = \overline{G}_0 \subset \dots \subset \overline{G}_{k-1} = \overline{G}$$

mit $\overline{G}_i \triangleleft \overline{G}$ und $\#\overline{G}_i = p^i$, $i = 0, \dots, k-1$. Setze

$$G_i = \varphi^{-1}(\overline{G}_{i-1}) \quad i = 1, \dots, k.$$

Nach Satz 1.31 gilt $G_i \triangleleft G$ und Abzählen liefert $\#G_i = p \cdot \#\overline{G}_{i-1} = p^i$. \square

Satz 5.25. Sei G eine p -Gruppe die auf einer endlichen Menge X operiert. Dann gilt

$$\#\text{Fix}_G(X) \equiv \#X \pmod{p}.$$

Insbesondere gilt:

- (i) Gibt es genau einen Fixpunkt, so gilt $\#X \equiv 1 \pmod{p}$.
- (ii) Ist $\#X$ durch p teilbar, so auch $\#\text{Fix}_G(X)$.
- (iii) Ist $\#X$ nicht durch p teilbar, so gibt es mindestens einen Fixpunkt.

Beweis. Sei x_1, \dots, x_n ein Vertretersystem der Bahnen mit mehr als einem Element. Die Bahngleichung Satz 5.11 liefert

$$\#X = \#\text{Fix}_G(X) + \sum_{i=1}^n (G : G_{x_i}).$$

Nun ist G eine p -Gruppe und wegen $G_{x_i} \neq G$ gilt $p \mid (G : G_{x_i})$ für $i = 1, \dots, n$. \square

5.3 Sylow-Gruppen

Definition 5.26. Sei p eine Primzahl und G eine endliche Gruppe. Eine Untergruppe $S \subset G$ heißt **p -Sylowgruppe**, wenn S eine p -Gruppe ist, und p nicht den Index $(G : S)$ teilt.

Bemerkung 5.27. Sei G eine endliche Gruppe, $S \subset G$ eine p -Sylowgruppe und $H \subset G$ eine p -Gruppe mit $S \subset H$. Dann gilt $H = S$.

Grund: $(H : S) \mid \#H \Rightarrow (H : S)$ ist p -Potenz. Außerdem gilt:

$(H : S) \mid (G : S)$ und $p \nmid (G : S)$. Also $(H : S) = p^0 = 1$, $H = S$.

Beispiel 5.28. Sei G eine endliche *abelsche* Gruppe. Dann ist $G(p) = \{g \in G \mid g^{p^n} = 1 \text{ für ein } n \in \mathbb{N}\}$ (der p -Torsionsmodul des \mathbb{Z} -Moduls G) die eindeutig bestimmte p -Sylowgruppe. (siehe LA II: $G \cong \bigoplus_{\ell \text{ PZ}} G(\ell)$.)

Satz 5.29 (Sylowsche Sätze). Sei G eine endliche Gruppe und p eine Primzahl.

- (i) Zu jeder p -Gruppe $H \subset G$ existiert eine p -Sylowgruppe $S \subset G$ mit $H \subset S$. Insbesondere existiert eine p -Sylowgruppe.
- (ii) Zwei beliebige p -Sylowgruppen in G sind konjugiert.
- (iii) Für die Anzahl s der p -Sylowgruppen in G gilt

$$s \mid \#G \quad \text{und} \quad s \equiv 1 \pmod{p}.$$

Bemerkungen 5.30. • $p \nmid \#G \Rightarrow \{1\}$ ist p -Sylowgruppe.

• G ist p -Gruppe $\Rightarrow G$ ist p -Sylowgruppe.

• Nach (ii) haben alle p -Sylowgruppen die gleiche Ordnung. Das sieht man auch einfacher. Ist $\#G = p^r m$, $(m, p) = 1$ so haben alle p -Sylowgruppen die Ordnung p^r (wegen $(G : S)$ prim zu p , $\#S$ p -Potenz).

Wir beginnen mit dem Beweis der Sylowsätze.

Lemma 5.31. *Es existiert stets eine p -Sylowgruppe.*

Beweis. Per Induktion nach $\#G$. Die Aussage ist trivial für $G = 1$. Nun nehmen wir an, die Aussage sei für alle Gruppen mit Ordnung kleiner als $\#G$ bereits bewiesen. Existiert eine Untergruppe $H \subsetneq G$ mit $p \nmid (G : H)$, so ist eine p -Sylowgruppe in H auch eine für G und wir sind fertig. Also OE: $p \mid (G : H)$ für jede Untergruppe $H \subsetneq G$, insbesondere $p \mid \#G$. Die Klassengleichung Satz 5.19 liefert

$$\#G = \#Z + \sum_{i=1}^n (G : Z_{\{x_i\}})$$

wobei Z das Zentrum von G und x_1, \dots, x_n ein Vertretersystem der Bahnen von $G - Z$ bezüglich der Konjugation ist. Nun gilt wegen $x_i \notin Z$ dass $Z_{\{x_i\}} \subsetneq G$, also $p \mid (G : Z_{\{x_i\}})$ und somit $p \mid \#Z$. Daher finden wir ein Element a der Ordnung p in der endlichen (abelschen) Gruppe Z . Sei $H = \langle a \rangle$. Dann hat H die Ordnung p und ist, weil in Z , ein Normalteiler von G . Wir betrachten die kanonische Projektion

$$\phi : G \longrightarrow G/H.$$

Sei p^n die exakte p -Potenz in $\#G$. Dann ist p^{n-1} die exakte p -Potenz in $\#(G/H)$. Sei nun $S \subset G/H$ eine p -Sylowgruppe. Dann gilt $\#S = p^{n-1}$, also $\#\phi^{-1}(S) = p^n$ und somit ist $\phi^{-1}(S)$ eine p -Sylowgruppe in G . \square

Lemma 5.32. *Sei $S \subset G$ eine p -Sylowgruppe und H eine Untergruppe von p -Potenzordnung. Es sei X die Menge der zu S konjugierten Untergruppen, auf der H durch Konjugation wirkt. Dann gilt für $Q \in X$*

$$Q \in \text{Fix}_H(X) \iff H \subset Q.$$

Beweis. Nach Lemma 5.18 gilt

$$Q \in \text{Fix}_H(X) \iff H \subset N_Q.$$

Wir zeigen nun die Äquivalenz

$$H \subset Q \iff H \subset N_Q.$$

Wegen $Q \subset N_Q$ ist die Richtung \Rightarrow trivial. Es gelte nun $H \subset N_Q$. Dann ist die Menge HQ eine Untergruppe in N_Q . Wegen $Q \triangleleft N_Q$ liefert der 1. Isomorphiesatz Satz 1.36

$$H/(H \cap Q) \cong HQ/Q.$$

Da $H/(H \cap Q)$ p -Potenzordnung hat, gilt gleiches auch für HQ/Q . Mit S ist auch Q eine p -Sylowgruppe. Daher hat auch HQ p -Potenzordnung und wegen der Maximalitätseigenschaft von Q folgt $HQ = Q$, also $H \subset Q$. \square

Beweis der Sylowschen Sätze. Sei $H \subset G$ eine p -Untergruppe und $S \subset G$ eine p -Sylowgruppe. Es sei X die Menge der zu S konjugierten Untergruppen, auf der H durch Konjugation wirkt. Nach Lemma 5.17 gilt $\#X = (G : N_S)$ und wegen $N_S \supset S$ folgt $p \nmid \#X$. Nach Satz 5.25 (iii) existiert ein Fixpunkt $Q = gSg^{-1}$ der H -Wirkung auf X . Nach Lemma 5.32 folgt $H \subset Q$. Dies zeigt (i) und auch (ii), weil aus $H \subset gSg^{-1}$ im Falle, dass H selbst p -Sylowgruppe ist, schon $H = gSg^{-1}$ folgt. Es verbleibt, (iii) zu zeigen. Hierzu sei H eine p -Sylowgruppe. Dann hat die H -Wirkung auf X genau einen Fixpunkt, nämlich H selbst (siehe Lemma 5.32) und nach Satz 5.25(i) folgt $\#X \equiv 1 \pmod{p}$. Schließlich gilt $\#X = (G : N_S)$ nach Lemma 5.17, woraus $\#X \mid \#G$ folgt. \square

Wir geben zwei Anwendungen der Sylowsätze:

Korollar 5.33. *Sei G eine endliche Gruppe und p eine Primzahl.*

- (i) *Es gilt $p \mid \#G \iff \exists g \in G, \text{ord}(g) = p$.*
- (ii) *G ist p -Gruppe $\iff \forall g \in G: \text{ord}(g) = p^r, r \in \mathbb{N}_0$.*

Beweis. Wegen $\text{ord}(g) \mid \#G$ folgt (i) \Leftarrow und (ii) \Rightarrow .

(i) \Rightarrow : Gelte $p \mid \#G$. Dann gibt es eine p -Sylowgruppe $S \subset G$, $S \neq 1$. Sei $s \in S$, $s \neq 1$. Dann gilt $\text{ord}(s) \mid \#S$ also $\text{ord}(s) = p^n$, $n \geq 1$. Ersetzen wir s durch $s^{(p^{n-1})}$ erhalten wir ein Element der Ordnung p .

(ii) \Leftarrow : Sei $\text{ord}(g) = p^r$ für jedes $g \in G$. Angenommen es existiert eine Primzahl $q \neq p$ mit $q \mid \#G \xrightarrow{(i)}$ es existiert $g \in G$ mit $\text{ord}(g) = q$. Widerspruch. \square

Korollar 5.34. *Seien $p < q$ Primzahlen mit $p \nmid (q-1)$. Dann ist jede Gruppe der Ordnung pq zyklisch.*

Beweis. Für die Anzahl s_p der p -Sylowgruppen gilt $s_p \mid pq$, $s_p \equiv 1 \pmod{p}$.

Die Fälle $s_p = p, pq$ sind nicht möglich wegen $s_p = 1 \pmod{p}$, der Fall $s_p = q$ ist nicht möglich wegen $p \nmid q-1$. Daher gilt $s_p = 1$.

