Algebra II

VORLESUNGSMITSCHRIFT

Prof. Peter Bürgisser Sommersemester 2014

23. Juli 2014

Inhaltsverzeichnis

6 Algebraische Körpererweiterung (Fortsetzung)

6.7 Separable Polynome

Sei $\mathbb{K}$ ein Körper. In § 6.6. wurde gezeigt, dass $\mathbb{K}$ einen algebraischen Abschluss $\overline{\mathbb{K}}$ hat.

- $\mathbb{K} \subseteq \overline{\mathbb{K}}$ algebraische Körpererweiterung
- $\overline{\mathbb{K}}$ algebraisch abgeschlossen

Sei $f \in \mathbb{K}[X] \backslash \mathbb{K}$. Dann zerfällt f über $\overline{\mathbb{K}}$ in Linearfaktoren.

$$f = \lambda(X - \xi_1)^{e_1} \cdots (X - \xi_s)^{e_s},$$

wobei $\lambda \in \mathbb{K}^\times, e_i \in \mathbb{N}_{\geqslant 1}, \xi_1, \dots \xi_s \in \overline{\mathbb{K}}$ paarweise verschieden.
ξ_i heißt mehrfache Nullstelle, falls $e_i \geqslant 2$, ansonsten heißt ξ_i einfache Nullstelle von f.
Es gilt: ξ_i mehrfache Nullstelle von f $\Leftrightarrow f(\xi_i) = 0 \quad$ und $\quad f'(\xi_i) = 0$.
(siehe § 4.6. formale Ableitungen)

Folglich: f hat eine mehrfache Nullstelle in $\overline{\mathbb{K}} \Leftrightarrow \deg \operatorname{ggT}(f, f') \geqslant 1$.

Bemerkung 6.43. Da $\operatorname{ggT}(f, f') \in \mathbb{K}[X]$ (Euklids Algorithmus), hängt die rechte Bedingung nur von $\mathbb{K}$ ab.
Die linke Bedingung hängt scheinbar nur von $\overline{\mathbb{K}}$ ab.
Das sieht man auch so: Sei $\mathbb{K} \subseteq \widetilde{\mathbb{K}}$ ein weiterer algebraischer Abschluss von $\mathbb{K}$. Dann gibt es einen Isomorphismus $\varphi : \overline{\mathbb{K}} \to \widetilde{\mathbb{K}}$, der auf $\mathbb{K}$ die Identität ist.

Setzen wir $\widetilde{\xi_i} := \varphi(\xi_i)$, so folgt mit dem induktiven Isomorphismus $\varphi : \overline{\mathbb{K}} \to \widetilde{\mathbb{K}}$, dass
$f = \varphi(f) = \lambda(X - \widetilde{\xi_1})^{e_1} \cdots (X - \widetilde{\xi_s})^{e_s}$.

Lemma 6.44. *Sei $f \in \mathbb{K}[X]$ irreduzibel. Dann gilt:*

$$f \text{ hat mehrfache Nullstelle in } \overline{\mathbb{K}} \Leftrightarrow f' = 0$$

Beweis.

$$\begin{aligned} \deg \operatorname{ggT}(f, f') \geqslant 1 &\Leftrightarrow f \text{ teilt } f' \\ &\Leftrightarrow f' = 0 \end{aligned}$$

Beachte: $\deg f' < \deg f$ oder $f' = 0$. □

Definition 6.45. Ein irreduzibles Polynom $f \in \mathbb{K}[X]$ heißt *separabel* , falls $f' \neq 0$ gilt. D.h. ein irreduzibles Polynom f ist genau dann separabel, wenn es keine mehrfachen Nullstellen in $\overline{\mathbb{K}}$ hat.

Gilt $\operatorname{char}(\mathbb{K}) = 0$, d.h. $\mathbb{Q} \subseteq \mathbb{K}$, so ist jedes irreduzible $f \in \mathbb{K}[X]$ separabel.

Beispiel 6.46. Sei $\mathbb{K} = \mathbb{F}_p(t)$ der rationale Funktionenkörper über $\mathbb{F}_p$, p Primzahl.
$f := 1 \cdot X^p - t \in \mathbb{K}[X]$ ist irreduzibel nach Eisenstein.
$\mathbb{K}$ ist Quotientenkörper des Polynomrings.
$f' = \underbrace{p}_{=0} \cdot X^{p-1} - 0 = 0$, also ist f nicht separabel.
$F(X) = X - t$
$F(X^p) = X^p - t$

Satz 6.47. *Sei $f \in \mathbb{K}[X]$ irreduzibel und $p = \mathrm{char}(\mathbb{K}) > 0$. Dann gibt es ein separables $g \in \mathbb{K}[X]$ und $r \in \mathbb{N}_{\geqslant 0}$, sodass*

$$f(X) = g(X^{p^r}).$$

Jede Nullstelle hat Vielfachheit p^r. Davon gibt es deg *g-viele.*

Beweis. Ist f separabel, so setzen wir $r = 0$ und $g = f$.
Sei also f nicht separabel, d.h. $f' = 0$. Sei etwa $f = \sum a_i X^i$.
Dann ist $f' = \sum i a_i X^{i-1}$, also $i a_i = 0$ für alle i. Aus $a_i \neq 0$ folgt $p \mid i$.
Wir erhalten $f(X) = h(X^p)$, wobei h$= \sum_j a_{pj} X^j$. (vgl. § 4.6).
Wir wählen $r \in \mathbb{N}_{\geqslant 0}$ maximal mit der Eigenschaft

$$\exists g \in \mathbb{K}[X] \text{ s.d. } f(X) = g(X^{p^r}).$$

Dann gilt $g' \neq 0$ wegen der Maximalität von r.
Weiter ist g irreduzibel, da f irreduzibel ist. Also ist g separabel.
Sei nun $g = \lambda \prod_{i=1}^{d} (X - \eta_i)$ und $\lambda \in \mathbb{K}^\times$ und $\eta_1, \ldots, \eta_d$ paarweise verschieden.
Seien $\xi_1, \ldots, \xi_d \in \overline{\mathbb{K}}$ mit $\xi_i^{p^r} = \eta_i$.
Dann gilt:

$$f(X) = g(X^{p^r}) = \lambda \prod_{i=1}^{d} (X^{p^r} - \xi_i^{p^r}) = \lambda \prod_{i=1}^{d} (X - \xi_i)^{p^r}.$$

$d = \deg g$. □

6.8 Perfekte Körper

Definition 6.48. Sei $\mathbb{K} \subseteq \mathbb{L}$ algebraische Körpererweiterung.

- Ein Element $a \in \mathbb{L}$ heißt *separabel über* $\mathbb{K}$, wenn das Minimalpolynom von a über $\mathbb{K}$ separabel ist.
- Die Erweiterung $\mathbb{K} \subseteq \mathbb{L}$ heißt *separabel*, falls jedes $a \in \mathbb{L}$ separabel über $\mathbb{K}$ ist.

Definition 6.49. Ein Körper heißt *perfekt*, falls jede algebraische Erweiterung von $\mathbb{K}$ separabel ist.

Bemerkung 6.50.

1. In Charakteristik 0 ist jede algebraische Körpererweiterung separabel.
2. Jeder Körper der Charakteristik 0 ist perfekt.
3. $\mathbb{K}$ ist genau dann perfekt, wenn jedes irreduzible Polynom in $\mathbb{K}[X]$ separabel ist.

Beispiel 6.51. Die Erweiterung $\mathbb{F}_p(t^p) \subseteq \mathbb{F}_p(t)$ ist nicht separabel.
Grund: Das Minimalpolynom von t über $\mathbb{F}_p(t^p)$ ist gleich $f = X^p - t^p$.
(Beachte, dass $X^p - t^p$ irreduzibel in $\mathbb{F}_p(t^p)[X]$ ist.→ Übung!)
Aber $f' = 0$, also ist f nicht separabel. Insbesondere ist $\mathbb{F}_p(t^p)$ nicht perfekt.

Wir hatten perfekte Körper schon in § 4.6 eingeführt und zeigen jetzt, dass die neue Definition konsistent mit der früheren ist.

Satz 6.52. *Sei* $\mathrm{char}\,\mathbb{K} = p > 0$. *Der Körper $\mathbb{K}$ ist genau dann perfekt, wenn jedes Element aus $\mathbb{K}$ eine p–te Wurzel in $\mathbb{K}$ hat.*

Beweis. " $\Leftarrow$ " Angenommen jedes Element aus $\mathbb{K}$ hat eine p–te Wurzel.
Sei $f \in \mathbb{K}[X]$ irreduzibel.
$\Rightarrow$ (nach Satz 6.47) Es gibt $g = \sum_j a_j X^j \in \mathbb{K}[X]$ separabel und $r \geq 0$, sodass

$$f(X) = g(X^{p^r}) = \sum_j a_j X^{jp^r} \tag{6.1}$$

Nach Voraussetzung existieren $b_j \in \mathbb{K}$ mit $a_j = b_j^{p^r}$. $\Rightarrow f(X) = \sum_j b_j^{p^r} (X^j)^{p^r} = \left(\sum_j b_j X^j \right)^{p^r}$
Da f irreduzibel, folgt $r = 0$. Also ist f separabel.
" $\Rightarrow$ " Angenommen $a \in \mathbb{K}$ hat keine p–te Wurzel in $\mathbb{K}$.
Betrachte $f := X^p - a$. Sei $b \in \overline{\mathbb{K}}$ mit $b^p = a$. $\Rightarrow f = X^p - b^p = (X-b)^p$ über $\overline{\mathbb{K}}$
Sei $h \in \mathbb{K}[X]$ ein irreduzibler normierter Teiler von f. Dann gibt es $k \geq 1$, sodass $h = (X-b)^k$. Es gilt $k > 1$, da $b \notin \mathbb{K}$ (dh. da a keine p–te Wurzel in $\mathbb{K}$ hat). Also ist $h \in \mathbb{K}[X]$ nicht separabel, da b eine mehrfache Nullstelle ist. □

Satz 6.53. *Endliche Körper sind perfekt.*

Beweis. Sei $\mathbb{K}$ endlich, $p = \mathrm{char}(\mathbb{K}) > 0$. Der Frobenius-Homomorphismus $\Phi : \mathbb{K} \to \mathbb{K}, a \mapsto a^p$ hat den Kern 0, ist also injektiv. Da $\mathbb{K}$ endlich ist, ist Φ surjektiv. Mit Satz 6.52 folgt, dass $\mathbb{K}$ perfekt ist. □

6.9 Separable Körpererweiterungen

Definition 6.54. Für eine algebraische Körpererweiterung $\mathbb{K} \subseteq \mathbb{L}$ bezeichne $\mathrm{Hom}_{\mathbb{K}}\left(\mathbb{L}, \overline{\mathbb{K}}\right)$ die Menge der Homomorphismen $\mathbb{L} \to \overline{\mathbb{K}}$, welche die Elemente von $\mathbb{K}$ fixieren ($\mathbb{K}$-Homomorphismen). Der *Separabilitätsgrad* von $\mathbb{L}$ über $\mathbb{K}$ ist definiert als $[\mathbb{L} : \mathbb{K}]_S := |\mathrm{Hom}_{\mathbb{K}}\left(\mathbb{L}, \overline{\mathbb{K}}\right)|$.

Bemerkung 6.55. (1) $[\mathbb{L} : \mathbb{K}]_S$ ist unabhängig von der Wahl von $\mathbb{K}$, wegen Eindeutigkeit von $\overline{\mathbb{K}}$ bis auf Isomorphie.
(2) $[\mathbb{L} : \mathbb{K}]_S \in \mathbb{N} \cup \{\infty\}$

Lemma 6.56 (Schlüssellemma)**.** *Es sei $\mathbb{K} \subseteq \mathbb{L} = \mathbb{K}(a)$ eine einfache Körpererweiterung und $f \in \mathbb{K}[X]$ das Minimalpolynom von a.*
(1) $[\mathbb{L} : \mathbb{K}]_S$ ist gleich der Anzahl der verschiedenen Nullstellen von f in $\overline{\mathbb{K}}$.
(2) a ist genau dann separabel über $\mathbb{K}$, wenn $[\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{K}]_S$.
(3) Gilt $\mathrm{char}(\mathbb{K}) = p > 0$*, so gilt für ein $r \geq 0$*

$$[\mathbb{L} : \mathbb{K}] = p^r \, [\mathbb{L} : \mathbb{K}]_S \,, \tag{6.2}$$

wobei p^r die Vielfachheit der Nullstelle a von f ist.

Beweis. Seien $a = a_1, a_2, ..., a_s$ die verschiedenen Nullstellen von f in $\overline{\mathbb{K}}$. Ist $\sigma \in \mathrm{Hom}_{\mathbb{K}}\left(\mathbb{L}, \overline{\mathbb{K}}\right)$, so folgt aus $f(a) = 0$, da σ ein $\mathbb{K}$-Homomorphismus ist:

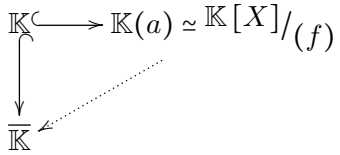
$$0 = \sigma(f(a)) = f(\sigma(a)), \text{ also: } \exists i \in \{1, ..., s\} \;\; \sigma(a) = a_i$$

Wegen $\mathbb{L} = \mathbb{K}(a)$ ist σ durch $\sigma(a)$ festgelegt.
Also $[\mathbb{L} : \mathbb{K}]_S = |\mathrm{Hom}_{\mathbb{K}}\left(\mathbb{L}, \overline{\mathbb{K}}\right)| \leq s$. (wobei s die Anzahl der verschiedenen Nullstellen von f ist).

Umgekehrt besagt der Erweiterungssatz für Körperhomomorphismen (§ 6.6.Lemma 6.40) Folgendes:

$$\forall i \exists \sigma_i \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}})\ \sigma_i(a) = a_i$$

Dafür erinnern wir uns an folgendes Diagramm:



Dies zeigt Behauptung (1).

Zu Behauptung (2): Weiterhin gilt

$$[\mathbb{L} : \mathbb{K}] = \deg f$$

daraus folgt folgende Äquivalenz zur Voraussetzung:

$$a \text{ separabel } \Leftrightarrow f \text{ hat keine mehrfache Nullstelle} \Leftrightarrow s = \deg f \Leftrightarrow [\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{K}]_S$$

Für Behauptung (3) verwenden wir Satz 6.47 :

$$\exists g \in \mathbb{K}[X] \text{ separabel}, \exists r \geq 0\ f(X) = g(X^{p^r}) \Rightarrow \deg f = p^r \deg g \text{ , dh. } [\mathbb{L} : \mathbb{K}] = p^r [\mathbb{L} : \mathbb{K}]_S$$

□

Satz 6.57 (Multiplikativität des Separabilitätsgrades)**.** *Für algebraische Körpererweiterungen* $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{M}$ *gilt:*

$$[\mathbb{M} : \mathbb{K}]_S = [\mathbb{M} : \mathbb{L}]_S \cdot [\mathbb{L} : \mathbb{K}]_S$$

Beweis. Sei $\overline{\mathbb{K}}$ ein algebraischer Abschluss von $\mathbb{M}$ (und damit ebenfalls algebraischer Abschluss von $\mathbb{K}$ und $\mathbb{L}$), also:

$$\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{M} \subseteq \overline{\mathbb{L}} = \overline{\mathbb{M}} = \overline{\mathbb{K}}$$

Seien $\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}}) = \{\sigma_i | i \in I\}$ und $\mathrm{Hom}_{\mathbb{L}}(\mathbb{M}, \overline{\mathbb{K}}) = \{\tau_j | j \in J\}$ mit (eventuell nicht endlichen) Indexmengen I, J. Wir setzen $\sigma_i : \mathbb{L} \to \overline{K}$ fort zu $\overline{\sigma}_i : \overline{\mathbb{K}} \to \overline{\mathbb{K}}$ (nach dem Erweiterungssatz § 6.6. Satz 6.41).
Sei $\tau \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{M}, \overline{\mathbb{K}})$. Dann gilt $\tau|_{\mathbb{L}} \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}})$, woraus $\exists i\ \tau|_{\mathbb{L}} = \sigma_i$. Nun fixiert $\overline{\sigma}_i^{-1} \circ \tau : \overline{\mathbb{M}} \to \overline{\mathbb{K}}$ die Elemente von $\mathbb{L}$. Also $\exists j\ \overline{\sigma}_i^{-1} \circ \tau = \tau_j$. Damit haben wir insgesamt gezeigt: $\mathrm{Hom}_{\mathbb{K}}(\mathbb{M}, \overline{\mathbb{K}}) = \{\overline{\sigma}_i \circ \tau_j | i \in I, j \in J\}$. Es bleibt zu zeigen, dass die Abbildungen $\overline{\sigma}_i \circ \tau_j$ für $i \in I, j \in J$ paarweise verschieden sind. Dazu sei $\overline{\sigma}_i \circ \tau_j = \overline{\sigma}_{i_1} \circ \tau_{j_1}$. Durch Einschränkung auf $\mathbb{L}$ erhalten wir $\sigma_i = \sigma_{i_1}$ und damit $i = i_1$. Also auch: $\overline{\sigma}_i = \overline{\sigma}_{i_1} \Rightarrow \tau_j = \tau_{j_1} \Rightarrow j = j_1$ □

Korollar 6.58. *Sei* $\mathbb{K} \subseteq \mathbb{L}$ *endliche Körpererweiterung. Dann gilt:*
(1) $\mathrm{char}(\mathbb{K}) = 0 \Rightarrow [\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{K}]_S$
(2) $\mathrm{char}(\mathbb{K}) = p > 0 \Rightarrow \exists r \in \mathbb{N}\ [\mathbb{L} : \mathbb{K}] = p^r [\mathbb{L} : \mathbb{K}]_S$ *Insbesondere gilt dabei:*
$1 \leq [\mathbb{L} : \mathbb{K}]_S \leq [\mathbb{L} : \mathbb{K}]$ *und* $[\mathbb{L} : \mathbb{K}]_S$ *ist ein Teiler von* $[\mathbb{L} : \mathbb{K}]$

Beweis. $\exists a_1, \ldots, a_n \in \mathbb{L}, \mathbb{L} = \mathbb{K}(a_1, \ldots, a_n), a_i$ algebraisch über $\mathbb{K}$.
Setze $\mathbb{L}_i := \mathbb{K}(a_1, \ldots, a_i)$. Dann ist $\mathbb{K} = \mathbb{L}_0 \subseteq \mathbb{L}_1 \subseteq \ldots \subseteq \mathbb{L}_n = \mathbb{L}$.
$\mathbb{L}_i = \mathbb{L}_{i-1}(a_i)$ ist einfache algebraische Erweiterung.

$$[\mathbb{L} : \mathbb{K}] = \prod_{i=1}^{n} [\mathbb{L}_i : \mathbb{L}_{i-1}], [\mathbb{L} : \mathbb{K}]_S = \prod_{i=1}^{n} [\mathbb{L}_i : \mathbb{L}_{i-1}]_S .$$

(1) $\operatorname{char}(\mathbb{K}) = 0$. Schlüssellemma 6.56 $\Rightarrow [\mathbb{L} : \mathbb{L}_{i-1}] = [\mathbb{L} : \mathbb{L}_{i-1}]_S \Rightarrow [\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{K}]_S$
(2) $\operatorname{char}(\mathbb{K}) = p > 0$. Schlüssellemma 6.56

$$\exists r_i \in \mathbb{N} : [\mathbb{L}_i : \mathbb{L}_{i-1}] = p^{r_i} [\mathbb{L}_i : \mathbb{L}_{i-1}]_S \Rightarrow [\mathbb{L} : \mathbb{K}] = p^{\sum_i r_i} [\mathbb{L} : \mathbb{K}]_S$$

□

Satz 6.59. *Sei $\mathbb{K} \subseteq \mathbb{L}$ endliche Körpererweiterung. Äquivalent sind:*
(1) $\mathbb{K} \subseteq \mathbb{L}$ separabel
(2) $\exists a_1, \ldots, a_n \in \mathbb{L}$ separabel über $\mathbb{K}$ mit $\mathbb{L} = \mathbb{K}(a_1, \ldots, a_n)$
(3) $[\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{K}]_S$

Beweis. (1) $\Rightarrow$ (2) trivial.
(2) $\Rightarrow$ (3) Schreibe $\mathbb{L}_i = \mathbb{K}(a_1, \ldots, a_i)$. Dann ist $\mathbb{L}_i = \mathbb{L}_{i-1}(a_i)$, a_i separabel über $\mathbb{L}_{i-1}$ (da a_i separabel über $\mathbb{K}$).
Schlüssellemma 6.56 $:\Rightarrow [\mathbb{L}_i : \mathbb{L}_{i-1}] = [\mathbb{L}_i : \mathbb{L}_{i-1}]_S$
Multiplikation $\Rightarrow [\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{K}]_S$.
(3) $\Rightarrow$ (1) Sei $a \in \mathbb{L}$. Müssen zeigen, dass a separabel über $\mathbb{K}$ ist.
Gemäß Schlüssellemma 6.56 heißt dies:
$[\mathbb{K}(a) : \mathbb{K}] = [\mathbb{K}(a) : \mathbb{K}]_S$. Ohne Einschränkung ist $\operatorname{char}(\mathbb{K}) = p > 0$.
Damit $[\mathbb{L} : \mathbb{K}(a)] \geq [\mathbb{L} : \mathbb{K}(a)]_S$
und $[\mathbb{K}(a) : \mathbb{K}] \geq [\mathbb{K}(a) : \mathbb{K}]_S$ und insgesamt
$[\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{K}(a)] [\mathbb{K}(a) : \mathbb{K}] \geq [\mathbb{L} : \mathbb{K}(a)]_S [\mathbb{K}(a) : \mathbb{K}]_S = [\mathbb{L} : \mathbb{K}]_S$
Da $[\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{K}]_S \Rightarrow [\mathbb{K}(a) : \mathbb{K}] = [\mathbb{K}(a) : \mathbb{K}]_S$ □

Korollar 6.60. *Sei $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{M}$ algebraische Körpererweiterung.*
Dann gilt: $\mathbb{K} \subseteq \mathbb{M}$ separabel $\Leftrightarrow \mathbb{K} \subseteq \mathbb{L}$ separabel und $\mathbb{L} \subseteq \mathbb{M}$ separabel

Beweis. " $\Rightarrow$ " fast trivial.
" $\Leftarrow$ " Falls $[\mathbb{M} : \mathbb{K}] < \infty$ folgt dies aus der Charakterisierung des Satzes und der Multiplikation der Grade.
Falls $[\mathbb{M} : \mathbb{K}] = \infty \Rightarrow$ Übungsaufgabe. □

6.10 Satz vom primitiven Element

Satz 6.61. *Sei $\mathbb{L} = \mathbb{K}(a_1, \ldots, a_k)$ eine endliche separable Körpererweiterung in $\mathbb{K}$. Dann existiert $\vartheta \in \mathbb{L}$ und $\mathbb{L} = \mathbb{K}(\vartheta)$.*
Ist $\mathbb{K}$ unendlich, so kann ϑ in der Form $\vartheta = \lambda_1 a_1 + \cdots + \lambda_k a_k$, $\lambda_1, \ldots, \lambda_k \in \mathbb{K}$ gewählt werden (und fast jede Wahl von $\lambda_1, \ldots, \lambda_k \in \mathbb{K}$ liefert ein geeignetes ϑ).

Beweis.
- Ist $\mathbb{K}$ endlich, so auch $\mathbb{L}$.
  Bekanntlich ist $\mathbb{L}^\times$ zyklisch (vgl. § 6.5.), etwa $\mathbb{L}^\times = \langle \vartheta \rangle$. Dann ist $\mathbb{L} = \mathbb{K}(\vartheta)$.

- Sei jetzt $\mathbb{K}$ unendlich. O.B.d.A. $k = 2$ (sonst Induktion nach k).
  Sei also $\mathbb{L} = \mathbb{K}(a, b)$ eine endliche separable Erweiterung von $\mathbb{K}$.
  Sei $n := [\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{K}]_S$, etwa $\mathrm{Hom}_{\mathbb{K}}\left(\mathbb{L}, \overline{\mathbb{K}}\right) = \{\sigma_1, \ldots, \sigma_n\}$. Suche $\lambda \in \mathbb{K}$ mit
  $(\star)$ $\quad \sigma_1(a + \lambda b), \ldots, \sigma_n(a + \lambda b)$ paarweise verschieden.
  Zeigen zunächst:
  $(\star) \Rightarrow \vartheta = a + \lambda b$ ist primitives Element.
  Denn aus $(\star)$ folgt: $[\mathbb{K}(\vartheta) : \mathbb{K}]_S \geq n$. Weiter gilt:
  $n = [\mathbb{L} : \mathbb{K}] \geq [\mathbb{K}(\vartheta) : \mathbb{K}] \geq [\mathbb{K}(\vartheta) : \mathbb{K}]_S \geq n \Rightarrow \mathbb{L} = \mathbb{K}(\vartheta)$.
  Die Bedingung $(\star)$ ist genau dann verletzt, wenn $\exists i \neq j : \sigma_i(a + \lambda b) = \sigma_j(a + \lambda b)$.

  $$\text{D.h.} \prod_{i \neq j} (\sigma_i(a) - \sigma_j(a) + \lambda(\sigma_i(b) - \sigma_j(b))) = 0$$

  Das Polynom $\prod_{i \neq j}(\sigma_i(a) - \sigma_j(a) + (\sigma_i(b) - \sigma_j(b))T) \in \overline{\mathbb{K}}[T]$ ist nicht das Nullpolynom.
  Für $i \neq j$ ist $\sigma_i \neq \sigma_j$.
  $\Rightarrow \sigma_i(a) \neq \sigma_j(a)$ oder $\sigma_i(b) \neq \sigma_j(b)$. (ansonsten wäre $\sigma_i = \sigma_j$ wegen $\mathbb{L} = \mathbb{K}(a, b)$).
  Da $\mathbb{K}$ unendlich ist, existiert $\lambda \in \mathbb{K}$ und $P(\lambda) \neq 0$ (alle bis auf endlich viele λ erfüllen $(\star)$).

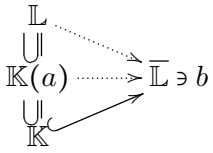
□

6.11 Normale Körpererweiterung

Definition 6.62. Eine *normale* Körpererweiterung $\mathbb{K} \subseteq \mathbb{L}$ ist eine algebraische Erweiterung mit der Eigenschaft, dass jedes irreduzible $g \in \mathbb{K}[X]$, das eine Nullstelle in $\mathbb{L}$ hat, über $\mathbb{L}$ in Linearfaktoren zerfällt.

