0.1 Galoistheorie und Anwendungen

Definition 0.1 (Fixkörper)**.** Seien E, K Körper, ist $G \leq \mathrm{Aut}(E)$ eine Untergruppe, so heißt

$$E^G = \{\alpha \in E \mid \sigma(\alpha) = \alpha, \forall \sigma \in G\}$$

der Fixkörper von E unter G.

Bemerkung. $E^G \subseteq E$ ist ein Unterkörper

Beweis. (Übung) Sei $\alpha \in E^G \backslash \{0\}$, dann: $1 = \sigma(1) = \sigma(\alpha \cdot \alpha^{-1}) = \sigma(\alpha)\sigma(\alpha^{-1}), \forall \sigma \in G \implies \alpha^{-1} = \sigma(\alpha^{-1}) \forall \sigma \in G.$ □

Definition 0.2.

(a) $\Gamma_E := \{G \leq \mathrm{Aut}(E)\}$

(b) $\Sigma_E := \{K \subseteq E \mid K \text{ Unterkörper}\}$

(c) $\mathrm{Inv}_E : \Gamma_E \to \Sigma_E, G \mapsto E^G = \mathrm{Inv}_E(G)$

(d) $\mathrm{Gal}_E : \Sigma_E \to \Gamma_E, K \mapsto \mathrm{Gal}_E(K) := \mathrm{Aut}_K(E) = \{\sigma \in \mathrm{Aut}(E) \mid \sigma|_K = \mathrm{id}_K\}$

Lemma 0.3. *(a) Die Abbildungen* Inv_E *und* Gal_E *sind inklusionsumkehrend.*

(b) $\mathrm{Inv}_E(\mathrm{Gal}_E(K)) \supseteq K$

(c) $\mathrm{Gal}_E(\mathrm{Inv}_E(G)) \supseteq G$

Beweis. TODO □

Bemerkung. Ziel: Unter geeigneten Einschränkungen an G bzw. K wollen wir "Gleichheit" in (b) und (c) (für $\Gamma_{E/K}$ und $\Sigma_{E/K}$), dann erhalten wir eine Bijektion:

$$G \in \Gamma_{E/K} \overset{1-1}{\longleftrightarrow} F \in \Sigma_{E/K}$$

Satz 0.4. *Für eine endliche Körpererweiterung $E \supset K$ sind äquivalent:*

(i) E ist Zerfällungskörper eines seperablen Polynoms in $K[X]$

(ii) $E \supseteq K$ ist normal und seperabel.

(iii) $E \supseteq K$ ist seperabel und $\mathrm{Hom}_K(E, \overline{E}) = \mathrm{Aut}_K(E)$

(iv) $\#\,\mathrm{Aut}_K(E) = [E : K]$

Beweis. TODO. □

Definition 0.5 (Galoiserweiterung/Galoisgruppe)**.** Erfüllt $E \supseteq K$ Oberkörper mit $[E : K] < \infty$ die äquivalenten Bedingungen aus Satz 4, so heißt E/K Galoissch (oder eine Galoiserweiterung von K) (genauer $E \supseteq K$ ist endlich Galoissch)In diesem Fall definiert man die **Galoisgruppe** von E über K als

$$\mathrm{Gal}(E/K) := \mathrm{Aut}_K(E) = \mathrm{Gal}_E(K)$$

Korollar 0.6. *Sei $E \supseteq K$ Galoissch und sei $F \subseteq E$ Unterkörper mit $F \supseteq K$, dann:*

(a) $E \supseteq F$ *ist Galoissch.*

(b) Es sind äquivalent:

(i) $F \supseteq K$ *Galoissch*

(ii) $F \supseteq K$ *normal*

(iii) $\forall \sigma \in \mathrm{Gal}(E/K) : \sigma(F) = F$.

Beweis. TODO □

Satz 0.7. *Sei* $G \leq \mathrm{Aut}(E)$ *endliche Untergruppe, dann gelten*

(a) $[E : E^G] = \#G$

(b) $E \supseteq E^G$ *ist Galoissch und* $G : \mathrm{Gal}(E/E^G) = \mathrm{Aut}_{E^G}(E)$

Beweis. TODO □

Korollar 0.8. $G \leq \mathrm{Aut}(E)$ *endliche Untergruppe* $\implies G = \mathrm{Gal}_E(\mathrm{Inv}_E(G))$

Korollar 0.9. *Sei* $E \supseteq K$ *Galoissch, dann gilt* $\mathrm{Inv}_E(\mathrm{Gal}_E(K)) = K$

Beweis. TODO □

Übung 0.10. Sei $G \leq \mathrm{Aut}(E)$ endliche Untergruppe und $K = E^G$, G wirkt auf E durch

$$G \times E \to E, (\sigma, \alpha) \mapsto \sigma(\alpha)$$

Sei $\alpha \in E$ und $A = G\alpha$ die G-Bahn durch α, definiere $\mu := \prod_{\beta \in A}(X - \beta)$, dann gelten: $\mu \in K[X], \mu = \mu_{\alpha,K}$ und μ ist seperabel.

