Körpertheorie: kurze Wiederholung

Themen

Algebraische Erweiterungen
Endliche Erweiterungen
Minimalpolynom
Algebraischer Abschluß
Zerfällungskörper
Normale Erweiterungen
Separable Erweiterungen
Primitives Element
Endliche Körper
Galoiserweiterungen
Galoistheorie
Endliche abelsche Erweiterungen
Symmetrische Polynome
Auflösbarkeit von Gleichungen durch Radikale
Zyklische Galoiserweiterungen
Konstruktionen mit Zirkel und Lineal

Einige wichtige Konzepte

Endliche Körpererweiterungen

K ein Körper (= kommutativer Ring mit Eins, so daß jedes Element $\neq 0$ invertierbar ist. Körpererweiterung: $K \subset L$, $A \subset L$ eine Teilmenge

$$\begin{aligned} K[A] &= \{x \in L; \exists n \in \mathbb{N}_0, f \in K[X_1, \ldots, X_n], a_1, \ldots, a_n : x = f(a_1, \ldots, a_n)\} \\ &= \text{„ kleinster Unterrring, der } K \cup A \text{ enthält“} \end{aligned}$$

$$\begin{aligned} K(A) &= \left\{x \in L; \exists y, z \in K[A], z \neq 0, : x = \frac{y}{z}\right\} \\ &= \text{„ kleinster Unterkörper, der } K \cup A \text{ enthält“} \end{aligned}$$

Ist $A = \{a_1, \ldots, a_n\}$, dann ist

$$\begin{aligned} K[A] = K[a_1, \ldots, a_n] &= \{f(a_1, \ldots, a_n) : f \in K[X_1, \ldots, X_n]\} \\ K(A) = K(a_1, \ldots, a_n) &= \left\{\frac{f(a_1, \ldots, a_n)}{g(a_1, \ldots, a_n)} : f, g \in K[X_1, \ldots, X_n], g(a_1, \ldots, a_n) \neq 0\right\}. \end{aligned}$$

Endlich erzeugt: wenn es $a_1, \ldots, a_n \in L$ gibt mit $L = K(a_1, \ldots, a_n)$
Einfach: wenn es $a \in L$ gibt mit $L = K(a)$.

Grad von L über K: $[L : K] := \dim_K L \in \mathbb{N} \cup \{\infty\}$
Die Körpererweiterung L/K heißt endlich, wenn $[L : K]$ endlich ist, andernfalls unendlich. **Gradmultiplikationsformel**: $K \subset L \subset M$ Körpererweiterungen. Die Erweiterung M/K ist genau dann endlich, wenn L/K und M/L endlich sind. Dann ist

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

Algebraische Erweiterungen

$x \in L$ heißt algebraisch über K, wenn es $f \in K[X]$ gibt mit $f(x) = 0$. Ansonsten heißt es transzendent.
L/K heißt algebraisch, wenn jedes Element $x \in L$ über K algebraisch ist, sie heißt transzendent, wenn sie nicht algebraisch ist.
Minimalpolynom: $x \in L$ algebraisch über K, sei

$$\varphi : K[X] \to L, g \mapsto g(x).$$

Es gibt genau ein normiertes, irreduzibles Polynom $f \in K[X]$ mit $\ker(\varphi) = (f)$. Die Abbildung

$$K[X]/(f) \to K[x], g + (f) \mapsto g(x)$$

ist K-Algebrenisomorphismus.
Der Ring $K[x]$ ist ein Unterkörper von L mit $[K[x] : K] = \deg(f)$. Ist $n = \deg(f)$, dann ist $1, x, \ldots, x^{n-1}$ K-Basis von $K[x]$ über K.
Für ein normiertes Polynom $f \in K[X]$ mit $f(x) = 0$ sind äquivalent:

(a) f ist das Minimalpolynom von x.

(b) Für alle $0 \neq g \in K[X]$ gilt: ist $g(x) = 0$, dann $f \big| g$.

(c) Für alle $0 \neq g \in K[X]$ gilt: ist $g(x) = 0$, dann ist $\deg(f) \leqslant \deg(g)$.

(d) f ist irreduzibel.

L/K ist endlich. $\Leftrightarrow$ L/K ist algebraisch und es gibt $x_1, \ldots, x_n \in L$ mit $L = K(x_1, \ldots, x_n)$. $\Leftrightarrow$ Es gibt über K algebraische Elemente $x_1, \ldots, x_n \in L$ mit $L = K(x_1, \ldots, x_n)$
$K \subset L \subset M$ Körpererweiterungen. M/K ist genau dann algebraisch, wenn L/K und M/L algebraisch sind.

Algebraischer Abschluss (in einem Oberkörper)

Die Menge $\overline{K}$ aller über K algebraischer Elemente von L sind ein Unterkörper von L, der K enthält. Es gilt $\overline{\overline{K}} = \overline{K}$. Der Körper $\overline{K}$ heißt algebraischer Abschluß von K in L. Der Körper K heißt algebraisch abgeschloßen in L, wenn $K = \overline{K}$.

Zerfällungskörper

Satz von Kronecker: K Körper, $f \in K[X]$ irreduzibel. Es gibt $L \supset K$ und $x \in L$ mit $f(x) = 0$ und $L = K(x)$.
Dies ist eindeutig bis auf Isomorphie: Sind $K(x_i) = L_i$ für $i = 1, 2$ Erweiterungen von K mit $f(x_i) = 0$, dann gibt es genau einen Ringisomorphismus $\sigma : L_1 \to L_2$ mit $\sigma(x_1) = x_2$ und $\sigma\big|_K = \mathrm{id}_K$, das heißt genau einen K-Algebrenisomorphismus $\sigma : L_1 \to L_2$ mit $\sigma(x_1) = x_2$.

Fortsetzungssatz: Sei $K \subset L$ endliche Körpererweiterung, $\varphi : K \to K'$ Ringhomomorphismus in einen Körper K'. Dann gibt es eine endliche Körpererweiterung $K' \subset L'$ und einen Ringhomomorphismus $\psi : L \to L'$ mit $\psi\big|_K = \varphi$.

$$\begin{array}{ccc} K & \hookrightarrow & L \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\psi} \\ K' & \to & L' \end{array}$$

Zerfällungskörper: Sei K ein Körper, $f \in K[X]$. Ein Oberkörper L von K heißt Zerfällungskörper von f, wenn:

(a) Es existieren $\alpha \in K$, $n \in \mathbb{N}_0$, $x_1, \ldots, x_n \in L$, so daß $f = \alpha \prod_{i=1}^{n}(X - x_i)$.