Satz 6.63. *Sei $\mathbb{L}$ ein Zerfällungskörper von $f \in \mathbb{K}[X] \backslash \mathbb{K}$. Dann ist $\mathbb{K} \subseteq \mathbb{L}$ eine endliche, normale Körpererweiterung.*

Beweis. Sei $f = (X - a_1) \cdots (X - a_n), \mathbb{L} = \mathbb{K}(a_1, \ldots, a_n)$. Sei $g \in \mathbb{K}[X]$ irreduzibel mit $g(a) = 0, a \in \mathbb{L}$. Angenommen es gibt $b \in \overline{\mathbb{L}}$ mit $g(b) = 0$. Zu zeigen: $b \in \mathbb{L}$.
Der Erweiterungssatz (§ 6.6. Lemma 6.40 und Satz 6.41) liefert die Existenz eines Morphismus:



$\sigma : \mathbb{L} \to \overline{\mathbb{L}}$ mit $\sigma|_{\mathbb{K}} = \mathrm{id}, \sigma(a) = b$
Nun gilt: $f(a_i) = 0 \Rightarrow f(\sigma(a_i)) = 0$. Deshalb permutieren die Nullstellen $a_1, \ldots, a_n$.
$\Rightarrow \sigma(\mathbb{L}) = \mathbb{L}$. Wegen $a \in \mathbb{L}$ folgt: $b = \sigma(a) \in \sigma(\mathbb{L})$. Also $b \in \mathbb{L}$. □

Satz 6.64. *Sei $\mathbb{K} \subseteq \mathbb{L}$ eine endliche, normale Erweiterung. Dann ist $\mathbb{L}$ der Zerfällungskörper eines Polynoms $f \in \mathbb{K}[X]$.*

Beweis. Sei $\mathbb{L} = \mathbb{K}(a_1, \ldots, a_n)$ und f_i das Minimalpolynom von a_i über $\mathbb{K}$. Seien $a_i = a_{i1}, \ldots, a_{id_i}$ die Nullstellen von f_i in $\overline{\mathbb{K}}$.
Da $\mathbb{K} \subseteq \mathbb{L}$ normal ist $\Rightarrow a_{ij} \in \mathbb{L}$
Haben $\mathbb{L} = \mathbb{K}(a_{11}, \ldots, a_{1d_1}, \ldots\ldots, a_{n1}, \ldots, a_{nd_n})$ und $a_{11}, \ldots, a_{nd_n}$ sind die Nullstellen von $F = f_1 \cdot f_2 \cdots f_n \in \mathbb{K}[X]$.
Also ist $\mathbb{L}$ der Zerfällungskörper von F. □

Bemerkung 6.65. Man definiert *Zerfällungskörper* $\mathbb{L}$ für eine (nicht notwendig endliche) Familie $\mathscr{F}$ von nicht-konstanten Polynomen über $\mathbb{K}$ auf naheliegende Weise durch die folgenden Eigenschaften:

1. Jedes Polynom in $\mathscr{F}$ zerfällt über $\mathbb{L}$.
2. Die Körpererweiterung $\mathbb{K} \subseteq \mathbb{L}$ wird von allen Nullstellen aller Polynome in $\mathscr{F}$ erzeugt.

Dann gilt:
$\mathbb{K} \subseteq \mathbb{L}$ normal $\Leftrightarrow \mathbb{K} \subseteq \mathbb{L}$ Zerfällungskörper.

Beweis. Analog zu den Beweisen von Satz 6.63 und Satz 6.64 □

Proposition 6.66. *Sei $\mathbb{K}$ endlicher Körper und $\mathbb{K} \subseteq \mathbb{L}$ algebraische Erweiterung. Dann ist $\mathbb{K} \subseteq \mathbb{L}$ separabel und normal.*

Beweis. $\mathbb{K} \subseteq \mathbb{L}$ separabel, da $\mathbb{K}$ perfekt.
Wir zeigen nun, dass $\mathbb{K} \subseteq \mathbb{L}$ normal ist:
Da $0 < \operatorname{char}\mathbb{K} = \operatorname{char}\mathbb{L}$, ist ($\mathbb{K} \subseteq \mathbb{L}$ eine endliche Erweiterung und) $\mathbb{L}$ endlicher Körper, etwa $\mathbb{L} \simeq \mathbb{F}_q$.
$\mathbb{F}_q$ ist Zerfällungskörper von $X^q - X \in \mathbb{F}_p[X]$, $q = p^n$. Also ist $\mathbb{K} \subseteq \mathbb{L}$ normal. □

Korollar 6.67. *Seien $\mathbb{K} \subseteq \mathbb{E} \subseteq \mathbb{L}$ Körpererweiterungen.*
Es gilt: $\mathbb{K} \subseteq \mathbb{L}$ normal $\Rightarrow \mathbb{E} \subseteq \mathbb{L}$ normal

Beweis. $\mathbb{K} \subseteq \mathbb{L}$ normal $\Rightarrow \mathbb{L}$ ist Zerfällungskörper einer Familie $\mathscr{F}$ von Polynomen über $\mathbb{K}$, also ist $\mathbb{L}$ auch Zerfällungskörper von $\mathscr{F}$ über $\mathbb{E}$. □

Voraussetzung für die nachfolgenden 2 Propositionen
Sei $\mathbb{K} \subseteq \mathbb{L}$ Körpererweiterung. Und die Gruppe der $\mathbb{K}$-Automorphismen von $\mathbb{L}$ sei
$\operatorname{Aut}_{\mathbb{K}}(\mathbb{L}) := \left\{\sigma \mid \sigma : \mathbb{L} \xrightarrow{\sim} \mathbb{L} \text{ Automorphismen mit } \sigma(a) = a \text{ für alle } a \in \mathbb{K}\right\}$
Sei $\mathbb{L} \subseteq \overline{\mathbb{L}}$ algebraischer Abschluss. Fasse $\sigma \in \operatorname{Aut}_{\mathbb{K}}(\mathbb{L})$ auf als $\mathbb{K}$-Homomorphismus. Es gilt $\mathbb{L} \overset{\sigma}{\underset{\sim}{\mapsto}} \mathbb{L} \hookrightarrow \overline{\mathbb{L}}$ und $\operatorname{Aut}_{\mathbb{K}}(\mathbb{L}) \subseteq \operatorname{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{L}})$

Proposition 6.68 (Proposition 1)**.** *Sei $\mathbb{K} \subseteq \mathbb{L}$ normale Körpererweiterung und $\sigma : \mathbb{L} \mapsto \overline{\mathbb{L}}$ ein $\mathbb{K}$-Homomorphismus. Dann gilt $\sigma(\mathbb{L}) = \mathbb{L}$, insbesondere $\sigma \in \operatorname{Aut}_{\mathbb{K}}(\mathbb{L})$.*

Beweis. Sei $a \in \mathbb{L}$ mit Minimalpolynom $g \in \mathbb{K}[X]$, etwa $g = (X - a_1)...(X - a_n)$ mit $a = a_1, a_2, ..., a_n \in \overline{\mathbb{L}}$. Da $\mathbb{K} \subseteq \mathbb{L}$ normal $\Rightarrow a_2, ..., a_n \in \mathbb{L}$. □

Proposition 6.69 (Proposition 2)**.** *Sei $\mathbb{K} \subseteq \mathbb{L}$ eine algebraische Erweiterung, für welche gilt:*

$$\forall \sigma \in \operatorname{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{L}})\ \sigma(\mathbb{L}) = \mathbb{L}$$

Dann ist $\mathbb{K} \subseteq \mathbb{L}$ normal.

Beweis. Sei $g \in \mathbb{K}(X)$ irreduzibel, $a \in \mathbb{L}$, $g(a) = 0$ und $g = (X - a_1)...(X - a_n)$ mit $a = a_1, a_2, ..., a_n \in \overline{\mathbb{L}}$. $\forall i \exists \sigma_i \in \operatorname{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{L}})$ mit $\sigma_i(a) = a_i$ (Erweiterungslemma § 6.6. Lemma 6.40)
Da $\sigma_i(\mathbb{L}) = \mathbb{L}$ gilt, folgt nach Voraussetzung $\Rightarrow a_i \in \mathbb{L}$.

□

7 Galois-Theorie

7.1 Galois-Erweiterung

Sei $\mathbb{K} \subseteq \mathbb{L}$ eine endliche, normale Körpererweiterung.
Nach Definition gilt: $[\mathbb{L} : \mathbb{K}]_S = |\operatorname{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{L}})|$
Wir identifizieren $\operatorname{Aut}_{\mathbb{K}}(\mathbb{L}) \equiv \operatorname{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{L}})$ (möglich da die Körpererweiterung normal ist).
Es gilt Gleichheit, wenn $\mathbb{K} \subseteq \mathbb{L}$ separabel.

Definition 7.1. Eine algbraische Körpererweiterung $\mathbb{K} \subseteq \mathbb{L}$ heißt *galoisch*, wenn sie normal und separabel ist. Man nennt $\operatorname{Gal}(\mathbb{L}/\mathbb{K}) := \operatorname{Aut}_{\mathbb{K}}(\mathbb{L})$ die *Galoisgruppe* von $\mathbb{K} \subseteq \mathbb{L}$.

Korollar 7.2. $\mathbb{K} \subseteq \mathbb{L}$ *endliche Galois-Erweiterung* $\Rightarrow |\operatorname{Gal}(\mathbb{L}/\mathbb{K})| = [\mathbb{L} : \mathbb{K}]$

Definition 7.3. Sei $\mathbb{L}$ ein Körper und G eine Untergruppe von $\operatorname{Aut}(\mathbb{L})$. Dann ist der *Fixkörper* von G definiert als $\mathbb{L}^G := \{a \in \mathbb{L} | \forall \sigma \in G\ \sigma(a) = a\}$

Bemerkung 7.4. Es ist klar, dass $\mathbb{L}^G \subseteq \mathbb{L}$ Unterkörper und $G \leq \operatorname{Aut}_{\mathbb{L}^G}(\mathbb{L})$

Proposition 7.5 (Emil Artin)**.** *Ist* $G \leq \operatorname{Aut}(\mathbb{L})$ *endlich so folgt:* $\mathbb{K} := \mathbb{L}^G \subseteq \mathbb{L}$ *ist eine Galois-Erweiterung mit Galoisgruppe* $\operatorname{Gal}(\mathbb{L}/\mathbb{L}^G) = G$

Beweis. Sei $a \in \mathbb{L}$. Betrachte die G-Bahn von a: $\{\sigma(a) | \sigma \in G\} = \{a_1, a_2, ..., a_r\}$, wobei $a = a_1, ..., a_r$ paarweise verschieden sind. Es gilt: $r \leq |G|$ und wir definieren
$f := \prod_{i=1}^{r}(X - a_i)$. Die Koeffizienten von f sind die elementarsymmetrischen Polynome in $a_1, .., a_r$, also insbesondere symmetrisch.
Da $\sigma \in G$ die Menge $\{a_1, ..., a_r\}$ permutiert, sind die Koeffizienten von f aus $\mathbb{K} = \mathbb{L}^G$.
Das Minimalpolynom g von a über $\mathbb{K}$ ist ein Teiler von f und zerfällt in verschiedene Linearfaktoren. Also:

$$[\mathbb{K}(a) : \mathbb{K}] = \deg g \leq \deg f = r \leq |G| =: n \quad (*)$$

Folglich ist die Erweiterung $\mathbb{K} \subseteq \mathbb{L}$ normal, separabel und algebraisch, d.h. $\mathbb{K} \subseteq \mathbb{L}$ ist eine Galois-Erweiterung.
Wir zeigen jetzt, dass $\mathbb{K} \subseteq \mathbb{L}$ endlich ist:
Wir haben also $n := |G|$ gesetzt (s.o.). Sei $\mathbb{K} \subseteq \mathbb{L}' \subseteq \mathbb{L}$ mit $[\mathbb{L}' : \mathbb{K}] < \infty$. Da $\mathbb{K} \subseteq \mathbb{L}'$ endlich und separabel ist, folgt $\exists a$ sodass $\mathbb{L}' \subseteq \mathbb{K}(a)$.
Nach $(*)$ gilt also: $[\mathbb{L}' : \mathbb{K}] = [\mathbb{K}(a) : \mathbb{K}] \leq n$ Wird $\mathbb{L}'$ mit maximalem Grad gewählt (möglich da $[\mathbb{L}' : \mathbb{K}] \leq n$), so muss $\mathbb{L}' = \mathbb{L}$ gelten (sonst existierte $a \in \mathbb{L}$ mit $\mathbb{L}' \subsetneq \mathbb{L}'(a) \subseteq \mathbb{L}$. Widerspruch zu Maximalität!). Wir zeigen damit also $[\mathbb{L} : \mathbb{K}] \leq n$.
$\mathbb{K} \subseteq \mathbb{L}$ eine endliche Galois-Erweiterung und wir wissen $|\operatorname{Gal}(\mathbb{L}/\mathbb{K})| = [\mathbb{L} : \mathbb{K}]$ (Wichtig!).
Es gilt $G \leq \operatorname{Gal}(\mathbb{L}/\mathbb{K})$. Wir zeigen im Folgenden Gleichheit:

$$n = |G| \leq |\operatorname{Gal}(\mathbb{L}/\mathbb{K})| = [\mathbb{L} : \mathbb{K}] \leq n \Rightarrow G = \operatorname{Gal}(\mathbb{L}/\mathbb{K})$$

□

Bemerkung 7.6. $\mathbb{K} \subseteq \mathbb{L}$ galoisch, $\mathbb{K} \subseteq \mathbb{E} \subseteq \mathbb{L} \Rightarrow \mathbb{E} \subseteq \mathbb{L}$ galoisch.

Beweis. $\mathbb{E} \subseteq \mathbb{L}$ normal, vergleiche früher. $\mathbb{E} \subseteq \mathbb{L} \ni a$ separabel, vergleiche früher. □

Satz 7.7 (Hauptsatz der Galois-Theorie)**.** *Sei* $\mathbb{K} \subseteq \mathbb{L}$ *endliche Galois-Erweiterung mit* $G = \mathrm{Gal}(\mathbb{L}/\mathbb{K})$.
Dann sind die Zuordnungen

$$\{\textit{Untergruppen von } G\} \longleftrightarrow \{\textit{Zwischenkörper von } \mathbb{K} \subseteq \mathbb{L}\}$$

$$H \longrightarrow \mathbb{L}^H$$

$$\mathrm{Gal}(\mathbb{L}/\mathbb{E}) \longleftarrow \mathbb{E}$$

bijektiv und invers zueinander.
Weiterhin gilt:

$$H_1 \leq H_2 \Leftrightarrow \mathbb{L}^{H_1} \supseteq \mathbb{L}^{H_2} \textit{ und } \mathbb{E}_1 \subseteq \mathbb{E}_2 \Leftrightarrow \mathrm{Gal}(\mathbb{L}/\mathbb{E}_1) \geq \mathrm{Gal}(\mathbb{L}/\mathbb{E}_2)$$

Beispiel 7.8. $\mathbb{K} = \mathbb{F}_p \subseteq \mathbb{L} = \mathbb{F}_{p^n}$ und $[\mathbb{L} : \mathbb{K}] = n$ $\forall m$ mit $m|n$ $\exists! \mathbb{E} \subseteq \mathbb{L}$ mit $|\mathbb{E}| = p^m$, dh. $[\mathbb{E} : \mathbb{F}_p] = m$ und $|H| = [\mathbb{L} : \mathbb{E}] = \frac{n}{m}$

Beweis. (1) $\mathrm{Gal}(\mathbb{L}/\mathbb{L}^H) = H$ wegen Artins Proposition 7.5.
Sei $\mathbb{K} \subseteq \mathbb{E} \subseteq \mathbb{L}$. Dann ist $\mathbb{E} \subseteq \mathbb{L}$ endliche Galois-Erweiterung. Sei $H := \mathrm{Gal}(\mathbb{K}/\mathbb{E})$. Wegen Korollar 7.2 $|H| = [\mathbb{L} : \mathbb{E}]$.
Offensichtlich $\mathbb{E} \subseteq \mathbb{L}^H$. Artins 7.5 $\Rightarrow \mathbb{L}^H \subseteq \mathbb{L}$ endliche Galois-Erweiterung mit Galoisgruppe H. Deshalb $|H| = |\mathrm{Gal}(\mathbb{L}/\mathbb{L}^H)| = \left[\mathbb{L} : \mathbb{L}^H\right]$.
Also $[\mathbb{L} : \mathbb{E}] = |H| = \left[\mathbb{L} : \mathbb{L}^H\right] \Rightarrow \mathbb{E} = \mathbb{L}^H$. Also sind die Zuordnungen invers zueinander.

(2) Die Implikationen

a) $H_1 \subseteq H_2 \Rightarrow \mathbb{L}^{H^1} \supseteq \mathbb{L}^{H_2}$
b) $\mathbb{E}_1 \subseteq \mathbb{E}_2 \Rightarrow \mathrm{Gal}(\mathbb{L}/\mathbb{E}_1) \supseteq \mathrm{Gal}(\mathbb{L}/\mathbb{E}_2)$

sind klar nach Definition.
Sei nun $\mathbb{L}^{H^1} \supseteq \mathbb{L}^{H_2}$, so folgt mit b) $H_1 \underset{(1)}{=} \mathrm{Gal}(\mathbb{L}/\mathbb{L}^{H_1}) \subseteq \mathrm{Gal}(\mathbb{L}/\mathbb{L}^{H_2}) \underset{(1)}{=} H_2$
Analog: $\mathrm{Gal}(\mathbb{L}/\mathbb{E}_1) \supseteq \mathrm{Gal}(\mathbb{L}/\mathbb{E}_2) \Rightarrow \mathbb{E}_1 \underset{(1)}{=} L^{\mathrm{Gal}(\mathbb{L}/\mathbb{E}_1)} \subseteq L^{\mathrm{Gal}(\mathbb{L}/\mathbb{E}_2)} = \mathbb{E}_2$ □

Korollar 7.9. *Jede endliche Galois-Erweiterung hat nur endlich viele Zwischenkörper.*

Sei $\mathbb{K} \subseteq \mathbb{L}$ endliche Galois-Erweiterung, $\mathbb{K} \subseteq \mathbb{E} \subseteq \mathbb{L}, \mathbb{K} \subseteq \mathbb{E}$ normal. Dann ist $\mathbb{K} \subseteq \mathbb{E}$ Galois-Erweiterung.
Sei $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$. Dies definiert einen $\mathbb{K}$-Morphismus $\mathbb{E} \to \mathbb{L} \hookrightarrow \overline{\mathbb{L}}, x \to \sigma(x)$, also $\sigma(\mathbb{E}) = \mathbb{E}$ gemäss Proposition 6.68, da $\mathbb{K} \subseteq \mathbb{E}$ normal. Wir erhalten Gruppenmorphismus
$\varphi : \mathrm{Gal}(\mathbb{L}/\mathbb{K}) \to \mathrm{Gal}(\mathbb{E}/\mathbb{K}), \sigma \to \sigma|_{\mathbb{E}}$, dessen Kern gleich $H := \mathrm{Gal}(\mathbb{L}/\mathbb{E})$ ist. Insbesondere ist H Normalteiler von G.

Behauptung. φ ist surjektiv.

Beweis. Sei $\sigma_1 \in G$. Erweitere σ_1 zu einem Morphismus.
$\sigma : \mathbb{L} \to \overline{\mathbb{L}}$. Da $\mathbb{K} \subseteq \mathbb{E}$ normal ist, gilt $\sigma(\mathbb{E}) = \mathbb{E}$, also $\varphi(\sigma) = \sigma_1$. □

Satz 7.10. *Sei* $\mathbb{K} \subseteq \mathbb{L}$ *endliche Galois-Erweiterung,* $\mathbb{K} \subseteq \mathbb{E} \subseteq \mathbb{L}$ *Zwischenkörper,*
$G := \mathrm{Gal}(\mathbb{L}/\mathbb{K})$, $H := \mathrm{Gal}(\mathbb{L}/\mathbb{E})$. *Dann gilt:*
H *ist Normalteiler in* $G \Leftrightarrow \mathbb{K} \subseteq \mathbb{E}$ *normal*
Dann gilt: $\mathrm{Gal}(\mathbb{E}/\mathbb{K}) \simeq G/H$

Beweis. " $\Leftarrow$ " wurde gerade vorher gezeigt. Der surjektive Morphismus φ :G$\to$ Gal($\mathbb{E}/\mathbb{K}$) mit ker φ =H zeigt $G/H \simeq \mathrm{Gal}(\mathbb{E}/\mathbb{K})$.
" $\Rightarrow$ " Sei $H \trianglelefteq G$. Müssen zeigen: $\forall \sigma \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{E}, \overline{\mathbb{L}}) \sigma(\mathbb{E}) = \mathbb{E}$.
Setze σ fort zu $\sigma : \mathbb{L} \to \overline{\mathbb{L}}$. Da $\mathbb{K} \subseteq \mathbb{L}$ normal $\to \sigma(\mathbb{L}) = \mathbb{L}$, also $\sigma \in G$.
Sei $a \in \mathbb{E}, b := \sigma(a)$. Wollen $b \in \mathbb{E}$ zeigen. Gemäss Hauptsatz 7.7 gilt $\mathbb{E} = \mathbb{L}^H$.
$H\sigma = \sigma H$, da $H \trianglelefteq G$. Zu $\tau \in H$ existiert $\tau' \in H$ mit $\tau\sigma = \sigma\tau'$.
Nun gilt: $\tau'(a) = a$, da $a \in \mathbb{E} = \mathbb{L}^H$. Also $\tau(b) = \tau(\sigma(a)) = \sigma(\tau'(a)) = \sigma(a) = b$. Also folgt $\mathbb{L} \in \mathbb{L}^H = \mathbb{E}$. □

Illustration des Hauptsatzes bei endlichen Körpern

Sei q Primpotenz, $\mathbb{F}_q \subseteq \mathbb{F}_{q^n}$ endliche Körpererweiterung. Sei $\Phi : \mathbb{F}_q \to \mathbb{F}_{q^n}, a \to a^n$ der (relative) Frobeniusmorphismus.
Darum gilt (vgl. § 6.5.) $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) = \langle\Phi\rangle \simeq C_n$ (zyklische Gruppe)
Wissen: Für jeden Teiler d von n gibt es genau eine Untergruppe mit d Elementen, wobei $md = n$.
Für $a \in \mathbb{F}_{q^n}$ gilt: $a \in \mathbb{F}_{q^m} \Leftrightarrow a^{q^m} = a \Leftrightarrow \Phi^m(a) = a$
Also gibt es für alle Teiler m von n genau einen Unterkörper mit a^m Elementen. Das wussten wir schon!

$$\begin{array}{c} \{\mathrm{id}\} \\ | \, \mathrm{d} \\ \langle\Phi^m\rangle \\ | \, m \\ \langle\Phi\rangle \end{array} \quad \Leftrightarrow \quad \begin{array}{c} \mathbb{F}_{q^n} \\ | \\ \mathbb{F}_{q^m} = \mathrm{Fix}(\Phi^m) \\ | \\ \mathbb{F} \end{array}$$

7.2 Die Galoisgruppe eines Polynoms

Wir nennen $f \in \mathbb{K}[X] \backslash \mathbb{K}$ separabel, wenn die Nullstellen von f in $\overline{\mathbb{K}}$ paarweise verschieden sind. Wissen (§ 6.7.): f separabel $\Leftrightarrow \mathrm{ggT}(f, f') = 1$.
Sei $\mathbb{L}$ ein Zerfällungskörper von f. Dann ist $\mathbb{K} \subseteq \mathbb{L}$ eine endliche Galois-Erweiterung. Man nennt Gal($\mathbb{L}/\mathbb{K}$) die Galoisgruppe des Polynoms f (über der Gleichung f=0").