Satz 0.11 (Hauptsatz der Galoistheorie)**.** *Sei* $E \supseteq K$ *Galoissch mit Galoisgruppe* $G = \mathrm{Gal}(E/K)$*, seien*

$$\Gamma_{E/K} = \{H \leq G\}, \quad \Sigma_{E/K} = \{F \subseteq E \text{ Unterkörper} \mid K \subseteq F\}$$

dann gelten:

(a) Die Abbildungen:

$$\Gamma_{E/K} \underset{\mathrm{Gal}(E/F) \hookleftarrow F : \mathrm{Gal}_E}{\overset{\mathrm{Inv}_E : H \mapsto E^H}{\rightleftarrows}} \Sigma_{E/K}$$

sind zueinander inverse Bijektionen.

(b) Inv_E *und* Gal_E *sind inklusionsumkehrend.*

(c) Es gelten $[E : E^H] = \#H$ *und* $\#\,\mathrm{Gal}(E/F) = [E : F]$

(d) Sei $F \in \Sigma_{E/K}$ *und* $H = \mathrm{Gal}(E/F)$*, dann:*

(i) $\forall \sigma \in G$ *gilt*

$$\sigma(F) \underset{\mathrm{Inv}_E(\cdot)}{\overset{\mathrm{Gal}_E(\cdot)}{\rightleftarrows}} \sigma H \sigma^{-1}$$

d.h. $E^{\sigma H \sigma^{-1}} = \sigma(E^H) = \sigma(F)$ *und* $\mathrm{Gal}(E/\sigma(F)) = \sigma\,\mathrm{Gal}(E/F)\sigma^{-1}$

(ii) Die Abbildung

$$\begin{aligned} \psi : {}^{N_G(H)}\!/_H &\longrightarrow \mathrm{Aut}_K(F) \\ \sigma H &\longmapsto \sigma|_F \end{aligned}$$

ist wohl-definiert und ein Gruppenisomorphismus.

(iii) $F \supseteq K$ *Galoissch* $\iff$ $H \trianglelefteq G$ *ist Normalteiler, in diesem Fall definiert* ψ *einen Gruppenisomorphismus*

$$\begin{aligned} \psi : {}^{G}\!/_H &\longrightarrow \mathrm{Gal}(F/K) \\ \sigma H &\longmapsto \sigma|_F \end{aligned}$$

Wiederholung. $N_G(H) := \{g \in G \mid gHg^{-1} = H\}$

Beweis. TODO □

Korollar 0.12. $E \supseteq K$ *endlich seperabel, dann gilt:*

$$M = \{F \subseteq E \text{ Unterkörper} \mid K \subseteq F\} \text{ ist endlich.}$$

Beweis. TODO □

Satz 0.13. *Jede endliche Gruppe* G *ist die Galoisgruppe für eine geeignete Galoiserweiterung* $E \supseteq K$*.*

Beweis. TODO □

Bemerkung 0.14.

$$\begin{aligned} \psi : G = \mathrm{Gal}(E/K) &\longrightarrow \mathrm{Bij}(\{\alpha_1, \ldots, \alpha_n\}) \cong S_n \\ \sigma &\longmapsto \sigma|_{\{\alpha_1, \ldots \alpha_n\}} \end{aligned}$$

ist wohl-definiert und ein injektiver Gruppenhomomorphismus. D.h. G ist isomorph zu einer Untergruppe von S_n. Ist f irred. so wirkt G transitiv.

Beispiel 0.15. Sei $E \subseteq \mathbb{C}$ der Zerfällungskörper über $\mathbb{Q}$ zu $f = X^4 - 5 \in \mathbb{Z}[X] \subseteq \mathbb{Q}[X]$. Wir wissen:

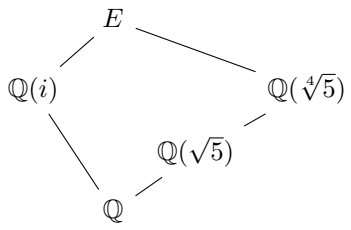
(a) f seperabel ($\mathbb{Q}$ perfekt)

(b) f irred. (Eisenstein mit $p = 5$)

(c) Nullstellenmenge von f ist $Z = \{\pm\sqrt[4]{5}, \pm i\sqrt[4]{5}\}$

(d) $E = \mathbb{Q}(Z) = \mathbb{Q}(i, \sqrt[4]{5})$

(e) Einige Unterkörper von E:



(f) $[E : \mathbb{Q}] = 8$. f ist irred. als Polynom in $\mathbb{Q}(i)[X]$ und $E \supseteq \mathbb{Q}(i)$ ist der Stammkörper zu f. (und auch der Zerfällungskörper von f über $\mathbb{Q}(i)$)

(g) $\mathbb{Q}(i) \supseteq \mathbb{Q}$ ist Galoissch, denn $\mathbb{Q}(i) \supseteq \mathbb{Q}$ ist der Zerfällungskörper von X^2+1.