Analog $s_q \mid pq$, $s_q \equiv 1 \pmod{q}$. Die Fälle $s_q = pq, q$ sind nicht möglich wegen $s_q \equiv 1 \pmod{q}$. Der Fall $s_q = p$ ist nicht möglich wegen $1 < p < q$, also $p \not\equiv 1 \pmod{q}$. Daher gilt $s_q = 1$.

Seien $S_p, S_q \subset G$ die Sylowgruppen. Für $g \in G$ ist gS_pg^{-1} auch eine p -Sylowgruppe, also $gS_pg^{-1} = S_p \Rightarrow S_p \triangleleft G$. Analog $S_q \triangleleft G$.

Es gilt $S_pS_q = G$ (wegen $pq \mid \#S_pS_q$), also hat jedes Element aus G eine Darstellung der Form gh , $g \in S_p$, $h \in S_q$.

Es gilt $\#S_p = p$, $\#S_q = q \Rightarrow S_p, S_q$ abelsch, d.h. beliebige Elemente von S_p (bzw. S_q) kommutieren. Für $g \in S_p$, $h \in S_q$ gilt $ghg^{-1}h^{-1} \in S_p \cap S_q = \{1\}$, also $gh = hg$. Daher ist G kommutativ. Nach dem Hauptsatz über endlich erzeugte abelsche Gruppen ist $\mathbb{Z}/pq\mathbb{Z}$ die einzige abelsche Gruppe der Ordnung pq . \square

5.4 Auflösbare Gruppen

Vorbemerkung (Satz 1.31): Sei G eine Gruppe und $G_2 \subset G_1 \subset G$ Untergruppen mit $G_2 \triangleleft G_1$. Es gibt eine 1 – 1 Korrespondenz:

$$\left\{ \begin{array}{c} \text{Untergruppen } U \\ G_2 \subset U \subset G_1 \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{Untergruppen } \bar{U} \\ \text{von } G_1/G_2 \end{array} \right\}$$

Es gilt $U \triangleleft G_1 \iff \bar{U} \triangleleft G_1/G_2$.

Definition 5.35. Eine Kette von Untergruppen

$$1 = G_n \subset G_{n-1} \subset \cdots \subset G_0 = G$$

heißt **Normalreihe**, wenn $G_i \triangleleft G_{i-1}$ für $i = 1, \dots, n$ gilt. Die Faktorgruppen G_{i-1}/G_i heißen die **Faktoren** der Normalreihe.

Beispiel 5.36. Nach dem Hauptsatz über endlich erzeugte abelsche Gruppen besitzt jede endlich erzeugte abelsche Gruppe eine Normalreihe mit zyklischen Faktoren.

Definition 5.37. Eine Gruppe G heißt **auflösbar**, wenn es eine Normalreihe mit abelschen Faktoren gibt.

Lemma 5.38. Eine endliche auflösbare Gruppe besitzt eine Normalreihe mit zyklischen Faktoren.

Beweis. Das folgt aus der Vorbemerkung und dem Beispiel. □

Satz 5.39. Eine endliche p -Gruppe ist auflösbar.

Beweis. Dies folgt aus Satz 5.24 (der mehr sagt!). □

Definition 5.40. Sei G eine Gruppe. Die Untergruppe $[G, G] = \langle ghg^{-1}h^{-1} | g, h \in G \rangle$ heißt die **Kommutatorgruppe** von G .

Bemerkungen 5.41. • Ein Element der Form $ghg^{-1}h^{-1}$ heißt **Kommutator**. Die Kommutatorgruppe $[G, G]$ wird von den Kommutatoren erzeugt, aber es ist nicht notwendig jedes Element in $[G, G]$ schon selbst ein Kommutator.

- $[G, G] = 1 \iff G$ abelsch.

Lemma 5.42. (i) $[G, G] \triangleleft G$.

(ii) Für eine Untergruppe $H \subset G$ gilt: $(H \triangleleft G \text{ und } G/H \text{ abelsch}) \iff H \supset [G, G]$.

Beweis. (i) Es gilt für $s, g, h \in G$ beliebig

$$s(ghg^{-1}h^{-1})s^{-1} = (sgs^{-1})(shs^{-1})(sgs^{-1})^{-1}(shs^{-1})^{-1} \in [G, G].$$

Jedes Element $x \in [G, G]$ ist Produkt von Elementen der Form $ghg^{-1}h^{-1}$ (beachte $(ghg^{-1}h^{-1})^{-1} = hgh^{-1}g^{-1}$). Daher gilt

$$s[G, G]s^{-1} \subset [G, G]$$

für alle $s \in G$ und somit $[G, G] \triangleleft G$.

(ii) (\Leftarrow) $G/[G, G]$ ist abelsch, weil $xyx^{-1}y^{-1} = 1$ für alle $x, y \in G/[G, G]$. Gilt $H \supset [G, G]$, so folgt mit der Vorbemerkung (und weil $G/[G, G]$ abelsch ist), dass $H \triangleleft G$ und G/H abelsch.

(\Rightarrow) Ist $H \triangleleft G$ und G/H abelsch, so gilt $xyx^{-1}y^{-1} \in H$ für alle $x, y \in G$ und daher $H \supset [G, G]$. \square

Bemerkung 5.43. Also ist $[G, G]$ der kleinste Normalteiler mit abelscher Faktorgruppe.

Definition 5.44. Wir definieren eine absteigende Folge von Untergruppen durch

$$D_0G := G, \quad D_{i+1}G := [D_iG, D_iG], \quad i \geq 1.$$

Insbesondere gilt $D_1 = [G, G]$.

Bemerkung 5.45. Nach Lemma 5.42 ist D_iG eine Normalreihe mit abelschen Faktoren, wenn $D_nG = 1$ für $n \gg 0$ gilt.

Lemma 5.46. Eine Gruppe G ist genau dann auflösbar, wenn $D_nG = 1$ für $n \gg 0$.

Beweis. Das Kriterium ist offenbar hinreichend. Sei G auflösbar und $1 = G_n \subset G_{n-1} \subset \dots \subset G_0 = G$ eine Normalreihe mit abelschen Faktoren. Dann gilt G/G_1 abelsch $\Rightarrow [G, G] \subset G_1$. Induktiv erhalten wir: $D_iG \subset G_i$ also $D_nG \subset G_n = 1$. \square

Korollar 5.47. Ist $U \subset G$ eine Untergruppe und G auflösbar, so auch U .

Beweis. $D_nU \subset D_nG = 1$ für $n \gg 0$. \square

Satz 5.48. Sei $G' \triangleleft G$ und $G'' = G/G'$. Dann gilt

$$G \text{ auflösbar} \iff G' \text{ und } G'' \text{ auflösbar.}$$

Insbesondere sind Faktorgruppen auflösbarer Gruppen wieder auflösbar.

Beweis. (\Rightarrow) G' auflösbar folgt aus Korollar 5.47. Wir bezeichnen die kanonische Projektion mit $\pi : G \twoheadrightarrow G''$. Sei nun $1 = G_n \subset \dots \subset G_0 = G$ eine Normalreihe mit abelschen Faktoren. Setze $G''_i = \pi(G_i) = G_iG'/G' \subset G/G' = G''$ und betrachte die Normalreihe $1 = G''_n \subset \dots \subset G''_0 = G''$. Wir haben Surjektionen

$$\begin{aligned} G_{i-1}/G_i &\twoheadrightarrow G_{i-1}/G_iG' \cap G_{i-1} \stackrel{1.\text{Isom.satz}}{\cong} G_{i-1}G_iG'/G_iG' \\ &= G_{i-1}G'/G_iG' \stackrel{2.\text{Isom.satz}}{\cong} G_{i-1}G'/G' \Big/ G_iG'/G' = G''_{i-1}/G''_i. \end{aligned}$$

Daher ist G''_{i-1}/G''_i abelsch für alle i und G'' auflösbar.

(\Leftarrow) Seien nun $1 = G'_n \subset \dots \subset G'_0 = G'$ und $1 = G''_m \subset \dots \subset G''_0 = G''$ Normalreihen mit abelschen Faktoren. Dann ist $1 = G'_n \subset \dots \subset G'_0 = \pi^{-1}(G''_m) \subset \dots \subset \pi^{-1}(G''_0) = G$ eine Normalreihe mit abelschen Faktoren. Daher ist G auflösbar. \square

Wir erweitern die Schreibweise (ab) für die Transposition in \mathfrak{S}_n , die a mit b vertauscht, durch die sogenannte Zykelschreibweise. Für paarweise verschiedene $a, b, c, d, \dots \in \{1, \dots, n\}$ setzt man

$$(abcd \dots) = \begin{pmatrix} a & b & c & \dots & \\ b & c & d & \dots & a \end{pmatrix}.$$

Satz 5.49. Die Gruppe \mathfrak{S}_n ist für $n \geq 5$ nicht auflösbar.

Beweis. Wir zeigen: Ist $U \subset \mathfrak{S}_n$ eine Untergruppe, die alle Dreierzyklen enthält, so auch $[U, U]$.

Grund: Sei $a, b, c, d, e \in \{1, \dots, n\}$ paarweise verschieden (hier braucht man $n \geq 5$). Z.z. $(abc) \in [U, U]$. Setze $x = (cad)$, $y = (bec)$. Nach Voraussetzung gilt $x, y \in U$, woraus $xyx^{-1}y^{-1} \in [U, U]$ folgt.

Nun gilt

$$\begin{aligned} xyx^{-1}y^{-1} &= (cad)(bec)(dac)(ceb) \\ &= \begin{pmatrix} a & b & c & d & e \\ b & c & a & d & e \end{pmatrix} = (abc). \end{aligned}$$

Hieraus folgt induktiv, dass für $i \in \mathbb{N}$ beliebig, alle Dreierzyklen in $D_i \mathfrak{S}_n$ sind. Nach Lemma 5.46 ist \mathfrak{S}_n nicht auflösbar. \square

Bemerkung 5.50. Für $n \leq 4$ ist \mathfrak{S}_n auflösbar.

6 Anwendungen der Galoistheorie

6.1 Auflösbarkeit von Gleichungen

In diesem Abschnitt sind alle Körper von der Charakteristik 0!