Satz 7.11. *Sei $f \in \mathbb{K}[X]$ separabel, $n = \deg f \geq 1, \mathbb{L}$ der Zerfällungskörper von f.*
(1) Sind $\alpha_1, \ldots, \alpha_n$ die Nullstellen von f, so definiert

$$\varphi : \mathrm{Gal}(\mathbb{L}/\mathbb{K}) \to S_{\{\alpha_1,\ldots,\alpha_n\}} \simeq S_n$$
$$\sigma \to \sigma|_{\{\alpha_1,\ldots,\alpha_n\}}$$

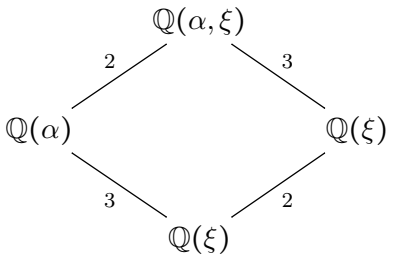
einen injektiven Gruppenmorphismus. Insofern können die Elemente von Gal($\mathbb{L}/\mathbb{K}$) *als Permutation der Nullstellen von f aufgefasst werden. Insbesondere ist*
$[\mathbb{L} : \mathbb{K}] = |\mathrm{Gal}(\mathbb{L}/\mathbb{K})|$ *Teiler von n!*
(2) f ist genau dann irreduzibel, wenn Gal($\mathbb{L}/\mathbb{K}$) *transitiv auf $\{\alpha_1, \ldots, \alpha_n\}$ operiert.*

Beweis. (1) Klar. Denn die Einschränkung auf die Nullstellen ist so möglich.
(2)" $\Rightarrow$ ": Da f irreduzibel über $\mathbb{Q}$, existiert für i, j $\sigma : \mathbb{K}(\alpha_i) \xrightarrow{\sim} \mathbb{K}(\alpha_j)$ mit $\sigma(\alpha_i) = \alpha_j$. Erweitern σ auf $\mathbb{L}$.
" $\Leftarrow$ ": Sei umgekehrt $f = gh$. Jedes $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ permutiert die Nullstellen von g und ebenso die von h. Es folgt, dass die Galoisgruppe nicht transitiv auf allen Nullstellen operiert. □

Beispiel 7.12. $f = X^3 - 2 \in \mathbb{Q}[X]$ ist irreduzibel. Sei $\alpha := \sqrt[3]{2}$, $\xi := e^{\frac{2\pi i}{3}}$.
Dann sind $\alpha, \xi\alpha, \xi^2\alpha$ die Nullstellen von f in $\mathbb{C}$.

$$f = X^3 - 2 = \prod_{j=0}^{2}(X - \xi^j\alpha)$$

Zerfällungskörper $\mathbb{L} = \mathbb{Q}(\alpha, \alpha\xi, \alpha\xi^2) = \mathbb{Q}(\alpha, \xi)$



$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, da $f \in \mathbb{Q}[x]$ irreduzibel.

$$\frac{X^3 - 2}{X - \alpha} = (X - \xi\alpha)(X - \xi^2\alpha) = X^2 - (\xi + \xi^2)\alpha + \xi^3\alpha = X^2 + \alpha X + \alpha =: g$$

g irreduzibel über $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$, da $\xi\alpha \notin \mathbb{R}$.

$$[\mathbb{L} : \mathbb{Q}] = [\mathbb{Q}(\alpha)(\xi) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \cdot 3 = 6$$

Also hat $G := \mathrm{Gal}(\mathbb{L}/\mathbb{Q})$ 6 Elemente. In G kommen alle $6 = 3!$ möglichen Permutationen der Nullstellen vor.
Konkrete Beschreibung:
Komplexe Konjugation liefert $\tau \in G : \tau(\alpha) = \alpha, \tau(\xi) = \overline{\xi} = \xi^2$
τ wirkt als Transposition. Es vertauscht die beiden hinteren Elemente von $\{\alpha, \xi\alpha, \xi^2\alpha\}$.
Es gibt ein $\sigma \in G$, das als 3-er Zyklus wirkt. Direkte Konstruktion: Es gilt $[\mathbb{Q}(\xi) : \mathbb{Q}] = 2$, da $\frac{X^3-1}{X-1} = X^2 + X + 1$ irreduzibel über $\mathbb{Q}$. $\Rightarrow [\mathbb{Q}(\alpha, \xi) : \mathbb{Q}(\xi)] = 3$, dh. f irreduzibel über $\mathbb{Q}(\xi)$ und wir haben $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{L})$ mit $\sigma(\alpha) = \xi\alpha$.

$$\begin{aligned} \sigma : \mathbb{Q}(\alpha, \xi) &\longrightarrow \mathbb{Q}(\alpha, \xi) \\ \alpha &\longmapsto \xi\alpha \\ \xi &\longmapsto \xi \end{aligned}$$

Dabei können wir übrigens $\mathbb{Q}(\alpha, \sigma)$ als $\mathbb{Q}$-Vektorraum mit Basis $\{1, \xi, \xi^2, \alpha, \xi\alpha, \xi^2\alpha\}$.
f ist das Minimalpolynom von α über $\mathbb{Q}(\xi)$ (also zur Erweiterung zu $\mathbb{Q}(\xi)(\alpha)$). Und wir wissen nun, dass ein $\mathbb{Q}(\xi)$-Isomorphismus existiert:

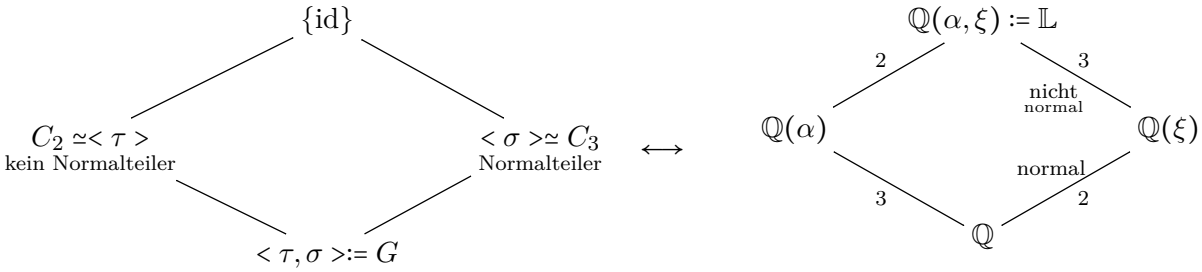
$$\begin{aligned} \sigma : \mathbb{Q}(\alpha)(\xi) &\xrightarrow{\sim} \mathbb{Q}(\xi)(\xi\alpha) \\ \alpha &\longmapsto \xi\alpha \end{aligned}$$

wobei $\mathbb{Q}(\alpha)(\xi) = \mathbb{Q}(\alpha, \xi) = \mathbb{Q}(\xi)(\xi\alpha)$ gilt.
Dann:

$$\begin{aligned} \sigma(\xi\alpha) &= \sigma(\xi)\sigma(\alpha) = \xi \cdot \xi\alpha = \xi^2\alpha \\ \sigma(\xi^2\alpha) &= \xi^2\sigma(\alpha) = \xi^2 \cdot \xi\alpha = \alpha \end{aligned}$$

Außerdem ist $\mathbb{Q}(\alpha) = \mathbb{L}^{<\tau>}$ der Fixkörper von $<\tau> = \{\mathrm{id}, \tau\}$. $\mathrm{Gal}(\mathbb{L}/\mathbb{Q}(\alpha)) = <\tau>$, $\mathbb{Q}(\xi) = \mathbb{L}^{<\sigma>}$

Wir erhalten eine Untergruppenstruktur der Galoisgruppe G in Korrespondenz zu den entsprechenden Unterkörpern von $\mathbb{L}$:



Weiterhin:
$< \sigma >$ ist die Untergruppe von G der Ordnung 3.
$\Rightarrow \mathbb{K} := \mathbb{Q}(\xi)$ ist der einzige Unterkörper $\mathbb{K}$ von $\mathbb{L}$ mit $[\mathbb{L} : \mathbb{K}] = 3$.
Alle Untergruppen von G der Ordnung 2:
$< \tau >, < \sigma\tau >, < \sigma^2\tau >$
Alle Unterkörper $\mathbb{E}$ von $\mathbb{L}$ mit $[\mathbb{L} : \mathbb{E}] = 2$:
$\mathbb{Q}(\alpha), \mathbb{Q}(\xi\alpha), \mathbb{Q}(\xi^2\alpha)$.

7.2.1 Kubische Polynome

Sei $\mathbb{K}$ ein Körper und $f \in \mathbb{K}[X]$ irreduzibel, normiert, mit $\deg f = 3$ und $\operatorname{char} \mathbb{K} \neq 3 \Rightarrow f$ separabel, da $f' \neq 0$
Seien $\alpha_1, \alpha_2, \alpha_3 \in \overline{\mathbb{K}}$ die Nullstellen von f. Da die Galoisgruppe G transitiv auf den Nullstellen operiert, gibt es nur zwei mögliche Galoisgruppen G: A_3 oder S_3.
Wir betrachten die Diskriminate (vgl. § 5.3.):

$$\operatorname{disc}(f) = \prod_{i<j} (\alpha_i - \alpha_j)^2$$

$$\operatorname{disc}(f) = -4p^3 - 27q^2, \text{falls } f = T^3 + pT + q$$

Gilt $\operatorname{disc}(f) = \delta^2$, wobei $\delta := \prod_{i<j}(\alpha_i - \alpha_j)$, beachte:

- δ ist A_3 invariant
- und Vertauschen zweier Nullstellen ändert das Vorzeichen von δ (δ ist antisymmetrisch)

Nach dem Hauptsatz gilt: $\mathbb{K} = \mathbb{L}^G$
1.Fall: $(G = A_3)$ $\delta \in \mathbb{L}^{A_3} = \mathbb{L}^G = \mathbb{K}$
2.Fall: $(G = S_3)$ $\delta \notin \mathbb{L}^{S_3} = \mathbb{L}^G = \mathbb{K}$
Ergebnis:
Sei $\operatorname{char} \mathbb{K} \notin \{2, 3\}$ und $f \in \mathbb{K}[X]$ irreduzibel, normiert mit $\deg f = 3$ und Galoisgruppe G, dann:

$$G \simeq S_3 \Leftrightarrow \sqrt{\operatorname{disc}(f)} \notin \mathbb{K}$$

Beispiel 7.13. $\mathbb{K} = \mathbb{Q}, f = X^3 - 2, \operatorname{disc}(f) = -27 \cdot 2^2 < 0$
$\sqrt{\operatorname{disc}(f)} \notin \mathbb{Q} \Rightarrow$ Galoisgruppe $G \simeq S_3$

7.2.2 Allgemeine Polynome

Definition 7.14. Seien $a_1, a_2, ...a_n$ Unbestimmte über dem Körper $\mathbb{K}$. Man nennt

$$f = X^n + a_1X^{n-1} + ... + a_n \in \mathbb{K}(a_1, ..., a_n)[X]$$

das *allgemeine Polynom* vom Grad n.

Satz 7.15. *Sei $\mathbb{K}(a_1, \dots, a_n) \subseteq \mathbb{L}$ Körpererweiterung mit $\mathbb{L}$ Zerfällungskörper des allgemeinen Polynoms $f = (x-\alpha_1)\cdots(x-\alpha_n)$, $\alpha_1, ..., \alpha_n \in \mathbb{L}$. Es gilt: $\alpha_1, \dots, \alpha_n$ sind algebraisch unabhängig über $\mathbb{K}$. Insbesondere ist $\mathbb{L} = \mathbb{K}(a_1, \dots, a_n)(\alpha_1, \dots, \alpha_n) = \mathbb{K}(\alpha_1, \dots, \alpha_n)$ ein rationaler Funktionenkörper über $\mathbb{K}$. Die Galoisgruppe von f über $\mathbb{K}(a_1, \dots, a_n)$ ist isomorph zu S_n.*

Beweis. Seien $X, T_1, \dots, T_n$ Unbestimmte über $\mathbb{K}$, betrachten

$$F = (X - T_1)\cdots(X - T_n) = X^n - \sigma_1X^{n-1} + \cdots + (-1)^n\sigma_n$$

wobei σ_i das i-te elementarsymmetrische Polynom in $T_1, \dots, T_n$ ist (vgl. § 5.3.).
$\mathbb{K}(T_1, \dots, T_n)$ ist Zerfällungskörper von $F \in \mathbb{K}(\sigma_1, \dots, \sigma_n)[X]$. Wissen (§ 5.3.):$\sigma_1, \dots, \sigma_n$ sind algebraisch unabhängig über $\mathbb{K}$.
Erhalten Isomorphismus $\mathbb{K}(a_1, \dots, a_n) \xrightarrow{\sim} \mathbb{K}(T_1, \dots, T_n), a_i \to (-1)^i\sigma_i$
Satz über Eindeutigkeit der Zerfällungskörper (§ 6.4.) haben einen Isomorphismus
$\mathbb{K}(\alpha_1, \dots, \alpha_n) \xrightarrow{\sim} \mathbb{K}(T_1, \dots, T_n), \alpha_i \to T_i$
$\Rightarrow \alpha_1, \dots, \alpha_n$ algebraisch unabhängig über $\mathbb{K}$. □

Verwenden Galoistheorie, um Variante des Hauptsatzen über symmetrische Polynome zu zeigen:

Proposition 7.16. *Jede symmetische rationale Funktion in den Unbestimmten $T_1, \dots, T_n$ lässt sich als rationale Funktion in $\sigma_1, \dots, \sigma_n$ schreiben.*

Beweis. $\mathbb{K}(\sigma_1, \dots, \sigma_n) \subseteq \mathbb{K}(T_1, \dots, T_n)^{S_n}$ klar.

- $\left[\mathbb{K}(T_1, \dots, T_n) : \mathbb{K}(T_1, \dots, T_n)^{S_n}\right] = |S_n| = n!$ Artins 7.5
- Genügt zu zeigen:
  $[\mathbb{K}(T_1, \dots, T_n) : \mathbb{K}(\sigma_1, \dots, \sigma_n)] \leq n! \qquad (*)$
  $\mathbb{K}(T_1, \dots, T_n)$ ist Zerfällungskörper von $(X - T_1)\cdots(X - T_n) =$
  $X^n - \sigma_1X^{n-1} + \cdots + (-1)^n\sigma_n$ über $\mathbb{K}(\sigma_1, \dots, \sigma_n)$
  $(*)$ folgt aus früherem Satz.

□

Übung: Hauptsatz für symmertrische Polynome ⇒ Proposition (Hauptsatz für symmetrische rationale Funktionen)

7.3 Kreisteilungskörper

Sei $\mathbb{K}$ Körper, $n \in \mathbb{N}_{>0}$. Die Nullstellen von $X^n - 1$ in $\overline{\mathbb{K}}$ heißen *n-te Einheitswurzeln* (in $\overline{\mathbb{K}}$). Diese bilden eine Untergruppe U_n von $\overline{\mathbb{K}}^\times$.

Beweis. $f = X^n - 1$ separabel $\Leftrightarrow \mathrm{ggT}(f, f') = 1 \Leftrightarrow f \neq 0 \Leftrightarrow \mathrm{char}\,\mathbb{K} \nmid n$
$f' = nX^{n-1}$. Dann gilt $|U_n| = n$.
Im allgemeinen: Sei $p = \mathrm{char}\,\mathbb{K}, n = p^r m, p \nmid m$. Dann $(X^n - 1) = (X^m - 1)^{p^r}$.
Also $U_n = U_m$. Deshalb im folgenden oBdA $\mathrm{char}\,\mathbb{K} \nmid n$.

□

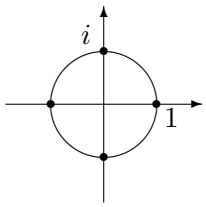
Wichtig: Als endliche Untergruppe in $\overline{\mathbb{K}}^\times$ ist U_n zyklisch. $U_n \simeq C_n$. Eine *primitive n-te Einheitswurzel* $\xi \in U_n$ ist definiert als ein Erzeuger der Gruppe U_n, d.h. $\mathrm{ord}_{U_n}(\xi) = n$.

Satz 7.17. *Sei* $\mathrm{char}\,\mathbb{K} \nmid n$.

- *Die Gruppe U_n der n−ten Einheitszwurzel ist zyklisch der Ordnung n.*
- *Sei $\xi \in U_n$ eine primitive n−te Einheitswurzel und $r \in \mathbb{Z}$. Dann*
  ξ^r primitve n−te Einheitswurzel $\Leftrightarrow \mathrm{ggT}(r, n) = 1$
  U_n hat genau $\varphi(n)$ viele primitive n−te Einheitswurzeln.

Beispiel 7.18. $(\mathbb{K} = \mathbb{Q})$ $\xi_n := e^{\frac{2\pi i}{n}} \in \mathbb{C}$ primitive n−te Einheitswurzel.
$U_n = \{\xi_n^j | 0 \leq j \leq n\}$ Ecken eines regelmäßigen n−Ecks

$n = 4$



Sei $\xi_n \in \overline{\mathbb{K}}$ eine primitive n−te Einheitswurzel. Dann ist $\mathbb{K}(\xi_n)$ ein Zerfällungskörper von $X^n - 1$ über $\mathbb{K}$. $\mathbb{K}(\xi_n)$ heißt n−ter *n-ter Kreisteilungkörper* über $\mathbb{K}$.
Da $X^n - 1$ separabel $\Rightarrow \mathbb{K} \subset \mathbb{K}(\xi_n)$ endliche Galois-Erweiterung.

$$\mathrm{Gal}(\mathbb{K}(\xi_n)/\mathbb{K}) \longrightarrow \mathrm{Aut}(U_n)$$

$$\sigma \longrightarrow \sigma|_{U_n}$$

Lemma 7.19. *Die Automorphismengruppe* $\mathrm{Aut}(\mathbb{Z}_n)$ *der zyklischen Gruppe $\mathbb{Z}_n$ ist isomorph zur Einheitengruppe $\mathbb{Z}_n^\times$ des Rings $\mathbb{Z}_n$*

Beweis. Sei $\varphi \in \mathrm{Aut}(\mathbb{Z}_n), a := \varphi(1)$. Dann $\varphi(2) = \varphi(1) + \varphi(1) = a + a = 2a$ etc...
$\varphi(x \mod n) = xa \mod n$ für $x \in \mathbb{Z}$.
$\exists b : ba \equiv 1 \mod n$, da φ surjektiv. Also $a \in \mathbb{Z}_n^\times$.
Die Abbildung $\mathbb{Z}_n^\times \to \mathrm{Aut}(\mathbb{Z}_n), a \to \varphi_a$, wobei $\varphi_a(x \mod n) = xa \mod n$, ist deshalb ein Gruppenisomorphismus. □

Korollar 7.20. $\mathrm{Gal}(\mathbb{K}(\xi_n)/\mathbb{K})$ *ist isomorph zu einer Untergruppe von* $\mathrm{Aut}(U_n) \simeq \mathbb{Z}_n^\times$ *und deshalb abelsch.*

Satz 7.21. *Sei $\xi_n \in \overline{\mathbb{Q}}$ primitive n-te Einheitswurzel. Dann ist der n-te Kreisteilungskörper $\mathbb{Q}(\xi_n)$ eine endliche Galois-Erweiterung vom Grad $\varphi(n)$ mit Galoisgruppe:*

$$\begin{array}{ccc} \mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q}) & \xleftarrow{\sim} & \mathbb{Z}_n^\times \\ (\xi_n \to \xi_n^r) & & r \end{array}$$

Beweis. z.Z.: $[\mathbb{Q}(\xi_n) : \mathbb{Q}] = \varphi(n)$ Beweis siehe weiter unten. □

Satz 7.22. *Sei $p > 2$ prim, $e \geq 1 \Rightarrow \mathbb{Z}_{p^e}$ zyklisch.*

Lemma 7.23 (Lemma 1)**.** *Für $p > 2$, $a \in \mathbb{N}$ gilt: $(1+p)^{p^a} = 1 + p^{a+1} \mod p^{a+2}$ (Bedingung $p > 2$ ist wichtig. Für $p = 2$ und $a = 1$ erhalten wir beispielsweise $9 = 3^2 \neq 5 \mod 8$)*

Beweisidee. Durch Induktion nach a: Ausmultiplizieren gibt $1+(p^a)p+(p^a)p^2+\ldots$ usw. □

Lemma 7.24 (Lemma 2)**.** *Sei $p > 2$ prim und $e \geq 1$. Dann hat das Element $1 + p$ in $\mathbb{Z}_{p^e}^\times$ die Ordnung p^{e-1}.*

Beweis. Induktion nach e:
Gilt für $e = 1$, da $1 + p$ in $\mathbb{Z}_p^\times$ Ordnung $p^0 = 1$ hat.
Sei nun $e \geq 2$ und sei $(1 + p)^m \equiv 1 \mod p^e$ $(*)$
Dann $(1+p)^m = 1 \mod p^{e-1}$. Per Induktionsvoraussetzung folgt: $p^{e-2} | m$, etwa $m = p^{e-2} \cdot n$.
Nach Lemma 1: $(1 + p)^{p^{e-2}} = 1 + p^{e-1} \mod p^e$
Also: $1 \underset{(*)}{\equiv} ((1 + p)^{p^{e-2}})^n \equiv (1 + p^{e-1})^n \mod p^e \underset{(**)}{\equiv} 1 + np^{e-1} \mod p^e$ Dabei folgt $(**)$ aus:
$(1 + p^{e-1})^n = 1 + np^{e-1} + \binom{n}{2} p^{2(e-1)} + \cdots \equiv 1 + np^{e-1} \mod p^e$ $(\Leftarrow 2(e-1) \geq e \Leftarrow e \geq 2)$
Es folgt nun also: $n \equiv 0 \mod p$. Insgesamt $p^{e-1} | m$.
Außerdem gilt: $(1 + p)^{p^{e-1}} \equiv 1 \mod p^e$, da $(1 + p)^{p^{e-1}} = 1 + p)^{p^{e-2}p} \overset{\text{L1}}{\equiv} (1 + p^{e-1})^p \mod p^e \equiv 1 * p \cdot p^{e-1} \mod p^e \equiv 1 \mod p^e$. □

Beweis des Satzes 7.22. Wir haben den kanonischen surjektiven Homomorphismus:

$$\mathbb{Z}_{p^e}^\times \twoheadrightarrow \mathbb{Z}_p^\times$$

und sei $\ker H$. Aus $|\mathbb{Z}_{p^e}| = \varphi(p^e) = p^{e-1}(p-1) \Rightarrow |H| = \frac{\varphi(p^e)}{p-1} = p^{e-1}$
Es gilt $1 + p \in H \overset{\text{Lemma 2}}{\Rightarrow} H$ ist zyklisch der Ordnung p^{e-1}. Wir wissen $\mathbb{Z}_p^\times$ ist zyklisch, etwa $< g >= \mathbb{Z}_p^\times$. Da $\mathrm{ord}(1 + p) = p^{e-1}$ und $\mathrm{ord}(g) = p - 1$ teilerfremd sind $\Rightarrow \mathrm{ord}(g(1 + p)) = (p - 1)p^{e-1} = \varphi(p^e) \Rightarrow g(1 + p)$ erzeugt $\mathbb{Z}_{p^e}^\times$. □

Bemerkung 7.25. Der Beweis ist bis auf das Finden eines Erzeugers von $\mathbb{Z}_p^\times$ effizient konstruktiv. Bsp: $\mathbb{Z}_5^\times =< 2 >$ Also ist $g(1 + p) = 2 \cdot (1 + 5) = 12$ ein Erzeuger von $\mathbb{Z}_{5^e}^\times$ für alle $e \geq 1$.

Bemerkung 7.26. Man kann ähnlich zeigen für $e \geq 3$ gilt: $\mathbb{Z}_{2^e}^\times \simeq \mathbb{Z}_2 \times \mathbb{Z}_{2^{e-2}}$.

Nun studieren wir das Minimalpolynom f von $\xi_n \in \overline{\mathbb{Q}}$, primitive n–te Einheitswurzel.
Verwende: $[\mathbb{Q}(\xi_n) : \mathbb{Q}] = \varphi(n)$
Die Gruppe $\mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q})$ besteht aus den Automorphismen $\xi \mapsto \xi^j, j \in \mathbb{Z}_n^\times$.
Im Detail:

$$\mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q}) \longrightarrow \mathrm{Aut}(U_n) \xrightarrow{\sim} \mathrm{Aut}(\mathbb{Z}_n) \xrightarrow{\sim} \mathbb{Z}_n^\times$$

$$\begin{array}{ccc} (\xi^x \mapsto \xi^{jx}) & & (x \mapsto jx) \longmapsto j \end{array}$$

Satz 7.27. *Für $n \geq 1$ gilt:*

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

Die Polynome Φ_n haben ganzzahlige Koeffizienten und sind normiert.

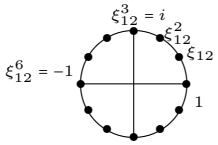
Beweis. Für $d \mid n$ sei $I_d := \{j \in \mathbb{Z}_n | \operatorname{ggT}(j,n) = \frac{n}{d}$.
Dann ist $\{I_d \mid d \mid n\}$ Partition von $\mathbb{Z}_n$ $\{\xi_n^j \mid j \in I_d\}$ Menge der primitiven Einheitswurzeln.

$$X^n - 1 = \prod_{j \in \mathbb{Z}_n} (X - \xi_n^j) = \prod_{d \mid n} \prod_{j \in I_d} (X - \xi_n^j) = \prod_{d \mid n} \Phi_d$$

Die Behauptung $\Phi_n \in \mathbb{Z}[X]$ folgt aus $X^n - 1 = \Phi_n \cdot \prod_{\substack{d \mid n \\ d \neq n}} \Phi_d$ durch Induktion. □

Beispiel 7.28. Wir berechnen Φ_n mit Hilfe des Satzes Φ_n
(1) p prim $X^p - 1 = \Phi_1 \cdot \Phi_p \Rightarrow \Phi_p = \frac{X^p - 1}{X - 1} = X^{p-1} + \ldots X + 1$
(2) $X^4 - 1 = \Phi_1 \cdot \Phi_2 \cdot \Phi_4 = (X-1)(X+1)\Phi_4 = (X^2-1)\Phi_4 \Leftrightarrow \Phi_4 = X^2 + 1$
(3) $X^6 - 1 = \Phi_1 \cdot \Phi_2 \cdot \Phi_3 \cdot \Phi_6 = (X-1)(X+1)(X^2+X+1)\Phi_6 = (X^2-1)(X^2+X+1)\Phi_6$
$\frac{(X^2)^3 - 1}{X^2 - 1} = X^2 + X^2 + 1 \Leftrightarrow \Phi_6 = X^2 - X - 1$

Beispiel 7.29. Unterkörper von $\mathbb{Q}(\xi_{12})$ Galoisgruppe $G \simeq \mathbb{Z}_{12}^\times \underset{\text{chin. RS}}{\simeq} \mathbb{Z}_4^\times \times \mathbb{Z}_3^\times \simeq C_2 \times C_2$ Kleinsche Vierergruppe. $C_2 \times C_2$ hat genau 3 echte Untergruppen. Also nach dem Hauptsatz hat $\mathbb{Q}(\xi_{12})$ genau 3 echte Unterkörper, diese haben den Grad 2 über $\mathbb{Q}$.



Es gilt $\mathbb{Q}(i) \subseteq \mathbb{Q}(\xi_n)$, da $i = \xi_{12}^3$.
Außerdem: $\mathbb{Q}(\sqrt{3}), \mathbb{Q}(-\sqrt{3}) \subseteq \mathbb{Q}(\xi_{12})$
$\xi^4 = -\frac{1}{2} + \frac{1}{2} i\sqrt{3} \Rightarrow i\sqrt{3} \in \mathbb{Q}(\xi_{12}) \Rightarrow \sqrt{3} \in \mathbb{Q}(\xi_{12})$
(Systematische Bestimmung dieser Zwischenkörper ist auch als Fixkörper der Untergruppe möglich.)

Lemma 7.30. *Sei $h \in \mathbb{Z}[X]$ normiert und $h = f \cdot g$ mit normierten $f, g \in \mathbb{Q}[X]$. Dann $f, g \in \mathbb{Z}[X]$.*

Beweis. Sei

$$f = \sum_{i=0}^{d} \frac{a_i}{b} X^i \text{ und } a_i, b \in \mathbb{Z}, b \neq 0,$$

so dass $\operatorname{ggT}(a_0, \ldots, a_d)$ und b teilerfremd sind. Da $1 = a_d = \frac{a_d}{b} \Rightarrow a_d = b$.

$$\text{Also } \operatorname{ggT}(a_0, \ldots, a_d) = 1 \Rightarrow bf = \tilde{f} := \sum_{i=0}^{d} a_i X^i, \tilde{f} \text{ primitiv}$$

Analog schreiben $cg = \tilde{g}, c \in \mathbb{Z} \backslash \{0\}, \tilde{g}$ primitiv.
Also $(bc)h = bcfg = \tilde{f}\tilde{g}$. Gauss-Lemma $\Rightarrow \tilde{f}\tilde{g}$ primitiv. Da $h \in \mathbb{Z}[X] \Rightarrow bc|1$, also $b, c \pm 1$, also $f, g \in \mathbb{Z}[X]$. □

Sei $f \in \mathbb{Q}[X]$ das Minimalpolynom in ξ_n über $\mathbb{Q}$. Wollen zeigen, dass $\deg f = \varphi(n)$.