(b) Der Körper L ist gegeben durch $K(x_1, \ldots, x_n)$.

Dann ist L endlich über K.

Existenz: Es gibt einen Zerfällungskörper $L \supset K$ von f.

Eindeutigkeit: Sind $K \subset L_i$, $i = 1, 2$, Zerfällungskörper von f, dann gibt es einen Ringismorphismus $\sigma : L_1 \to L_2$ mit $\sigma\big|_K = \mathrm{id}_K$.

Grad: Ist $f \neq 0$, dann gilt

$$[L : K] \big| \deg(f)!.$$

Speziell: Sei f irreduzibel vom Grad n, dann gilt

$$n \big| [L : K] \big| n!.$$

Normale Erweiterungen

Normale Erweiterung: Eine Körpererweiterung $K \subset L$ heißt normal, wenn sie algebraisch ist und jedes irreduzible Polynom in $K[X]$, das in L eine Nullstelle hat, über L in Linearfaktoren zerfällt.

Äquivalent:

(a) L ist normale Erweiterung von K.

(b) L ist Zerfällungskörper eines Polynoms in $K[X]$.

(c) Für alle Oberkörper $L \subset L'$ und alle K-Algebrenhomomorphismen $\sigma : L \to L'$ gilt $\sigma(L) = L'$.

Ist $K \subset L$ endlich und normal, $K \subset E \subset L$ ein Zwischenkörper, dann ist auch L/E endlich und normal.
Aber: Dagegen ist im Allgemeinen E/K nicht normal!

Galoisgruppe

Ist $K \subset L$ Körpererweiterung, dann ist

$$\mathrm{Gal}(L/K) = \left\{\sigma \in \mathrm{Aut}(L) \;\middle|\; \sigma\big|_K = \mathrm{id}_K\right\} \subset \mathrm{Aut}(L)$$

die Galoisgruppe von L/K. Es gilt

$$\mathrm{Gal}(L/K) \subset \mathrm{Alg}_K(L, L).$$

Wenn L_0 der Primkörper von L ist, dann gilt $\mathrm{Aut}(L) = \mathrm{Gal}(L/L_0)$.

Sei $K \subset L$ endlich und normal, $G = \mathrm{Gal}(L/K)$, $f \in K[X]$ ein irreduzibles Polynom, das über L in Linearfaktoren zerfällt. Sei Z die Menge der Nullstellen von f in L. Dann ist

$$G \times Z \to Z, (\sigma, x) \mapsto \sigma(x)$$

eine transitive Operation (G permutiert die Nullstellen). Für $x \in Z$ gilt $G_x = \mathrm{Gal}(L/K(x))$ (Stabilisatoruntergruppe).

Separable Erweiterungen

Sei K ein Körper.

(a) Ein irreduzibles Polynom $f \in K[X]$ heißt separabel, wenn f in einem (und dann jedem) Zerfällungskörper nur einfache Nullstellen hat.

(b) Der Körper K heißt perfekt oder vollkommen, wenn jedes irreduzible Polynom $f \in K[X]$ separabel ist.

(c) Sei $K \subset L$ Körpererweiterung. Ein Element $x \in L$ heißt separabel, wenn x algebraisch über K ist, und das Minimalpolynom von x über K separabel ist.

(d) Ein Oberkörper L heißt separabel über K, wenn jedes Element in L über K separabel ist.

Äquivalent: Für eine endliche Körpererweiterung $K \subset L$ sind folgende Aussagen äquivalent:

(a) Die Erweiterung L/K ist separabel.

(b) Es gibt über K separabel Elemente $x_1, \ldots, x_n \in L$ mit $L = K(x_1, \ldots, x_n)$.

Sei L/K normal. L/K ist genau dann separabel, wenn $|\mathrm{Gal}(L/K)| = [L : K]$ ist.

Transitivität: Sei $K \subset L$ endliche Erweiterung, $K \subset E \subset L$ ein Zwischenkörper. L/K ist genau dann separabel, wenn E/K und L/E separabel sind.

Satz vom primitiven Element: Jede endliche separabel Erweiterung $K \subset L$ ist einfach, dh. es gibt $x \in L$ mit $L = K(x)$.

Kriterium für Separabilität von Polynomen: Sei $f \in K[X]$ irreduzibel. Das Polynom f ist genau dann separabel, wenn $f' \neq 0$ ist.

Charakteristik = 0: Für $f \in K[X]$ gilt $f' = 0$ genau dann, wenn $f \in K$. Das heißt jedes irreduzible Polynom in $K[X]$ ist separabel.
Insbesondere ist jeder Körper von Charkteristik 0 vollkommen.

Charakteristik = $p \neq 0$: Für $f \in K[X]$ gilt $f' = 0$ genau dann, wenn $f \in K[X^p]$. Das heißt ein irreduzibles Polynom $f \in K[X]$ ist genau dann separabel, wenn $f \notin K[X^p]$.
Insbesondere ist K genau dann vollkommen, wenn $K = K^p$, das heißt der Frobenius $\sigma : K \to K, a \mapsto a^p$ ist surjektiv.

Endliche Körper

$p > 0$, p prim. Setze $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.
Frobenius: $\sigma : \mathbb{F}_p \to \mathbb{F}_p$ ist injektiv, also bijektiv. $\Rightarrow \mathbb{F}_p$ ist vollkommen.

Körper mit p^n Elementen: Man bezeichnet mit $\mathbb{F}_{p^n}$ den Zerfällungskörper des Polynoms $f = X^{p^n} - X \in \mathbb{F}_p[X]$. Er besteht genau aus den Nullstellen des Polynoms f und hat p^n Elemente.
Ist K ein endlicher Körper, so gibt es $n \in \mathbb{N}$ und eine Primzahl $p \in \mathbb{N}$ mit $K \cong \mathbb{F}_{p^n}$.