Definition 6.1. Eine endliche Erweiterung L/K heißt **durch Radikale auflösbar** wenn es einen Erweiterungskörper E/L sowie eine Körperkette $K = E_0 \subset \dots \subset E_m = E$ gibt, so dass E_{i+1} aus E_i durch Adjunktion einer Nullstelle eines Polynoms $X^n - a \in E_i[X]$ entsteht.

Definition 6.2. Eine endliche Körpererweiterung L/K heißt **auflösbar**, wenn es einen Oberkörper $E \supset L$ mit E/K galoissch mit auflösbarer Galoisgruppe gibt.

Bemerkung 6.3. Ist L/K galoissch, so gilt: L/K auflösbar $\Leftrightarrow \text{Gal}(L/K)$ auflösbar.

Grund: \Leftarrow : setze $E = L$. \Rightarrow : $\text{Gal}(L/K)$ ist als Faktorgruppe der auflösbaren Gruppe $\text{Gal}(E/K)$ auflösbar.

Ziel:

Satz 6.4. Eine endliche Körpererweiterung L/K ist genau dann auflösbar, wenn sie durch Radikale auflösbar ist.

Anwendung: Sei $f \in K[X]$ ein Polynom. Eine algebraische Lösungsformel für die Nullstellen von f ist ein Ausdruck der sich sukzessive aus Additionen, Subtraktionen, Multiplikationen, Divisionen und Wurzelziehen zusammensetzt. Z.B. hat die quadratische Gleichung $f = X^2 + pX + q$ die Lösungen $x_{1/2} = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}$.

Mit anderen Worten: Die Gleichung $f(X) = 0$ ist genau dann auflösbar wenn der Zerfällungskörper L von f über K durch Radikale auflösbar ist.

Beweis von von Satz 6.4. Sei L/K auflösbar und E/L mit $\text{Gal}(E/K)$ auflösbar. Sei $K = E_0 \subset \dots \subset E_n = E \subset \overline{K}$ eine Kette von Zwischenkörpern so dass für alle i die Erweiterung E_i/E_{i-1} galoissch mit zyklischer Galoisgruppe ist (existiert nach Lemma 5.38 und dem Hauptsatz der Galoistheorie). Sei $N = [E : K]$ und $F = K(\zeta_N) \subset \overline{K}$. Dann ist für $i = 1, \dots, n$ $E_i F / E_{i-1} F$ galoissch und das Diagramm

$$\begin{array}{ccccc}
 & & E_i F & & \\
 & \swarrow & & \searrow & \\
 E_i & & & & E_{i-1} F \\
 & \searrow & & \swarrow & \\
 & & E_i \cap (E_{i-1} F) & & \\
 & & | & & \\
 & & E_{i-1} & &
 \end{array}$$

und Satz 4.17 liefern uns eine Injektion

$$\text{Gal}(E_i F / E_{i-1} F) \xrightarrow{\sim} \text{Gal}(E_i / E_i \cap (E_{i-1} F)) \hookrightarrow \text{Gal}(E_i / E_{i-1}).$$

Nach Satz 1.45 ist $\text{Gal}(E_i F / E_{i-1} F)$ als Untergruppe einer zyklischen Gruppe zyklisch.

Sei $r_i = [E_i F : E_{i-1} F]$. Dann gilt $r_i \mid [E_i : E_{i-1}] \mid N$. Wegen $\zeta_N \in F$ gilt $\zeta_{r_i} \in E_{i-1} F$. Nach Satz 4.66 gilt $E_i F = E_{i-1} F(\sqrt[r_i]{a})$ für ein $a \in E_{i-1} F$. Daher ist

$$K \subset F \subset E_1 F \subset \dots \subset E_n F = E F$$

eine Kette der gesuchten Art und $L \subset E \subset EF$. Also ist L/K durch Radikale auflösbar.

Sei nun L/K durch Radikale auflösbar und E/L , $K = E_0 \subset \dots \subset E_n = E \subset \overline{K}$ wie in der Definition. Wir zeigen: $E \subset E'$ mit E'/K galoissch und $\text{Gal}(E'/K)$ auflösbar. Wir gehen induktiv vor. Sei $E_1 = K(\sqrt[r_1]{a})$, $a \in K$.

$a = 1 \Rightarrow E_1/K$ galoissch mit kommutativer Galoisgruppe.

$a \neq 1 \Rightarrow E'_1 = E_1 K(\zeta_{r_1}) = K(\sqrt[r_1]{a}, \zeta_{r_1})$ ist galoissch $/K$ und wegen der Kette $K \subset K(\zeta_{r_1}) \subset K(\zeta_{r_1})(\sqrt[r_1]{a})$ auflösbar.

Grund: Sei α eine Nullstelle von $X^{r_1} - a$ in \overline{K} , die anderen Nullstellen von $X^{r_1} - a$ in \overline{K} sind von der Form $\zeta_{r_1}^i \alpha$ mit $i \in \mathbb{Z}/r_1\mathbb{Z}$, also ist $K(\zeta_{r_1})(\alpha)/K(\zeta_{r_1})$ galoissch. Für $\sigma \in \text{Gal}(K(\zeta_{r_1})(\alpha)/K(\zeta_{r_1}))$ ist $\sigma(\alpha) = \zeta_{r_1}^i \alpha$ für ein i und σ ist durch i eindeutig bestimmt. Daher gilt für Elemente $\sigma, \tau \in \text{Gal}(K(\zeta_{r_1})(\alpha)/K(\zeta_{r_1}))$ mit $\sigma(\alpha) = \zeta_{r_1}^i \alpha$ und $\tau(\alpha) = \zeta_{r_1}^j \alpha$, dass $\sigma\tau(\alpha) = \sigma(\zeta_{r_1}^j \alpha) = \zeta_{r_1}^j(\sigma(\alpha)) = \zeta_{r_1}^{i+j} \alpha = \tau\sigma(\alpha)$. Daher ist $\text{Gal}(K(\zeta_{r_1})(\alpha)/K(\zeta_{r_1}))$ kommutativ.

Nächster Schritt: $E_2 = E_1(\sqrt[r_2]{a}) \subset E'_1(\sqrt[r_2]{a})$. Wir bilden $E'_2 = E'_1(\zeta_{r_2}, \sqrt[r_2]{a})$ und wie vorher: E'_2/E'_1 galoissch.

Problem: E'_2/K nicht notwendig galoissch. Ein galoisscher Oberkörper von E'_2/K ist

$$E''_2 = E'_1\left(\zeta_{r_2}, \left(\sqrt[r_2]{\sigma(\alpha)}\right)_{\sigma \in \text{Gal}(E'_1/K)}\right).$$

Nun ist $E''_2/E_1(\zeta_{r_2})$ das Kompositum abelscher Galoisweiterungen und nach Satz 4.17 (ii) (induktiv anzuwenden) abelsch. Somit ist E''_2/E'_1 auflösbar, E'_1/K auflösbar $\xrightarrow{5.47} E''_2/K$ auflösbar. Umbenennung: $E'_2 = E''_2$.

Jetzt macht man induktiv weiter und erhält E'_n/K galoissch mit auflösbarer Galoisgruppe und $L \subset E \subset E'_n$. \square

Korollar 6.5. Eine algebraische Gleichung $f(X) = 0$ mit $f \in K[X]$ ist genau dann auflösbar, wenn die Galoisgruppe $\text{Gal}(L/K)$ des Zerfällungskörpers L von f über K auflösbar ist.

Korollar 6.6. Die allgemeine Gleichung $f(X) = 0$ vom Grad n , also

$$f(X) = X^n + t_1 X^{n-1} + \dots + t_n \in K(t_1, \dots, t_n)[X]$$

ist

- auflösbar für $n \leq 4$,
- nicht auflösbar für $n \geq 5$.

Beweis. Die allgemeine Gleichung vom Grad n hat die Galoisgruppe \mathfrak{S}_n . Das Ergebnis folgt aus Satz 5.49. \square

Bemerkung 6.7. Mit etwas mehr Aufwand kann man auch Polynome $f \in \mathbb{Q}[X]$ finden, deren Galoisgruppe nicht auflösbar ist.

6.2 Konstruktionen mit Zirkel und Lineal

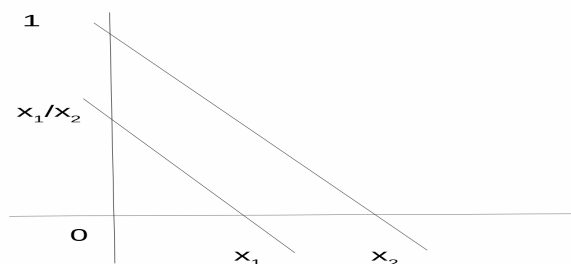
Zu einer Teilmenge $S \subset \mathbb{C}$ sei $\text{Ko}(S)$ die Menge aller komplexen Zahlen, die man in endlich vielen Schritten mit Zirkel und Lineal aus S konstruieren kann. Erlaubt sind folgende Operationen um die Menge zu vergrößern

- A) Zu z_1, \dots, z_4 bilde man den Schnittpunkt der Geraden $\overline{z_1 z_2}$ und $\overline{z_3 z_4}$.
- B) Zu z_1, \dots, z_5 bilde man die Schnittpunkte zwischen der Geraden $\overline{z_1 z_2}$ und dem Kreis um z_3 mit Radius $d(z_4, z_5)$.
- C) Zu z_1, \dots, z_6 bilde man die Schnittpunkte der Kreise um z_1 mit Radius $d(z_2, z_3)$ und um z_4 mit Radius $d(z_5, z_6)$.

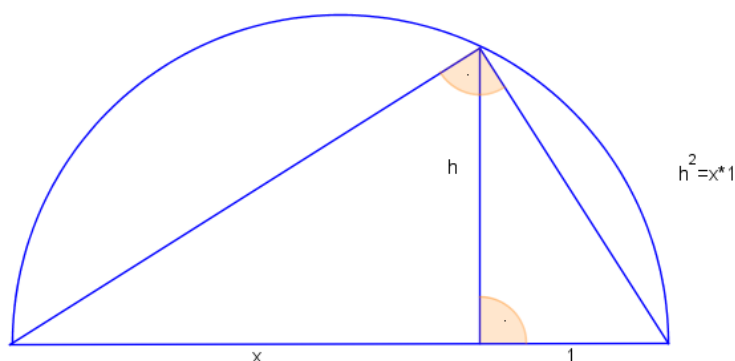
Standardvoraussetzung: $0, 1 \in S$.