Behauptung. $\xi \in U_n, f(\xi) = 0, p \nmid n$ prim $\Rightarrow f(\xi^p) = 0$

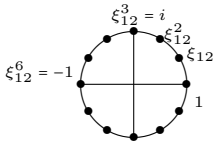
Beweis. Sei $f(\xi) = 0$. Da f irreduzibel $\Rightarrow f$ ist Minimalpolynom von $\xi \Rightarrow X^n - 1 = fh$ mit $h \in \mathbb{Q}[X]$. Da f normiert $\Rightarrow h$ normiert. Lemma 7.30 $\Rightarrow f, h \in \mathbb{Z}[X]$.
Angenommen p prim mit $f(\xi^p) \neq 0$. Möchten zeigen, dass dann $p|n$.
Aus $f(\xi^p) \neq 0 \Rightarrow h(\xi^p) = 0$, also ist ξ Nullstelle in $h(X^p)$. Da f Minimalpolynom von ξ ist $\Rightarrow f|h(X^p)$, etwa $h(X^p) = fg$ mit $g \in \mathbb{Q}[X]$. Offensichtlich ist $g \in \mathbb{Z}[X]$. Reduktion modulo p:
Ringmorphismus $\mathbb{Z}[X] \to \mathbb{F}_p, f \to \overline{f}$.
Dann $h(X^p) = \overline{fg}$.Sei

$$h = \sum_i h_i X^i \Rightarrow \overline{h(X^p)} = \sum_i \underbrace{\overline{h_i}}_{\in \mathbb{F}_p} X^{pi} = \sum_i \overline{h_i^p} X^{pi} = (\sum_i \overline{h_i} X^i)^p = \overline{h^p}$$

Also $\overline{h^p} = \overline{h(X^p)} = \overline{fg}$ in $\mathbb{F}_p[X]$. Sei $q \in \mathbb{F}_p[X]$ irreduzibler Teiler von $\overline{f}$. Dann $\overline{q}|\overline{h}$. Andererseits: $X^n - 1 = \overline{fh}$ in $\mathbb{F}_p[X] \Rightarrow \overline{q^2}|X^n - 1$. Also $X^n - 1$ nicht separabel über $\mathbb{F}_p$
$\Rightarrow p|n$. □

Beweis. (von Satz 7.21) Sei ξ_n^m eine primitive n-te Einheitswurzel. Dann $\mathrm{ggT}(n, m) = 1$
Also $m = p_1^{e_1} \cdots p_r^{e_r}$ mit $p_i \nmid n$
Durch mehrfaches Anwenden der vorherigen Behauptung
$\Rightarrow f(\xi_n) = 0 \Rightarrow f(\xi_n^{p_1}) = 0 \Rightarrow \ldots \Rightarrow f(\xi_n)^{p_1^{e_1}} = 0$
$\Rightarrow f(\xi_n^{p_1^{e_1} p_2}) = 0 \Rightarrow \ldots \Rightarrow f(\xi_n^m) = 0$. Somit verschwindet f auf allen primitiven n-ten Einheitswurzeln. $\Rightarrow \deg f \geqslant \varphi(n)$ Also $\deg f = \varphi(n)$ □

Beispiel 7.31. $\mathbb{K} = \mathbb{Q}(\xi_{12})$
$\mathrm{Gal}(\mathbb{Q}(\xi_{12})/\mathbb{Q}) \simeq \mathbb{Z}_{12}^\times \simeq \mathbb{Z}_4^\times \times \mathbb{Z}_3^\times \simeq C_2 \times C_2$.
$C_2 \times C_2$ hat genau 3 echte Untergruppen, also hat $\mathbb{Q}(\xi_{12})$ genau 3 echte Unterkörper $\mathbb{E}$.
Es gilt:$[\mathbb{E} : \mathbb{Q}] = 2$.



$\mathbb{Z}_{12}^\times = \{1, 5, 7, 11\}, \quad 5^2 = 1, 7^2 = 1, 11^2 = 1, 5 \cdot 7 = 1$
Für $j \in \mathbb{Z}_{12}^\times$ schreibe $\sigma_5(\xi^3) = \xi^{15} = \xi^3$. Also ist $\mathbb{Q}(\xi^3)$ der $\langle \sigma_5 \rangle$ entsprechende Unterkörper.
$\xi^3 = i = \sqrt{-1} \Rightarrow \mathbb{Q}(\xi^3) = \mathbb{Q}(\sqrt{-1})$
$\sigma_7(\xi^4) = \xi^{28} = \xi^4 \quad \mathbb{Q}(\xi^4)$ ist Fixkörper in $\langle \sigma_7 \rangle$
ξ^4 ist primitive 3-te Einheitswurzel. $\xi^4 = -\frac{1}{2} + i\frac{\sqrt{3}}{2} = -\frac{1}{2} + \frac{1}{2}\sqrt{-3} \Rightarrow \mathbb{Q}(\xi^4) = \mathbb{Q}(\sqrt{-3})$
$i(i\sqrt{3}) = -\sqrt{3} \Rightarrow \mathbb{Q}(\sqrt{3})$ ist Unterkörper von $\mathbb{Q}(\xi_{12})$

Untersuchen nun die Kreisteilungskörper über $\mathbb{F}_1$. Seien ξ primitive n-te Einheitswurzlen (existiert falls $\mathrm{ggT}(q, n) = 1$).
$\mathbb{F}_q \subseteq \mathbb{F}_q(\xi)$ endliche Galois-Erweiterung. $\mathrm{Gal}(\mathbb{F}_q(\xi)/\mathbb{F}_q)$ ist zyklisch und wird erzeugt von *relativen Frobeniusmorphismus* $\Phi : \Phi(a) = a^p$ (vgl. §6.5.)
Der injektive Morphimus

$$\begin{aligned} \langle \Phi \rangle = \mathrm{Gal}(\mathbb{F}_q(\xi)/\mathbb{F}_q) &\hookrightarrow \mathrm{Aut}(U_n) \simeq \mathbb{Z}_n^\times \\ \sigma &\to \sigma|_{U_n} \end{aligned}$$

bildet den Erzeuger Φ ab auf $\xi \to \xi^p$.
Unter dem Isomorphismus $\mathrm{Aut}(U_n) \simeq \mathbb{Z}_n^\times$ entspricht die dem Element $q \mod n \in \mathbb{Z}_n^\times$.

Satz 7.32. *Sei $\xi \in \mathbb{F}_q$ primitive n-te Einheitswurzel. Sei d die Ordnung von $q \mod n$ in $\mathbb{Z}_n^\times$. Dann gilt: $[\mathbb{F}_q(\xi) : \mathbb{F}_q] = d$ und $\mathbb{F}_q \subseteq \mathbb{F}_q(\xi)$ hat die zyklische Galoisgruppe der Ordnung d. Insbesondere ist $\Phi_n \in \mathbb{F}_q[X]$ genau dann irreduzibel, wenn $q \mod n$ die Gruppe $\mathbb{Z}_n^\times$ erzeugt.*

Beispiel 7.33. (1.)$\Phi_5 = X^4 + X^3 + X^2 + X + 1$ ist irreduzibel in $\mathbb{F}_3[X]$, da $\langle 3 \mod 5 \rangle$
(2.)Φ_5 zerfällt über $\mathbb{F}_4[X]$, da $\mathrm{ord}(4 \mod 5) = \mathbb{Z}_5^\times = \mathrm{ord}(-1 \mod 5) = 2$
(3.)$\Phi_4 = X^2 + 1$ zerfällt in $\mathbb{F}_5[X]$, da $\mathrm{ord}(5 \mod 4) = \mathrm{ord}(1 \mod 4) = 1$.
Tatsächlich $(X^2 + 1) = (X + 2)(X - 2)$ in $\mathbb{F}_5[X]$

7.4 Zyklische Körpererweiterungen

Definition 7.34. Eine endliche Galois-Erweiterung heißt *zyklisch* , falls ihre Galoisgruppe zyklisch ist.
Die Erweiterung heißt *abelsch* , falls ihre Galoisgruppe abelsch ist.

Proposition 7.35 (Proposition 1)**.** *$\mathbb{K}$ enthalte eine primitive n-te Einheitswurzel ξ. Sei $a \in \overline{\mathbb{K}}$ eine Nullstelle von $X^n - c \in \mathbb{K}[X]$ Dann ist $\mathbb{L} = \mathbb{K}(a)$ eine zyklische Galois-Erweiterung von $\mathbb{K}$. Weiter ist $d := [\mathbb{L} : \mathbb{K}]$ ein Teiler von n und es gilt: $a^d \in \mathbb{K}$ und $X^d - a^d \in \mathbb{K}[X]$ ist das Minimalpolynom von a über $\mathbb{K}$.*

Beweis. O.B.d.A.: $a \neq 0$.
Die Elemente $\xi^0 a, \xi^1 a, \ldots, \xi^{n-1} a$ sind paarweise verschiedene Nullstellen von $X^n - c$. Also ist $\mathbb{L} = \mathbb{K}(a)$ ein Zerfällungskörper von $X^n - c$ über $\mathbb{K}$. Weiter ist $\mathbb{K} \subseteq \mathbb{L}$ eine Galois-Erweiterung. Für $\sigma \in G := \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ existiert $\omega_\sigma \in U_n$ $(= \{\xi^0, \xi^1, \ldots, \xi^{n-1}\})$ mit $\sigma(a) = \omega_\sigma a$.
Es gilt $\omega_{\sigma\tau} a = (\sigma\tau)(a) = \sigma(\tau(a)) = \sigma(\omega_\tau a) = \omega_\tau \omega_\sigma a \Rightarrow \omega_{\sigma\tau} = \omega_\sigma \omega_\tau$. Also ist

$$G \longrightarrow U_n, \sigma \longmapsto \omega_\sigma$$

ein injektiver Gruppenhomomorphismus. Da U_n zyklisch, folgt: G zyklisch.
Sei $G = <\sigma>, d = |G|$. Dann ist ω_σ eine primitive d-te Einheitswurzel für die $\sigma(a^d) = \sigma(a)^d = (\omega_\sigma a)^d = \omega_\sigma^d a^d = a^d$. Also $a^d \in \mathbb{L}^G = \mathbb{K}$. Also ist a eine Nullstelle von $X^d - a^d \in \mathbb{K}[X]$. Aus Gradgründen ist dies das Minimalpolynom von a. □

Definition 7.36. Sei G eine Gruppe und $\mathbb{K}$ ein Körper. Ein Homomorphismus $\chi : G \to \mathbb{K}^\times$ heißt ($\mathbb{K}$-wertiger) *Charakter* von G.
Definiert man das Produkt zweier Charaktere $\chi_1, \chi_2 : G \to \mathbb{K}^\times$ durch

$$\chi_1 \chi_2 : G \to \mathbb{K}^\times, g \longmapsto \chi_1(g)\chi_2(g)$$

so prüft man sofort, dass die Menge $\hat{G}$ der Charaktere $G \to \mathbb{K}^\times$ eine Gruppe bildet. Man nennt $\hat{G}$ die zu G *duale Gruppe*.

Übungsaufgabe 7.1. $G \simeq C_n$ zyklisch der Ordnung n, $C_n = <g>$ und $\mathbb{K} = \mathbb{C}^\times$, ξ primitive n-te Einheitswurzel.
z.Z.: Duale Gruppe $\simeq$ Gruppe der Einheitswurzeln (siehe Hausaufgaben.)
Lösungsidee: Für einen Charakter $\chi : C_n \to \mathbb{C}^\times$ gilt $\chi(g) \in \mathbb{C}^\times$ und $1 = \chi(e) = \chi(g^n) = \chi(g)^n$.
Wir erhalten einen Isomorphismus:
$G \to \hat{G}, g^j \longmapsto \chi$ mit $\chi(g) = \xi^j$

Beispiel 7.37 (siehe Hausaufgaben). $G = S_n \Rightarrow 1$ und sgn sind die einzigen $\mathbb{K}$-wertigen Charaktere von S_n.

Satz 7.38 (E.Artin)**.** *Paarweise verschiedene Charaktere eine Gruppe G mit Werten in einem Körper $\mathbb{K}$ sind linear unabhängig im $\mathbb{K}$-Vektorraum der Abbildungen $G \to \mathbb{K}$.*

Indirekter Beweis. Sei $\chi_1, \dots, \chi_n$ ein linear abhängiges System von Charakteren mit minimalem n. Dann $n \geq 2$. Sei (1) $a_1\chi_1 + \cdots + a_n\chi_n = 0$ mit nicht nicht-trivialen Koeffizienten $(a_1, \dots, a_n) \in (\mathbb{K}^\times)^n$.
Es gilt $a_i \neq 0$ für alle i wegen der Minimalität von n.
Für $g, h \in G$ gilt dann auch $a_1\chi_1(g)\chi_1(h)+\dots+a_n\chi_n(g)\chi_n(h) = a_1\chi_1(gh)+\dots+a_n\chi_1(gh) = 0$.
Wähle dabei spezielles $g \in G$ mit $\chi_1(g) \neq \chi_2(g)$ (möglich da $\chi_1 \neq \chi_2$) Und variert man h in G, folgt (2) $a_1\chi_1(g)\chi_1 + \dots + a_n\chi_n(g)\chi_n = 0$.
Als Differenz aus (1) mit $\chi_1(g)$ multipliziert und (2) erhalten wir:
$a_2(\chi_1(g) - \chi_2(g))\chi_2 + \dots + a_n(\chi_1(g) - \chi_n(g))\chi_n = 0$.
Und damit haben wir wegen $a_2(\chi_1(g) - \chi_2(g)) \neq 0$ eine nicht-triviale Kombination der 0 mit Länge $n-1$. Das steht im Widerspruch zur angenommenen Minimalität von n, was den Satz beweist. □

Proposition 7.39 (Proposition 2)**.** $\mathbb{K}$ *enthalte eine primitive n-te Einheitswurzel ξ. Ist $\mathbb{K} \subseteq \mathbb{L}$ eine zyklische Galois-Erweiterung vom Grad n, so existiert $a \in \mathbb{L}$ mit $\mathbb{L} = \mathbb{K}(a)$ und das Minimalpolynom von a über $\mathbb{K}$ hat die Form $X^n - c$ mit $c \in \mathbb{K}$.*

Beweis. Sei die Galoisgruppe $G =< \sigma >$. Wähle $X \in \mathbb{L}$. Wir bilden die sogenannte *Lagrange-Resolvente* $\vartheta := X + \xi\sigma(X) + \xi^2\sigma^2(X) + \cdots + \xi^{n-1}\sigma^{n-1}(X)$

Behauptung. $\mathrm{id} + \xi\sigma + \xi^2\sigma^2 + \cdots + \xi^{n-1}\sigma^{n-1} \neq 0$

Um diese Behauptung zu zeigen betrachten wir nun die Homomorphismen $\mathbb{L} \xrightarrow{\sigma^j} \mathbb{L}$ bzw. eingeschränkt $\mathbb{L}^\times \xrightarrow{\sigma^j} \mathbb{L}^\times$:
$\mathrm{id}, \sigma, \dots, \sigma^{n-1} : \mathbb{L}^\times \to \mathbb{L}^\times$ sind paarweise verschiedene $\mathbb{L}$-wertige Charaktere der Gruppe $\mathbb{L}^\times$.
Nach dem 7.38 von Artin sind diese Charaktere linear unabhängig.
Zu den Homomorphismen $\mathbb{L}^\times \to \mathbb{L}^\times$ können wir weiterhin sagen, dass wegen $\sigma^n = \mathrm{id}$ gilt:

$$\sigma(\vartheta) = \sigma(X) + \xi\sigma^2(X) + \dots + \xi^{n-2}\sigma^{n-1}(X) + \xi^{n-1}\underbrace{\sigma^n(X)}_{=X} =$$
$$= \xi^{-1}(\xi\sigma(X) + \xi^2\sigma^2(X) + \cdots + \xi^{n-1}\sigma^{n-1}(X) + X) = \xi^{-1}\vartheta$$

$\Rightarrow \sigma(\vartheta^n) = \sigma(\vartheta)^n = \xi^{-n}\vartheta^n = \vartheta^n$. Also $\vartheta^n \in \mathbb{K}$.
Weiterhin folgt: $\sigma^i(\vartheta) = \xi^i\vartheta$. Und da diese Elemente für $0 \leq i \leq n$ paarweise verschieden sind, folgt dann: $[\mathbb{K}(\vartheta) : \mathbb{K}]_S \geq n$. Also $\mathbb{K}(\vartheta) = \mathbb{L}$. Das Minimalpolynom von ϑ über $\mathbb{K}$ ist $X^n - \vartheta^n \in \mathbb{K}[X]$. □

8 Anwendungen der Galois-Theorie

8.1 Auflösungen von Gleichungen durch Radikale

Im Folgenden nehmen wir an : $\operatorname{char}\mathbb{K} = 0$.
Wir kennen eine Lösungsformel für quadratische Gleichungen der Form $X^2 - pX + q = 0$:

$$X = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}$$

Außerdem ist eine Formel für kubische Gleichungen der Form $X^3 + pX + q = 0$ bekannt:

$$\sqrt[3]{-\frac{q}{2} + \sqrt[2]{\frac{p^3}{27} + \frac{q^2}{4}}} + \sqrt[3]{-\frac{q}{2} - \sqrt[2]{\frac{p^3}{27} + \frac{q^2}{4}}}$$

(Um diese im Allgemeinen zu nutzen wird X durch X+Konstante substituiert, so dass X^2 verschwindet.) Für allgemeine n möchte man die Lösungen von

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 = 0 \text{ aus } a_{n-1}, \ldots, a_0$$

durch (endlich viele) rationale Operationen und das Ziehen von Wurzeln erhalten.
Wann ist das möglich?
Wir formulieren die als eine Eigenschaft des Zerfällungskörpers von f in der Sprache der Körpertheorie.

Definition 8.1. Eine endliche Körpererweiterung $\mathbb{K} \subseteq \mathbb{L}$ heiße *durch Radikale auflösbar*, wenn es einen Erweiterungskörper $\mathbb{L} \subseteq \mathbb{E}$ und eine Körperkette $\mathbb{K} = \mathbb{E}_0 \subseteq \mathbb{E}_1 \subseteq \ldots \subseteq \mathbb{E}_t = \mathbb{E}$ gibt, so dass $\mathbb{E}_i = \mathbb{E}_{i-1}(\alpha_i)$ für eine Nullstelle α_i von $X^{n_i} - a_i \in \mathbb{E}_{i-1}[X]$ für $i = 1, 2, \ldots, t$.

Erinnern an den Begriff *Auflösbarkeit* einer endlichen Gruppe (vgl. § 3.3.). Eine *Normalreihe* von G ist eine Kette

$$G = G_0 \geqslant G_1 \geqslant \cdots \geqslant G_r = \{e\}$$

von Untergruppen, so dass $G_i \trianglerighteq G_{i+1}$. Die Gruppen G_i/G_{i+1} heißen *Faktoren* der Normalreihe.

Definition 8.2. G heißt auflösbar, falls G eine Normalreihe mit abelschen Faktoren besitzt.

Beispiel 8.3.

$$S_4 \underset{S_4/A_4 \simeq C_2}{\geqslant} A_4 \underset{C_3}{\geqslant} K \underset{C_2}{\geqslant} C_2 \underset{C_2}{\geqslant} \{e\} \quad \begin{matrix}\text{Normalreihe} \\ \text{Faktoren}\end{matrix}$$

Lemma 8.4. *G ist genau dann auflösbar, wenn G eine Normalreihe besitzt, deren Faktoren zyklisch von Primzahlordnung sind.*

Beweis. zu zeigen: Eine Normalreihe mit abelschen Faktoren kann zu einer Normalreihe verfeinert werden, deren Faktoren zyklisch von Primzahlgrad sind. Dazu genügt folgende Feststellung: Sei A abelsch mit $|A| = p_1 \cdot p_2 \cdots p_r, p_i$ prim. Dann existiert eine Kette

$$A = A_0 \geqslant A_1 \geqslant \ldots A_r = \{e\}$$

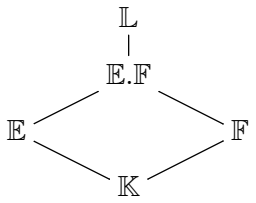
von Untergruppen mit $|A_i/A_{i+1}| = p_{i+1}$
Bekannte Fakten (vgl. Algebra I, Blatt 9):

- Untergruppen auflösbarer Gruppen sind auflösbar.
- Homomorphe Bilder auflösbarer Gruppen sind auflösbar
- $H \trianglelefteq G, H$ auflösbar, G/H auflösbar $\Rightarrow G$ auflösbar

□

Definition 8.5. Eine endliche Körpererweiterung heißt *auflösbar* , wenn es eine Erweiterung $\mathbb{L} \supseteq \mathbb{E}$ gibt, so dass $\mathbb{K} \subseteq \mathbb{E}$ eine endliche Galois-Erweiterung mit auflösbarer Galoisgruppe $\mathrm{Gal}(\mathbb{E}/\mathbb{K})$ ist.

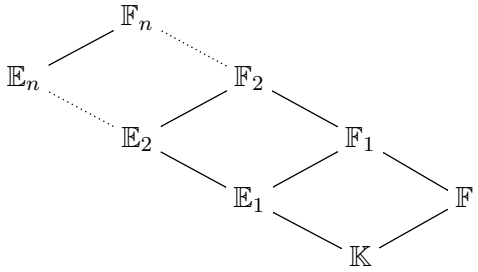
Vorüberlegung: Seien $\mathbb{E}$ und $\mathbb{F}$ Zwischenkörper von $\mathbb{K} \subseteq \mathbb{L}$. Das *Kompositum* $\mathbb{E}.\mathbb{F}$ ist definiert als der kleinste Unterkörper von $\mathbb{L}$, der $\mathbb{E}$ und $\mathbb{F}$ enthält.



Bemerkung 8.6. $\mathbb{E} = \mathbb{K}(a_1, \ldots, a_n) \Rightarrow \mathbb{E}.\mathbb{F} = \mathbb{F}(a_1, \ldots a_n)$

Lemma 8.7. *Seien $\mathbb{E}$ und $\mathbb{F}$ Zwischenkörper von $\mathbb{K} \subseteq \mathbb{L}$, so dass $\mathbb{K} \subseteq \mathbb{E}$ und $\mathbb{K} \subseteq \mathbb{F}$ endlich sind. Dann ist $\mathbb{F} \subseteq \mathbb{E}.\mathbb{F}$ endlich und $[\mathbb{E}.\mathbb{F} : \mathbb{F}]$ teilt $[\mathbb{E} : \mathbb{K}]$. Insbesondere teilt $[\mathbb{E}.\mathbb{F} : \mathbb{K}]$ das Produkt $[\mathbb{E} : \mathbb{K}]\,[\mathbb{F} : \mathbb{K}]$*

Beweis. (1) Sei $\mathbb{E} = \mathbb{K}(a)$ einfach algebraisch, $f \in \mathbb{K}[X]$ das Minimalpolynom von a. Dann gilt $\mathbb{E}.\mathbb{F} = \mathbb{F}(a)$. Ist $g \in \mathbb{F}[X]$ das Minimalpolynom von a über $\mathbb{F}$, so gilt $g|f$. Aber $[\mathbb{E} : \mathbb{K}] = \deg f, [\mathbb{E}.\mathbb{F} : \mathbb{F}] = \deg g$.



(2) Sei $\mathbb{E} = \mathbb{K}(a_1, \ldots, a_n)$. Betrachte $\mathbb{E}_i = \mathbb{K}(a_1, \ldots, a_i), \mathbb{F}_i := \mathbb{E}_i.\mathbb{F} = \mathbb{F}(a_1, \ldots, a_i)$.
Dann ist $\mathbb{E}_i = \mathbb{E}_{i-1}(a_i)$. $[\mathbb{F}_i : \mathbb{F}_{i-1}] \,|\, [\mathbb{E}_i : \mathbb{E}_{i-1}]$ gemäss (1).
Mit Grad-Multiplikation-Satz $\Rightarrow [\mathbb{F}_n : \mathbb{F}] \,|\, [\mathbb{E}_n : \mathbb{K}]$ □

Theorem 8.8 (Galois)**.** *Eine Körpererweiterung ist genau dann durch Radikale auflösbar, wenn sie auflösbar ist.*

Wissen: die alternierende Gruppe A_n ist einfach, falls $n \geqslant 5$ (vgl. § 3.3.)
Also ist A_n nicht auflösbar für $n \geqslant 5$
$\Rightarrow S_n$ nicht auflösbar für $n \geqslant 5$

Korollar 8.9 (Abel, Ruffini)**.** *Die allgemeine Gleichung vom Grad $n \geqslant 5$ ist nicht durch Radikale auflösbar. Hingegen ist S_4 auflösbar: $S_4 \trianglerighteq A_4 \trianglerighteq \mathbb{K} \trianglerighteq C_2 \trianglerighteq \{e\}$*

Korollar 8.10. *Jede Körpererweiterung $\mathbb{K} \subseteq \mathbb{L}$ mit $[\mathbb{L} : \mathbb{K}] \leqslant 4$ ist durch Radikale auflösbar.*

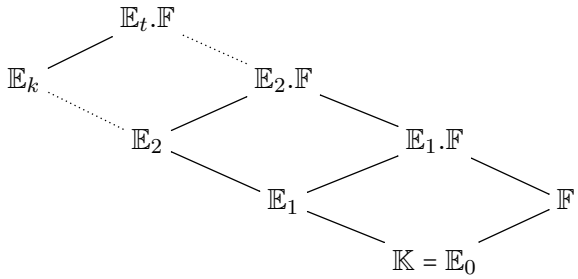
Beweis. Satz vom primitiven Element 6.61 $\Rightarrow \exists a \in \mathbb{L}$ mit $\mathbb{L} = \mathbb{K}(a)$. Sei $f \in \mathbb{K}[X]$ das Minimalpolynom von a. Dann $\deg f = [\mathbb{L} : \mathbb{K}] \leqslant 4$. Sei $\mathbb{L} \subseteq \mathbb{L}'$ ein Zerfällungskörper von f. Dürfen $\mathrm{Gal}(\mathbb{L}'/\mathbb{K})$ als Untergruppe von S_4 auffassen. Also ist $\mathrm{Gal}(\mathbb{L}'/\mathbb{K})$ auflösbar. Nach Theorem 8.8 ist $\mathbb{K} \subseteq \mathbb{L}$ durch Radikale auflösbar. □

Gibt es rationale Polynome $f \in \mathbb{Q}[X]$ mit $\deg f \geqslant 5$, deren Galoisgruppe nicht auflösbar ist?