(h) $G = \mathrm{Gal}(E/Q)$ ist eine Gruppe mit 8 Elementen. G wirkt auf $Z \overset{\#Z}{\Longrightarrow} G$ ist isomorph zu einer Untergruppe von S_4

(i) $[E : \mathbb{Q}(i)] = 4$ (nach (f) und (a)) und $N := \mathrm{Gal}(E/\mathbb{Q}(i)) \subseteq \mathrm{Bij}(Z) \cong S_4$ und sie ist transitiv, da $f \in \mathbb{Q}(i)[X]$ irred. Sei $\rho \in N$ der Automorphismus mit $\rho(\underbrace{\sqrt[4]{5}}_{\alpha_1}) = \underbrace{i\sqrt[4]{5}}_{\alpha_2}$ (Gruppe transitiv).

$$\Longrightarrow \rho^2(\sqrt[4]{5}) = \rho(i\sqrt[4]{5}) \underset{\rho|_{\mathbb{Q}(i)}=\mathrm{id}_{\mathbb{Q}(i)}}{=} i\rho(\sqrt[4]{5}) = ii\sqrt[4]{5} = \underbrace{-\sqrt[4]{5}}_{\alpha_3}$$

analog ist

$$\rho^3(\sqrt[4]{5}) = \underbrace{-i\sqrt[4]{5}}_{\alpha_4}, \quad \rho^4 = \mathrm{id}_E$$

d.h. $N = \langle\rho\rangle$ unr ρ hat Ordnung 4 ($N \cong {}^{\mathbb{Z}}\!/_{4\mathbb{Z}}$)

(j) Wir wissen $N \trianglelefteq G$, da $\mathbb{Q}(i) \supseteq \mathbb{Q}$ Galoissch ($\Longrightarrow \mathrm{Gal}(E/\mathbb{Q}(i)) \trianglelefteq \mathrm{Gal}(E/\mathbb{Q})$ normal)

$$\overset{\text{als U.G von } S_4}{\Longrightarrow} G \leq N_{S_4}(\underbrace{N}_{\langle(1\ 2\ 3\ 4)\rangle})$$

Behauptung: $\#N_{S_4}(N) = 8 \iff G = N_{S_4}(N)$ ist vollständig bestimmt.

Beweis. Sei $\tau \in N_{S_4}(N) \implies \tau\rho\tau^{-1} \in \langle\rho\rangle \implies \tau\rho\tau^{-1} \in \{\rho, \rho^{-1}\}$

Fall 1: Betrachte $\tau\rho\tau^{-1} = \rho$ ($\iff \tau(1\ 2\ 3\ 4)\tau^{-1} = (1\ 2\ 3\ 4)$)

$$(\tau(1)\ \tau(2)\ \tau(3)\ \tau(4)) = (1\ 2\ 3\ 4)$$

Zykeldarstellung ist eindeutig bis auf Zykelpermutation der Einträge.

$$\Longrightarrow \tau = \mathrm{id}, \tau = \rho, \underbrace{\tau = \rho^2}_{(\tau(1)\ \tau(2)\ \tau(3)\ \tau(4))=(3\ 4\ 1\ 2)}, \tau = \rho^3$$

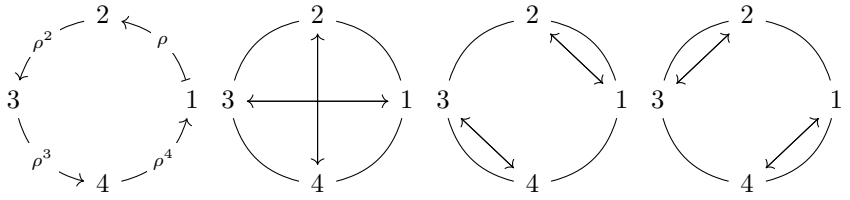
$\iff \tau \in \langle\rho\rangle$.

Fall 2: Für $\tau\rho\tau^{-1} = \rho^{-1} \iff (\tau(1)\ \tau(2)\ \tau(3)\ \tau(4)) = (4\ 3\ 2\ 1)$ also $(= (3\ 2\ 1\ 4) = (2\ 1\ 4\ 3) = (1\ 4\ 3\ 2)) \implies$ 4 Möglichkeiten für τ :

$$\tau \in \{\underbrace{(1\ 3)}_{=:\sigma}, (2\ 4), (1\ 4)(2\ 3), (1\ 2)(4\ 3)\} = \sigma \cdot \langle\rho\rangle$$