Jeder endliche Körper, $K \cong \mathbb{F}_{p^n}$ ist vollkommen (Frobenius σ ist ein Isomorphismus).
Es gilt $\mathrm{Aut}(K) = \mathrm{Gal}(K/K_0) = \langle\sigma\rangle$, und diese Gruppe hat Ordnung n. Dabei ist σ der Forbeniushomomorphismus von K.

Endliche Erweiterungen: Sei $K \cong \mathbb{F}_{p^n}$ endlicher Körper, $K \subset L$ endliche Körpererweiterung vom Grad m. Dann ist

$$\begin{aligned} &L \cong \mathbb{F}_{p^{mn}} \\ &\mathrm{Gal}(L/K) = \langle\sigma^n\rangle \\ &|\,\mathrm{Gal}(L/K)| = m \end{aligned}$$

Die Erweiterung L/K ist normal und separabel.

Galoiserweiterungen

Eine Körpererweiterung $K \subset L$ heißt Galois'sch oder Galoiserweiterung, wenn L/K normal und separabel ist.

Für eine Körpererweiterung $K \subset L$ sind äquivalent:

(a) Die Erweiterung L/K ist endlich und Galois'sch.
(b) Es gibt eine endliche Untergruppe G von $\mathrm{Aut}(L)$ mit $K = \mathrm{Fix}(G)$.
(c) Die Erweiterung L/K ist endlich und $K = \mathrm{Fix}(\mathrm{Gal}(L/K))$.
(d) Die Erweiterung L/K ist endlich und $|\,\mathrm{Gal}(L/K)| = [L : K]$.

Hauptsatz der Galoistheorie
Sei $K \subset L$ eine endliche Galoiserweiterung mit $G = \mathrm{Gal}(L/K)$, sei $\mathscr{K}$ die Menge aller Zwischenkörper zwischen K und L, $\mathscr{G}$ die Menge aller Untergruppen von G. Dann gilt:

(a) Die Abbildungen

$$\begin{aligned} \mathscr{K} \to \mathscr{G}, &\quad E \mapsto \mathrm{Gal}(L/E) \\ \mathscr{G} \to \mathscr{K} &\quad H \mapsto \mathrm{Fix}_L(H) \end{aligned}$$

sind zueinander invers und antiton. Das heißt, sie sind antiton (monoton und ordnungsumkehrend), und für alle $E \in \mathscr{K}$ gilt $E = \mathrm{Fix}_L(\mathrm{Gal}(L/E))$, und für alle $H \in \mathscr{G}$ gilt $H = \mathrm{Gal}(L/\mathrm{Fix}_L(H))$.

(b) Für $E \in \mathscr{K}$ ist L/E Galois'sch und es gilt

$$\begin{aligned} [L : E] &= |\,\mathrm{Gal}(L/E)| \\ [E : K] &= [G : \mathrm{Gal}(L/E)]\,. \end{aligned}$$

Für $E \in \mathscr{K}$, $H = \mathrm{Gal}(L/E)$ sind äquivalent:

(i) Die Erweiterung E/K ist Galois'sch.

(ii) Für alle $\sigma \in G$ ist $\sigma(E) = E$.

(iii) Die Gruppe H ist ein Normalteiler von G.

Gilt eine der Aussagen (i)-(iii), dann ist die Abbildung

$$G \to \mathrm{Gal}(E/K), \sigma \mapsto \sigma\big|_E$$

ein surjektiver Gruppenhomomorphismus mit Kern H. Dann ist

$$G/H \to \mathrm{Gal}(E/K), \sigma H \mapsto \sigma\big|_E,$$

Isomorphismus.

Konjugierte Galoisgruppen
Sei $K \subset L$ endliche Galoiserweiterung Für $K \subset E, E \subset L$ und $\sigma \in \mathrm{Gal}(L/K)$ sind äquivalent:

(a) $E' = \sigma(E)$,

(b) $\mathrm{Gal}(L/E') = \sigma\,\mathrm{Gal}(L/E)\sigma^{-1}$.

Minimalpolynome über Zwischenkörpern
Sei $K \subset L$ endliche Galoiserweiterung mit $G = \mathrm{Gal}(L/K)$.

(a) Sei $K \subset E \subset L$ und $x \in E$ ein primitives Element über K. Ist $H = \mathrm{Gal}(L/E)$ und $\sigma_1, \ldots, \sigma_m$ eine Linkstransversale von H in G. Dann ist $\prod_{i=1}^{m}(X - \sigma_i(x))$ das Minimalpolynom von x über K. Ist insbesondere x ein primitives Element von L über K, dann ist $\prod_{\sigma\in G}(X-\sigma(x))$ das Minimalpolynom von x über K.

(b) Sei $L = K(x)$, $H \in \mathscr{G}$, $E = \mathrm{Fix}_L(H)$ und $g = \prod_{\sigma\in H}(X - \sigma(x)) = \sum_{i=0}^{t}\alpha_i X^i$. Dann gilt $E = K(\alpha_0, \ldots, \alpha_{t-1})$.

Komposita als Galoiserweiterungen

Kompositum von E und F $= EF = E(F) = F(E) = K(E \cup F)$

Sei $K \subset L$ Körpererweiterung, seien E, E', F Körper zwischen K und L mit $E \subset E'$. Wenn E'/E eine endliche Galoiserweiterung ist, dann ist auch $E'F/EF$ eine endliche Galoiserweiterung und die Abbildung

$$\varphi : \mathrm{Gal}(E'F/EF) \to \mathrm{Gal}(E'/E), \sigma \mapsto \sigma\big|_{E'}$$

ist ein injektiver Gruppenhomomorphismus.

Sei $K \subset L$ Körpererweiterung, seien E, F Körper zwischen K und L, so daß E/K und F/K endliche Galoiserweiterungen sind.

(a) Die Erweiterung EF/K ist endliche Galoiserweiterung und die Abbildung

$$\varphi : \mathrm{Gal}(EF/E) \to \mathrm{Gal}(F/E \cap F), \sigma \mapsto \sigma\big|_F,$$

ist ein Gruppenisomorphismus.

(b) Die Abbildung

$$\psi : \mathrm{Gal}(EF/K) \to \mathrm{Gal}(E/K) \times \mathrm{Gal}(F/K), \sigma \mapsto (\sigma\big|_E, \sigma\big|_F),$$

ist injektiver Homomorphismus. Wenn $E \cap F = K$ ist, dann ist ψ auch surjektiv.