Lemma 8.11. *Sei p prim, $G \subseteq S_p$ Untergruppe, die transitiv auf $\{1, 2, \ldots, p\}$ operiert. Dann enthält G einen Zykel der Länge p.*

Beweis. Bahnformel $\Rightarrow p \| G|$
Sylow $\Rightarrow G$ enthält Untergruppe H der Ordnung p, etwa $H = \langle g \rangle$
Die Permutation g habe eine Zykelzerlegung vom Format $(n_1, n_2, \ldots, n_t)$ mit
$n_1 + n_2 + \cdots + n_t = p$. $p = \mathrm{ord}(g) | \,\mathrm{kgV}(n_1, \ldots, n_t)$ (Übung)
$\Rightarrow t = 1, n_1 = p$. Also ist g Zykel der Länge p. □

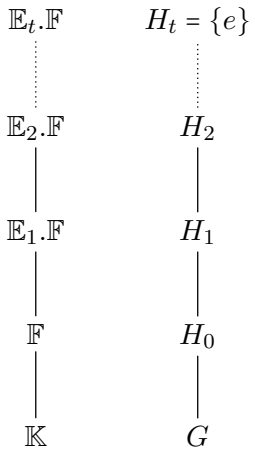
Beweis des Galoistheorem 8.8. Sie $\mathbb{K} \subseteq \mathbb{L}$ durch Radikale auflösbar etwa $\mathbb{L} \subseteq \mathbb{E}$ und $\mathbb{K} = \mathbb{E}_0 \subseteq \mathbb{E}_1 \subseteq \ldots \subseteq \mathbb{E}_k = \mathbb{E}$, wobei $\mathbb{E}_i = \mathbb{E}_{i-1}(\alpha_i)$, α_i Nullstelle von $X^{n_i} - a_i \in \mathbb{E}_{i-1}[X]$.
Sei $N := \mathrm{kgV}(n_1, \ldots, n_k)$ und $\zeta \in \overline{\mathbb{E}}$ N-te primitive Einheitswurzel. Dann enthält der Kreisteilungskörper $\mathbb{K}(\zeta)$ alle n_i-ten primitiven Einheitswurzeln, $i = 1, 2, \ldots, t$.
Wir wissen $\mathbb{E}_i.\mathbb{F} = \mathbb{E}_{i-1}.\mathbb{F}(\alpha_i)$.



Außerdem enthält $\mathbb{F}$ eine primitive n_i-te Einheitswurzel ζ_i. Also enthält $\mathbb{E}_i.\mathbb{F}$ alle Nullstellen $\zeta_i^j \alpha_i, 0 \leq j < n_i$ von $X^{n_i} - a_i$ Mit Proposition 7.35 folgt: $\mathbb{E}_{i-1} \subseteq \mathbb{E}_i.\mathbb{F}$ zyklische Galois-Erweiterung.

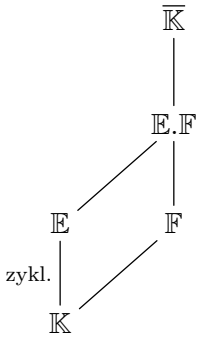
Behauptung. $\mathbb{K} \subseteq \mathbb{E}_i.\mathbb{F}$ endliche Galoiserweiterung. (zu prüfen bleibt die Normalität)

Sei $G := \mathrm{Gal}(\mathbb{E}_t.\mathbb{F}/\mathbb{K})$.
Nun folgt mit dem Hauptsatz der Galoistheorie:



$H_i := \mathrm{Gal}(\mathbb{E}_t.\mathbb{F}/\mathbb{E}_i.\mathbb{F})$
$H_i \trianglelefteq G$, da $\mathbb{K} \subseteq \mathbb{E}_i.\mathbb{F}$ normal ist.
Weiter $H_i/H_{i+1} \simeq \mathrm{Gal}(\mathbb{E}_{i+1}.\mathbb{F}/\mathbb{E}_i.\mathbb{F})$ zyklisch.
$\Rightarrow G \geq H_0 \geq H_1 \geq \cdots \geq H_t = e$ Normalreihe mit zyklischen Faktoren.
Deshalb ist $\mathbb{K} \subseteq \mathbb{L}$ auflösbar (beachte $\mathbb{L} \subseteq \mathbb{E} \subseteq \mathbb{E}_t.\mathbb{F}$).

Für die umgekehrte Richtung sei $\mathbb{K} \subseteq \mathbb{L}$ auflösbar. Etwa $\mathbb{L} \subseteq \mathbb{E}$ und $\mathbb{K} \subseteq \mathbb{E}$ endliche Galois-Erweiterungen mit $G := \mathrm{Gal}(\mathbb{E}/\mathbb{K})$ auflösbar. Sei N das Produkt der verschiedenen Primteiler von $|G|$ und $\zeta \in \overline{\mathbb{E}}$ primitive N-te Einheitswurzel.
Wir setzen wieder $\mathbb{F} := \mathbb{K}(\zeta)$ und betrachten Folgendes:



Ist $\mathbb{E} = \mathbb{K}(a_1, \ldots, a_m)$, dann gilt auch $\mathbb{E}.\mathbb{F} = \mathbb{F}(a_1, \ldots, a_m)$.
Da $\mathbb{K} \subseteq \mathbb{E}$ normal ist, folgt $\mathbb{F} \subseteq \mathbb{E}.F$ ist ebenfalls normal.
Überlegung:
$\sigma \in \mathrm{Aut}_{\mathbb{F}} \overline{\mathbb{K}} \Rightarrow \sigma \in \mathrm{Aut}_{\mathbb{K}} \overline{\mathbb{K}} \Rightarrow \sigma(\mathbb{E}) = \mathbb{E} \Rightarrow \sigma(\mathbb{E}.\mathbb{F}) = \mathbb{E}.\mathbb{F}$

Wir erhalten einen injektiven Gruppenhomomorphismus:
$\mathrm{Gal}(\mathbb{E}.\mathbb{F}/\mathbb{F}) \to \mathrm{Gal}(\mathbb{E}/\mathbb{K})$ $\sigma \longmapsto \sigma|_{\mathbb{E}}$
Da $\mathrm{Gal}(\mathbb{E}/\mathbb{K})$ auflösbar $\Rightarrow \mathrm{Gal}(\mathbb{E}.\mathbb{F}/\mathbb{F})$ auflösbar.
Wir haben wir eine Normalreihe $H = H_0 \geq H_1 \geq \cdots \geq H_t = \{e\}$ mit zyklischen Faktoren von Primzahlordnung p_i. Es gilt $p_i | N$. Also: $|H| | |G|$ und $p_i | |H|$
Nach dem Hauptsatz entspricht diese Normalreihe einer Kette von Unterkörpern:
$\mathbb{F} = \mathbb{L}_0 \subseteq \mathbb{L}_1 \subseteq \ldots \subseteq \mathbb{L}_t = \mathbb{E}.\mathbb{F}$, sodass $\mathbb{L}_{i-1} \subseteq \mathbb{L}_i$ galoisch ist und $\mathrm{Gal}(\mathbb{L}_i/\mathbb{L}_{i-1}) \simeq H_{i-1}/H_i$ zyklisch der Ordnung p_i.
Mit Proposition 7.39: $\exists \alpha_i \in \mathbb{L}_{i-1}(\alpha_i)$ und das Minimalpolynom von α_i hat die Form $X^{p_i} - a_i$ für ein $a_i \in \mathbb{L}_{i-1}$. Deshalb ist die Erweiterung $\mathbb{F} \subseteq \mathbb{E}.\mathbb{F}$ durch Radikale auflösbar. Folglich ist auch $\mathbb{K} \subseteq \mathbb{E}.\mathbb{F}$ durch Radikale auflösbar und somit schließlich auch $\mathbb{K} \subseteq \mathbb{L}$ durch Radikale auflösbar. □

Korollar 8.12. *Sei $p \geq 5$, $f \in \mathbb{Q}[X]$ irreduzibel, $\deg f = p$ und f habe genau $p-2$ reelle Nullstellen. Dann ist die Galoisgruppe von f isomorph zu S_p. Insbesondere ist für $\mathbb{L}$ Zerfällungskörper von f die Erweiteung $\mathbb{Q} \subseteq \mathbb{L}$ nicht durch Radikale auflösbar.*

Beispiel 8.13. $f = X^5 - 4X - 2$ irreduzibel (nach Eisenstein)
f hat genau drei reelle Nullstellen (Kurvendiskussion).
Mit dem Korollar folgt: Die Galoisgruppe von f ist $G = S_5$
Dabei $f' = 5X^4 - 4$ und $\zeta = \sqrt[4]{\frac{4}{5}}$.

Beweis von Korollar. Seien $\alpha_1, \dots, \alpha_{p-2}, \beta, \overline{\beta}$, wobei $\alpha_i \in \mathbb{R}$ und $\beta \in \mathbb{C}\backslash\mathbb{R}$.
Die komplexe Konjugation τ defininiert einen Automorphismus des Zerfällungskörpers $\mathbb{E} := \mathbb{Q}(\alpha_1, \dots, \alpha_{p-2}, \beta)$ mit $\tau(\alpha_i) = \alpha_i$ und $\tau(\beta) = \overline{\beta}$. τ definiert eine Transposition der Nullstellen-Menge. Da f irreduzibel, folgt $G := \mathrm{Gal}(\mathbb{E}/\mathbb{Q})$ operiert transitiv auf der Nullstellen-Menge. Fasse G als Untergruppe von S_p auf und verwende Lemma 8.11 $\Rightarrow G$ enthält einen Zykel der Länge p. Da dieser und eine Transposition die Gruppe S_p erzeugen, folgt $G = S_p$. □

Bemerkung 8.14. Man kann zeigen, dass "fast alle" $f \in \mathbb{Q}[X]$ von Grad n als Galoisgruppe S_n haben. (van der Waerden 1934).

Satz 8.15. *Sei $f \in \mathbb{Z}[X]$ normiert vom Grad $n \geq 1$.*
Sei p prim, sodass $\overline{f} = f \mod p \in \mathbb{F}_p[X]$ quadratfrei. Sei $\overline{f} = g_1 g_2 \dots g_r$ mit irreduziblen Faktoren $g_i \in \mathbb{F}_p[X]$ deren Grad je $n_i = \deg g_i$. Dann enthält die Galoisgruppe von f eine Permutation mit Zykeltyp $(n_1, n_2, \dots, n_r)$(dh. eine Permutation die aus r dijunkten Zykeln c_i mit jeweiliger Länge n_i besteht).

Beispiel 8.16. $f = X^5 - 4X + 2 \in \mathbb{Z}[X]$ mit Galoisgruppe G
$f \mod 2 = X^5 \in \mathbb{F}_2[X]$ nicht quadtratfrei
$f \mod 3 = X^5 + 2X + 2 \in \mathbb{F}_3[X]$ irreduzibel
$f \mod 7 = (X^2 - 4X + 6)(X^3 + 3X^2 + 3X + 5) \in \mathbb{F}_7[X]$ mit irreduziblen Faktoren
Nach dem Satz folgt: G enthält Zykel c der Länge 5 und eine Permutation $\rho\tau$ mit τ 2-er-Zykel und ρ 3-er-Zykel, wobei τ und ρ disjunkt. Es folgt $(\tau\rho)^3 = \tau^3\rho^3 = \tau \in G$
Da $< c, \tau >= S_5$ folgt $G \simeq S_5$.

Beispiel 8.17. $f = X^6 + X + 1 \in \mathbb{Z}[X]$ G Galoisgruppe von f
$f \mod 2 \in \mathbb{F}_2[X]$ irreduzibel
$f \mod 3 = (X + 1)(X^2 + 2X + 2)(X^3 + 2X^2 + 2X + 1) \in \mathbb{F}_3[X]$ mit irreduziblen Faktoren
$\overset{\text{Satz}}{\Rightarrow}$ G enthält 6-er Zyklel c und $\pi\delta$ mit π 2-er-Zykel und δ 3-er-Zykel disjunkt
$\overset{\text{s.o}}{\Rightarrow} \pi, c \in G \Rightarrow G \simeq S_6$.

8.2 Gleichungen vom Grad 3 und 4

Sei im Folgenden $\mathbb{K}$ ein Körper mit $\mathrm{char}\,\mathbb{K} = 0$ und $\zeta \in \mathbb{K}$ primitive 3. Einheitswurzel.

8.2.1 Kubische Gleichung

Eine *kubische Gleichung* hat die Form $X^3 + aX^2 + bX + c = 0$. Mit der Transformation $X \mapsto X - \frac{1}{3}c$ bringt man die Gleichung auf die einfachere Form $f = 0$, wobei $f = X^3 + pX + q \in \mathbb{K}[X]$.
Sei $\mathbb{L} = \mathbb{K}(X_1, X_2, X_3)$ der Zerfällungskörper und X_1, X_2, X_3 die Nullstellen von f. Für die Herleitung nehmen wir an, dass $\mathrm{Gal}(\mathbb{L}/\mathbb{K}) = S_3$ gelte. (Nachträglich werden wir sehen, dass die Formeln allgemein gelten.)
Der Normalreihe $S_3 \overset{2}{\geq} A_3 \overset{3}{\geq} \{e\}$ entspricht die Körperkette $\mathbb{K} = \mathbb{L}^{S_3} \subseteq \mathbb{E} = \mathbb{L}^{A_3} \subseteq \mathbb{L}$.

Wissen bereits aus Abschnitt 7.2.1, dass $\mathbb{E} = \mathbb{L}^{A_3} = \mathbb{K}(\delta)$, wobei δ eine Quadratwurzel der Diskriminante $\Delta = -4p^3 - 27q^2$ von f ist, und $\mathbb{K} \subseteq \mathbb{E} = \mathbb{K}(\delta) \overset{3}{\underset{\text{zykl.}}{\subseteq}} \mathbb{L} = \mathbb{E}(\sqrt[3]{\vartheta})$.

Sei $f = X^3 + pX + q \in \mathbb{K}[X]$. Sei $\mathbb{L} = \mathbb{K}(x_1, x_2, x_3)$ der Zerfällungskörper von f, x_1, x_2, x_3 Nullstellen von f.
Annahme: $\mathrm{Gal}(\mathbb{L}/\mathbb{K}) = S_3$. Die Normalreihe

$$S_3 \overset{2}{\geqslant} A_3 \overset{3}{\geqslant} \{e\}$$

entspricht der Körperkette

$$\mathbb{K} = \mathbb{L}^{S_n} \overset{2}{\subseteq} \mathbb{E} := \mathbb{L}^{A_n} \overset{3}{\subseteq} \mathbb{L}$$

Die Diskriminante von f : $\Delta = (x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2$.
Bekannt:$\Delta = -4p^3 - 27q^2$. Sei $\delta = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$.
Dann ist $\delta^2 = \Delta$. Außerdem wissen wir:
$\mathbb{E} = \mathbb{L}^{A_3}\mathbb{K} = (\delta)$ (δ ist A_3-invariant, aber nicht S_3 invariant $(12)\delta = -\delta$)
Die Theorie zyklischer Körpererweiterungen sagt, dass die Erweiterung $\mathbb{E} \subseteq \mathbb{L}$ mit $\mathrm{Gal}(\mathbb{L}/\mathbb{E}) = \langle\sigma\rangle \simeq C_3$ von der Form $\mathbb{L} = \mathbb{E}(\vartheta)$ ist, wobei ϑ Nullstelle eines Polynoms $x^3 - c \in \mathbb{E}[X]$ ist.
Voraussetzung: $\mathbb{K}$ enthält eine primitive 3-te Einheitswurzel ξ. Der Beweis von Proposition 2 sagt, dass wir ϑ als Lagrange-Resultante finden können.
$\vartheta = x + \xi\sigma(x) + \xi^2\sigma^2(x)$, wobei $x \in \mathbb{L}$. Es gilt: $\sigma(\vartheta) = \xi^{-1}\vartheta \Rightarrow \sigma^i = \xi^{-1}\vartheta$
$\Rightarrow \sigma^i = \xi^{-1}\vartheta$ paarweise verschieden für $i = 0, 1, 2$ falls $\vartheta \neq 0$.
Dann $[\mathbb{E}(\vartheta) : \mathbb{E}] \geqslant 3 \Rightarrow \mathbb{E}(\vartheta) = \mathbb{L}$.
Wähle $x = x_1$ als Nullstelle von f. Die beiden primitiven 3-ten Einheitswurzeln liefern zwei Resultanten. Beachte: $\sigma(x_1) = x_2, \sigma(x_2) = x_3, \sigma(x_3) = x_1$

$$(\star)\ \begin{cases} (\xi, x) := x_1 + \xi x_2 + \xi^2 x_3 \\ (\xi^2, x) := x_1 + \xi^2 x_2 + \xi x_3 \end{cases} \qquad 0 = x_1 + x_2 + x_3$$

Die Theorie sagt dass $(\xi, x) \in \mathbb{E}$. Rechnen das konkret nach:
$\delta = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3) = x_1^2x_2 + x_2^2x_3 + x_3^2x_1 - x_1^2x_3 - x_2^2x_1 - x_3^2x_2$
δ ist A_3-invariant, aber S_3-antisymmetrisch:

$$(\star\star)\ \begin{cases} (\xi, x)^3 &= (x_1 + \xi x_2 + \xi^2 x_3)^3 = \\ &= x_1^2 + x_2^2 + x_3^2 + 3\xi(x_1^2x_2 + x_2^2x_3 + x_1x_3^2) + 3\xi^2(x_1^2x_3 + x_2^2x_1 + x_2x_3^2) + 6x_1x_2x_3 \end{cases}$$

Gemäss Theorie gilt:$(\xi, x)^3 = a - b\delta$ mit $a, b \in \mathbb{K} = \mathbb{L}^{S_3} = \mathbb{K}[x_1, x_2, x_3]^{S_3}$. Berechnung von a und b:

$$(12)(\xi, x)^3 = a - b\delta \Rightarrow (\xi, x)^3 - (12)(\xi, x)^3 = 2b\delta$$

$(\star\star)$ einsetzen liefert:

$$\begin{aligned}(\xi, x)^3 - (12)(\xi, x)^3 = {} & 3\xi(x_1^2x_2 + x_2^2x_3 + x_3^2x_1 - x_1^2x_3 - x_2^2x_1 - x_3^2x_2) + \\ & + 3\xi^2(x_1^2x_3 + x_2^2x_1 + x_3^2x_2 - x_1^2x_2 - x_2^2x_3 - x_3^2x_1)\end{aligned}$$

Da δ schon ein Polynom vom Grad 3 ist, muss also $2b$ konstant sein.
$2b\delta = 2bx_1^2x_2 \Rightarrow 2b = 3\xi - 3\xi^2$ und wegen
$1 + \xi + \xi^2 = 0$ und $(\xi - \xi^2)^2 = \xi^2 + \xi^4 - 2\xi^3 = \xi^2 + \xi^4 - 2 = -3$ folgt $b = \frac{2}{3}\sqrt{-3}$
Durch Erweitern von b in $(\xi, x)^3 = a + b\xi$ folgt nach einer kurzen Rechnung

$$a = \sum_i x_i^3 - \frac{3}{2}\sum_{i \neq j} x_i^2x_j + 6x_1x_2x_3$$

Wir schreiben a als Polynom in

$$\begin{aligned}\sigma_1 &= x_1 + x_2 + x_3 = 0\\ \sigma_2 &= x_1x_2 + x_1x_3 + x_2x_3 = p\\ \sigma_2 &= x_1x_2x_3 = -q\end{aligned}$$

Das geht mit dem Algorithmus aus dem Beweis des Hauptsatzes für symmetrische Polynome. $x_1x_2x_3$ ist der lexiographisch größte Term in a (auch in σ_1^3).

$$\sigma_1^3 = \sum_i x_i^3 + 3\sum_{i\neq j} x_i^2x_j + 6x_1x_2x_3$$

$$\Rightarrow a - \sigma_1^3 = -\frac{9}{2}\sum_{i\neq j} x_i^2x_j$$

Der lexiographisch größte Term ist nun $x_1^2x_2^1x_3^0$ (auch in $\sigma_1^1\sigma_2^1\sigma_3^0$).

$$\sigma_1\sigma_2 = \sum_{i\neq j} +x_i^2x_j + 3x_1x_2x_3$$

$$\Rightarrow (a - \sigma_1^3) + \frac{9}{2}\sigma_1\sigma_2 = \frac{27}{2}x_1x_2x_3$$

Ergebnis: $a = \sigma_1^3 - \frac{9}{2}\sigma_1\sigma_2 + \frac{27}{2}\sigma_3 \overset{\sigma_1=0}{=} -\frac{27}{2}q$

$$\begin{aligned}\Rightarrow(\xi,x)^3 &= a + b\delta = -\frac{27}{2}q + \frac{3}{2}\sqrt{-3}\delta\\ (\xi,x)^3 &= -\frac{27}{2}q + \sqrt{\frac{9(-3)}{4}(-4p^3 - 27q^2)}\\ (\xi,x)^3 &= -\frac{27}{2}q + 27\sqrt{(\frac{p}{3})^3 + (\frac{q}{2})^2}\end{aligned}$$

Die gleiche Überlegung für $(\xi^2,x)^3$ liefert:
$(\xi^2,x)^3 = (a + \tilde{b}\delta)$, wobei $\tilde{b} = \frac{3}{2}((\xi^2) - (\xi^2)^2)$, weil $b = \frac{3}{2}(\xi - \xi^2)$. Also $\tilde{b} = \frac{3}{2}(\xi^2 - \xi) = -b$.
Folglich: $(\xi^2,x)^3 = \frac{27}{2}q - \frac{3}{2}\sqrt{-3}\delta = -\frac{27}{2}q - 27\sqrt{(\frac{p}{3})^3 + (\frac{q}{2})^2}$.
Die 3-ten Wurzeln $(\xi,x),(\xi^2,x)$ können nicht unabhängig gewählt werden.

$$\begin{aligned}(\xi,x)(\xi^2,x) &= (x_1 + \xi x_2 + \xi^2x_3)(x_1 + \xi^2x_2 + \xi x_3)\\ &= x_1^2 + x_2^2 + x_3^2 + \underbrace{(\xi + \xi^2)}_{=-1}\underbrace{(x_1x_2 + x_1x_3 + x_2x_3)}_{=\sigma_2}\end{aligned}$$

Definiere $u_i = \frac{1}{3}(\xi,x), \quad v_i = \frac{1}{3}(\xi^2,x)$.
Dann $uv = -\frac{1}{3}p$
Schließlich können x_1,x_2,x_3 aus u,v durch Lösen eines Gleichungssystems finden (siehe $\star$)

$$\begin{aligned}x_1 + x_2 + x_3 &= 0\\ x_1 + \xi x_2 + \xi^2x_3 &= (\xi,x) = \xi u\\ x_1 + \xi^2x_2 + \xi x_3 &= (\xi^2,x) = \xi v\end{aligned}$$

$$\Rightarrow \begin{bmatrix}x_1\\x_2\\x_3\end{bmatrix} = \begin{bmatrix}1 & 1 & 1\\ 1 & \xi^2 & \xi\\ 1 & \xi & \xi^2\end{bmatrix}\begin{bmatrix}0\\u\\v\end{bmatrix} = \begin{bmatrix}u+v\\ \xi^2u + \xi v\\ \xi u + \xi^2 v\end{bmatrix}$$

Satz 8.18 (Cardano)**.** *Die Lösung der kubischen Gleichung* $x^3 + px + q = 0$ *sind gegeben durch*

$$\begin{aligned} x_1 &= u + v \\ x_2 &= \xi^2 u + \xi v \\ x_3 &= \xi u + \xi^2 v \end{aligned}$$

wobei ξ *eine primitive* 3*–te Einheitswurzel ist und*

$$\begin{aligned} u &= \sqrt[3]{-\frac{q}{2} + \sqrt{(\frac{p}{3})^3 + (\frac{q}{2})^2}} \\ v &= \sqrt[3]{-\frac{q}{2} + \sqrt{(\frac{p}{3})^3 - (\frac{q}{2})^2}} \end{aligned}$$

Dabei sind u *und* v *mit der Nebenbedingung* $uv = -\frac{1}{3}p$ *zu wählen.*

8.2.2 Gleichung vom Grad 4

Eine *Gleichung vom Grad 4* hat die Form $X^4 + aX^3 + bX^2 + cX + d = 0$. Mit der Transformation $x \mapsto x - \frac{1}{4}a$ erhalte die einfachere Form $f = X^4 + pX^2 + qX + r \in \mathbb{K}[X]$.
Strategie: Reduktion auf Lösung einer kubischen Gleichung
$x_1, \ldots, x_4$ die Nullstellen von f, $\mathbb{L} := \mathbb{K}(x_1, \ldots, x_4)$
Annahme: $\mathrm{Gal}(\mathbb{L}/\mathbb{K}) \simeq S_4$
Dann ergibt sich für S_4 folgende Untergruppenstruktur (jeweils mit Index):
$S_4 \overset{2}{\geq} A_4 \overset{3}{\geq} V \overset{2}{\geq} H \geq \{e\}$ mit $V = \{e, (12)(34), (13)(24), (14)(23)\}$
Und ebenso erhalten wir die entsprechenden Fixkörper als Unterkörper (jeweils mit Erweiterungsgraden):
$\mathbb{K} = \mathbb{L}^{S_4} \overset{2}{\subseteq} \mathbb{L}^{A_4} \overset{3}{\subseteq} \underset{=:\mathbb{E}}{\mathbb{L}^V} \overset{2}{\subseteq} \mathbb{L}^H \overset{2}{\subseteq} \mathbb{L}$. Wir wissen,dass $\mathbb{L}^{A_4} = \mathbb{K}(\delta), \delta = \sqrt{\mathrm{disc}\, f}$
Weiterhin setzen wir $z_1 := (x_3 + x_4)(x_1 + x_2)$. Es gilt $z_1 \in \mathbb{L}^V$, wobei $z_1 \notin \mathbb{L}^{A_4}$ (da x_i allgemein gewählt werden können).
Die Menge $\{\sigma(z_1) | \sigma \in S_4\}$ der zu z_1 konjugierten Elemente besteht aus

$$\begin{aligned} z_1 &= (x_1 + x_2)(x_1 + x_3) \\ z_2 &= (x_1 + x_3)(x_2 + x_4) \\ z_3 &= (x_1 + x_4)(x_2 + x_3) \end{aligned}$$

Es gilt $z_1, z_2, z_3 \in \mathbb{E} = \mathbb{L}^V$. Das Minimalpolynom von z_1 über $\mathbb{K} = \mathbb{L}^{S_4}$ ist .
$(z - z_1)(z - z_2)(z - z_3) = z^3 - b_1 z^2 + b_2 z - b_3$ mit

$$\begin{aligned} b_1 &= z_1 + z_2 + z_3 = 2 \sum_{i<j} x_i x_j \\ b_2 &= z_1 z_2 + z_1 z_3 + z_2 z_3 \\ b_3 &= z_1 z_2 z_3 = \sum_{i,j,k} x_i^3 x_j x_k + 2 \sum_{j<k<l} x_i^3 x_j x_k x_l + 2 \sum_{i<j<k} x_i^2 x_j^2 x_k^2 + 4 \sum_{i<j} x_i^2 x_j^2 x_k x_l \end{aligned}$$

Wir drücken nun die symmetrischen Polynome b_1, b_2, b_3 mit Hilfe des entsprechenden Algorithmus durch die elementarsymmetrischen Polynome aus.
Rechnung:
$\omega_1 = 2\sigma_2, b_2 = \sigma_2^2 + \sigma_1\sigma_3 - 4\sigma_4$ $b_3 = \sigma_1\sigma_2\sigma_3 - \sigma_1^2\sigma_4 - \sigma_3^2$

Wegen $\sigma_1 = 0, \sigma_2 = p, \sigma_3 = -q, \sigma_4 = r$ gilt: $b_1 = 2p, b_2 = p^2 - 4r, b_3 = -q^2$
z_1, z_2, z_3 sind die Lösungen der *kubischen Resolvente* $z^3 - 2pz^2 + (p^2 - 4r)z + q^2 = 0$
Für eine gegebene Gleichung $X^4 - pX^2 + qX + r = 0$ kann man z_1, z_2, z_3 mit Cardanos Formel finden. Die z_1, z_2, z_3 sind (bei allgemeinen x_i) genau unter den $\sigma \in V$ invariant, dh. $\mathrm{Gal}(\mathbb{L}/\mathbb{K}(z_1, z_2, z_3)) = V$.