Wir bemerken:

- 1) $i, \zeta_6 \in \text{Ko}(S)$.
- 2) $z_1, z_2 \in \text{Ko}(S) \Rightarrow z_1 \pm z_2 \in S$.
- 3) für reelle x_1, x_2 liegen $x_1 x_2, \frac{x_1}{x_2} \in \text{Ko}(S)$ (Strahlensätze).



- 4) $z \in \text{Ko}(S) \iff \text{Re}(z), \text{Im}(z) \in \text{Ko}(S)$ (Lot fällen).
- 5) $\text{Ko}(S)$ ist ein Teilkörper von \mathbb{C} (wegen 2)–4)).
- 6) Für reelles $x \in \text{Ko}(S)$ liegt $\sqrt{x} \in \text{Ko}(S)$. Höhensatz:



- 7) Für beliebiges $z \in \text{Ko}(S)$ liegt $\pm\sqrt{z} \in \text{Ko}(S)$ (Winkelhalbierung)

Bei A) bleibt man im Körper, bei B) und C) erhält man quadratische Gleichungen für die Koordinaten der neuen Punkte, also erhalten wir:

Lemma 6.8. $z \in \text{Ko}(S) \iff$ es existiert eine endliche Kette

$$\mathbb{Q}(S) = K_0 \subset K_1 \subset \dots \subset K_n$$

mit $z \in K_n$ und $[K_i : K_{i-1}] = 2$ für $i = 1, \dots, n$.

Satz 6.9. $z \in \text{Ko}(S) \iff$ es existiert eine endliche Galoiserweiterung $L/\mathbb{Q}(S)$ mit $z \in L$ und so dass $\text{Gal}(L/\mathbb{Q}(S))$ eine 2-Gruppe ist.

Beweis. (\Leftarrow) Nach Satz 5.24 hat die 2-Gruppe $\text{Gal}(L/\mathbb{Q}(S))$ eine Normalreihe mit Faktoren isomorph zu $\mathbb{Z}/2\mathbb{Z}$.

(\Rightarrow) Wir zeigen zunächst:

Behauptung: Es sei E/K galoissch, $\text{Gal}(E/K)$ eine 2-Gruppe, M/E eine Erweiterung vom Grad 2 und \widetilde{M} die normale Hülle von M über K . Dann ist auch $\text{Gal}(\widetilde{M}/K)$ eine 2-Gruppe.

Grund: Sei $M = E(\sqrt{a})$, $a \in E$. Dann ist $\widetilde{M} = E((\sqrt{\sigma(a)})_{\sigma \in \text{Gal}(E/K)})$. Nach Satz 4.17 ist $\text{Gal}(\widetilde{M}/E)$ Untergruppe der 2-Gruppe

$$\prod_{\sigma \in \text{Gal}(E/K)} \text{Gal}(E(\sqrt{\sigma(a)})/E).$$

Somit ist $\text{Gal}(\widetilde{M}/E)$ eine 2-Gruppe und daher auch $\text{Gal}(\widetilde{M}/K)$.

Sei nun $K_i = K_{i-1}(\sqrt{a_i})$, $a_i \in K_{i-1}$. Dann setzt man $L_1 = K_1$ und für $i \geq 2$

$$L_i = \text{normale Hülle von } L_{i-1}(\sqrt{a_i}) \text{ über } K_0.$$

Nach der obigen Behauptung ist L_i/K galoissch und $\text{Gal}(L_i|K_0)$ eine 2-Gruppe. Wir erhalten $L_n \supset K_n$ und $\text{Gal}(L_n/K_0)$ ist eine 2-Gruppe. \square

Konstruktion eines regelmäßigen n -Ecks:

Gegeben sei eine Kreislinie.

Aufgabe: Man konstruiere mit Zirkel und Lineal ein regelmäßiges n -Eck.

Ohne Einschränkung sei der Radius = 1. Dann ist die Aufgabe genau dann lösbar, wenn $\zeta_n \in \text{Ko}(\{0, 1\})$. Nach Satz 4.48 ist $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ abelsch vom Grad $\varphi(n)$. Wir erhalten mit Satz 6.9:

Satz 6.10. Ein regelmäßiges n -Eck ist genau dann konstruierbar, wenn $\varphi(n)$ eine 2-Potenz ist.

Beispiel 6.11. $n = 3, 4, 5, 6, 8, 10, 12, 15, 16, 17$ ok.
 $n = 7, 9, 11, 13, 14, 18, 19$ nicht möglich.

Nun gilt für $n = 2^e p_1^{e_1} \dots p_m^{e_m}$, dass $\varphi(n) = 2^{e-1}(p_1 - 1)p_1^{e_1-1} \dots (p_m - 1)p_m^{e_m-1}$. Also $\varphi(n) = 2$ -Potenz $\Leftrightarrow e_i = 1$ und $p_i - 1 = 2$ -Potenz für $i = 1, \dots, m$.

Lemma 6.12. Ist $2^a + 1$ eine Primzahl, so gilt $a = 2^r$ für ein $r \geq 0$.

Beweis. Es sei $a = bu$ mit $b = 2^r$, $2 \nmid u$. Dann gilt

$$2^a + 1 = 2^{bu} + 1 = (2^b + 1)(2^{b(u-1)} - 2^{b(u-2)} \dots \pm \dots + 1).$$

Weil $2^a + 1$ eine Primzahl ist, muß $u = 1$ gelten. □

Definition 6.13. Primzahlen der Form $2^{2^r} + 1$ heißen **Fermatsche Primzahlen**.

Bislang hat man nur $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ und $F_4 = 65537$ gefunden. Der kleinste mögliche Kandidat für eine weitere Fermatsche Primzahl ist im Moment (Januar 2021) F_{33} .

Korollar 6.14. Das regelmäßige n -Eck ist genau dann konstruierbar, wenn

$$n = 2^e \cdot p_1 \cdots p_m$$

mit paarweise verschiedenen Fermatschen Primzahlen p_1, \dots, p_m .

Das Problem der Winkeldrittung:

Zu gegebenem Winkel φ konstruiere man $\frac{1}{3}\varphi$.

Antwort negativ für allgemeines φ . Z.B. $\varphi = 60^\circ$. $\frac{1}{3}\varphi = 20^\circ$ nicht konstruierbar wegen $\zeta_{18} \notin \text{Ko}(\{0, 1\}) = \text{Ko}(\{0, 1, \zeta_6\})$.

Das Problem der Würfelverdopplung:

Gegeben sei die Kantenlänge r eines Würfels mit Volumen V . Man konstruiere die Kantenlänge R zum Würfel mit Volumen $2V$.

Geht nicht weil $R = \sqrt[3]{2V} = \sqrt[3]{2} \cdot r$. Liegt z.B. $r \in \mathbb{Q}$, so entspricht dies $R \in \text{Ko}(\{0, 1\})$ also $\sqrt[3]{2} \in \text{Ko}(\{0, 1\})$. Aber: $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

Die Quadratur des Kreises:

Man konstruiere zu einem gegebenem Kreis ein Quadrat mit gleichem Flächeninhalt.

Nicht möglich. Für $r = 1$ gilt $F = \pi$ und $\sqrt{\pi} \notin \text{Ko}(\{0, 1\})$ wegen $\pi \notin \text{Ko}(\{0, 1\})$ wegen $\pi \notin \overline{\mathbb{Q}}$ (Beweis später).

6.3 Die Cardanosche Formel

Wir lösen die allgemeine Gleichung vom Grad 3:

$$X^3 + aX^2 + bX + c = 0.$$

Nach der Substitution $X \mapsto X - \frac{a}{3}$ sei OE $a = 0$. Aus historischen Gründen wählen wir die Notation: $f(X) = X^3 + pX + q$ mit Unbestimmten p, q . Sei $\text{char } k \neq 2, 3$ und $K = k(p, q)$ der Funktionenkörper in 2 Variablen über k , d.h. $f \in K[X]$.

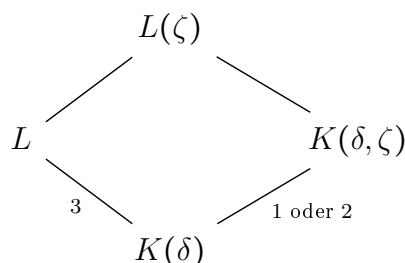
Sei L der Zerfällungskörper von f über K . Wir wissen $\text{Gal}(L/K) = \mathfrak{S}_3$. In \mathfrak{S}_3 haben wir $\mathfrak{A}_3 \triangleleft \mathfrak{S}_3$ und es gilt $\mathfrak{A}_3 \cong \mathbb{Z}/3\mathbb{Z}$. Wir haben auch schon gesehen:

$$\delta = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1) \in L^{\mathfrak{A}_3},$$

wobei x_1, x_2, x_3 die Nullstellen von f in L sind und $\Delta = \delta^2 = -4p^3 - 27q^2 \in K$. Es gilt $\sigma(\delta) = \text{sgn}(\sigma) \cdot \delta$ für $\sigma \in \text{Gal}(L/K)$ und wegen $\text{Gal}(L/K) = \mathfrak{S}_3$ folgt $\delta \notin K$. Wir erhalten den Körperturm

$$L \xrightarrow{\text{zykl. Ordnung } 3} K(\delta) \xrightarrow{\text{zykl. Ordnung } 2} K.$$

Jetzt sei $\zeta \in \overline{K}$ eine primitive 3-te Einheitswurzel. Dann hat $K(\delta, \zeta)/K(\delta)$ Grad 1 oder 2 und das Diagramm



zusammen mit Satz 4.17(i) gibt uns eine Inklusion

$$\text{Gal}(L(\zeta)/K(\delta, \zeta)) \hookrightarrow \text{Gal}(L/K(\delta)) \cong \mathbb{Z}/3\mathbb{Z},$$

die aus Gradgründen ein Isomorphismus ist. Es gilt daher nach Satz 4.66

$$L(\zeta) = K(\delta, \zeta)(a) \quad \text{mit} \quad a^3 \in K(\delta, \zeta).$$

Erinnern wir uns an den Beweis von Satz 4.66: Sei $\text{Gal}(L(\zeta)/K(\delta, \zeta)) = \langle \sigma \rangle$. Dann hat jedes $0 \neq a \in L(\zeta)$ mit $\zeta^{-1} = a/\sigma(a)$ die benötigte Eigenschaft. Nach dem Beweis von Hilberts Satz 90 (4.65) können wir $a = x + \zeta\sigma(x) + \zeta^2\sigma^2(x)$ mit beliebigem $x \in K(\zeta, \delta)$ wählen, jedenfalls solange $a \neq 0$.