Kreistielungsteilungskörper

Einheitswurzeln: Sei K ein Körper, $n \in \mathbb{N}$. Das Element $\xi \in K$ heißt n-te Einheitswurzel, wenn $\xi^n = 1$. Menge der n-te Einheitswurzeln: $\mu_n(K)$.

(a) Die Menge der n-te Einheitswurzeln ist eine zyklische Untergruppe von K^*, deren Ordnung n teilt.

(b) Sei L Zerfällungskörper von $X^n - 1 \in K[X]$.

(i) Ist $\mu_n(L) = \langle\zeta\rangle$, dann ist $L = K(\zeta)$.

(ii) $\operatorname{char} K \nmid n$, dann hst $\mu_n(L)$ Ordnung n.

(iii) $\operatorname{char}(K) = p$ prim mit $p \mid n$, und ist $n = p^k m$ mit $k \in \mathbb{N}$ und $p \nmid m$, dann gilt $\mu_n(L) = \mu_m(L)$.

Primitive Einheitswurzel: Eine n-te Einheitswurzel $\zeta \in K$ heißt primitiv, wenn $\operatorname{ord}(\zeta) = n$ ist, das heißt, wenn $\mu_n(K) = \langle\zeta\rangle$ und $\mu_n(K)$ Ordnung n hat. Dann gibt es $\varphi(n)$ primitive n^{te} Einheitswurzeln.

Zerfällungskörper von $X^n - a$: Seien K ein Körper, $0 \neq a \in K$, $n \in \mathbb{N}$ mit $\operatorname{char}(K) \nmid n$ und L ein Zerfällungskörper von $X^n - a \in K[X]$. Dann gilt:

(a) Die Erweiterung L/K ist endlich und Galois'sch.

(b) Die Gruppe $\operatorname{Gal}(L/K)$ ist isomorph zu einer Untergruppe des semidirekten Produktes $\mathbb{Z}/n\mathbb{Z} \times_j (\mathbb{Z}/n\mathbb{Z})^*$, wobei $j : (\mathbb{Z}/n\mathbb{Z})^* \to \operatorname{Aut}(\mathbb{Z}/n\mathbb{Z})$ der bekannte Isomorphismus $j(\overline{x})(\overline{y}) = \overline{xy}$ für $x \in (\mathbb{Z}/n\mathbb{Z})^*$, $y \in \mathbb{Z}/n\mathbb{Z}$ ist.

Zerfällungskörper von $X^n - 1$: Sei K Körper, $n \in \mathbb{N}$ mit $\operatorname{char}(K) \nmid n$ und $K^{(n)}$ ein Zerfällungskörper von $X^n - 1 \in K[X]$.

(a) Die Erweiterung $K^{(n)}/K$ ist Galois'sch.

(b) Die Gruppe $\operatorname{Gal}(K^{(n)}/K)$ ist isomorph zu einer Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^*$. Sie ist also abelsch und ihre Ordnung teilt $\varphi(n)$.

Der Körper $K^{(n)}$ heißt Körper der n^{ten} Einheitswurzeln oder n^{ter} Kreisteilungskörper über K.

Kreisteilungspolynome: Sei K ein Körper, $n \in \mathbb{N}$ mit $\operatorname{char}(K) \nmid n$ und $K^{(n)}$ ein Zerfällungskörper von $X^n - 1 \in K[X]$. Ferner sei P_n die Menge aller primitiven n^{ten} Einheitswurzeln in $K^{(n)}$ und $\phi_{K,n} = \phi_n = \prod_{\zeta \in P_n}(X - \zeta)$.

(a) Das Polynom ϕ_n ist in $K[X]$ enthalten, und $\deg(\phi_n) = \varphi(n)$.

(b) Das Polynom $X^n - 1$ zerfällt über K als $X^n - 1 = \prod_{\mathbb{N} \ni d \mid n} \phi_d$.

Das Polynom ϕ_n heißt n^{tes} Kreisteilungspolynom.

Über den rationalen Zahlen:

(a) Das n^{te} Kreisteilungspolynom ϕ_n über $\mathbb{Q}$ liegt in $\mathbb{Z}[X]$ und ist irreduzibel in $\mathbb{Z}[X]$ und $\mathbb{Q}[X]$.

(b) Der Körper $\mathbb{Q}^{(n)}$ der n^{ten} Einheitswurzeln ist Galoiserweiterung von $\mathbb{Q}$ vom Grad $\varphi(n)$. Ist $\varepsilon \in \mathbb{Q}^{(n)}$ eine primitive n^{te} Einheitswurzel, dann gilt $\mathbb{Q}^{(n)} = \mathbb{Q}(\varepsilon)$ und das Minimalpolynom von ε über $\mathbb{Q}$ ist ϕ_n.

(c) Die Abbildung $\rho : \operatorname{Gal}(\mathbb{Q}^{(n)}/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^*$ mit $\rho(\sigma) = \bar{l}$, wenn $\sigma(\varepsilon) = \varepsilon^l$, ist Gruppenisomorphismus.

Über endlichen Körpern: Sei p eine Primzahl, $k \in \mathbb{N}$, $q = p^k$, $K = \mathbb{F}_q$ der Körper mit q Elementen. Ferner sei $n \in \mathbb{N}$ mit $p \nmid n$, $K^{(n)}$ der Zerfällungskörper von $X^n - 1 \in K[X]$

(a) Ist $\varepsilon \in K^{(n)}$ eine primitive n^{te} Einheitswurzel, dann ist $K^{(n)} = K(\varepsilon)$.

(b) $\rho : \operatorname{Gal}(K^{(n)}/K) \to \mathbb{Z}/n\mathbb{Z}^*$ mit $\rho(\tau) = \bar{l}$, wenn $\tau(\varepsilon) = \varepsilon^l$, ist ein injektiver Homomorphismus ist. Es gilt $\operatorname{Gal}(K^{(n)}/K) = \langle\sigma^k\rangle$, wobei σ der Frobeniushomomorphismus ist, da $K^{(n)}$ ebenfalls endlich ist.
Genauer $\rho(\sigma^k) = \overline{q}$, und $\operatorname{im}(\rho) = \langle\overline{q}\rangle$. Damit folgt $[K^{(n)} : K] = \operatorname{ord}(\overline{q}) = \operatorname{ord}_n(q)$.