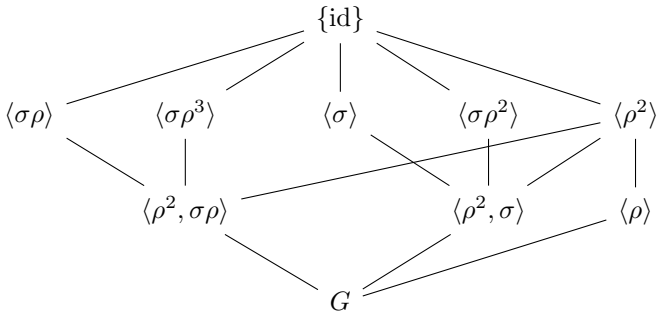
□

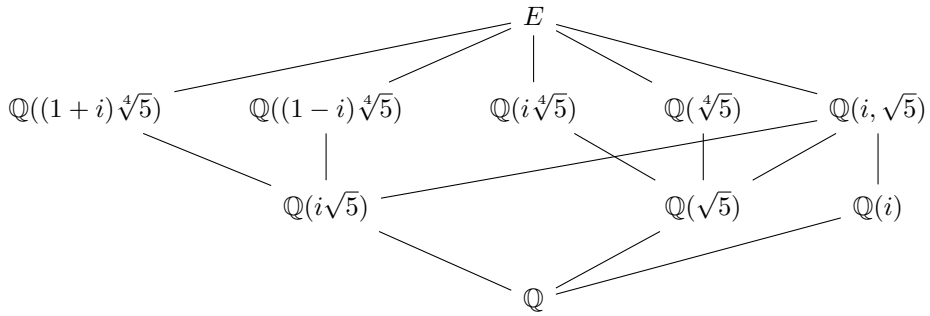
Fazit: $G = N_{S_4}(N)$ hat 8 Elemente. Veranschaulichung der Permutationen $(1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 2)(3\ 4)$ und $(1\ 4)(2\ 3)$



$G \cong D_4$ Diedergruppe auf regulärem 4-Eck.

Untergruppenverband:





5 Unterkörper mit $[E : F] = 2, [F : \mathbb{Q}] = 4$ und 3 Unterkörper mit $[F : \mathbb{Q}] = 2$

0.2 Beispielklassen von Galoiserweiterungen

0.2.1 Endliche Körper

Sei p Primzahl und $\overline{\mathbb{F}}_p$ ein (fest gewählter) algebraischer Abschluss von $\mathbb{F}_p$. Sei $\varphi : \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p, \alpha \mapsto \alpha^p$, es gilt $\varphi \in \mathrm{Aut}(\overline{\mathbb{F}}_p)$. φ ist surjektiv, da $\overline{\mathbb{F}}_p$ perfekt (als algebraischer Abschluss) und φ injektiv, Homom. klar
$\Longrightarrow$ Es gibt auch φ^{-1}, d.h. jedes $\alpha \in \overline{\mathbb{F}}_p$ besitzt eine eindeutige p-te Wurzel.
$\Longrightarrow$ $\forall m \in \mathbb{Z}$ haben $\varphi^m \in \mathrm{Aut}(\overline{\mathbb{F}}_p)$, d.h. $\mathbb{Z} \cong \{\varphi^m : m \in \mathbb{Z}\} \leq \mathrm{Aut}(\overline{\mathbb{F}}_p)$ ist Untergruppe.

Satz 0.16.

(a) $\mathbb{F}_{p^n} := (\overline{\mathbb{F}}_p)^{\varphi^n} = \{\alpha \in \overline{\mathbb{F}}_p \mid \varphi^n(\alpha) = \alpha^{p^n} \overset{!}{=} \alpha\} \subseteq \overline{\mathbb{F}}_p$ *ist Unterkörper.*

(b) $\#\mathbb{F}_{p^n} = p^n$ *und* $\mathbb{F}_{p^n}$ *ist der Zerfällungskörper von* $f_n := X^{p^n} - X \in \mathbb{F}_p[X]$.

(c) Bis auf Isomorphie $\exists!$ *Körper mit* p^n *Elementen.*

(d) Für $m, n \in \mathbb{N}$ *gilt:* $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n} \iff m \mid n$

(e) Gilt $m \mid n$*, so ist* $\mathbb{F}_{p^n} \supseteq \mathbb{F}_{p^m}$ *Galoissch mit Gruppe* $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m}) = \langle \varphi^m \rangle$ *ist zyklisch von der Ordnung* $\ell = \frac{n}{m}$.

Beweis. TODO □

0.2.2 Einheitswurzelkörper (Kreisteilungskörper)

Definition 0.17. Sei $n \in \mathbb{N}$, ein Element $\rho \in \overline{K}^\times$ heißt primitive n-te Einheitswurzel (EW) $\iff \mathrm{ord}(\rho) = n$ als Element der Gruppe $(\overline{K}^\times, 1, \cdot)$.

Lemma 0.18. *Sei* $G \leq (\overline{K}^\times, 1, \cdot)$ *endliche Untergruppe, dann ist* G *zyklisch.*

Beweis. Sei $n = \#G$ und $n' := \exp(G)$, wir wissen $n' \mid n$. Da G abelsch: G zyklisch $\iff n' = n$. Annahme $n' < n$ ($\implies \forall \alpha \in G$ gilt $\alpha^{n'} - 1 = 0$)

$$\implies G \subseteq \underbrace{\{\alpha \in K \mid \alpha \text{ ist Nst. von } X^{n'} - 1\}}_{\text{Menge hat höchstens Kardinalität } n'} \implies n = \#G \leq n' \text{ Widerspruch.}$$

$\implies n' = n$ (wissen schon n' teilt n). □

Beispiel. $\mathbb{F}_{p^n}^\times$ ist zyklische Gruppe der Ordnung p^{n-1}

Proposition 0.19. *Sei* $p = \mathrm{char}\, K$*, sei* $n \in \mathbb{N}$*, dann:* $\overline{K}$ *enthält eine primitive* n*-te Einheitswurzel* $\iff p \nmid n$.