Idee: Seien x_1, x_2, x_3 die Nullstellen von f in L und setze

$$\begin{aligned} u &= x_1 + \zeta x_2 + \zeta^2 x_3 \\ v &= x_1 + \zeta^2 x_2 + \zeta x_3 \end{aligned}$$

Dann gilt $u^3, v^3 \in K(\delta, \zeta)$.

1. Schritt: Berechne u^3, v^3
2. Schritt: Löse das lineare Gleichungssystem

$$\begin{aligned} x_1 + x_2 + x_3 &= 0 \\ x_1 + \zeta x_2 + \zeta^2 x_3 &= u \\ x_1 + \zeta^2 x_2 + \zeta x_3 &= v \end{aligned}$$

(einfach: $x_1 = \frac{u+v}{3}$, $x_2 = \frac{\zeta^2 u + \zeta v}{3}$, $x_3 = \frac{\zeta u + \zeta^2 v}{3}$)

3. Schritt: Finde u, v .

Beobachtung: die Nummerierung von x_1, x_2, x_3 war willkürlich, daher kann man u als beliebige 3. Wurzel aus u^3 wählen. Außerdem gilt:

$$\begin{aligned} uv &= (x_1 + \zeta x_2 + \zeta^2 x_3)(x_1 + \zeta^2 x_2 + \zeta x_3) \\ &= x_1^2 + x_2^2 + x_3^2 + (\zeta + \zeta^2)(x_1 x_2 + x_1 x_3 + x_2 x_3). \end{aligned}$$

Nun betrachten wir

$$\begin{aligned} s_1 &= x_1 + x_2 + x_3 = 0 \\ s_2 &= x_1 x_2 + x_1 x_3 + x_2 x_3 = p \\ s_3 &= x_1 x_2 x_3 = -q. \end{aligned}$$

Dann gilt wegen $\zeta + \zeta^2 = -1$

$$uv = s_1^2 - 2s_2 - s_2 = -3p.$$

D.h. nach der Wahl von u ist besteht keine Freiheit für die Wahl von v .

Außerdem erhalten wir

$$u^3 v^3 = -27p^3.$$

Wir berechnen $u^3 + v^3$:

$$\begin{aligned} u^3 + v^3 &= (u + v)(u + \zeta v)(u + \zeta^2 v) \\ &= (3x_1)(3\zeta x_2)(3\zeta^2 x_3) \\ &= 27x_1 x_2 x_3 = -27q \end{aligned}$$

Daher sind u^3, v^3 die Nullstellen von $X^2 + 27qX - 27p^3$ (sogar schon quadratische Gleichung über K , a priori hatten wir quadratische Gleichung über $K(\zeta)$ erwartet), also (indem man eine Quadratwurzel fixiert):

$$\begin{aligned} u^3 &= -\frac{27}{2}q + \sqrt{\left(\frac{27q}{2}\right)^2 + 27p^3} \\ v^3 &= -\frac{27}{2}q - \sqrt{\left(\frac{27q}{2}\right)^2 + 27p^3} \end{aligned}$$

Wir erhalten

$$\begin{aligned} \frac{u}{3} &= \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}} \\ \frac{v}{3} &= \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}} \end{aligned}$$

also

Satz (Cardanosche Formel). Die Nullstellen von $f(X) = X^3 + pX + q$ sind durch

$$\sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}}$$

gegeben. Hierbei wählt man die Quadratwurzel beliebig aber fest und die Kubikwurzeln so, dass ihr Produkt $-\frac{p}{3}$ ist.

Bemerkung 6.15. Eine andere Wahl der Quadratwurzel permutiert nur die Nullstellen.

Dies ist die Lösung der allgemeinen Gleichung. Hat man nun die *spezielle* Gleichung $X^3 + pX + q = 0$ mit $p, q \in k$ so erhält man die Lösung in \bar{k} genau so.

Spezialfall: $k \subseteq \mathbb{R}$.

1. Fall: f hat 3 reelle Nullstellen

$\Rightarrow \delta = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1) \in \mathbb{R}$ also $\Delta = \delta^2 \geq 0$.

2. Fall: f hat eine reelle und zwei komplexe, nicht reelle Nullstellen $x_1 \in \mathbb{R}$, $x_2 \in \mathbb{C} \setminus \mathbb{R}$, $x_3 = \bar{x}_2$

$$\begin{aligned} \delta &= (x_1 - x_2)(x_2 - \bar{x}_2)(\bar{x}_2 - x_1) \\ &= \underbrace{(x_1 - x_2)(x_1 - x_2)(-1)}_{\text{reell}}(x_2 - \bar{x}_2) \end{aligned}$$

also δ rein imaginär $\neq 0 \Rightarrow \Delta = \delta^2 < 0$.

Wegen $\Delta = -4p^3 - 27q^2$ entspricht der 2. Fall gerade $\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2 > 0$.

In diesem Fall kann man die Quadratwurzel im Reellen ziehen und erhält die reelle Nullstelle von f .

– Ist $\Delta = 0$ ist die Sache einfach.

– ist $\Delta > 0$ so muß man komplexe Quadratwurzeln ziehen um die 3 reellen Lösungen zu bekommen. Das konnte man im 16. Jh. noch nicht („casus irreducibilis“).

6.4 Die Transzendenz von π

Lemma 6.16. Seien $\beta_1, \dots, \beta_r \in \mathbb{C}$ und $\theta \in \mathbb{C}[X]$. Sei $c \in \mathbb{C}$ fest und $f(X) := \frac{c^{r_{p-1}}}{(p-1)!} X^{p-1} \theta(X)^p$ für ein $p \in \mathbb{N}$. Setze

$$S = \sum_{i=1}^r \beta_i \int_0^1 e^{(1-t)\beta_i} f(\beta_i t) dt.$$

Dann gilt für $p \gg 0$, dass $|S| < 1$.

Beweis. Für jede stetige komplexwertige Funktion $\phi : [0, 1] \rightarrow \mathbb{C}$ gilt

$$\left| \int_0^1 \phi(x) dx \right| \leq \int_0^1 |\phi(x)| dx.$$

Zudem gilt

$$|yz| = |y||z|, \text{ und } |z_1 + \dots + z_n| \leq |z_1| + \dots + |z_n|.$$

Wir erhalten

$$|S| \leq \sum_{i=1}^r \int_0^1 \left| \frac{(c^r \beta_i \theta(\beta_i t))^p}{(p-1)!} \cdot \left(\frac{1}{c} e^{(1-t)\beta_i} \right) \right| dt$$

Mit $A = \sup_{\substack{t \in [0,1] \\ i=1,\dots,r}} |c^r \beta_i \theta(\beta_i t)|$ und $B = \sup_{\substack{t \in [0,1] \\ i=1,\dots,r}} |\frac{1}{c} e^{(1-t)\beta_i}|$ erhalten wir

$$|S| \leq r \cdot \frac{A^p}{(p-1)!} \cdot B.$$

Nun gilt $\lim_{p \rightarrow \infty} \frac{A^p}{(p-1)!} = 0$, was die Ungleichung für $p \gg 0$ zeigt. \square

Lemma 6.17. Sei $\theta(X) = c_r X^r + \dots + c_0 \in \mathbb{Z}[X]$, $r \geq 1$, $c_0 \neq 0$, $c_r \neq 0$, und $\beta_1, \dots, \beta_r \in \mathbb{C}$ die Nullstellen von θ . Setze $f(X) := \frac{c_r^{rp-1}}{(p-1)!} X^{p-1} \theta(X)^p$ und

$$F = f + f' + f'' + \dots + f^{(rp+p-1)}.$$

Dann gilt für p Primzahl $p \gg 0$:

- (i) $\sum_{i=1}^r F(\beta_i) \in p\mathbb{Z}$,
- (ii) $F(0) \in \mathbb{Z} \setminus p\mathbb{Z}$.

Insbesondere gilt für $k \in \mathbb{N}$ und jede (in Abhängigkeit von k) hinreichend große Primzahl p :

$$\sum_{i=1}^r F(\beta_i) + kF(0) \in \mathbb{Z} \setminus \{0\}.$$

Beweis. Das „Insbesondere“ folgt, wenn p so groß ist, dass (i) und (ii) gelten und außerdem $p > k$ (also $p \nmid k$) gilt.

Die β_i sind p -fache Nullstellen von f , daher gilt

$$\sum_{i=1}^r f^{(t)}(\beta_i) = 0 \text{ für } 0 \leq t < p.$$

Wegen $n(n+1)\dots(n+p-1) = p! \binom{n+p-1}{p}$ ist das Produkt p aufeinanderfolgender natürlicher Zahlen stets durch $p!$ teilbar. Daher sind alle Koeffizienten der p -ten oder höheren Ableitung eines beliebigen Polynoms mit ganzzahligen Koeffizienten durch $p!$ teilbar. Wir sehen, dass für $t \geq p$ die Koeffizienten im Polynom $f^{(t)}$ ganzzahlig und durch $c_r^{rp-1} p$ teilbar sind (insbesondere gilt $f^{(t)}(0) \in p\mathbb{Z}$). Für $t \geq p$ ist daher das Polynom

$$P_t(X_1, \dots, X_r) = \sum_{i=1}^r f^{(t)}(X_i)$$

ein ganzzahliges, symmetrisches Polynom vom Grad $\leq pr - 1$ mit ganzzahligen durch $c_r^{pr-1} p$ teilbaren Koeffizienten.