(c) Das Bild $\overline{\phi}_n \in \mathbb{F}_p[X]$ des n^{ten} Kreisteilungspolynoms $\phi_n \in \mathbb{Z}[X]$ ist genau dann irreduzibel über K, wenn $\mathbb{Z}/n\mathbb{Z}^* = \langle\overline{q}\rangle$, dh. wenn $\operatorname{ord}_n(q) = \varphi(n)$.

Galoisgruppe von Polynomen

Sei K ein Körper, $f = f_1 \cdots f_r \in K[X]$ mit paarweise nicht assoziierten, irreduziblen $f_1, \ldots, f_r$. Sei L ein Zerfällungskörper von f über K, $M = \{x \in L \mid f(x) = 0\}$, $M_i = \{x \in L \mid f_i(x) = 0\}$ für $i = 1, \ldots, r$.
Es gilt $M = \bigcup_{i=1}^{r} M_i$.
Galoisgruppe von f: $G(f) = \mathrm{Gal}(L/K)$
Operation: $G(f) \times M \to M, (\sigma, x) \mapsto \sigma(x)$

(a) Die Bahnen dieser Operationen sind $M_1, \ldots, M_r$.

(b) Die Abbildung $G(f) \to \mathfrak{S}_M, \sigma \mapsto (x \mapsto \sigma(x))$ ist injektiver Gruppenhomomorphismus.

f ist irreduzibel $\Leftrightarrow$ $G(f)$ operiert auf $M = \{x_1, \ldots, x_n\}$ transitiv
Sei f separabel: also Galois'sch und $|\mathrm{Gal}(L/K)| = |G(f)| = [L : K]$.

(a) Man hat die Einbettung $\varphi : G(f) \to \mathfrak{S}_n$ mit $\varphi(\sigma)(i) = j$ falls $\sigma(x_i) = x_j$. Die Ordnung von $G(f)$ teilt $n!$.

(b) Ist f irreduzibel, dann teilt n die Ordnung von $G(f)$.

Diskriminante: Sei $G(f)_+ = \varphi^{-1}(A_n)$.

$$G(f)_+ \triangleleft G(f)$$

$[G(f) : G(f)_+] \leqslant [S_n : A_n] = 2$.

$$\begin{aligned} \delta = \delta(f) &= \prod_{i<j}(x_i - x_j) \in L\backslash\{0\} \\ D = D(f) &= \delta^2 = \prod_{i<j}(x_i - x_j)^2. \end{aligned}$$

Für $\sigma \in G(f)$ gilt

$$\sigma(\delta) = \prod_{i<j}(\sigma(x_i) - \sigma(x_j)) = \prod_{i<j}(x_{\varphi(\sigma)(i)} - x_{\varphi(\sigma)(j)}) = (-1)^m \delta,$$

wobei m die Anzahl der Transversionen von $\varphi(\sigma)$ ist. Es folgt $\sigma(D) = D$ für alle $\sigma \in G(f)$. Also ist $D \in \mathrm{Fix}(G(f)) = K$. Man nennt D die Diskriminante von f.

Sei $\mathrm{char}(K) \neq 2$.

(a) Der Fixkörper von G_+ ist $\mathrm{Fix}(G_+) = K(\delta)$, die Erweiterung $K(\delta)/K$ ist Galois'sch mit Galoisgruppe $\mathrm{Gal}(K(\delta)/K) \cong G/G_+$ vom Grad $[K(\delta) : K] \leqslant 2$.

(b) Genau dann gilt $G = G_+$, wenn D Quadrat eines Elementes von K ist.

Polynome vom Grad 3 und 4: Sei $\mathrm{char}(K) \neq 2$, $f \in K[X]$ normiert irreduzibel, separabel vom Grad 3 und $G = G(f)$.

(a) Es gilt $G \cong A_3$ oder $G \cong \mathfrak{S}_3$.

(b) Genau dann gilt $G \cong A_3$, wenn D Quadrat in K ist.

Sei $f \in K[X]$ normiert, irreduzibel und separabel vom Grad 4,

$$\begin{aligned} M &= \{x_1, \ldots, x_4\} \quad \text{die Menge der Nullstellen im Zerfällungskörper } L \\ &\text{definiere } \alpha = x_1x_2 + x_3x_4, \beta = x_1x_3 + x_2x_4, \gamma = x_1x_4 + x_2x_3 \in L \quad \text{und } E = K(\alpha, \beta, \gamma) \\ G &= G(f) \\ G(f)_+ &= \varphi^{-1}(A_4) \\ N &= \varphi^{-1}(V) \triangleleft G, \quad \text{wobei } V \text{ die Klein'sche Vierergruppe ist,} \end{aligned}$$

Es gilt $\mathrm{Fix}(N) = E$, $\mathrm{Gal}(L/E) = N$, und E/K ist Galois'sch mit $\mathrm{Gal}(E/K) \cong G/N$.
Sei $m = [E : K] = [G : N]$. Dann gilt:

(a) Ist $m = 6$, dann ist $G \cong \mathfrak{S}_4$.

(b) Ist $m = 3$, dann ist $G \cong A_4$.

(c) Ist $m = 1$, dann ist $G \cong V$.

(d) Im Fall $m = 2$ ist entweder $G \cong D_4$ oder $G \cong \mathbb{Z}/(4)$. Der erste Fall tritt genau dann ein, wenn f über E irreduzibel bleibt.

Erweiterungen zu vorgegebenen Galoisgruppen:
Jede endliche Gruppe ist isomorph zur Galoisgruppe einer endlichen Galoiserweiterung. In der Regel ist der Basiskörper "riesig":
Sei $M = K(U_1, \ldots, U_n)$ der rationale Funktionenkörper in den Unbestimmten $U_1, \ldots, U_n$ über K, sei Y eine weitere Unbestimmte. Sei

$$F = Y^n + U_1 Y^{n-1} + \cdots + U_{n-1} Y + U_n \in M[Y].$$

das allgemeine Polynom n^{ten} Grades. Die Galoisgruppe des allgemeinen Polynoms $F = Y^n + U_1 Y^{n-1} + \cdots + U_{n-1} Y + U_n \in M[Y]$ ist isomorph zu $\mathfrak{S}_n$.