Beispiel.

(a) $\mathrm{char}\, K = 0 \implies \overline{K}$ enthält primitive n-te Einheitswurzel für alle $n \in \mathbb{N}$

(b) $K = \mathbb{C} \implies e^{2\pi i/n}$ ist primitive n-te Einheitswurzel. Die Elemente

$$\{(e^{2\pi i/n})^j \mid j \in \{0, \ldots, n-1\}\}$$

bilden ein regelmäßiges n-Eck, deswegen heißt auch $\mathbb{Q}(e^{2\pi i/n})$ n-ter Kreisteilungskörper (über $\mathbb{Q}$). $e^{2\pi i/n}$ ist algebraisch, da Nst. von $X^n - 1$

Beweis (von Proposition 19). TODO. □

Proposition 0.20. *Sei* $\zeta \in \overline{K}^\times$ *primitive* n*-te Einheitswurzel (insbesondere* $p = \mathrm{char}\, K \nmid n$*), dann:*

(a) $K(\zeta)$ *ist Zerfällungskörper des seperablen Polynoms* $h_n = X^n - 1$ *über* K *und insbesondere ist* $K(\zeta)$ *Galoissch über* K.

(b) Sei $H := \{\xi \in \overline{K}^\times \mid \xi^n = 1\}$*, dann gibt es zu* ξ *ein eindeutiges* $n_\xi \in \{1, \ldots, n\}$ *mit* $\zeta^{n_\xi} = \xi$.

(c) Die Abbildung

$$G := \mathrm{Gal}(K(\zeta)/K) \to \left(\mathbb{Z}/n\mathbb{Z}\right)^\times, \sigma \mapsto n_{\sigma(\zeta)} \mod n$$

ist wohl-definiert und ein Gruppenmonomorphismus. Insbesondere ist G abelsch (also auflösbar)

Beweis. TODO.

□

Satz 0.21.

(a) ϕ_n ist irred. in $\mathbb{Z}[X]$

(b) $\mathbb{Q}(\zeta_n) : \mathbb{Q} = \mathrm{Grad}\,\phi_n = \#\mathbb{Z}_n^\times$

(c) $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to \left(\mathbb{Z}/n\mathbb{Z}\right)^\times, \sigma \mapsto \overline{m}_\sigma$ aus Bew. von 20 ist Gruppenisomorphismus.

Beweis. TODO.

□

0.2.3 Galoiserweiterungen von Grad p (eine Primzahl)

Satz 0.22 (Kummererweiterungen)**.** *Gelte p Primzahl, $p \nmid \mathrm{char}\, K$, gelte: K enthält eine primitive p-te Einheitswurzel ζ_p (d.h. $K^\times \supseteq N_p := \langle \zeta_p \rangle$ und $N_p \cong \mathbb{Z}/p\mathbb{Z}$). Sei $f = X^p - a, a \in K$, sei E ein Zerfällungskörper von f und $b \in \overline{K}$ eine Nullstelle von f. Dann:*

(a) f hat die Nullstelle $b \cdot \zeta_p^i, i \in \{0, \dots, p-1\}$

(b) $E = K(b)$ ist Zerfällungskörper von f und $E \supseteq K$ Galoissch. (f seperabel)

(c) Die Abbildung $\varphi : \mathrm{Gal}(E/K) \to N_p, \sigma \mapsto \frac{\sigma(b)}{b}$ ist wohl-definiert und ein Gruppenmonomorphismus.

(d) Es sind äquivalent:

- *(i) $[E : K] = p$*
- *(ii) f ist irred.*
- *(iii) f hat keine Nullstelle in K*
- *(iv) φ ist ein Isomorphismus.*

(e) Ist Umgekehrt $E \supseteq K$ Galoissch mit $\mathrm{Gal}(E/K) \cong \mathbb{Z}/p\mathbb{Z}$, so ist E ein Zerfällungskörper über K eines irred. Polynoms der Form $X^p - c \in K[X]$, wobei $c \in K^\times/K^{\times p}$.

Proposition 0.23 (Übung, Lineare Algebra)**.** *Sei V ein endlich dimensionaler K-Vektorraum und $\sigma \in \mathrm{Aut}_K(V)$ mit $\mathrm{ord}(\sigma) = p$, dann:*

(a) Das Minimalpolynom von σ ist $X^p - 1$

(b) *Gilt $p \neq \operatorname{char} K$, so besitzt σ einen Eigenwert ζ, welcher eine primitive p-te Einheitswurzel ist.*

(c) *Gilt $p = \operatorname{char} K$, so enthält die Jordanform von σ einen $d \times d$-Block folgender Form mit $d > 1$*

$$\begin{pmatrix} 1 & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & 1 \end{pmatrix}$$