Also gilt $\mathbb{K}(z_1, z_2, z_3) = \mathbb{L}^V = \mathbb{E}$ und $\mathbb{E} \overset{2}{\subseteq} \mathbb{L}^H \overset{2}{\subseteq} \mathbb{L}$, wähle z.B. $H = \{e, (12)(34)\} \leq V$. Bei allgemeinen x_i gilt $u := x_1 + x_2 \in \mathbb{L}^H \backslash \mathbb{L}^V$ und $\{\sigma(x_1 + x_2) | \sigma \in V\} = \{x_1 + x_2, x_3 + x_4\}$. Das Minimalpolynom von u über $\mathbb{E} = \mathbb{L}^V$ ist
$(U - (x_1 - x_2))(U - (x_3 + x_4)) = U^2 - (x_1 + x_2 + x_3 + x_4)U + (x_1 + x_2)(x_3 + x_4) = U^2 + z_1$
Also $x_1 + x_2 = \sqrt{-z_1}, x_3 + x_4 = -\sqrt{-z_1}$
Analog:

$$\begin{aligned} x_1 + x_3 &= \sqrt{-z_2} \\ x_2 + x_4 &= -\sqrt{-z_2} \\ x_1 + x_4 &= \sqrt{-z_3} \\ x_1 + x_3 &= -\sqrt{-z_3} \end{aligned}$$

Beachte: $(x_1 + x_2)(x_1 + x_3)(x_1 + x_4) = x_1^2 \underbrace{(x_1 + x_2 + x_3 + x_4)}_{=0} + \sum_{i<j<k} x_i x_j x_k = \sigma_3 = -q$
Die Quadratwurzel müssen so gewählt werden, dass ihr Produkt $\sqrt{-z_1}\sqrt{-z_2}\sqrt{-z_3} = -q$.
Die $x_1, \ldots, x_4$ können aus $\sqrt{-z_1}, \sqrt{-z_2}, \sqrt{-z_3}$ durch Lösen des linearen Gleichungssystems

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 &= 0 \\ x_1 + x_2 &= \sqrt{-z_1} \\ x_1 + x_3 &= \sqrt{-z_2} \\ x_1 + x_4 &= \sqrt{-z_3} \end{aligned}$$

berechnet werden.

Satz 8.19. *Die Lösungen der Gleichungen $X^4 + pX^2 + qX + r = 0$ sind gegeben durch*

$$\begin{aligned} x_1 &= \frac{1}{2}(\sqrt{-z_1} + \sqrt{-z_2} + \sqrt{-z_3}), \\ x_2 &= \frac{1}{2}(\sqrt{-z_1} - \sqrt{z_1} - \sqrt{-z_2}), \\ x_3 &= \frac{1}{2}(-\sqrt{-z_1} + \sqrt{z_2} - \sqrt{-z_3}) \text{ und} \\ x_4 &= \frac{1}{2}(-\sqrt{-z_1} - \sqrt{-z_2} + \sqrt{-z_3}), \end{aligned}$$

wobei z_1, z_2, z_3 die Lösungen der kubischen Resolvente. $z^3 - 2pz^2 + (p^2 - 4r)z + q^2 = 0$ sind und die Quadratwurzeln mit der Nebenbedingung. $\sqrt{-z_1}\sqrt{-z_2}\sqrt{-z_3} = -q$ zu wählen sind.

8.3 Konstruktionen mit Zirkel und Lineal

Dieser Abschnitt behandelt die Konstruktion von Geometrischen Objekten in der Ebene mit Zirkel und Lineal in endlich vielen Schritten. **Konstruktionsschritt**:
Sei $M \subseteq E$. Dann bestehen 3 Möglichkeiten für einen Konstruktionsschritt.
(1) Wähle $x_1, y_1, x_2, y_2 \in M$, sodass $x_1 \neq y_1$ und $x_2 \neq y_2$, wenn $G_1 \neq G_2$ und G_1, G_2 nicht parallel sind, so haben G_1 und G_2 genau einen Schnittpunkt z. Füge z zu M hinzu.

(2) Wähle $x_1, \ldots, x_5 \in M$ und $x_2 \neq x_3$ und $x_4 \neq x_5$. Sei K der Kreis mit Zentrum x_1 und Radius $\operatorname{dist}(x_2, x_3)$. Sei G die Gerade durch x_4 und x_5. Füge zu M alle Schnittpunkte von G und K hinzu.
(3) Wähle $x_1, y_1, z_1, x_2, y_2, z_2 \in M$ mit $y_1 \neq x_1$, $y_1 \neq z_1$ $y_2 \neq z_2$. Sei $\mathbb{K}_i$ der Kreis mit Zentrum x_i und Radius $\operatorname{dist}(y_i,z_i)$ von K_1 und K_2 hinzu.

Definition 8.20. Sei $M \subseteq E$. Ein Punkt $z \in E$ heißt *aus M konstruierbar* (mit Zirkel und Lineal), wenn es eine Folge $M_0 \subseteq M_1 \subseteq \ldots \subseteq M_t$ von $M_i \subseteq E$ gibt, sodass $M_0 = M$, $z \in M_t$ und man M_{i+1} aus M_i durch einen Konstruktionsschritt erhält.

Algebraisierung des Problems $E = \mathbb{C}$.

Lemma 8.21 (Lemma 1)**.** *Sei $M \subseteq \mathbb{C}$ und M' entstehe aus M durch einen Konstruktionsschritt. Sei K der von M erzeugte Unterkörper in $\mathbb{C}$. Dann gibt es ein $a \in \mathbb{C}$ mit $M' \subseteq K(\sqrt{a})$*

Beweis. Beweis ist elementare analytische Geometrie. □

Lemma 8.22 (Lemma 2)**.** *Sei $M \subseteq \mathbb{C}$ und $0, 1 \in M, K$ der von M erzeugte Unterkörper von $\mathbb{C}$ und $a \in \mathbb{C}$. Dann ist jedes $z \in K(\sqrt{a})$ konstruierbar aus M.*

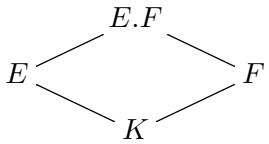
Beweis. Idee: Simuliere arithmetische Operationen $+, -, \cdot, /$ in $\mathbb{C}$, sowie das Quadratwurzelziehen mittels elementargeometrischer Konstruktion (Details aus Übung)

- Parallele zur Gerade G durch Punkt P
- Multiplikation und Division reeller Zahlen
- Reelle Addition und Subtraktion durch "Abtragen von Strecken"
- Wurzelziehen (reell)
- Operationen in $\mathbb{C}$
  - Addtion und Subtraktion
  - Multiplikation und Division
    $z_k = r_k e^{i\varphi_k} \qquad k = 1, 2$
    $z_1 \cdot z_2 = (r_1 \cdot r_2) e^{i(\varphi_1 + \varphi_2)}$
    $z_1 / z_2 = (r_1 / r_2) e^{i(\varphi_1 - \varphi_2)}$
  - Wurzelziehen
    $z = r e^{i\varphi} \qquad r > 0$
    $\sqrt{z} = \sqrt{r} e^{i\frac{\varphi}{2}}$

□

Satz 8.23. *Sei $M \subseteq \mathbb{C}$ endlich mit $0, 1 \in M$ und K der von M erzeugte Unterkörper von $\mathbb{C}$. Ein Punkt $z \in \mathbb{C}$ ist genau dann aus M konstruierbar, wenn der Grad von z über K eine Potenz von 2 ist.* $[K(z) : K] = 2^s$

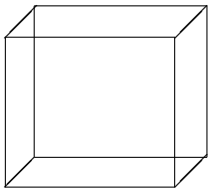
Beweis. (1) Sei z aus M konstruierbar. Dann existiert $M = M_0 \subseteq M_1 \subseteq \ldots \subseteq M_t, \quad z \in M_t$.
M_{i+1} entsteht aus M_i durch einen Konstruktionsschritt. Sei K_i der von M_i erzeugte Unterkörper. Dann $K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_t, z \in K_t$.
Lemma 1 8.21 $\exists a_i \in K_i, \quad K_{i+1} \subseteq K_i(\sqrt{a_i}) \Rightarrow [K_{i+1} : K_i] = \{1, 2\}$
Grad-Multiplikations-Satz $\Rightarrow \exists s \in \mathbb{N} : [K_t : K] = 2^s$
Da $K(z) \subseteq K_t \Rightarrow [K(z) : K] \,|\, [K_t : K] = 2^s \Rightarrow \exists s' \quad [\, K(z) : K] = 2^{s'}$
(2) Sei $E = K(z)$ und $\mathrm{Hom}_K(E, \mathbb{C}) = \{\sigma_1, \cdots, \sigma_r\}$. Dann $[\sigma_1(E) : K] = [E : K]$.
Sei $L := \sigma_1(E) \subseteq \ldots \subseteq \sigma_r(E) \subseteq \mathbb{C}$ das Kompositum. Dann ist $K \subseteq L$ normal nach Konstruktion. $\Rightarrow$ Lemma 8.7 Etwa $[L : K] = 2^t$. $K \subseteq L$ ist Galois-Erweiterung. Die Galoisgruppe

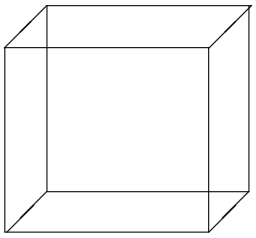


$[E.F : K] \,|\, [E : K] = [F : K]$
Induktion $\Rightarrow$
$[L : K] \,|\, \underbrace{\prod_{i=1}^{r} [\sigma_i(E) : K]}_{\text{2er Potenz}}$

G erfüllt $|G| = 2^t$, ist also 2-Gruppe. Gemäss §3.3.. ist G auflösbar und es existiert eine Normalreihe $G = G_0 \geq G_1 \geq \cdots \geq G_t = \{e\}$ mit $|G_i/G_{i+1}| = 2$
Hauptsatz der Galoistheorie 7.7 $\Rightarrow$ es gibt Körperkette $K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_t = L$
mit $[K_{i+1} : K_i] = 2$. Also $\exists a_i \in K_i$ mit $K_{i+1} = K_i(\sqrt{a_i})$. Definieren induktiv $M_0 := M, \quad M_{i+1} = M_i \cup \{\sqrt{a_i}\}$. Dann erzeugt M_i den Körper K_i (Ind.)
Lemma 2 8.22 $\Rightarrow \sqrt{a_i}$ konstruierbar aus M_i, M_t erzeugt den Körper K_t. z ist konstruierbar aus M. □

Beispiel 8.24.

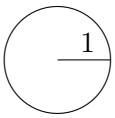




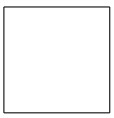
Seitenlänge $\sqrt[3]{2}$

$\sqrt[3]{2}$ ist nicht aus $\{0, 1\}$ konstruierbar, da $\left[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}\right] = 3$ keine 2er Potenz.

Beispiel 8.25. Quadratur des Kreises



Fläche π



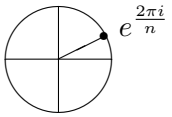
Seitenlänge $\sqrt{\pi}$

Flächengleiches Quadrat Seitenlänge $\sqrt{\pi}$

Theorem 8.26 (Hermite 1873)**.** *Die Zahl π ist nicht algebraisch über $\mathbb{Q}$. Folglich ist π (und damit auch $\sqrt{\pi}$) nicht konstruierbar aus $\{0, 1\}$*

Konstruktion regelmäßiger n-Ecke

Wann ist $e^{\frac{2\pi i}{n}}$ konstruierbar aus $\{0,1\}$?



Wissen (§7.3):$\left[\mathbb{Q}(e^{\frac{2\pi i}{n}}) : \mathbb{Q}\right] = \varphi(n)$

Satz 8.27. *Konstruktion möglich, wenn $\varphi(n)$ 2er-Potenz.*

Satz 8.28. $n = 2^{e_0} \cdot p_1^{e_1} \cdots p_r^{e_r}, \quad 2 < p_1 < \cdots < p_r$ *Primzahlen.*

$$\varphi(n) = \varphi(2^{e_0}) \prod_{i=1}^{r} \varphi(p_i^{e_i})$$

Wissen: $\varphi(2) = 1, \quad \varphi(2^{e_0}) = 2^{e_0-1}$, *falls* $e_0 \geq 1$
$\varphi(p_i^{e_i}) = p_i^{e_i-1}(p_i - 1)$
Also $\varphi(n)$ Potenz von 2 $\Leftrightarrow e_1 = \cdots = e_r = 1$ *und* $\forall i \quad p_i - 1$ *ist 2er-Potenz*

Lemma 8.29. *Sei $p = 2^k + 1$ prim, $k \in \mathbb{N}$. Dann $\exists l \in \mathbb{N} \quad k = 2^l$*

Beweis. Sei $k = 2^l r, 2 \nmid r$
$(X^r + 1) = (X + 1)(X^{r-1} - X^{r-2} + \cdots - X + 1)$ in $\mathbb{Z}[X] \Rightarrow 2^{2^l} + 1$ teilt $(2^{2^l})^r + r = 2^k +^{=} p$
$\underset{p \text{ prim}}{\Rightarrow} \quad r = 1$ □

Man nennt Primzahlen der Form $F_l = 2^{2^l} + 1$ *Fermatsche Primzahlen.*
$F_0 = 3 \qquad F_3 = 257$
$F_1 = 5 \qquad F_4 = 65537$
$F_2 = 17$
Dies sind alle bekannten Fermatschen Primzahlen.

Satz 8.30 (Gauss)**.** *Das regelmäßige n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn*
$n = 2^e p_1 p_2 \cdots p_r, \quad e \in \mathbb{N}$ *und* $p_1, \ldots, p_r$ *verschiedene Fermatsche Primzalhen sind*

n	$\varphi(n)$	...	
3	2	11	10
4	2	12	4
5	4	13	12
6	2	14	6
7	6	15	8
8	4	16	8
9	6	17	16
10	4	18	6

Sei $n = 2^e p_1 \ldots p_t$, wobei $p_1 \ldots p_t$ verschiedene Fermatsche Primzahlen. $p = 2^{2^k} + 1$ regelmäßiges 18-Eck nicht konstruierbar. Denn $18 = 2 \cdot 3^2$ (Winkel 3-Teilung) regelmäßiges 6-Eck ist konstruierbar, denn $6 = 2 \cdot 3$.

8.4 Fundamentalsatz der Algebra

Definition 8.31. Ein *angeordneter Körper* ist ein Körper R zusammen mit einer totalen Ordnung $\leq$, sodass für alle $a, b, c \in R$ gilt:
$a \leq b \Longrightarrow a + c \leq b + c$
$0 \leq a, 0 \leq b \Rightarrow 0 \leq a \cdot b$

Beispiel 8.32. $\mathbb{Q}, \mathbb{R}$ sind angeordnete Körper.

Bemerkung 8.33. $\mathbb{R}$ angeordneter Körper $\Rightarrow \operatorname{char} R = 0 \ \forall \sigma \in R \Rightarrow 0 \leq \sigma^2$
Ein angeordneter Körper heißt *reell abgeschlossen* falls gilt:
(1) $\forall a \in R : 0 \leq a \Rightarrow \exists b \in R \ a = b^2$
(2) $\forall f \in R[X], \deg f$ ungerade $\Rightarrow \exists \sigma \in R \ f(\sigma) = 0$
Bekannt aus Analysis: $\mathbb{R}$ ist reell abgeschlossen.

Bemerkung 8.34. Der Körper der reellen algebraischen Zahlen ist reell abgeschlossen.
$f \in \mathbb{R}_{alg}[X] \ a \in R, \ f(a) = 0 \ \underbrace{\mathbb{Q} \overset{\text{alg.}}{\subseteq} \mathbb{R}_{\text{alg}} \overset{\text{alg.}}{\subseteq} \mathbb{R}_{\text{alg.}}}_{\text{alg.Erw.}}$
Sei $\mathbb{R}$ reell abgeschlossen und C der Zerfällungskörper von $X^2 + 1 \in R[X]$.
Also $C = R(i)$ mit $i \in C, i^2 = -1$. Offensichtlich ist $i \notin R$ (da $i^2 = -1 < 0$)
$\operatorname{Gal}(C/R) = \{\mathrm{id}, \tau\}$, wo $\tau(a + ib) = a - ib$

Lemma 8.35. *Jedes quadratische Polynom in $C[X]$ hat eine Nullstelle in C.*

Beweis. Genügt zu zeigen, dass jedes $z \in C$ eine Quadratwurzel in C hat.
Sei $z = x + iy$, $x + y \in R$. Wir suchen nun $a, b \in R$ mit $z = (x + iy) = (a + ib)^2 = (a^2 - b^2) + 2iab$, dh. $x = a^2 - b^2 \ y = 2ab$ Eine Lösung ist gegeben durch

$$a = \sqrt{\frac{x}{2} + \frac{1}{2}\sqrt{x^2 + y^2}}$$

$$b = \pm\sqrt{\frac{-x}{2} + \frac{1}{2}\sqrt{x^2 + y^2}}$$

Beachte:

$$x^2 + y^2 \geq 0 \pm \frac{x}{2} + \frac{1}{2}\sqrt{x^2 + y^2} \geq 0$$

□

Satz 8.36. *R reell abgeschlossen $\Rightarrow C = R(\sqrt{-1})$ algebraisch abgeschlossen*

Beweis. Sei $f = X^n + \sum_{i=0}^{n-1} a_i X^i \in C[X]$. Sei L der Zerfällungskörper von f und $\tau(f) = X^n + \sum_{i=0}^{n-1} a_i X^i \in C[X]$
Sei L der Zerfällungskörper von f und $\tau(f) = X^n + \sum_{i=0}^{n-1} a_i X^i \in C[X]$.
Dann ist $R \subseteq C$ normal. Denn $\sigma \in \operatorname{Aut}_R L \ \sigma|_C \in \operatorname{Aut}_R C$. Falls $\sigma|_C = id_C$ σ permutiert von die Nullstellen $f \Rightarrow \sigma$ permutiert die Nullstellen von $\overline{f} = \tau f$. Falls $\sigma|_C = \tau \Rightarrow \sigma$ führt die Nullstellen von f in die von $\tau(f)$ über und umgekehrt. Da $\operatorname{char} R = 0 \Rightarrow R \subseteq L$ Galois-Erweiterung. Sei $[L : R] = |G| = 2^k m, 2 \nmid m$. Es gilt $k \geq 1$, da $[C : R] = 2 \overset{\text{Sylowscher Satz}}{\Rightarrow} G$ enthält eine Untergruppe der Ordnung 2^k. Dann gilt: $[L : L^H] \cdot |H| = 2^k - 1$
$[L^H : R] = m \overset{\text{Satz vom primitiven Element}}{\Rightarrow} \exists a \in L^H \ L^H = R(a)$ Das Minimalpolynom g von a über R hat den Grad m. m ist ungerade. $\overset{\text{2. Axiom für reell abgeschlossene Körper}}{\Rightarrow} m = 1$ Also

gilt: $[L:R] = 2^k \Rightarrow [L:C] = 2^{k-1}$ Annahme $k > 1$: Die 2-Gruppe $d := \mathrm{Gal}(L/C)$ hat eine Untergruppe H' der Ordnung 2^{k-2} (beachten Ordnung von σ' ist 2^{k-1}) $\Rightarrow [L:L^H] = 2^{k-2}$ $[L:L^{H'}] = 2^{k-2}$, $[L^{H'}:C] = 2$
Nach Lemma hat C keine Erweiterung von Grad 2. $\lightning$
Es folgt $k = 1$ und damit $L = C$ □

8.5 Quadratisches Reziprozitätsgesetz

Sei $p > 2$ prim. $\xi_p = e^{2\pi\frac{i}{p}} \in \mathbb{C}$ primitiv p-te Einheitswurzel.
Wissen: $\mathrm{Gal}(\mathbb{Q}(\xi_p)/\mathbb{Q}) \simeq \mathbb{Z}_p^\times$ zyklisch. Da $\varphi(p) = |\mathbb{Z}_p^\times| = p-1$ gerade, hat $\mathbb{Z}_p^\times$ genau eine Untergruppe H der Ordnung $\frac{p-1}{2}$. Deshalb hat $\mathbb{Q}(\xi_p)$ genau einen Unterkörper $\mathbb{E} \subseteq \mathbb{Q}(\xi_p)$ mit $[\mathbb{E}:\mathbb{Q}] = 2$. Betrachte zuerst H. Für $x \in \mathbb{Z}_p^\times$ gilt $x^{p-1} \equiv 1 \mod p$, also $x^{\frac{p-1}{2}} \equiv \pm 1 \mod p$. Ein Erzeuger G von $\mathbb{Z}_p^\times$ erfüllt $g^{\frac{p-1}{2}} \equiv -1 \mod p$. Deshalb ist $\mathbb{Z}_p^\times \to \{-1,1\}, x \longmapsto x^{\frac{p-1}{2}}$ surjektiver Gruppenmorphismus. Der Kern $H := \{x \in \mathbb{Z}_p^\times | x^{\frac{p-1}{2}}\} \equiv 1 \mod p$ ist eine Untergruppe von $\mathbb{Z}_p^\times$ von Index 2.

Bemerkung 8.37. $H = \{y^2 | y \in \mathbb{Z}_p^\times\} = \{\text{Quadrate } \mod p\}$

Beweis. $\mathbb{Z}_p^\times \to \{y^2 | y \in \mathbb{Z}_p^\times\}$
$y \to y^2$ ist surjektiver Gruppenhomomorphismus mit Kern $\{-1,1\}$.
Also $|\{y^2 | y \in \mathbb{Z}_p^\times\}| = \frac{p-1}{2}$
Außerdem $\{y^2 | y \in \mathbb{Z}_p^\times\} \subseteq H$, wobei die gleiche Ordnung vorliegt. □

Korollar 8.38. *Für $x \in \mathbb{Z}_p^\times$ gilt:*
x ist Quadrat $\mod p \Leftrightarrow x^{\frac{p-1}{2}} \equiv 1 \mod p$
Diese Charakterisierung liefert einen effizienten Test für prime p.