Da P_t symmetrisch und die β_i die Nullstellen eines Polynoms mit rationalen Koeffizienten sind, gilt $\sum_{i=1}^r f^{(t)}(\beta_i) \in \mathbb{Q}$. Da $c_r \beta_i$, $i = 1, \dots, r$, ganz- algebraisch ist,

und eine rationale, ganz-algebraische Zahl ganzzahlig ist, folgt $\sum_{i=1}^r f^{(t)}(\beta_i) \in p\mathbb{Z}$ für $t \geq p$. Dies zeigt (i).

Nun betrachten wir die Werte von $f^{(t)}$ an der Stelle 0. Oben haben wir schon gesehen, dass $f^{(t)}(0) \in p\mathbb{Z}$ für $t \geq p$ gilt. Nun gilt nach Definition und binomischer Formel

$$f(X) = \frac{c_r^{rp-1}}{(p-1)!} (c_0^p X^{p-1} + \text{Terme mit höheren } X\text{-Potenzen}).$$

Also

$$\begin{aligned} f^{(t)}(0) &= 0 & 0 \leq t \leq p-2 \\ f^{(p-1)}(0) &= c_r^{p^{r-1}} \cdot c_0^p \\ f^{(t)}(0) &\in p\mathbb{Z} & t \geq p. \end{aligned}$$

Für $p > \max(|c_r|, |c_0|)$ gilt daher $F(0) \in \mathbb{Z} \setminus p\mathbb{Z}$, d.h. (ii). \square

Theorem 6.18. *Es sei $\Psi \in \mathbb{Q}[X]$ mit $r = \deg \Psi \geq 1$ und $\Psi(0) \neq 0$. Es seien $\beta_1, \dots, \beta_r \in \mathbb{C}$ die Nullstellen von Ψ . Dann gilt für $k \in \mathbb{N}$*

$$e^{\beta_1} + \dots + e^{\beta_r} + k \neq 0.$$

Beweis. Für geeignetes $a \in \mathbb{N}$ gilt

$$\theta(X) := a \cdot \Psi(X) = c_r X^r + \dots + c_0 \in \mathbb{Z}[X],$$

$c_r \neq 0$, $c_0 \neq 0$, und β_1, \dots, β_r sind die Nullstellen von θ .

Seien $f(X) := \frac{c_r^{rp-1}}{(p-1)!} X^{p-1} \theta(X)^p$ und $F = f + f' + f'' + \dots + f^{(rp+p-1)}$ wie in Lemma 6.17 (wobei wir p noch geeignet wählen werden). Die Produktregel liefert $(e^{-x} F(x))' = -e^{-x} f(x)$. Daher gilt

$$\begin{aligned} e^{-x} F(x) - e^0 F(0) &= \int_0^x -e^{-s} f(s) ds \\ (\text{Variablentransformation}) &= \int_0^1 -e^{-tx} f(tx) \cdot x dt \end{aligned}$$

und daher

$$F(x) - e^x F(0) = -x \int_0^1 e^{(1-t)x} f(tx) dt \quad (*).$$

Wäre nun $e^{\beta_1} + \dots + e^{\beta_r} + k = 0$, $k \in \mathbb{N}$, so folgte durch Aufsummieren von (*) für $x = \beta_i$, $i = 1, \dots, r$:

$$\sum_{i=1}^r F(\beta_i) + kF(0) = - \sum_{i=1}^r \beta_i \int_0^1 e^{(1-t)\beta_i} f(\beta_i t) dt.$$

Für $p \gg 0$ Primzahl steht nach Lemma 6.17 links eine ganze Zahl $\neq 0$ und nach Lemma 6.16 rechts eine komplexe Zahl vom Betrag < 1 . Widerspruch. \square

Satz 6.19. π ist transzendent.

Beweis. Angenommen π und damit auch πi wäre algebraisch. Sei $f \in \mathbb{Q}[X]$ das Minimalpolynom von πi über \mathbb{Q} und seien $\alpha_1, \dots, \alpha_n$ die Nullstellen von f . OE $\alpha_1 = \pi i$. Wegen $e^{\pi i} = -1$ gilt

$$(e^{\alpha_1} + 1) \cdots (e^{\alpha_n} + 1) = 0.$$

Sei für eine Teilmenge $I \subset \{1, \dots, n\}$

$$\beta_I := \sum_{i \in I} \alpha_i.$$

Das Polynom

$$\Phi(X) = \prod_{I \subset \{1, \dots, n\}} (X - \beta_I)$$

ist symmetrisch in den α_i und hat daher rationale Koeffizienten. Wir numerieren die β 's, so dass

$$\beta_1, \dots, \beta_r \neq 0, \quad \beta_{r+1} = \dots = \beta_{2^n} = 0.$$

Wegen $\alpha_1 \neq 0$ und $\beta_\emptyset = 0$ gilt $1 \leq r \leq 2^n - 1$. Also $\Phi(X) = X^{(2^n - r)} \Psi(X)$ mit $\Psi(X) \in \mathbb{Q}[X]$, $\Psi(0) \neq 0$. Aus

$$(e^{\alpha_1} + 1) \cdots (e^{\alpha_n} + 1) = 0$$

folgt

$$e^{\beta_1} + \dots + e^{\beta_r} + (2^n - r) = 0.$$

Das ist nach Theorem 6.18 nicht möglich. Widerspruch. \square

6.5 Der Fundamentalsatz der Algebra

Satz 6.20. \mathbb{C} ist algebraisch abgeschlossen.

Zum Beweis erinnern wir uns, dass der Zwischenwertsatz der Analysis die folgenden Resultate impliziert:

- 1) Jedes $a \in \mathbb{R}$, $a > 0$ hat eine Quadratwurzel in \mathbb{R} .
- 2) Jedes Polynom ungeraden Grades $f \in \mathbb{R}[X]$ hat eine reelle Nullstelle.

Aus 1) erhält man durch einfache Rechnung:

- 3) Jede komplexe Zahl besitzt eine Quadratwurzel in \mathbb{C} .

Beweis von Satz 6.20. Sei L/\mathbb{C} eine endliche Erweiterung. Z.z. $L = \mathbb{C}$. Durch Übergang zur normalen Hülle können wir annehmen, dass L/\mathbb{R} galoissch ist. Sei $G = \text{Gal}(L/\mathbb{R})$, $\#G = 2^r \cdot n$, n ungerade, $r \geq 1$.

Sei $H \subset G$ eine 2-Sylowgruppe. Dann ist $[L^H : \mathbb{R}] = n$. Nach dem Satz vom primitiven Element gilt $L^H = \mathbb{R}(a)$ und a hat Minimalpolynom f vom Grad n über \mathbb{R} . n ungerade + f irreduzibel $\xrightarrow{2)} n = 1. \Rightarrow \#G = 2^r$.

Z.z. $r = 1$. Wäre $r > 1$, d.h. $\#\text{Gal}(L/\mathbb{C}) = 2^{r-1} > 1$, so gibt es in $\text{Gal}(L/\mathbb{C})$ einen Normalteiler vom Index 2 (Satz 5.24). Dieser entspricht einer Galoiserweiterung vom Grad 2 von \mathbb{C} . Nach (3) gibt es eine solche nicht. \square

Es gilt $[\mathbb{C} : \mathbb{R}] = 2$. Wann ist der algebraische Abschluss noch nahe?

Satz 6.21. *Sei k nicht algebraisch abgeschlossen und $[\bar{k} : k] < \infty$. Dann gilt $[\bar{k} : k] = 2$, $\text{char}(k) = 0$ und $\bar{k} = k(i)$, $i^2 = -1$.*

Beweis. Wir beschränken uns im Beweis auf den Fall $\text{char}(k) = 0$. (Das kann man aber mit mehr Aufwand folgern).

1. Schritt: $G = G(\bar{k}/k)$ ist 2-Gruppe. Wenn nicht, enthält G eine Untergruppe $H \subset G$ mit $H \cong \mathbb{Z}/p\mathbb{Z}$, p Primzahl, $p \neq 2$. Ersetze k durch \bar{k}^H . Also OE $G \cong \mathbb{Z}/p\mathbb{Z}$. Dann hat k keine Erweiterung vom Grad prim zu p . Wegen $[k(\zeta_p) : k] \leq p-1$ folgt $\zeta_p \in k$. Nach Satz 4.66 folgt $\bar{k} = k(a)$, $a^p = c \in k$. Wähle ein $\alpha \in \bar{k}$ mit $\alpha^p = a$. Dann gilt $N_{\bar{k}/k}(\alpha)^p = N_{\bar{k}/k}(\alpha^p) = N_{\bar{k}/k}(a) = a^p = c \Rightarrow c$ hat p -te Wurzel in $k \Rightarrow X^p - c$ nicht irreduzibel. Widerspruch.

2. Schritt: Angenommen $\bar{k} \neq k(i)$, $i^2 = -1$. Nach Schritt 1 ist $G = \text{Gal}(\bar{k}/k(i))$ eine 2-Gruppe, also existiert $H \subset G$, $H \cong \mathbb{Z}/2\mathbb{Z}$. Dann wie in Schritt 1:

$L = \bar{k}^{H'}$, $\bar{k} = L(a)$, $a^2 = c \in L$. Wähle $\alpha \in \bar{k}$ mit $\alpha^2 = a$. Dann gilt $N_{\bar{k}/L}(\alpha)^2 = N_{\bar{k}/L}(a) = -c$ und $i \cdot N_{\bar{k}/L}(\alpha)$ ist eine Wurzel aus c in L . Widerspruch $\Rightarrow \bar{k} = k(i)$. \square

Definition 6.22. Ein Paar $(k, P \subset k^\times)$ heißt **angeordneter Körper** wenn gilt:

- (i) Für $x \in k$ gilt genau eine der drei Möglichkeiten $x = 0$, $x \in P$, $-x \in P$, und
- (ii) Für $x, y \in P$ gilt $x + y \in P$, $xy \in P$.

Man sagt dann $x < y$, wenn $y - x \in P$ und es gilt: $(x < y) \Rightarrow (x + z < y + z) \forall z$ und $(x < y) \Rightarrow (xz < yz) \forall z > 0$.

Beispiel 6.23. $k = \mathbb{R}$ mit der gewöhnlichen Anordnung $P = \{x \in \mathbb{R}, x > 0\}$.