Jede endliche abelsche Gruppe G ist isomorph zur Galoisgruppe einer endlichen Galoiserweiterung $\mathbb{Q} \subset K$ mit $\mathrm{Gal}(K/\mathbb{Q}) \cong G$.

Auflösbare Erweiterungen

Eine endliche Galoiserweiterung L/K heißt
— zyklisch, wenn $\mathrm{Gal}(L/K)$ zyklisch ist.
— abelsch, wenn $\mathrm{Gal}(L/K)$ abelsch ist.
— auflösbar, wenn $\mathrm{Gal}(L/K)$ auflösbar ist.

Zyklische Erweiterungen: Hier unterscheidet man, ob die Charakteristik des Grundkorpers den Grad des Polynoms teilt oder nicht:

Sei K ein Körper und $n \in \mathbb{N}$ mit $\mathrm{char}(K) \nmid n$. Wir nehmen an, daß K eine primitive n^{te} Einheitswurzel enthält.

(a) Ist $f = X^n - a \in K[X]$, L ein Zerfällungskörper von f und $x \in L \backslash K$ eine Nullstelle von f, dann gilt $L = K(x)$ und L/K ist eine zyklische Galoiserweiterung. Ferner ist $d = [L : K]$ Teiler von n, es gilt $x^d \in K$ und $X^d - x^d$ ist das Minimalpolynom von x über K. Ist f irreduzibel, dann ist L/K zyklische Galoiserweiterung vom Grad n.

(b) Wenn umgekehrt $K \subset L$ eine zyklische Galoiserweiterung vom Grad n ist, dann gibt es $x \in L$ mit $x^n \in K$ und $L = K(x)$. Also ist $X^n - x^n$ das Minimalpolynom von x und L ist sein Zerfällungskörper.

Sei K ein Körper mit Primzahlcharakteristik p.

(a) Ist $f = X^p - X - a \in K[X]$, L ein Zerfällungskörper von f und $x \in L$ eine Nullstelle von f, so ist $L = K(x)$ und L/K ist zyklische Galoiserweiterung vom Grad 1 oder p. Genau dann ist $[L : K] = p$, wenn f irreduzibel ist.

(b) Ist L/K zyklische Galoiserweiterung vom Grad p, so gibt es $a \in K$ und eine Nullstelle des irreduziblen Polynoms $f = X^p - X - a \in K[X]$ mit $L = K(x)$.

Durch Radikale auflösbare Erweiterungen: Eine endliche Erweiterung $K \subset L$ heiße vom
Typ I wenn L aus K durch Adjunktion einer Einheitswurzel entsteht.
Typ II wenn L aus K durch Adjunktion einer Nullstelle des Polynoms $X^n - a \in K[X]$ mit $\mathrm{char}(K) \nmid n$ entsteht.
Typ III wenn L aus K durch Adjunktion einer Nullstelle eines Polynoms $X^p - X - a \in K[X]$ mit $\mathrm{char}(K) = p > 0$ entsteht.
Die adjungierten Elemente heißen auch Radikale.

(a) Eine endliche Erweiterung $K \subset M$ heißt Radikalerweiterung, wenn es eine Folge von Zwischenkörpern $K = M_0 \subset M_1 \subset \ldots \subset M_r = M$ gibt, so daß die Erweiterungen $M_i \subset M_{i+1}$ von einem der Typen I,II oder III sind. Offenbar ist dann M/K separabel.

(b) Eine endliche Erweiterung $K \subset L$ heißt durch Radikale auflösbar, wenn es eine Radikalerweiterung $K \subset M$ gibt, mit $L \subset M$.

(c) Eine endliche Erweiterung $K \subset L$ heißt auflösbar, wenn es eine Erweiterung $L \subset M$ gibt, so daß M/K endliche auflösbare Galoiserweiterung ist.

Es gilt:

— Seien $K \subset E \subset L$ endliche Erweiterungen. Die Erweiterung L/K ist genau dann auflösbar, beziehungsweise durch Radikale auflösbar, wenn E/K und L/E die jeweiligen Eigenschaften haben

— Eine endliche Körpererweiterung $K \subset L$ ist genau dann durch Radikale auflösbar, wenn sie auflösbar ist.

Konstruktionen mit Zirkel und Lineal

Sei $M \subset \mathbb{R}^2 \cong \mathbb{C}$ eine Menge mit $0, 1 \in M$, $g(M)$ die Menge aller Geraden durch zwei verschiedenen Punkte in M, $k(M)$ die Menge aller Kreise, deren Mittelpunkte in M liegen und deren Radius jeweils die Abstände zweier Punkte in M sind. Mit folgenden Operationen werden aus Punkten in M Punkte in $\mathbb{R}^2$ konstruiert:

(S1) Schnitt zweier verschiedener Geraden in $g(M)$.
(S2) Schnitt einer Geraden in $g(M)$ mit einem Kreis in $k(M)$.
(S3) Schnitt zweier verschiedener Kreise.

Die Menge der aus M konstruierten Punkte sei M'. Offenbar gilt $M \subset M'$. Wir setzen induktiv

$$\begin{aligned} M_0 &= M \\ M_1 &= M' \\ &\vdots \\ M_{n+1} &= (M_n)' \\ \hat{M} &= \bigcup_{n \geqslant 0} M_n \end{aligned}$$

Die Punkte aus $\hat{M}$ heißen (mit Zirkel und Lineal) konstruiert. Jeder Punkt aus $\hat{M}$ kann durch endlich viele Operationen (S1), (S2), (S3) aus M erhalten werden. Es gilt $(\hat{M})' = \hat{M}$, denn ist $p \in (\hat{M})'$, so kann P aus endlich vielen Punkten in $\hat{M}$ konstituiert werden, diese liegen in M_n für $n \geqslant 0$ groß genug, also gilt $P \in M_n' = M_{n+1} \subset \hat{M}$.

Es gilt:

(a) Die Menge $\hat{M}$ ist der kleinste Unterkörper von $\mathbb{C}$ mit folgenden Eigenschaften:

$$M \subset \hat{M}, \qquad \overline{\hat{M}} = \hat{M}, \qquad \forall z \in \mathbb{C} : z^2 \in \hat{M} \Rightarrow z \in \hat{M}.$$

(b) Der Körper $K = \mathbb{Q}(M \cup \overline{M})$ ist Unterkörper von $\hat{M}$ und $K = \overline{K}$.