Sei $\mathrm{Gal}(\mathbb{Q}(\xi_p)/\mathbb{Q}) \simeq \mathbb{Z}_p^\times$ zyklisch der Ordnung $p-1$. Sei $H \leq \mathbb{Z}_p^\times$ die eindeutig bestimme Untergruppe vom Index 2. Haben gezeigt: $H = \{y^2 | y \in \mathbb{Z}_p^\times\} = \{x \in \mathbb{Z}_p^\times | x^{\frac{p-1}{2}} = 1\}$
Zu H gehört ein Zwischenkörper $\mathbb{Q} \subseteq \mathbb{E} \subseteq \mathbb{Q}(\xi_p)$ mit $[\mathbb{E}:\mathbb{Q}] = 2$
Nächstes Ziel: Bestimme $\mathbb{E}$ konkret.
Erinnern an Diskriminante (§5.4.). Sei allgemein $f \in \mathbb{K}[X]$ mit Nullstellen $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{K}}, n = \deg f$. $\mathrm{disc}(f) = \prod_{i<j}(\alpha_i - \alpha_j)^2 \in \mathbb{K}$.

$$\sqrt{\mathrm{disc}(f)} := \prod_{i<j}(\alpha_i - \alpha_j) \in \mathbb{K}(\alpha_1, \ldots, \alpha_n)$$

ist Unterkörper vom Grad 2, falls $\mathrm{disc}\, f \notin \mathbb{K}$
$\overset{Kor.5.45}{\Rightarrow} \mathrm{disc}(f) = (-1)^{\frac{n(n-1)}{2}} \mathrm{res}(f, f')$.
Wir betrachten nun die Diskriminante von

$$(\star)\Phi_p = X^{p-1} + \cdots + X + 1 = \prod_{k=1}^{p-1}(X - \xi^k), \quad \xi \text{ primitive } p\text{-te EW}$$

Proposition 8.39. $\mathrm{disc}(\Phi_p) = (-1)^{\frac{p-1}{2}} p^{p-2}$ *für $p > 2$ prim.*

Beweis.

$$\begin{aligned} X^p - 1 &= (X-1)\Phi_p(X) \\ \Rightarrow pX^{p-1} &= (X-1)\Phi_p'(X) + \Phi_p(X) \\ = p(\xi^k)^{p-1} &= (\xi^k - 1)\Phi_p'(\xi^k) \\ = p^{p-1} &= p^{p-1}\boxed{\xi^{(p-1)(\sum_{k=1}^{p-1} k)}}_{=1} \\ &= \prod_{k=1}^{p-1}(\xi^k - 1)\prod_{k=1}^{p-1}\Phi_p'(\xi^k) \end{aligned}$$

In $(\star)$ setze $X = 1$

$$p = \prod_{k=1}^{p-1}(1-\xi^k) = \prod_{k=1}^{p-1}(\xi^k - 1)$$

Schreibweise: $p^* = (-1)^{\frac{p-1}{2}}p = \begin{cases} p & \text{falls } p \equiv 1 \mod 4 \\ -p & \text{falls } p \equiv 3 \mod 4 \end{cases}$

Also $\operatorname{disc}(\Phi_p) = p^* p^{p-3} = p^*(p^{\frac{p-3}{2}})^2$

Ergebnis: $\mathbb{E} = \mathbb{Q}(\sqrt{p^*})$ ist der gesuchte quadratische Unterkörper von $\mathbb{Q}(\xi_p)$.

Ergänzung/Korrektur:

$p > 2$ prim, $p^* = (-1)^{\frac{p-1}{2}}p$

ξ primitive p-te Einheitswurzel

$$\sqrt{p^*} = \pm \sum_{a \in \mathbb{Z}_p^\times} (\frac{a}{p})\xi^a$$

Erklärung:

Es gibt genau einen quadratischen Unterkörper $\mathbb{E}$ mit $\mathbb{Q} \subseteq \mathbb{E} = \mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}(\xi_p)$

Was ist d? $d = (p^*)^2$.

$$\begin{aligned} \mathbb{Z}_p^\times &\xrightarrow{\sim} \operatorname{Gal}(\mathbb{Q}(\xi_p)/\mathbb{Q}) \\ a &\longmapsto (\xi \longmapsto \xi^a) = \sigma_a \\ \sigma_a(\mathbb{E}) = \mathbb{E}, \sigma_a(\sqrt{p^*}) &= \underbrace{\chi(a)}_{\pm 1}\sqrt{p^*} \end{aligned}$$

$\chi : \mathbb{Z}_p^\times \to \{-1, 1\}$ Homomorphismus

$\operatorname{Gal}(\mathbb{Q}(\xi_p)/\mathbb{E}) \simeq \{\text{Quadrate in } \mathbb{Z}_p^\times\} =: H$ einzige Untergruppe vom Index 2.

$\chi(a) = \begin{cases} 1 & \text{falls } a \in H \\ -1 & \text{sonst} \end{cases} = (\frac{a}{p})$ Legendresches Polynom □

Studieren Wirkung der Galoisgruppe $G = \operatorname{Gal}(\mathbb{Q}(\xi_p)/\mathbb{Q})$ auf $\mathbb{E}$. Für $a \in \mathbb{Z}_p^\times$ sei $\sigma_a \in G$ definiert durch $\sigma_a(\xi) = \xi^a$ für $\xi \in U_p := \{p\text{-te Einheitswurzel}\}$. Da $\sigma_a(\mathbb{E}) = \mathbb{E}$, so gilt:

$\sigma_a(\sqrt{p^*}) = \chi(a)\sqrt{p^*}$ mit $\chi(a) \in \{-1, 1\}$

Aus $\sigma_a \circ \sigma_b = \sigma_{ab} \Rightarrow \chi(a)\chi(b) = \chi(ab)$ für $a, b \in \mathbb{Z}_p$. Das heißt $\chi : \mathbb{Z}_p^\times \to \{-1, 1\}$ ist Gruppenmorphismus (Charakter).

Da $\{\sigma_a | a \in H\} = \operatorname{Gal}(\mathbb{Q}(\xi_p)/\mathbb{E})$ gilt:

$\chi(a) = 1 \Leftrightarrow a \in H \Leftrightarrow a$ Quadrat $\mod p$

Definition 8.40. Für eine Primzahl p und $a \in \mathbb{Z}$ mit $p \nmid a$ definiert das *Legendre-Symbol*

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{falls } a \text{ Quadrat} \mod p \\ -1 & \text{sonst} \end{cases}$$

[Man sagt $\left(\frac{a}{p}\right) = 0$, falls $p|a$]
D.h. $\chi(a) = \left(\frac{a}{p}\right)$. Es gilt $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$
Eulersches Kriterium: $\left(\frac{a}{p}\right) = 1 \Leftrightarrow a^{\frac{p-1}{2}} \equiv 1 \mod p$

Folglich: $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{falls } p \equiv 1 \mod 4 \\ -1 & \text{falls } p \equiv 3 \mod 4 \end{cases}$
$\sigma_a(\sqrt{p^*}) = \left(\frac{a}{p}\right)\sqrt{p^*}$
Sei $\xi \in U_p\{1\}$ eine beliebige primitive p-te Einheitswurzel. Da $\Phi_p = X^{p-1} + \cdots + X + 1$ das Minimalpolynom von ξ über $\mathbb{Q} \Rightarrow 1, \xi, \xi^2, \ldots, \xi^{p-1}$ $\mathbb{Q}$-Basis von $\mathbb{Q}(\xi_p)$. Diese Basis ist die Bahn von ξ unter der Wirkung der Galoisgruppe.
Schreibe $\sqrt{p^*} = \sum_{\tau \in G} c(\tau)\tau(\xi)$. Für $\sigma \in G$ gilt:

$$\sigma(\sqrt{p^*}) = \sum_{\tau \in G} c(\tau)\tau(\xi) \overset{\tilde{\tau}+\sigma\tau \Rightarrow \sigma^{-1}\tilde{\tau}=\tau}{=} \sum_{\tilde{\tau} \in G} c(\sigma^{-1}\tilde{\tau})\tilde{\tau}(\xi)$$

Andererseits nach Definition von χ:

$$\sigma(\sqrt{p^*}) = \chi(\sigma)\sqrt{p^*} = \sum_{\tau \in G} \chi(\sigma)c(\tau)\tau(\xi)$$

Koeffizienten-Vergleich $\Rightarrow c(\sigma^{-1}\tau) = \xi(\sigma)c(\tau)$. Insbesondere $\tau = \mathrm{id} : c(\sigma^{-1}) = \chi(\sigma)c(\mathrm{id})$. Mit $c := c(\mathrm{id}) \in \mathbb{Q}$ erhalten $c(\tau) = \sigma\chi(\tau)$
Erhalten endlich:

$$\sqrt{p^*} = \sum_{\tau \in G} \chi(\tau)\tau(\xi) = c\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\xi^a$$

Zeigen als nächstes, dass $c = \pm 1$

Behauptung. Es gilt $c = \pm 1$.

Beweis. Sei $\alpha = \sum_{\tau \in G} \chi(\tau)\tau(\xi)$. Rechne direkt nach, dass $\alpha^2 = p^*$ gilt:

$$\alpha^2 = \sum_{\sigma,\tau \in G} \frac{\chi(\sigma\tau)}{\chi(\sigma)\chi(\tau)}\sigma(\xi)\tau(\xi)$$

Variablentransformation liefert: $(\sigma, \tau) \to (\sigma, \underbrace{\sigma^{-1}\tau}_{\varphi}) = (\sigma, \varphi)$

$$a^2 = \sum_{\sigma,\varphi \in G} \chi(\varphi)\underbrace{\sigma(\xi)\sigma(\varphi(\xi))}_{\sigma(\xi\varphi(\xi)))}$$
$$a^2 = \sum_{\varphi \in G} \chi(\varphi)\sum_{\sigma \in G}\sigma(\xi\varphi(\xi))$$

Für $\eta \in U_p$ gilt:

$$\eta = \sum_{\sigma \in G}\sigma(\eta) = \eta + \eta^2 + \cdots + \eta^{p-1} = \begin{cases} p-1 & \text{falls } \eta = 1 \\ -1 & \text{sonst} \end{cases}$$

Wende dies an auf $\eta = \xi\varphi(\xi)$. Es gilt:

$$\eta = 1 \Leftrightarrow \varphi(\xi) = \xi^{-1} = \sigma_{-1}(\xi) \Leftrightarrow \varphi = \sigma_{-1}$$

Erhalten

$$\alpha^2 = \chi(\sigma_{-1}(p-1) + \sum_{\varphi \neq \sigma_{-1}} \chi(\varphi)(-1)$$

Wegen $\sum_{\varphi \in G} \chi(\varphi) = \sum_{\varphi \in H} 1 + \sum_{\varphi \in G \setminus H}(-1) = 0$ folgt:

$$\alpha^2 = \chi(\sigma_{-1}(p-1) + \chi(\sigma_{-1} = p\chi(\sigma_{-1})$$
$$\chi(\sigma_{-1}) = \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \Rightarrow$$
$$\alpha^2 = p(-1)^{\frac{p-1}{2}} = p^*$$

□

Ergebnis: $\sqrt{p^*} = \pm \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \xi^a$ (Gaussche Summe)

Definition 8.41. $R_p := \mathbb{Z}[\xi_p] = \{\sum_{k=0}^{p-2} c_k \xi_p^k | c_k \in \mathbb{Z}\}$ Ring der "ganzen Zahlen" in $\mathbb{Q}(\xi_p)$.

Es gilt: $1, \xi_p, \ldots, \xi_p^{p-2}$ $\mathbb{Q}$-Basis von $\mathbb{Q}(\xi_p)$
$\xi^{p-1} = -1 - \xi - \cdots - \xi^{p-2}$
Sei $q > 2$ Primzahl $q \neq p$. Es gilt: $\sigma_q(R_p) = R_p$

Lemma 8.42. *Für $\alpha \in R_p$ gilt $\sigma_q(\alpha) \equiv \alpha^q \mod qR_p$.*

Beweis. Sei $\alpha = \sum_{k=0}^{p-2} c_k \xi_p^k$, $c_k \in \mathbb{Z}$. Es gilt: $c_k^q \equiv c_k \mod q$ $\sigma_q(\alpha) = \sum_k c_k \sigma_q(\xi_p^k) = \sum_k c_k \xi_p^{kq} \equiv \sum_k c_k^q \xi_p^{kq} \equiv (\sum_k c_k \xi^{kq}) \mod qR_p$ □

Bemerkung 8.43. Man kann sehen, dass gilt: $qR_p \cap \mathbb{Z} = q\mathbb{Z}$.

Kombinieren wir unsere Einsichten, erhalten wir:
$\sigma_q(\sqrt{p^*}) = (\frac{q}{p})\sqrt{p^*}$
$\overset{\text{Lemma}}{\Rightarrow} \sigma_q(\sqrt{p^*}) \equiv \sqrt{p^*}^q \mod qR_p \Rightarrow (\frac{q}{p})\sqrt{p^*} \equiv \sqrt{p^*}^q \mod qR_p$
$\Rightarrow (\frac{q}{p})p^* \equiv \sqrt{p^*}^{q+1} = p^*(p^*)^{\frac{q-1}{2}} \mod qR_p$
$\overset{\text{Bem.}}{\Rightarrow} (\frac{q}{p})p^* \equiv p^*(p^*)^{\frac{q-1}{2}} \mod q\mathbb{Z}$
$\mathbb{Z}/q\mathbb{Z} \overset{\text{Integritätsbereich}}{\Rightarrow} (\frac{q}{p}) \equiv (p^*)^{\frac{q-1}{2}} \mod q\mathbb{Z}$
Eulerkriterium:
$(\frac{p^*}{q}) \equiv (p^*)^{\frac{q-1}{2}} \mod q\mathbb{Z}$
Wir erhalten $(\frac{q}{p}) \equiv (\frac{p^*}{q}) \mod q\mathbb{Z}$
Da $(\frac{q}{p}), (\frac{p^*}{q}) \in \{-1, 1\} \Rightarrow (\frac{q}{p}) = (\frac{p^*}{q})$.
Mit $p^* = (-1)^{\frac{p-1}{2}} p$: $(\frac{p^*}{q}) = (\frac{-1}{q})^{\frac{p-1}{2}} (\frac{p}{q}) = ((-1)^{\frac{q-1}{2}})^{\frac{p-1}{2}} (\frac{p}{q})$

Theorem 8.44 (Quadratisches Reziprozitätsgesetz)**.** *Für ungerade Primzahlen $p \neq q$ gilt* $(\frac{q}{p}) = (-1)^{(\frac{p-1}{2})(\frac{q-1}{2})} (\frac{p}{q})$.
Mit anderen Worten:
(1) $p \equiv 1 \mod 4$ oder $q \equiv 1 \mod 4$, so gilt:
q quadratischer Rest $\mod p \Leftrightarrow p$ quadratischer Rest $\mod q$.
(2) Falls $p \equiv 3 \mod 4$ und $q \equiv 3 \mod 4$, dann:
q quadratischer Rest $\mod p \Leftrightarrow p$ nicht quadratischer Rest $\mod q$.

Beispiel 8.45. Für, welche Primzahlen $p > 2$, $p \neq 5$, ist 5 quadratischer Rest $\bmod p$?
Nach dem Theorem: $(\frac{5}{p}) = (\frac{p}{5})$
Es gilt: $(\frac{p}{5}) = 1 \Leftrightarrow p^{(\frac{5-1}{2})} \equiv 1 \mod 5 \Leftrightarrow p^2 \equiv 1 \mod 5 \Leftrightarrow p = \pm 1 \mod 5$
Es handelt sich bei den gesuchten p um die unterstrichenen der folgenden Primzahlen:
$3, 5, 7, \underline{11}, 13, 17, \underline{19}, 23, \underline{29}, \underline{31}, 37$

Beispiel 8.46. Für welche $p > 2$, $p \neq 3$ ist 3 ein quadratischer Rest $\bmod p$?
1.Fall $p \equiv 1 \mod 4$:
Es gilt: $\underline{p \equiv 1 \mod 4}, (\frac{3}{p}) = (\frac{p}{3}), (\frac{p}{3}) = 1 \Leftrightarrow \underline{p \equiv 1 \mod 3}$.
Weiterhin sind die beiden unterstrichenen Aussagen zusammen äquivalent zu: $p \equiv 1 \mod 12$
2. Fall $p \equiv 3 \mod 4$:
Es gilt: $p \equiv 3 \mod 4, (\frac{3}{p}) = -(\frac{p}{3}) = 1 \Leftrightarrow p \equiv 2 \mod 3$
Mit Chinesischem Restsatz: $p \equiv 3 \mod 4$ und $p \equiv 2 \mod 3 \Leftrightarrow p \equiv 11 \mod 12$.
Lösung:
$p > 2, p \neq 3$ quadrat. Rest $\bmod p \Leftrightarrow p \mod 12 \in \{1, 11\}$

Korollar 8.47. *Sei $q > 2$ prim. Der Wert von $(\frac{q}{p})$ für $p > 2$ prim, hängt nur von der Restklasse $p \bmod (4q)$ ab. Im Fall $q \equiv 1 \mod 4$ sogar nur von der Restklasse $p \bmod q$. (Beweis Übung!)*

Satz 8.48. *Für $p > 2$ prim gilt:*

$$(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{falls } p \equiv 1, -1 \mod 8 \\ -1 & \text{falls } p \equiv 3, -3 \mod 8 \end{cases}$$

Skizze. Als Übung. Arbeite in $\mathbb{Q}(\xi_8)$, $\mathrm{Gal}(\mathbb{Q}(\xi_8)/\mathbb{Q}) \simeq \mathbb{Z}_8^\times \simeq C_2 \times C_2$
Zeige $\sqrt{2} = \xi_8 + \xi_8^{-1}$
$\sigma_p(\sqrt{2}) = (\frac{2}{p}\sqrt{2})$
$\sigma_p(\sqrt{2}) = \sqrt{2}^p \mod pR_8$ □

Beispiel 8.49. $(\frac{q}{p})$ ist sowieso für allgemeine a definiert.
Für $b = q_1 \dots q_s$ mit $q_1, ..., q_s$ prim, definieren wir das *Jacobisymbol*:
$(\frac{a}{b}) := (\frac{a}{q_1}) \dots (\frac{a}{q_s})$
Für $1 \leq a \leq p$ ist $p = ua + r, r < n$ und damit:
$(\frac{a}{p}) = \pm(\frac{p}{a}) = \pm(\frac{r}{a}) = \pm(\frac{a}{r})$

9 Lineare Algebra

9.1 Moduln über Ringen

Nun verallgemeinern wir das Konzept des Vektorraums über einem Körper. Sei A ein Ring.

Definition 9.1. Ein *(Links-)Modul über A* ist eine abelsche Gruppe M zusammen mit einer Abbildung $A \times M \to M$, $(a, x) \longmapsto ax$, welche die folgenden Eigenschaften hat:

(i) $a(x + y) = ax + ay$

(ii) $(a + b)x = ax + bx$

(iii) $a(bx) = (ab)x$

(iv) $1x = x$ für alle $a, b \in A$

Wir sprechen auch kurz von A-Moduln.

Ist $A = \mathbb{K}$ ein Körper. So ist ein A-Modul das selbe wie ein $\mathbb{K}$-Vektorraum.
Für eine abelsche Gruppe M bezeichnen $\mathrm{End}(M) := \{\varphi | \varphi : M \to M \text{ Gruppenhomomorphismus}\}$.
Offensichtlich ist $\mathrm{End}(M)$ (mit den Verknüpfungen $+, \circ$) ein Ring.
Jeder A-Modul M definiert einen Ringhomomorphismus

$$D : A \to \mathrm{End}(M)$$
$$a \longmapsto D(a)$$
$$D(a)(x) = ax (a \in A, x \in M)$$

Denn

$$D(a + b) = D(a) + D(b)$$
$$D(a \cdot b) = D(a)D(b)$$
$$D(1) = \mathrm{id}$$

Umgekehrt definiert jeder Ringhomomorphismus

$$D : A \to \mathrm{End}(M)$$
$$a \longmapsto D(a)$$

einen A-Modul via

$$A \times M \to M, ax := D(a)(x).$$

Man nennt D eine *Darstellung des Rings A*. (Jedes A wird durch einen Homomorphismus $D(a)$ dargestellt.)

Bemerkung 9.2 (Übungsaufgabe). Sei G eine endliche Gruppe, $\mathbb{K}$ ein Körper und $\mathbb{K}[G] := \mathbb{K}[X_g | g \in G]/I_G$ der sogenannte *Gruppenring* wobei I_G das Ideal ist, welches von den Polynomen $X_g X_h - X_{gh} X_e$ für alle $g, h \in G$ und dem Polynom $X_e - 1$ erzeugt wird. Weiterhin sei V ein $\mathbb{K}[G]$-Modul.
Dann ist $D : \mathbb{K}[G] \to \mathrm{End}_{\mathbb{K}}(V)$ $g \longmapsto D(g)$ Ringhomomorphismus

Beispiel 9.3. A ist ein A-Modul bezüglich der Ringmultiplikation $A \times A \to A$. Dazu gehört die reguläre Darstellung

$$A \to \mathrm{End}(A), \quad a \to (x \to ax)$$

Definition 9.4. Sei M ein A-Modul. Ein *Untermodul* N von M ist eine additive Untergruppe von M, so dass

$$\forall a \in A \quad \forall x \in N \quad ax \in N$$

Wichtiger Spezialfall: Untermoduln des A-Moduls A heißen *Linksideale*. Das heißt

$$I \subseteq A \text{ und } \forall a \in A \quad \forall x \in N \quad ax \in N.$$

Bei kommutativen Ringen stimmen die Konzepte von Idealen und Linksidealen überein.

Definition 9.5. Seien M, N A-Moduln. Ein *A-Modulmorphismus* ist ein Gruppenmorphismus

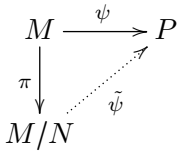
$$\varphi : M \to N \text{ mit } \forall a \in A \quad \forall x \in M \quad \varphi(ax) = a\varphi(x)$$

Dies verallgemeinert das Konzept der $\mathbb{K}$-linearen Abbildung.

Ist M ein A-Modul und $N \subseteq M$ Untermodul, so definieren wir auf der Faktorgruppe M/N eine A-Modulstruktur durch
$a(x + N) := ax + N$ (wohldefiniert!)
M/N heißt *Faktormodul*. Erhalten surjektiven A-Modulmorphismus

$$\pi : M \to M/N, \quad x \to x + N \text{ mit Kern } N.$$

Dieser ist durch eine universelle Eigenschaft charakterisiert: für alle A-Moduln P und A-Modulmorphismen $\psi : M \to P$ mit $N \subseteq \ker \psi$ exisiert genau ein A-Modulmorphismus $\tilde{\psi} : M/N \to P$ so dass



kommutatives Diagramm ist, das heißt $\psi = \tilde{\psi} \circ \pi$.

Produkte und Summen

Sei $(M_i)_{i \in I}$ eine Familie von A-Moduln. Das kartesische Produkt $\prod_{i \in I} M_i$ bildet bezüglich komponentenweise definierten Operationen einen A-Modul. Dieser heißt das *direkte Produkt* der Familie $(M_i)_{i \in I}$. Haben Einbettung

$$\tau_i : M_i \to \prod_{j \in J} M_j, \quad m \to (x_j)_{j \in J},$$

wobei $x_i = m$ und $x_j = 0$ für $i \neq j$. Der von $\bigcup_{i \in I} M_i$ erzeugte Untermodul heißt die *direkte Summe* $\bigoplus_{j \in J} M_j$ der gegebenen Familie.
Wenn wir M_i mit $\tau_i(M_i)$ identifizieren, so bestehen die Elemente aus $\bigoplus_{j \in J} M_j$ aus den Summen $\sum_{j \in I} m_j$, wobei $m_j \in M_j$ und $\{j \in I | m_j \neq 0\}$ endlich ist. Falls I endlich ist, so stimmen direkte Summe und direktes Produkt überein.

Interne direkte Summe

Sei M A-Modul, $M_i \subseteq M$ Familie von Untermoduln. Haben einen Modulmorphismus

$$\bigoplus_{i \in I} M_i \to M$$

Man nennt das Bild die *Summe* $\sum_{i\in I} M_i$ der Untermoduln. Diese besteht aus den (endlichen) Summen $\sum_{i\in I} x_i$.
Man nennt M eine *interne direkte Summe*, falls der Morphismus $\bigoplus_{i\in I} M_i \to M$ ein Isomorphismus ist. Das heißt jedes $x \in M$ hat eine eindeutige Darstellung $x = \sum_{i\in I} x_i$ und $x_i \in M_i$.
Sei $(X_i)_{i\in I}$ eine Familie von Elementen des A-Moduls M. Eine *Linearkombination* dieser Familie ist ein Element der Form $\sum_{i\in I} a_i x_i$, wobei $a_i \in A$ und $\{i \in I | a_i \neq 0\}$ endlich ist. Die Menge dieser Linearkombinationen bildet die Summe $\sum_{i\in I} Ax_i$,
wobei $Ax_i = \{ax_i | a \in A\}$. Man nennt $\sum_{i\in I} Ax_i$ den von der Familie erzeugten $(X_i)_{i\in I}$ Untermodul. Offensichtlich ist dies der kleinste Untermodul, der alle x_i enthällt.
Die Familie $(X_i)_{i\in I}$ heißt *linear unabhängig*, falls

$$\sum_{i\in I} a_i x_i = 0 \Rightarrow \forall i \quad a_i = 0$$

Das heißt $\sum_{i\in I} Ax_i$ ist eine interne direkte Summe der Ax_i.
Eine *Basis* von M ist eine linear unabhängige Familie $(X_i)_{i\in I}$, die M erzeugt, das heißt $\bigoplus_{i\in I} Ax_i = M$.

Definition 9.6. Ein A-Modul heißt *frei*, wenn er eine Basis hat.

Warnungen:

- Nicht jeder A-Modul hat eine Basis

  Beispiel 9.7. $A = \mathbb{Z}, \quad M = {}^{\mathbb{Z}}/_{\mathbb{Z}m}, \quad m > 1$
  Sei $x \in M\backslash\{0\}$. Dann $mx = 0$. Also ist $\{x\}$ linear abhängig. Also hat M keine Basis.

- Nicht jeder Untermodul eines freien Moduls ist frei.

  Beispiel 9.8. $A = \mathbb{Z}[X], \quad M = A$ ist frei (Basis 1)
  $N = A2 + AX = (2, X)$. Dann ist N nicht frei. (Beweis: Übung)

Satz 9.9. *Sei A ein kommutativer Ring und M ein endlich erzeugter freier A-Modul. Alle Basen von M haben die gleiche Kardinalität.*
Man nennt die Kardinalität von Basen den Rang $R(M)$ *von M (Manchmal auch Dimension).*

Sei $I \subseteq A$ Ideal. Betrachte den Untermodul IM von M, der von $\{ax | a \in I \quad x \in M\}$ erzeugt wird. Dann ist ${}^{M}/_{IM}$ ein ${}^{A}/_{I}$-Modul via

$$(a \mod I)(x \mod IM) := ax \mod IM \text{ (wohldefiniert: } a \equiv a_i \mod I, x \equiv x_1 \mod IM$$
$$ax - a_1x_1 = a\underbrace{(x - x_1)}_{\in IM} + (a - a_1)x_1 \in IM)$$

Behauptung. Ist $B = (x_i)_{1\leq i\leq r}$ eine A-Basis von $M \Rightarrow \overline{B} = (x_i \mod IM)_{1\leq i\leq r}$ ist eine ${}^{A}/_{I}$-Basis von ${}^{M}/_{IM}$.