Notation. Für $m \in \mathbb{N}$ mit $\operatorname{char} K \nmid n$, so sei $N_k := \{\zeta \in \overline{K} \mid \zeta^n = 1\}$ $(= {}^{\mathbb{Z}}\!/_{n\mathbb{Z}})$

Satz 0.24 (Kummererweiterungen)**.** *Sei p primzahl mit $p \nmid \operatorname{char} K$ und gelte: K enthält eine primitive p-te Einheitswurzel ζ_p (d.h. $K^\times \supseteq N_p := \langle \zeta_p \rangle$ und $N_p \cong {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$) und $b \in \overline{K}$ eine Nst. von f, dann:*

(a) *f hat die Nst. $b \cdot \zeta_p^i, i \in \{0, \ldots, p-1\}$*

(b) *$E = K(b)$ ist ZK von f und E/K galoissch. (f seperabel)*

(c) *Die Abbildung $\varphi : \operatorname{Gal}(E/K) \to N_p, \sigma \mapsto \frac{\sigma(b)}{b}$ ist wohl-def Gruppenn-monomorphismus.*

(d) *Es sind äquivalent:*

  (i) $[E : K] = p$
  (ii) *f ist irred.*
  (iii) *f hat keine Nst in K*
  (iv) *φ ist ein Isomorphismsus.*

(e) *Ist umgekehrt E/K galoissch mit $\operatorname{Gal}(E/K) \cong \mathbb{Z}_p$, so ist E ZK über K eines irred. Polynoms der Form $X^p - c \in K[X]$ (wobei $c \in K^\times \setminus K^{\times p}$)*

Satz 0.25 (Artin-Schreier Erweiterungen)**.** *Sei $p = \operatorname{char} K > 0, f = X^p - X - a \in K[X]$ und sei E/K der ZK von f in $\overline{K}$ und sei $\beta \in E$ ein Nst. von f, dann:*

(a) *$E = K(\beta)$ und $T = \{\beta + i \cdot 1_K\}, i$ $in\{0, \ldots, p-1\}$ ist die Nullstellenmenge von f.*

(b) *E/K ist galoiisch*

(c) *$\varphi : \operatorname{Gal}(E/K) \to \mathbb{F}_p, \sigma \mapsto \sigma(\beta) - \beta$ ist ein Gruppenmonom. ($\mathbb{F}_p$ sei identifiziert mit dem Primkörper von K)*

(d) *Es sind äquivalent*

  (i) $[E : K] = p$
  (ii) *f ist irred.*
  (iii) *f hat keine Nst. in K*
  (iv) *φ ist bijektiv*
  (v) *$a \in K \setminus y(K)$ für $y : K \to K$ der Gruppenhom. $X \mapsto X^p - X$*

(e) *Ist Umgekehrt F/K galoissch vom Grad p, so ist F ZK eines Polynoms der Form $X^p - X - b \in K[X]$ mit $b \in K \setminus y(K)$ (verwendet z.B. 23c)*

0.3 Auflösbarkeit durch Radikale

Definition 0.26. Sei $p = \operatorname{char} K \geq 0$,

(i) Eine Kette von Körpererweiterungen $K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n$ heißt:

(a) Wurzelturm $\iff$ für $i \in \{1, \ldots, n\}$ existieren $\alpha_i \in K_i$ und $e_i \in \mathbb{N} \setminus p\mathbb{N}$ sodass $K_i = K_{i-1}(\alpha_i)$ und $\alpha_i^{e_i} \in K_{i-1}$.

(b) Quadratwurzelturm $\iff$ $p \neq 2$ und für $i \in \{1, \ldots, n\}$ existieren $\alpha_i \in K_i$ mit $\alpha_i^2 \in K_{i-1}$ und $K_i = K_i(\alpha_i)$.

(ii) Ein Oberkörper E/K heißt (Quadrat-)Wurzelerweiterung $\iff \exists$ (Quadrat-)Wurzelturm wie in (i) mit $E \subseteq K_n$

(iii) $f \in K[X]$ heißt auflösbar durch Radikale (Wurzelausdrücke) $\iff$ der ZK von f ist eine Wurzelerweiterung.

Notation. QW = Quadratwurzel und W- = Wurzel

Bemerkung (Übung)**.** Wegen $e_i \in \mathbb{N} \setminus p\mathbb{N}$ ist $K_i \supseteq K_{i-1}$ stets seperabel ($X^{e_i} - \alpha_i^{e_i} \in K_{i-1}[X]$)

Lemma 0.27. *Seien $E, E' \subseteq \overline{K}$ Oberkörper von K, dann:*

(a) Ist E/K eine (Q)W-Erweiterung und $\sigma \in \operatorname{Hom}_K(E, \overline{E})$, so ist $\sigma(E) \supseteq K$ eine (Q)W-Erweiterung

(b) Sind E, E' (Q)W-Erweiterungen von K, so auch $E[E'] = E'[E]$

(c) Ist E/K eine Q(W)-Erweiterung, so ist die normale Hülle von E eine (Q)W-Erweiterung von K.