Konstruierbarkeit: Sei $M \subset \mathbb{C}$ mit $0, 1 \in M$ und $K = \mathbb{Q}(M, \overline{M})$. Für einen Punkt $z \in \mathbb{C}$ sind folgende Aussagen äquivalent:

(a) Es ist $z \in \hat{M}$, das heißt z ist aus M (mit Zirkel und Lineal) konstruierbar.

(b) Es gibt eine Folge von Erweiterungen $K = L_0 \subset L_1 \subset \ldots \subset L_r = L$, $r \in \mathbb{N}_0$, und $w_i \in L_i$ mit $w_i^2 \in L_{i-1}$ und $L_i = L_{i-1}(w_i)$ für $1 \leqslant i \leqslant r$, so daß $z \in L$ ist. (Spezielle Radikalerweiterungen)

(c) Das Element z ist algebraisch über K und die Galoisgruppe des Minimalpolynoms $f \in K[X]$ von z ist eine 2-Gruppe.

Beispiele

Beispiele: endliche Erweiterungen

(a) Ist L/K eine endliche Körpererweiterung, $n = [L : K]$ und $x \in L$, dann sind $1, x, \ldots, x^n$ linear abhängig über K, dh. es existieren $\alpha_0, \ldots, \alpha_n \in K$ nicht alle Null mit $\sum_{i=0}^n \alpha_i x^i = 0$, d.h. x ist Nullstelle des Polynoms $f = \sum_{i=0}^n \alpha_i X^i \in K[X] \backslash \{0\}$.

(b) Sei $d \in \mathbb{N}$ mit $\sqrt{d} \notin \mathbb{Q}$. $\mathbb{Q} \subset \mathbb{Q}[\sqrt{d}]$ ist quadratische Körpererweiterung.

(c) $\mathbb{R} \subset \mathbb{C} = \mathbb{R}[i]$ ist endliche Erweiterung, also algebraisch. Ein Element $x \in \mathbb{C}$ ist Nullstelle von $(X-x)(X-\overline{x}) = X^2 - (x+\overline{x})X + x\overline{x} \in \mathbb{R}[X]$. Für $x \in \mathbb{R}$ ist $X - x$ das Minimalpolynom, für $x \in \mathbb{C} \setminus \mathbb{R}$ ist $X^2-(x+\overline{x})X+x\overline{x}$ das minimalpolynom. Insbesondere ist X^2+1 das Minimalpolynom von i über $\mathbb{R}$ und es gilt

$$\mathbb{R}[X]/(X^2+1) \cong \mathbb{C}\,.$$

(d) $\sqrt[3]{2} \in \mathbb{R}$ ist algebraisch über $\mathbb{Q}$ mit Minimalpoynom $X^3 - 2$. Also gilt

$$\mathbb{Q}[X]/(X^3-2) \cong \mathbb{Q}[\sqrt[3]{2}] = \mathbb{Q}(\sqrt[3]{2}).$$

(e) $K \subset K(X)$ ist transzendent, denn X/K ist transzendent, $\dim_K K[X] = \infty$, $K[X] \subsetneq K(X)$.

(f) $\mathbb{Q} \subset \mathbb{R}$ ist transzendent, denn zum Beispiel sind e, π transzendent über $\mathbb{Q}$ (Hermite: 187, Lindemann: 1882).

Beispiele: algebraischer Abschluß

(a) Der algebraische Abschluß $\overline{\mathbb{Q}}$ von $\mathbb{Q}$ in $\mathbb{C}$ ist eine unendliche algebraische Erweiterung von $\mathbb{Q}$. Er heißt Körper der algebraischen Zahlen.

(b) Der Körper $\overline{\mathbb{Q}}$ ist abzählbar unendlich.

(c) Die Mengen $\mathbb{R} \setminus \overline{\mathbb{Q}}$, $\mathbb{C} \setminus \overline{\mathbb{Q}}$ sind überabzählbar.

Beispiele: Zerfällungskörper

(a) Die komplexen Zahlen $\mathbb{C}$ sind Zerfällungskörper von $X^2 + 1 \in \mathbb{R}[X]$.

(b) Der Körper $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ ist Zerfällungskörper von $(X^2-2)(X^2-3) \in \mathbb{Q}[X]$.

(c) Sei $K = \mathbb{Z}/(2)$, $f = X^2 + X + 1 \in K[X]$. Das Polynom f ist irreduzibel, also ist $L = K[X]/(f)$ Körpererweiterung von K. L ist Zerfällungskörper von f denn mit $x = X + (f)$ gilt $f = (X + x)(X + x + 1)$ und $L = K(x)$. Es gilt $[L : K] = 2$, also hat L 4 Elemente.

(d) Sei $f = X^3 - 2 \in \mathbb{Q}[X]$. Das Polynom f ist irreduzibel (Eisenstein). Sei

$$\omega = \frac{1}{2}(-1 + \sqrt{-3}) = e^{\frac{2\pi i}{3}} \in \mathbb{C}\,.$$

Es gilt $\omega^2 = \overline{\omega}$ und $\omega^3 = 1$. Die Nullstellen von f sind

$$\sqrt[3]{2}, \omega\sqrt[3]{2}, \overline{\omega}\sqrt[3]{2},$$

also ist

$$f = (X - \sqrt[3]{2})(X - \omega\sqrt[3]{2})(X - \overline{\omega}\sqrt[3]{2}) = (X - \sqrt[3]{2})(X^2 + \sqrt[3]{2}X + \sqrt[3]{2}^2).$$

Also ist $\mathbb{Q}(\sqrt[3]{2}, \omega) = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ Zerfällungskörper von f. Es gilt

$$[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 2 \cdot 3 = 6 = 3!$$

Beispiele: Normale Erweiterungen

(a) Quadratische Erweiterungen sind normal.