Beweis.
- $\overline{B}$ erzeugt ${}^{M}/_{IM}$ klar
- $\overline{B}$ linear unabhängig. Betrachte $IM = \{\sum_{i=1}^{r} b_i x_i | b_i \in I\}$
  Sei $\sum_{i=1}^{r} a_i x_i \in IM$ Eindeutigkeit der Darstellung $\Rightarrow a_i \in I \Rightarrow a_i \mod I = 0$

□

Beweis. (von Satz 9.9)
Sei ohne Einschränkung $A \neq \{0\}$. Bekannt: ein kommutativer Ring $A \neq \{0\}$ hat ein maximales Ideal (siehe §6.6.).
Dann ist $K := {}^{A}/_{I}$ ein Körper. Nach obiger Behauptung gilt $(x_1, \ldots, x_r)$ A-Basis von $M \Rightarrow (x_1 \mod IM, \ldots, x_r \mod IM)$ K-Basis von ${}^{M}/_{IM}$. Also $r = \dim_K {}^{M}/_{IM}$. Also ist r unabhängig von der Wahl der Basis. □

Definition 9.10. M freier A-Modul, $N \subseteq M$ freier Untermodul. Ein *Modulkomplement* von N ist ein freier Untermodul $P \subseteq M$, sodass $M = N \oplus P$.

Bemerkung 9.11. Im Allgemeinen hat N kein Modulkomplement. (Siehe Übungsblatt!)

Lemma 9.12. *Sei $\varphi : M \to M'$ ein surjektiver Morphismus von A-Moduln. Sei M' frei. Dann existiert ein Untermodul $P \subseteq M$ mit $M = \ker\varphi \oplus P$ und $\varphi|_P : P \to M'$ ist Moduliso-morphismus. Speziell: ${}^{M}/_{N}$ frei $\Rightarrow$ Modulkomplement existiert.*

Beweis. Sei $(x'_i)_i \in I$ Basis von M'. Sei $x_i \in M$ mit $\varphi(x_i) = x'_i$. P der von $\{x_i | i \in I\}$ erzeugte Untermodul.

- $(x_i)_{i\in I}$ ist linear unabhängig: $\sum_{i\in I} a_i x_i = 0$ $a_i \in A$
  $\Rightarrow \sum_i a_i x'_i = 0 \Rightarrow \forall i a_i = 0$
- $\ker\varphi \cap P = \{0\} : \sum_{i\in I} a_i x_i \ker\varphi \Rightarrow \sum_i a_i x'_i = 0$
  $\Rightarrow \forall i a_i = 0$
- $M = \ker\varphi + P$: Sei $x \in M$. Dann $\exists a_i \in A$ $\varphi(X) = \sum_i a_i x'_i$
  $\Rightarrow y := x - \sum_i a_i x'_i \in \ker\varphi$
  $\Rightarrow x = y + \sum_i a_i x_i \in \ker\varphi + P$

Es folgt $M = \ker\varphi + P$. Der Rest ist klar. □

9.2 Freie Moduln über Hauptidealbereichen

Hier sei generell vorausgesetzt A ein Hauptidealbereich.
1. wichtiger Spezialfall: $A = \mathbb{Z}$
$\mathbb{Z}$-Moduln $\hat{=}$ abelsche Gruppen
2. wichtiger Spezialfall: $A = \mathbb{K}[X]$, $\mathbb{K}$ Körper
Gesucht: konkrete Beschreibung von $\mathbb{K}[X]$-Moduln. Sei V endlich-dimensionaler Vektorraum und $\varphi \in \mathrm{End}_{\mathbb{K}}(V)$. Haben Ringhomomorphismus

$$\varphi v_\varphi : \mathbb{K}[X] \longmapsto \mathrm{End}(V)$$

$$f = \sum \lambda_i x^i \to \sum \lambda_i \varphi^i = f(\varphi),$$

dabei $\mathrm{Im}(\varphi v_\varphi) = \mathbb{K}[\varphi]$.
Der Kern von φv_φ ist ein Ideal$\neq 0$ in $\mathbb{K}[X]$. Dessen normierter Erzeuger heißt das *Minimalpolynom* m_φ von φ.
Die Darstellung φv_φ definiert die folgende Aktion von $\mathbb{K}[X]$ auf V:

$$\mathbb{K}[X] \to V, (f, v) \longmapsto f.v := f(\varphi)(v)$$

(für $m \in \mathbb{N}$: $X^m.v = \varphi^m(v)$)

Bemerkung 9.13. In diesem Zusammenhang kann man auch die universelle Eigenschaft des Polynomrings betrachten.

Beispiel 9.14. φ nilpotent $\Leftrightarrow \exists m \geq 1\ \varphi^m = 0$
$\varphi^m = 0$ bedeutet $X^m.v = 0$ für alle $v \in V$.
Dann gilt

$$m_\varphi = X^m,$$

wobei m minimal mit $\varphi^m = 0$.

Satz 9.15. *Sei M endlich erzeugter freier A-Modul und $N \subseteq M$ Untermodul. Dann ist N frei, endlich erzeugt und* $\operatorname{Rang} N \leq \operatorname{Rang} M$.

Beweis. Induktion nach $n = \operatorname{Rang}(M)$.
Für $n = 1$: Sei $\{m\}$ Basis von M. Dann ist

$$\mu : A \to M, a \longmapsto am$$

ein Modulisomorphismus. Also ist $\mu^{-1}(N) \subseteq A$ Untermodul, d.h. ein Ideal von A.
Da A Hauptidealbereich $\Rightarrow \exists b \in A\ \mu^{-1}(N) = Ab$
O.B.d.A. $N \neq 0$. Dann $b \neq 0$ und $\{b\}$ ist Basis von Ab.
Also ist $\{\mu(b)\}$ Basis von N. Also ist N frei von Rang 1.
Für $n \geq 2$: Sei $(x_1, \ldots, x_n)$ Basis von M. Also gilt:

$$M = Ax_1 \bigoplus \cdots \bigoplus Ax_n$$

Betrachte die Projektion (A-Modulmorphismus):

$$\varphi : \mu \to Ax_1, \sum_{i=0}^{n} a_i x_i \longmapsto a_i x_i$$

Dann gilt:

$$\ker \varphi = Ax_2 \bigoplus \cdots \bigoplus Ax_n \simeq A^{n-1}$$

Betrachte $N_1 := N \cap \ker \varphi \subseteq \ker \varphi \simeq A^{n-1}$
Induktionsvoraussetzung $\Rightarrow N_1$ frei von Rang $\leq n-1$. Der Untermodul $\varphi(N) \subseteq Ax_1 \simeq A$ ist frei von Rang ≤ 1 (Fall $n = 1$)
Nun wenden wir Lemma 9.12 auf $\varphi|_N : N \twoheadrightarrow \varphi(N)$ mit $\ker \varphi|_N = N_i$.($\varphi(N)$ frei). Dies liefert uns Untermodul $P \subseteq N$ mit $N = N_1 \oplus P$, wobei $P \simeq \varphi(N)$ frei von Rang ≤ 1. Also ist N frei von Rang $\leq (n-1) + 1 = n$. □

Korollar 9.16. *Sei M endlich erzeugter A-Modul und $N \subseteq M$ Untermodul. Dann ist N endlich erzeugt.*

Beweis. Sei $x_1, \ldots, x_s$ Erzeugendensystem von M. Dann ist

$$A^s \to M : (a_1, \ldots, a_s) \longmapsto \sum_{i=1}^{s} a_i x_i$$

surjektiver Modulmorphismus.
$\overset{\text{Satz}}{\Rightarrow} \varphi^{-1}(N) \subseteq A^s$ frei und endlich erzeugt. $\Rightarrow N = \varphi(\varphi^{-1}(N))$ endlich erzeugt. □

Warnung: Wenn M endlich erzeugter freier A-Modul, $N \subseteq M$ Untermodul und $\operatorname{Rang} N = \operatorname{Rang} M$, dann gilt **nicht** notwendigerweise $N = M$!!!
Zum Gegenbeispiel: $A = \mathbb{Z}$, $M = \mathbb{Z}$, $N = \mathbb{Z}2$

Definition 9.17. Sei M ein A-Modul. Der *Torsionsmodul von M* ist definiert als

$$M_t := \{x \in M | \exists a \in A \backslash \{0\} \; ax = 0\}.$$

M heißt *torsionsfrei*, falls $M_t = \{0\}$, dh. aus $ax = 0$ und $a \neq 0$ folgt $x = 0$.
M heißt *Torsionsmodul*, falls $M_t = M$.

Beispiel 9.18. $A = \mathbb{Z}$, M abelsche Gruppe, aufgefasst als $\mathbb{Z}$-Modul. $M_t = \{x \in M | \operatorname{ord}(x) < \infty\}$

Beispiel 9.19. $A = \mathbb{Z}, M$ abelsche Gruppe, endlich erzeugt. $M_t = \{x \in M | \operatorname{ord}(x) < \infty\}$

Satz 9.20. *M Torsionsmodul $\Leftrightarrow$ M endlich.*

Beweis. " $\Leftarrow$ " klar
" $\Rightarrow$ " Sei $x_1, \ldots, x_s$ Erzeugendensystem von M und $m_i = \operatorname{ord}(x_i)$. Für alle $x \in M$ existiert $x = \sum_{i=1}^{s} a_i x_i, \quad 0 \leq a_i < m_i, a_i \leq \mathbb{N}$. Also $|M| = m_1 m_2 \ldots m_s$ □

Beispiel 9.21. $A = \mathbb{K}[X], V$ endlich dimensionaler $\mathbb{K}$-Vektorraum, $\varphi \in \operatorname{End}_{\mathbb{K}}(V)$,
$X.v = \varphi(v), v \in V$.

$$p(X)v = p(\varphi)(v)$$

V ist ein $\mathbb{K}[X]$ Torsionsmodul, da $\forall v \in V$ ist das Minimalpolynom $m_{\varphi.v} = 0$

Lemma 9.22. *(1) ${}^{M}/_{M_t}$ torsionsfrei*
(2) freie Moduln sind torsionsfrei

Beweis. (1) $M \to {}^{M}/_{M_t}$, $x \to \bar{x}$ kanonischer Morphismus.
Sei $a\bar{x} = 0, a \in A, a \neq 0 \Rightarrow ax \in M_t \Rightarrow \exists b \in A\backslash\{0\} : (ba)x = 0$
Da $ba \neq 0 \Rightarrow x \in M_t \Rightarrow \bar{x} = 0$. Also ${}^{M}/_{M_t}$ torsionsfrei.
(2) Sei $(X_i)_{i \in I}$ Basis von M. Sei $x = \sum_i b_i x_i$
$0 = ax = \sum_i ab_i x_i \Rightarrow \forall i \; ab_i = 0$ falls $a \neq 0$.
$\Rightarrow \forall i \; b_i = 0 \Rightarrow x = 0$ □

Satz 9.23. *Ein endlich erzeugter A-Modul M ist frei.*

Beweis. Sei $S \subseteq M$ ein endliches Erzeugendensystem von M. Wähle $x_1, \ldots, x_n \in S$ linear unabhängig mit maximalem n. Dann ist $N := Ax_1 \oplus \cdots \oplus Ax_n$ frei. Für $y \in S$ ist $y, x_1, \ldots, x_n$ linear abhängig, also existieren $b, a_1, \ldots, a_n \in A$, nicht alle 0, so dass

$$by + a_1 x_1 + \cdots + a_n x_n = 0$$

Dabei ist $b \neq 0$ (da sonst $x_1, \ldots, x_n$ linear abhängig).
Haben gezeigt: $\forall y \in S \; \exists b(y) \in A\backslash\{0\} \; b(y)_y \in N$
Setze $b := \prod_{y \in S} b(y) \neq 0$. Erhalten $bM \subseteq N$. Da N frei $\Rightarrow bM$ frei.
Der surjektive Morphismus $M \twoheadrightarrow bM, x \to bx$ ist injektiv, weil M torsionsfrei ist. Also $M \simeq bM$ frei. □

Beispiel 9.24. $M = \mathbb{Z}^2$
$S = \{(1,0), (0,1), (2,0)\}$ linear abhängig.
$N = \mathbb{Z}(1,0) \oplus \mathbb{Z}(2,0) = (2\mathbb{Z}) \times \mathbb{Z} \neq \mathbb{Z}^2$

Beispiel 9.25. $\mathbb{Q}$ als $\mathbb{Z}$-Modul ist torsionsfrei. $\mathbb{Q}$ ist nicht frei.
Fazit: Vor allem endlich erzeugt ist notwendig.

Korollar 9.26. *Sei M endlich erzeugter A-Modul. Dann existiert ein endlich erzeugter freier Untermodul $N \subseteq M$ mit $M = M_t \oplus N$*

Beweis. Lemma 9.22 M/M_t torsionsfrei
Satz 9.23 M/M_t frei
Lemma angewandt auf

$$\pi : M \to \underbrace{M/M_t}_{\text{frei}} \Rightarrow \exists \text{ Untermodul } N \subseteq M \text{ mit}$$

$$M = \underbrace{\ker \pi}_{M_t} \oplus N, N \simeq M/M_t \text{ frei}$$

□

Korollar 9.27. *Jede endlich erzeugte abelsche Gruppe M ist isomorph zu einer Gruppe $M_t \oplus \mathbb{Z}^r$, wobei M_t endlich ist und $r = \operatorname{Rang}(M/M_t)$*

9.3 Torsionsmoduln über Hauptidealbereichen

Im folgenden sei A Hauptidealbereich.

Definition 9.28. Sei M A-Modul, $x \in M$. Betrachte die Ideale
$\operatorname{ann}(x) = \{a \in A | a \cdot x = 0\}$
$\operatorname{ann}(M) = \{a \in A | \forall x \in M \quad ax = 0\}$
Diese heißen der *Annulator* von x bzw. von M.

Bemerkung 9.29. (1) $x \in M_t \Leftrightarrow \operatorname{ann}(x) \neq 0$
(2) Sei $x_1, \dots, x_s$ Erzeugendensystem von M. Dann $\operatorname{ann}(M) = \operatorname{ann}(x_1) \cap \dots \cap \operatorname{ann}(x_s)$

Sei $\operatorname{ann}(x_i) = (d_i)$. Dann $\operatorname{ann}(M) = (\operatorname{kgV}(d_1, \dots, d_s))$

Beispiel 9.30. $A = \mathbb{Z}$, M endlich erzeugte abelsche Gruppe, $x \in M$
$\operatorname{ann}(x) = (\operatorname{ord}(x))$
$\operatorname{ann}(M) = (\exp(M))$

Beispiel 9.31. $A = \mathbb{K}[X], V$ endlich dimensionaler $\mathbb{K}$-Vektorraum, $\varphi \in \operatorname{End}(V)$.
M zugehöriger $\mathbb{K}[X]$-Modul. Dann $\operatorname{ann}(M) = (m_\varphi)$ (Minimalpolynom)

Sei M endlich erzeugter Torsionsmodul, $M \neq 0$. Dann existiert $d \in A \backslash \{0\}$ mit $\operatorname{ann}(M) = (d)$
Man nennt d den *Annulator* von M (eindeutig bis auf Multiplikation mit Einheiten).

Definition 9.32. Sei M A-Modul, $p \in A$ prim. Der Untermodul

$$M(p) := \{x \in M | \quad \exists e \in \mathbb{N} \quad p^e x = 0\}$$

heißt die *p-primäre Komponente von M*

Beispiel 9.33. $A = \mathbb{Z}$, $p \in \mathbb{Z}$ prim, M endliche abelsche Gruppe
$\Rightarrow M(p)$ ist p-Sylowgruppe von M.

Bemerkung 9.34. (1) $\exists e \in \mathbb{N} \quad \operatorname{ann}(M(p)) = (p^e)$
(2) $M = \mathbb{N}_1 \oplus N_2$, $N_i \subseteq M$ Untermoduln
$p \in A$ prim $\Rightarrow M(p) = N_1(p) + N_2(p)$

Satz 9.35. *Sei M endlich erzeugter Torsionsmodul über A. Sei $a = p_1^{e_1} \dots p_r^{e_r}$ die Primfaktorzerlegung des Annulators a von M (d.h. p_i paarweise nicht assoziierte Primelemente, $e_i \in \mathbb{N}_{>0}$). Dann gilt:*
$M = M(p_1) \oplus \dots \oplus M(p_r)$
Weiter gilt:
$\operatorname{ann}(M(p_i)) = (p_i^{e_1})$ *und* $M(p) = 0$
für alle Primelemente, die nicht zu $p_1, \dots, p_r$ assoziiert sind gilt

$$\underbrace{\mathbb{Z}/_{p_1^{e_1} \dots p_r^{e_r}\mathbb{Z}}}_{M} \simeq \bigoplus_{i=1}^{r} \underbrace{\mathbb{Z}/_{p_i^{e_i}\mathbb{Z}}}_{M(p_i)}$$

Beweis. (Analogie zum Chinesischen Restsatz)
(1) Sei $a_i := \prod_{j \neq i} p_j^{e_j}$, also $d = p_i^{e_i} a_i$. Da $a_1, \dots, a_r$ teilerfremd $\Rightarrow (a_1, \dots, a_r) = (1) \Rightarrow \exists u_1, \dots, u_r \in A$ $1 = \sum_{i=1}^{r} u_i a_i$ Für $x \in M$ gilt $x = \sum_{i=1}^{r} u_i a_i x$.
Setzen $M_i := u_i a_i M$ Untermodul. Es gilt: $M = M_1 + \dots + M_r$
Weiter

$$p_i^{e_i} u_i a_i x = u_i d x = 0$$

$$(p_i^{e_i}) \subseteq \operatorname{ann}(M_i)$$

(2) Sei $x \in (M_1 + \dots M_{i-1} \cap M_i$. Dann $p_1^{e_1} \cdot \dots \cdot p_{i-1} \in \operatorname{ann}(x)$, $p_i^{e_i} \in \operatorname{ann}(x) \Rightarrow 1 \in \operatorname{ann}(x) \Rightarrow x = 0$
Es folgt: $M = M_1 \oplus \dots \oplus M_r$
(3) $M_i(p_i) = M_i$, da $p_i^{e_i} M_i = 0$. Weiter $M_i = 0$ falls $p \nsim p_i$ (**!!**)
Aus $M = M_1 \oplus \dots \oplus M_r \Rightarrow M(p) = M_1(p) \oplus \dots \oplus M_r(p)$ folgt
$M(p_i) = M_i$ für $p = p_i$
und $M(p) = 0$ für $p \nsim p1, \dots, p_r$
(4) Sei $\operatorname{ann}(M_i) = (p_i^{e_i'}) \Rightarrow (p_1^{e_1} \dots p_r^{e_r}) = (d) = (p1^{e_1'} \cdot \dots \cdot r^{e_r'}) \Rightarrow e_i = e_i'$ □

Definition 9.36. Ein Modul M heißt *p-primär*, falls $M = M(p)$ gilt und $M \neq 0$.

Im Weiteren werden wir nun solche p-primären Moduln analysieren.

Definition 9.37. Ein A-Modul M heißt *zyklisch*, wenn er von einem Element x erzeugt wird, dh.

$$M = Ax$$

Es gibt zwei Fälle:
(1) $\operatorname{ann}(M) = \operatorname{ann}(x) = 0$ Dann $\{x\}$ Basis von $M \Rightarrow$

$$M \xleftarrow{\sim} A \text{ frei von Rang f}$$

$$ax \leftarrow\!\shortmid a$$

(2)

$$\operatorname{ann}(M) = \operatorname{ann}(x) = (d) \neq (0)$$

Dann gilt $M \simeq {}^{A}/_{Ad}$, wobei $A \twoheadrightarrow M, a \mapsto ax$ und $\ker = \operatorname{ann}(x) = Ad$.
(Tipp: Vergleiche mit Beispiel $A = \mathbb{Z}$!)
Ein p-primärer zyklischer Modul ist isomorph zu ${}^{A}/_{Ap^e}$.
Ziel:

Zu zeigen, dass jeder endlich erzeugte p-primäre A-Modul M isomorph zu einer direkten Summe von zyklischen p-primären Moduln ist:

$$M \simeq {}^{A}\!/_{Ap^{r_i}} \oplus \cdots \oplus {}^{A}\!/_{Ap^{r_s}},$$

wobei O.B.d.A. $r_1 \geq \cdots \geq r_s \geq 1$.
Wir zeigen zunächst, dass $(r_1, \ldots, r_s)$ durch M eindeutig bestimmt ist.
Wir nennen $(r_1, \ldots, r_s)$ den *Typ von* M.

Allgemeine Überlegung:
Sei M ein A-Modul, $p \in A$ prim.
Wir betrachten nun den Untermodul $Mp := \{x \in M | px = 0\}$.
M_p ist in natürlicher Weise ein Vektorraum über dem Körper $\mathbb{K} := {}^{A}\!/_{Ap}$.
Falls M endlich erzeugter A-Modul, dan folgt: M_p endlich erzeugt $\Rightarrow \dim_{\mathbb{K}} M_p < \infty$
Offenbar gilt für A-Moduln M_i mit $i = 1, \ldots, t$:

$$(M_1 \oplus \cdots \oplus M_t)_p = (M_1)_p \oplus \cdots \oplus (M_t)_p$$

Für $M = {}^{A}\!/_{Ap^r}$, $r \geq d$ gilt

$$M_p = {}^{Ap^{r-1}}\!/_{Ap^r} \simeq {}^{A}\!/_{Ap} = \mathbb{K} \quad (*)$$

$$\Rightarrow \dim_{\mathbb{K}} M_p = 1$$

Folglich erfüllt $M = {}^{A}\!/_{Ap^{r_1}} \oplus \cdots \oplus {}^{A}\!/_{Ap^{r_s}}$:

$$\dim_{\mathbb{K}} M_p = s \text{ (Anzahl der Summanden)}$$

Lemma 9.38. *Sei M gegeben als ${}^{A}\!/_{Ap^{r_1}} \oplus \cdots \oplus {}^{A}\!/_{Ap^{r_s}}$ und*

$$M := {}^{A}\!/_{Ap^{r_1}} \oplus \cdots \oplus {}^{A}\!/_{Ap^{r_s}} \simeq {}^{A}\!/_{Ap^{m_1}} \oplus \cdots \oplus {}^{A}\!/_{Ap^{m_t}}$$

mit $r_1 \geq \cdots \geq r_s \geq 1$ und $m_1 \geq \cdots \geq m_t \geq 1$. Dann impliziert dies alles:
$s = t$ und $r_i = m_i$ für $1 \leq i \leq s$.

Beweis. Induktion nach $\sum_{i=1}^{s} r_i$
Der Start $\sum_{i=1}^{s} r_i = 0$ ist klar.
Sei $\sum_{i=1}^{s} r_i \geq 1$ also $s \geq 1$.
Wir wissen $\dim_{\mathbb{K}} M_p = s = t$.
Wir schreiben:

$$(r_1, \ldots, r_s) = (r_1, \ldots, r_\alpha, 1, \ldots, 1) \text{ mit } r_\alpha > 1$$

$$(m_1, \ldots, m_t) = (m_1, \ldots, m_\beta, 1, \ldots, 1) \text{ mit } m_\beta > 1$$

Aus $(*)$ folgt:

$$pM = \bigoplus_{i=0}^{\alpha} {}^{Ap}\!/_{Ap^{r_i}} \simeq \bigoplus_{i=0}^{\alpha} {}^{A}\!/_{Ap^{r_i-1}} \simeq \bigoplus_{i=0}^{\beta} {}^{A}\!/_{Ap^{m_i-1}}$$

Denn nach Induktionsvoraussetzung gilt: $\alpha = \beta$ und $r_i - 1 = m_i - 1$ für $1 \leq i \leq \alpha$.
Insgesamt folgt mit $s = t$, dass $r_i = m_i$ für $1 \leq i \leq s$. □

Wir zeigen als nächstes die Existenz solcher Zerlegungen.

Lemma 9.39. *Sei M A-Modul, $x \in M$* $\operatorname{ann}(x) = (a) \quad a \neq 0$
(1)

$$a = a_1 \cdot a_2 \Rightarrow \operatorname{ann}(a_1 x) = (a_2)$$

$$\operatorname{ord}(g) = a_1 \cdot a_2 \Rightarrow \operatorname{ord}(g^{a_1}) = a_2$$

(2) $b \in A$ teilerfremd zu $a \Rightarrow \operatorname{ann}(bx) = \operatorname{ann}(x)$

Beweis. Übung □

Bemerkung 9.40. *M p-primär $\Rightarrow M_p \neq 0$*

Beweis. Sei $x \in M, x \neq 0$.
$\operatorname{ann}(x) = (p^e), e \geq 1$
Es folgt mit dem Lemma 9.39:

$$\operatorname{ann}(p^{e-1}x) = (p) \text{also } 0 \neq p^{e-1}x \in M_p$$

□

Bemerkung 9.41. *$\varphi : M \to N$ A-Modulmorphismus, $x \in M$*
Dann gilt: $\operatorname{ann}(x) \subseteq \operatorname{ann}(\varphi(x))$
Bei abelschen Gruppen folgt auch noch: $\operatorname{ord}(\varphi(x))$ teilt $\operatorname{ord}(x)$.

Satz 9.42 (Struktursatz)**.** *Jeder endlich erzeugte p-primärer A-Modul M ist isomorph zu einer direkten Summe*

$$A/Ap_1^{r_1} \oplus \cdots \oplus A/Ap^{r_s}$$

von zyklischen p-primären M-Moduln, wobei $r_1 \geq r_2 \geq \cdots \geq r_s \geq 1$.
Der Typ $(r_1, \ldots, r_s)$ ist durch M eindeutig bestimmt.

Beispiel 9.43. *$A = \mathbb{Z}$*
M primitiv abelsch, endlich
$\mathbb{Z}/\mathbb{Z}p^{r_1} \oplus \cdots \oplus \mathbb{Z}/\mathbb{Z}p^{r_s} \simeq \mathbb{Z}_{p^{r_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{r_s}}$
(1) $\left[\mathbb{Z}_{p^3}, \mathbb{Z}_{p^2} \times \mathbb{Z}_p, \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p\right]$
(2) $\left[\mathbb{Z}_{p^2}, \mathbb{Z}_p \times \mathbb{Z}_p\right]$
(3) $\left[|M| = 18 = 2 \cdot 3^2 \Rightarrow M(2) \simeq \mathbb{Z}_2 \text{ und } M(3) \begin{cases} \simeq \mathbb{Z}_9 \\ \simeq \mathbb{Z}_3 \times \mathbb{Z}_3 \end{cases}\right]$

Index