Satz 6.24. *Sei k wie in Satz 6.21. Dann existiert auf k eine Anordnung.*

Beweis. Definiere

$$x \in P \stackrel{\text{df}}{\Leftrightarrow} \exists y \in k^\times, x = y^2.$$

Nun gilt für $x \neq 0$ höchstens $x \in P$ oder $-x \in P$ (wegen $i \notin k$). Ist $x \neq 0$ kein Quadrat in k , so ist $-x$ Quadrat. Das sieht man wie in Schritt 2 des Beweises von Satz 6.21: Es gibt ein $a \in \bar{k} \setminus k$ mit $a^2 = x$. Wähle $\alpha \in \bar{k}$ mit $\alpha^2 = a$. Dann gilt $N_{\bar{k}/k}(\alpha)^2 = N_{\bar{k}/k}(\alpha^2) = N_{\bar{k}/k}(a) = -x$. Also gilt (i).

Zu (ii): Die Implikation $x, y \in P \Rightarrow xy \in P$ ist offensichtlich. Sei $x = a^2$, $y = b^2$, $a, b \in k^\times$. Wähle $c, d \in k$ mit $(c + id)^2 = a + bi$ in \bar{k} . Dann gilt $x + y = a^2 + b^2 = N_{\bar{k}/k}(a + bi) = N_{\bar{k}/k}(c + id)^2 = (c^2 + d^2)^2$, wegen $i \notin k$ gilt $c^2 \neq -d^2$, also $x + y \in P$. \square

Bemerkung 6.25. Körper mit einer Anordnung heißen **formal reell**. Körper wie in Satz 6.21 heißen **formal reell abgeschlossen**.

Man kann zeigen:

- k formal reell $\iff -1$ ist nicht Summe von Quadraten in k .
- Jeder formal reelle Körper ist in einem formal reell abgeschlossenen Körper enthalten.

7 Transzendente Erweiterungen

7.1 Transzendenzbasen

Sei L/K eine Körpererweiterung.

Erinnerung: Eine Teilmenge $S \subset L$ heißt algebraisch unabhängig über K , wenn der nach Satz 2.51 eindeutig bestimmte Ringhomomorphismus

$$\varphi : K[(X_s)_{s \in S}] \longrightarrow L$$

mit $\varphi|_K = (K \xrightarrow{\text{kan}} L)$ und $\varphi(X_s) = s$ für alle $s \in S$, injektiv ist.

Bemerkungen 7.1. 1.) Da in einem Element von $K[(X_s)_{s \in S}]$ also insbesondere von $\text{Kern}(\varphi)$ stets nur endlich viele der Variablen X_s vorkommen, gilt

$$S \text{ alg. unabhängig} \iff$$

jede endliche Teilmenge von S ist alg. unabhängig.

2.) Ist L/K algebraisch, so ist $S = \emptyset$ die einzige algebraisch unabhängige Teilmenge.

3.) Ist S algebraisch unabhängig, so induziert der kanonische K -Homomorphismus

$$\varphi : K[(X_s)_{s \in S}] \longrightarrow L, \quad \varphi(X_s) = s,$$

einen Isomorphismus

$$K((X_s)_{s \in S}) \xrightarrow{\sim} K(S).$$

Die Menge Σ der über K algebraisch unabhängigen Teilmengen in L ist durch Inklusion halbgeordnet.

Bemerkung 7.2. Es gilt $\Sigma \neq \emptyset$. (Ist L/K algebraisch, so gilt $\Sigma = \{\emptyset\}$).

Lemma 7.3. Σ enthält maximale Elemente.

Beweis. Ist $\mathcal{T} \subset \Sigma$ eine Kette, so folgt aus Bemerkung (1), dass

$$B := \bigcup_{S \in \mathcal{T}} S$$

selbst in Σ liegt, also eine obere Schranke für \mathcal{T} ist. Das Zornsche Lemma impliziert die Existenz maximaler Elemente. \square

Definition 7.4. Eine maximale algebraisch unabhängige Teilmenge $S \subset L$ heißt **Transzendenzbasis** von L über K .

Lemma 7.5. Für eine Teilmenge $S \subset L$ sind äquivalent:

- (i) S ist Transzendenzbasis von L/K .
- (ii) S ist algebraisch unabhängig und $L/K(S)$ ist algebraisch.

Beweis. Sei S algebraisch unabhängig. Dann ist $L/K(S)$ genau dann algebraisch, wenn jedes Element $x \in L$ Nullstelle eines normierten Polynoms mit Koeffizienten in $K(S)$ ist. Insbesondere ist dann für $x \notin S$ die Menge $S \cup \{x\}$ nicht algebraisch unabhängig, also ist S maximal. Sei S maximal algebraisch unabhängig und $x \in L$. Ist $x \in S$, so ist x trivialerweise algebraisch über $K(S)$. Sei also $x \notin S$. Dann ist $S \cup \{x\}$ nicht algebraisch unabhängig, d.h. es gibt eine nichttriviale Polynomgleichung in x und gewissen $x_1, \dots, x_n \in S$. Hierbei taucht x mindestens in erster Potenz auf (weil S algebraisch unabhängig ist). Wir ordnen nach Potenzen von x und teilen durch den Koeffizienten vor der höchsten x -Potenz um eine Gleichung für x über $K(S)$ zu erhalten. Daher ist $L/K(S)$ algebraisch. \square

Lemma 7.6. Sei $S \subset L$ algebraisch unabhängig über K und sei $T \subset L$ eine Teilmenge so dass $L/K(T)$ algebraisch ist. Dann kann S durch Hinzunahme von Elementen aus T zu einer Transzendenzbasis von L/K erweitert werden. Insbesondere (setze $S = \emptyset$) kann eine Transzendenzbasis aus T gewählt werden.

Beweis. Wir betrachten die Menge Σ aller Teilmengen $T' \subset T$, so dass $S \cup T'$ algebraisch unabhängig ist. Nach dem Zornschen Lemma hat Σ maximale Elemente. Sei $T_{\max} \subset T$ maximal in Σ . Dann sind alle Elemente von T algebraisch über $K(T_{\max})$ und daher die Erweiterung $K(S \cup T)/K(S \cup T_{\max})$ algebraisch. Da mit $L/K(T)$ auch $L/K(S \cup T)$ algebraisch ist, ist $L/K(S \cup T_{\max})$ algebraisch; und nach Lemma 7.5 ist $S \cup T_{\max}$ eine Transzendenzbasis. \square

Satz 7.7. Existiert eine endliche Transzendenzbasis S für L/K , so ist jede Transzendenzbasis endlich von der Mächtigkeit $\#S$.

Beweis. Wir zeigen per Induktion nach $\#S$, dass für jede andere Transzendenzbasis T von L/K gilt $\#T \leq \#S$. Aus Symmetriegründen folgt dann $\#T = \#S$.

Induktionsanfang: $\#S = 0$, also $S = \emptyset$. Dann ist L/K algebraisch und es gilt $T = \emptyset$ für jede andere Transzendenzbasis T .

Induktionsschritt: Sei $\#S \geq 1$. Dann ist L/K nicht algebraisch und es gilt daher $T \neq \emptyset$. Sei $y \in T \setminus S$ (im Fall $T \subset S$ ist die Aussage trivial). Nach Lemma 7.6 können wir $\{y\}$ durch Hinzunahme von Elementen aus S zu einer Transzendenzbasis T' erweitern. Da $S \cup \{y\}$ algebraisch abhängig ist, haben nicht alle Elemente von S Verwendung gefunden und es folgt $\#T' \leq \#S$.

Nun sind $T' \setminus \{y\}$ und $T \setminus \{y\}$ beides Transzendenzbasen der Erweiterung $L/K(y)$. Nach Induktionsvoraussetzung für die Erweiterung $L/K(y)$ sowie $T' \setminus \{y\}$ und $T \setminus \{y\}$ folgt

$$\#T - 1 = \#(T \setminus \{y\}) \leq \#(T' \setminus \{y\}) = \#T' - 1,$$

also $\#T \leq \#T' \leq \#S$. □

Nach Satz 7.7 ist die folgende Definition sinnvoll:

Definition 7.8. Gibt es eine endliche Transzendenzbasis von L/K , so nennt man ihre Mächtigkeit den **Transzendenzgrad** von L über K ($\deg.\text{tr}(L/K)$). Gibt es keine endliche Transzendenzbasis, so setzt man $\deg.\text{tr}(L/K) = \infty$.

Bemerkung 7.9. Man kann zeigen, dass zwei beliebige (nicht nur endliche) Transzendenzbasen gleichmächtig sind.

Satz 7.10. Sei $M/L/K$ ein Körperturm. Dann gilt

$$\deg.\text{tr}(M/K) = \deg.\text{tr}(M/L) + \deg.\text{tr}(L/K).$$

Beweis. Sei T eine Transzendenzbasis von M/L und S eine Transzendenzbasis von L/K . Dann gilt $S \cap T = \emptyset$ (alle Elemente aus S sind algebraisch über L).

Behauptung: $S \cup T$ eine Transzendenzbasis von M/K .

Begründung: 1.) Wir haben Inklusionen

$$K[(X_s)_{s \in S}] \hookrightarrow L \quad \text{und} \quad L[(X_t)_{t \in T}] \hookrightarrow M.$$

Folglich erhalten wir die Inklusion

$$K[(X_i)_{i \in S \cup T}] = K[(X_s)_{s \in S}][[(X_t)_{t \in T}]] \hookrightarrow L[(X_t)_{t \in T}] \hookrightarrow M,$$

und sehen, dass $S \cup T$ algebraisch unabhängig über K ist.

2.) Es ist $L/K(S)$ algebraisch, also auch $L(T)/K(S \cup T)$ (weil durch die über $K(S)$ und damit erst recht über $K(S, T)$ algebraischen Elemente aus L erzeugt). Da auch $M/L(T)$ algebraisch ist, folgt die Algebraizität der Erweiterung $M/K(S \cup T)$.

Nach Lemma 7.5 folgt aus 1) und 2), dass $S \cup T$ eine Transzendenzbasis von M/K ist. Hieraus folgt insbesondere die Gleichung für die Transzendenzgrade. □

7.2 Rein transzendente Erweiterungen

Definition 7.11. Eine Erweiterung L/K heißt **rein transzendent**, wenn $L = K(S)$ mit einer Transzendenzbasis S von L über K gilt.