Bemerkung. Gilt $E' = K[\alpha_1, \ldots, \alpha_n]$, so hat man $E[E'] = E[\alpha_1, \ldots, \alpha_n]$

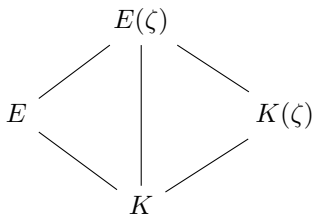
Beispiel 0.28. Sei $n \in \mathbb{N}$ mit $p \nmid n$ und $\zeta \in \overline{K}$ eine primitive n-te EW, dann ist $K[\zeta] \supseteq K$ eine W-Erweiterung ($\zeta^n = 1 \in K$)

Bemerkung 0.29 (Übung)**.** Sei $\zeta \in \overline{K}$ eine primitive n-te EW, und $E \subseteq \overline{K}$ ein Oberkörper von K, mit $[E : K] < \infty$, dann:

(a) Die Abbildung $\varphi : \operatorname{Gal}(E(\zeta)/E) \to \operatorname{Gal}(K(\zeta)/K), \sigma \mapsto \sigma|_{K(\zeta)}$ ist wohl def und ein Gruppenmonom.

(b) $[E(\zeta) : E]$ teilt $[K(\zeta) : K]$

(c) $[E(\zeta) : K]$ teilt $[E : K]$



Satz 0.30. *Für eine Galoiserweiterung E/K sind äquivalent:*

(i) E/K *ist Wurzelerweiterung*

(ii) $\mathrm{Gal}(E/K)$ *ist auflösbar und* $\exists m \in \mathbb{N}, p \nmid m : p \nmid [E[N_m] : K[N_m]]$

Bemerkung. Im Fall $p = 0$ entfällt.

Korollar 0.31. *Sei* $f \in K[X] \backslash K$ *seperabel mit ZK* E_f/K*, dann:* f *ist auflösbar durch Radikale* $\overset{5.30}{\iff}$ $\mathrm{Gal}(E_f/K)$ *ist auflösbar und* $\exists m$ *(mit* $\mathrm{char}\, K \nmid m$*), sodass* $\mathrm{char}\, K \nmid [E_f(\zeta_m) : K(\zeta_m)]$.

In den Übungen: $\exists f \in \mathbb{Q}[X] \setminus \mathbb{Q}, \deg f = 5, \mathrm{Gal}(\mathbb{Q}_f/\mathbb{Q}) \cong S_5 \implies f$ *nicht auflösbar durch Radikale.*

Andersherum: Alle Untergruppen von S_n *für* $n \leq 4$ *sind auflösbar (Ordnung* < 60*)* $\implies$ *ist* $f \in \mathbb{Q}[X] \setminus \mathbb{Q}$ *irred. vom Grad* $n \leq 4$*, so ist* f *auflösbar durch Radikale* $\implies$ *Die allgemeine Gleichung vom Grad* 5 *(oder* $n \geq 5$*) ist nicht auflösbar.*

Bemerkung 0.32. Die Galoistheorie hilft auch, die Lösungsformeln zu finden ($n \leq 4$) (Hungerford - Algebra).

0.4 Konstruierbarkeit mit Zirkel und Lineal

Sei S eine endliche Teilmenge der reellen Ebene $\mathbb{R}^2$ (üblicherweise $S = \{(0,0),(1,0)\}$), Frage: Welche Punkte der Ebene lassen sich mit Zirkel und Lineal aus S konstruieren?
Konkrete Fragen (alle Konstr. mit Zirkel und Lineal):

A) Lassen sich beliebige Winkel 3-teilen?

B) Kann ein zum Einheitskreis flächengleiches Quadrat konstruieren? (Quadratur des Kreises)

C) Kann man die Seitenlänge eines Würfels mit Volumen 2 konstruieren?

D) Für welche $n \in \mathbb{N}$ kann man ein regelmäßiges n-Eck konstruieren.

Im Weiteren: Wir identifizieren R^2 mit $\mathbb{C}$ und nehmen an, $0, 1 \in S \subset \mathbb{C}$ mit der Metrik $d(z, z') = |z - z'|$.

- Für $P \neq Q$ in $\mathbb{C}$ sei $\overline{PQ}$ die Gerade durch P und Q
- Für $P \in \mathbb{C}, r \in \mathbb{R}_{\geq 0}$ sei $C_r(P) = \{z \in \mathbb{C} \mid |z - P| = r\}$ die Kreislinie um P zum Radius r.

Definition 0.33 (Elementare Konstruktionen mit Zirkel und Lineal)**.** Zu $P_1 \neq P_2, P_3 \neq P_4, P_5 \neq P_6$ in S konstruiere

(1) Schnittpunkt $\overline{P_1P_2} \cap \overline{P_3P_4}$

(2) Schnittpunkte $\overline{P_1P_2} \cap C_r(P_5), r = |P_6 - P_5|$

(3) Schnittpunkte $C_{r_1}(P_1) \cap C_{r_3}(P_3), r_1 = |P_1 - P_2|, r_3 = |P_3 - P_4|$

Notation. Zu geg. S definiere $\widetilde{S} = S \cup$ Menge der aus S elementar konstruierbaren Punkte.