Beispiel 7.12. Der Körper der rationalen Funktionen $K(X)$ ist eine rein transzendente Erweiterung von K .

Satz 7.13. Zwei rein transzendente Erweiterungen von K mit demselben endlichen Transzendenzgrad sind K -isomorph.

Beweis. Es seien $L = K(S)$ und $L' = K(S')$ mit endlichen Transzendenzbasen S, S' und $\#S = \#S' =: n$. $L = K(S)$ bedeutet, dass man jedes Element aus L als rationale Funktion in den Elementen von S schreiben kann und weil S algebraisch unabhängig ist, ist diese Darstellung eindeutig. Wir finden daher einen K -Isomorphismus

$$L \cong K(X_1, \dots, X_n)$$

(vergleiche Bemerkungen 7.1, 3.). Dasselbe gilt für L' , weshalb L und L' K -isomorph sind. \square

Satz 7.14. Ist L/K rein transzendent, so ist jedes Element $x \in L \setminus K$ über K transzendent, d.h. K ist algebraisch abgeschlossen in L .

Beweis. Sei $x \in L$ beliebig und S eine Transzendenzbasis von L/K mit $L = K(S)$. Dann existiert eine endliche Teilmenge $S' \subset S$ mit $x \in K(S')$. Damit können wir ohne Einschränkung annehmen, dass $S = \{x_1, \dots, x_m\}$ endlich ist.

Sei nun x algebraisch über K und sei

$$f = T^n + c_{n-1}T^{n-1} + \dots + c_0 \in K[T]$$

das Minimalpolynom von x über K . Nach dem Satz von Gauß ist der Ring $K[x_1, \dots, x_m]$ faktoriell, also können wir

$$x \in K(S) = K(x_1, \dots, x_m) = Q(K[x_1, \dots, x_m])$$

als gekürzten Bruch schreiben:

$$x = \frac{g}{h}, \quad g, h \in K[x_1, \dots, x_m], \quad \text{ggT}(g, h) = 1.$$

Wegen $f(x) = 0$ folgt

$$g^n + c_{n-1}g^{n-1}h + \dots + c_0h^n = 0.$$

Jedes Primelement von $K[x_1, \dots, x_m]$, das h teilt, teilt somit auch g . Weil der Bruch teilerfremd ist, gibt somit kein solches und h ist eine Einheit. Wegen $K[x_1, \dots, x_m]^\times = K^\times$ erhalten wir $h \in K^\times$. Analog schließt man, dass jeder Primteiler von g die Einheit $c_0h^n \in K^\times$ teilt, also gibt es keinen solchen und $g \in K^\times$. Wir erhalten $x \in K^\times$. \square

Beispiel 7.15. Die Körper $K(X^2) \subset K(X)$ sind beide rein transzendent von Transzendenzgrad 1, also nach Satz 7.13 K -isomorph. Trotzdem haben wir eine echte Inklusion zwischen diesen Körpern, die eine endliche algebraische Erweiterung ist.

7.3 Der Satz von Lüroth

Frage (Lürothsches Problem): Ist jede Teilerweiterung einer rein transzendenten Erweiterung wieder rein transzendent?

Antwort: im allgemeinen falsch, aber richtig für Transzendenzgrad 1. Es gilt der

Satz 7.16 (Satz von Lüroth). *Jeder echte Zwischenkörper*

$$K \subsetneq L \subset K(X)$$

ist rein transzendent (vom Transzendenzgrad 1) über K und es gilt $[K(X) : L] < \infty$.

Wir beginnen mit zwei Lemmata.

Lemma 7.17. *Es seien $f, g \in K[X]$, $g \neq 0$, teilerfremd und nicht beide konstant (also $\frac{f}{g} \notin K$). Sei Y eine weitere Variable. Dann ist das Polynom*

$$gY - f \in K(Y)[X]$$

irreduzibel.

Beweis. Es gilt $\deg_Y(gY - f) = 1$, daher ist $gY - f$ irreduzibel in $K(X)[Y]$. Wegen der Teilerfremdheit von f und g ist $gY - f$ primitiv in $K[X][Y]$, also ist $gY - f$ irreduzibel in $K[X][Y] = K[Y][X]$. Wegen $gY - f \notin K(Y)$ folgt die Irreduzibilität von $gY - f$ in $K(Y)[X]$. \square

Lemma 7.18. *Sei $h \in K(X) \setminus K$ und $h = \frac{f}{g}$ mit $f, g \in K[X]$ teilerfremd. Dann gilt*

$$[K(X) : K(h)] = \max(\deg(f), \deg(g)) < \infty.$$

Beweis. Nach Satz 7.14 ist h transzendent über K . Nach Lemma 7.17 (mit $X = T$, $Y = h$) ist das Polynom

$$g(T)h - f(T) \in K(h)[T]$$

irreduzibel. Nun ist X eine Nullstelle dieses Polynoms und wir erhalten somit

$$[K(X) : K(h)] = \deg_T(g(T)h - f(T)) = \max(\deg(f), \deg(g)). \quad \square$$

Beweis des Satzes von L uroth. Sei $K \subsetneq L \subset K(X)$. Nach Lemma 7.18 gilt $[K(X) : K(h)] < \infty$ f ur ein beliebiges $h \in L \setminus K$ und daher auch $[K(X) : L] < \infty$. Sei

$$f_X(T) = T^n + t_{n-1}T^{n-1} + \cdots + t_0 \in L[T]$$

das Minimalpolynom von X  uber L (also $n = [K(X) : L]$). Sei $c_n(X) \in K[X]$ das kgV der Nenner von $t_0, \dots, t_{n-1} \in L \subset K(X)$ in gek urzter Schreibweise. Setzt man $c_i(X) = c_n(X)t_i \in K[X]$, so ist

$$c_n(X)f_X(T) = c_n(X)T^n + \cdots + c_0(X)$$

primitiv in $K[X][T]$. Da X nicht algebraisch  uber K ist, existiert ein r , $0 \leq r \leq n-1$, mit $t_r \notin K$.

Es gilt $K(t_r) \subset L \subset K(X)$ und t_r ist nach Satz 7.14 transzendent  uber K . Es gilt $t_r = \frac{c_r(X)}{c_n(X)}$ und nach Lemma 7.18 gilt:

$$[K(X) : K(t_r)] \leq \max(\deg(c_r), \deg(c_n)). \quad (\dagger)$$

(Der Grund f ur das \leq -Zeichen ist, dass wir (noch) nicht wissen, dass c_r und c_n teilerfremd sind, also Lemma 7.18 erst nach K urzen anwenden k onnen.) Wir zeigen nun $K(t_r) = L$. Wegen $K(t_r) \subset L$ gen ugt es zu zeigen, dass $[K(X) : K(t_r)] \leq [K(X) : L] = n$ gilt. Nach (\dagger) gen ugt es zu zeigen, dass $\max(\deg(c_r), \deg(c_n)) = n$ gilt.

Es ist X Nullstelle des Polynoms

$$c_n(T)t_r - c_r(T) \in K(t_r)[T] \subset L[T].$$

Daher gilt $f_X(T) \mid c_n(T)t_r - c_r(T)$ in $L[T]$. Wir multiplizieren mit $c_n(X)$ und erhalten

$$c_n(X)T^n + \cdots + c_0(X) \mid c_n(T)c_r(X) - c_r(T)c_n(X) \text{ in } K(X)[T].$$

Nach Konstruktion ist die linke Seite primitiv in $K[X][T]$, also liegt nach Satz 2.37 ($v_p(fg) = v_p(f) + v_p(g)$) der Quotient bereits in $K[X][T]$, d.h. es gibt ein $q = q(X, T) \in K[X][T]$ mit

$$q(X, T)(c_n(X)T^n + \cdots + c_0(X)) = c_n(T)c_r(X) - c_r(T)c_n(X) \quad (*)$$

in $K[X][T]$. Wegen

$$\begin{aligned} \deg_X(c_n(X)T^n + \cdots + c_0(X)) &= \max(\deg(c_i(X))) \\ &\geq \max(\deg(c_n(X), c_r(X))) = \deg_X(c_n(T)c_r(X) - c_r(T)c_n(X)) \end{aligned}$$

folgt $\deg_X(q(X, T)) = 0$, also $q \in K[T]$. Weil demnach q durch kein Polynom teilbar ist, in dem die Variable X auftaucht, folgt durch Betrachtung von $(*)$, dass

$$\text{ggT}_{K[X]}(c_r(X), c_n(X)) \mid \text{ggT}_{K[X]}(c_0(X), \dots, c_n(X)) = 1.$$

Also sind $c_r(X)$ und $c_n(X)$ teilerfremd in $K[X]$, und somit auch $c_r(T)$ und $c_n(T)$ in $K[T]$. Wegen $(*)$ ist $c_n(T)c_r(X) - c_r(T)c_n(X)$ in $K(X)[T]$ durch $q(T)$ teilbar, also teilt $q(T)$ das Polynom $c_n(T)t_r - c_r(T)$ in $K(X)[T]$ und damit auch in $K(t_r)[T]$.

Es ist t_r transzendent über K und die Polynome $q(T)$ und $c_n(T)t_r - c_r(T)$ liegen schon in $K[t_r][T]$. Als Polynom in $K[t_r][T]$ ist $q(T)$ primitiv und wie vorher schließt man, dass $q(T) \mid c_n(T)t_r - c_r(T)$ auch in $K[t_r][T] = K[T][t_r]$ gilt. Hieraus folgt $q(T) \mid c_n(T)$ und $q(T) \mid c_r(T)$ in $K[T]$ und weil die beiden Polynome teilerfremd sind, folgt $q \in K^\times$. Wir erhalten aus $(*)$:

$$\begin{aligned} n &= \deg_T(c_n(X)T^n + \dots + c_0(X)) \\ &= \deg_T(c_n(T)c_r(X) - c_r(T)c_n(X)) \\ &= \max(\deg(c_n), \deg(c_r)). \end{aligned}$$

Dies beendet den Beweis. □