Definition 0.34. (rekursiv) $S_0 = S$, $S_{n+1} = \widetilde{S}_n$ und $C(S) = \cup_{n\in\mathbb{N}_0} S_n \subseteq \mathbb{C}$ Menge aller aus S konstruierbaren Punkte.

Beispiel 0.35. Folgende Konstruktionen sind mit Zirkel und Lineal durchführbar (siehe Schule Klasse 9)

(a) Die Parallele zu einer Geraden durch einer geg. Punkt

(b) Die Senkrechte zu einer Geraden durch einer geg. Punkt

(c) die Mittepunkt zu 2 geg. Punkten

(d) Das Spiegelbild eines Punktes an einer Geraden

(e) Die Summe von Winkeln

(f) Die Halbierung von Winkeln

(g) Die Negation von Winkeln

Lemma 0.36. *Seien $z, z_1, z_2 \in C(S), S \supseteq \{0,1\}, z \neq 0$, dann:*

(a) $z_1 + z_2 \in C(S)$

(b) $-z \in C(S)$

(c) $\Re(z), \Im(z), \overline{z} \in C(S)$

(d) $|z| \in C(S)$

(e) $|z_1| \cdot |z_2|$ *und* $z_1 \cdot z_2 \in C(S)$

(f) $|z|^{-1}, z^{-1} \in C(S)$

(g) $\sqrt{|z|} \in C(S)$

(h) $\{\xi \in \mathbb{C} \mid \xi^2 = z\} \subseteq C(S)$ *(2 Punkte in $\mathbb{C}$)*

Satz 0.37. *Sei $\overline{S} = \{\overline{z} \mid z \in S\}$, dann gelten:*
$C(S)$ ist ein Unterkörper von $\mathbb{C}$ der $C(S \cup \overline{S})$ enthält.
$z \in C(S) \iff \mathbb{Q}(S \cup \overline{S})(z)$ ist eine QW-Erweiterung von $\mathbb{Q}(S \cup \overline{S})$

Korollar 0.38. *Für $S = \{0,1\}$ sind äquivalent:*

(a) $z \in C(S)$

(b) $\mathbb{Q}(z)/\mathbb{Q}$ *ist eine QW-Erweiterung von* $\mathbb{Q}$

(c) z *ist algebraisch über* $\mathbb{Q}$ *und der ZK E von $\mu_{z,\mathbb{Q}}$ erfüllt $[E : \mathbb{Q}]$ ist 2-Potenz*

(d) z *ist algebraisch über* $\mathbb{Q}$ *und für E aus (c) gilt* $\mathrm{Gal}(E/\mathbb{Q})$ *ist 2-Gruppe*

0.5 Anwendungen

Satz 0.39. *$\pi, \sqrt[3]{2}, \zeta_n = e^{2\pi i/n}$ sind nicht konstruierbar über $\mathbb{Q}$*

Bemerkung. Frage D: reguläre n-Ecke. die eulersche ϕ-Funktion ist die Abbildung:

$$\mathbb{N} \to \mathbb{N}, n \mapsto \#\mathbb{Z}_n^\times =: \phi(n)$$

Lemma 0.40. *Sei p Primzahl, $k \in \mathbb{N}$, es gelten:*

(a) $\phi(p^k) = p^k - p^{k-1} = \phi(p)p^{k-1}$ *($\phi(p) = p - 1$)*

(b) $\phi(mn) = \phi(m)\phi(n)$ *sofern* $\mathrm{ggT}(n, m) = 1$

(c) Für $n = 2^k p_1^{e_1} \cdot \ldots \cdot p_k^{e_k}$ *mit Primzahlen* $2 < p_1 < \cdots < p_k$ *und* $e_i \in \mathbb{N}$ *gilt*

$$\phi(n) = 2^{k-1}(p_1 - 1) \cdots (p_{k-1}) p_1^{e_1 - 1} \cdot \ldots \cdot p_k^{e_k - 1}$$

Satz 0.41 (Gauß)**.** *Sei $\zeta_n = e^{2\pi i/n}$, dann sind äquivalent:*

(a) Das reguläre n-Eck (mit Umkreisradius 1) ist konstruierbar

(b) $\zeta_n \in C(\{0, 1\})$

(c) $\phi(n)$ ist 2-Potenz

(d) n ist von der Form $2^k p_1 \cdot \ldots \cdot p_k$ *mit* $p_1 < \cdots < p_k$ *Fermatprimzahlen*

Definition 0.42. $F_\ell = 2^{2^\ell} + 1$ heißt ℓ-te Fermatzahl.

Fermat vermutet: F_ℓ ist eine Primzahl $\forall \ell \in \mathbb{N}_0$, falsch! da $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537, F_5 = 2^{32} + 1 \approx 4$ Milliarden. Nach Euler ist $641 \mid F_5$. Inzwischen ist bekannt $F_5, \ldots, F_{11}$ sind keine Primzahlen und für 324 Fermatzahlen bekannt, sie sind nicht Primzahlen. Außer F_0 bis F_4 keine Primzahlen bisher. Neue Vermutung: Das sind alle??