(b) Beispiel eines Körperturms $K \subset L \subset M$ an, so daß $K \subset L$ und $L \subset M$ normal sind, aber $K \subset M$ nicht.
Lösung: Betrachte die Erweiterungen $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$. Die Erweiterung $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$ ist quadratisch, das Minimalpolynom von $\sqrt{2}$ über $\mathbb{Q}$ ist $X^2 - 2$. Die Erweiterung $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$ ist ebenso quadratisch, das Minimalpolynom von $\sqrt[4]{2}$ über $\mathbb{Q}(\sqrt{2})$ ist $X^2 - \sqrt{2}$. Aber $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{2})$ ist nicht normal, denn das Minimalpolynom $X^4 - 2$ von $\sqrt[4]{2}$ über $\mathbb{Q}$ zerfällt über $\mathbb{Q}(\sqrt[4]{2})$ nicht in Linearfaktoren, sondern nur in $(X - \sqrt[4]{2})(X + \sqrt[4]{2})(X^2 + \sqrt{2})$.

Beispiele: Separable Erweiterungen

(a) Das Polynom $f = X^3 - 2 \in \mathbb{Q}[X]$ ist separabel.

(b) Sei $K = \mathbb{Z}/(2)(X)$, $f = Y^2 + X \in K[Y]$. Dann ist f irreduzibel, denn f ist irreduzibel in $\mathbb{Z}/(2)[X][Y]$ nach Eisenstein. Es gibt eine Erweiterung $K \subset L = K(y)$ vom Grad 2 mit $0 = f(y) = y^2 + X$, also $y^2 = X$ über $\mathbb{Z}/(2)$ und es gilt

$$(Y + y)^2 = Y^2 + 2Yy + y^2 = Y^2 + y^2 = Y^2 + X = f.$$

Also ist f nicht separabel.

(c) Sei $K/\mathbb{Q}$ der Zerfällungskörper von $f = X^3 - 2 \in \mathbb{Q}[X]$. Wir wissen, daß

$$K = \mathbb{Q}(\sqrt[3]{2}, \omega) = \mathbb{Q}(\sqrt[3]{2})(\omega),$$

wobei $\omega = \frac{1}{2}(-1 + \sqrt{-3}) = e^{\frac{2\pi i}{3}} \in \mathbb{C}$. Das Minimalpolynom von ω über $\mathbb{Q}$ oder $\mathbb{Q}(\sqrt[3]{2})$ ist $\phi_3 = X^2 + X + 1$. $K/\mathbb{Q}$ ist normal und separabel, also gilt $|\operatorname{Gal}(K/\mathbb{Q})| = [K : \mathbb{Q}] = 6$. Die Gruppe $\operatorname{Gal}(K/\mathbb{Q})$ besteht genau aus folgenden Elementen

$$\begin{aligned}
\mathrm{id}_K: &\quad \sqrt[3]{2} \mapsto \sqrt[3]{2}, &\quad \omega \mapsto \omega \\
\alpha: &\quad \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega, &\quad \omega \mapsto \omega \\
\alpha^2: &\quad \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega^2, &\quad \omega \mapsto \omega \\
\beta: &\quad \sqrt[3]{2} \mapsto \sqrt[3]{2}; &\quad \omega \mapsto \omega^2, \\
\alpha\beta: &\quad \sqrt[3]{2} \mapsto \omega\sqrt[3]{2}, &\quad \omega \mapsto \omega^2 \\
\alpha^2\beta: &\quad \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega^2, &\quad \omega \mapsto \omega^2
\end{aligned}$$

Damit sieht man $\operatorname{ord}(\alpha) = 3$, $\operatorname{ord}(\beta) = 2$, $\beta\alpha\beta = \alpha^2$, dh. $\operatorname{Gal}(K/\mathbb{Q}) \cong \mathfrak{S}_3$.

Beispiele: Galoisgruppe

(a) Ist die Erweiterung $K \subset L$ endlich, dann gilt $\operatorname{Gal}(L/K) = \operatorname{Alg}_K(L, L)$, denn jeder K-Algebrenhomomorphismus $\sigma : L \to L$ ist injektiv, also bijektiv.

(b) Wenn L_0 der Primkörper von L ist, dann gilt $\operatorname{Aut}(L) = \operatorname{Gal}(L/L_0)$.

Beispiele: Endliche Körper

(a) $L = \mathbb{Z}/(9)$ ist kein Körper, da 9 nicht prim ist. Insbesondere keine Erweiterung von $\mathbb{F}_3$.

(b) $L = \mathbb{Z}[\sqrt{2}]/(3)$ ist ein Körper: (3) ist ein Primdeal in $\mathbb{Z}[\sqrt{2}]$, also ist L ein endlicher Integritätsbereich, und damit ein Körper. Es gibt einen Isomorphismus

$$\mathbb{Z}[\sqrt{2}]/(3) \xrightarrow{\sim} \mathbb{F}_3[X]/(X^2 + 1) \cong \mathbb{F}_9, \sqrt{2} \mapsto \overline{X}.$$

Beispiele: Galoiserweiterungen

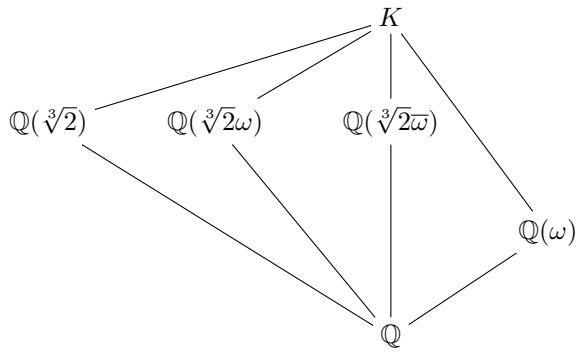
(a) Endliche Erweiterungen von endlichen Körpern sind Galois'sch.
Sei $K \cong \mathbb{F}_{p^n}$ und $K \subset L$ endliche Erweiterung vom Grad m. Die Erweiterung L/K ist Galois'sch mit Galoisgruppe $\operatorname{Gal}(L/K) = \langle \sigma^n \rangle$, wobei σ der Frobeniushomomorphismus von L ist. Die Körper zwischen K und L sind genau die Fixkörper $\operatorname{Fix}_L(\langle \sigma^{nd} \rangle)$ mit $d \in \mathbb{N}$, $d \big| m$. Ist $m = dd'$, $E = \operatorname{Fix}_L(\langle \sigma^{nd} \rangle)$, dann gilt

$$[E : K] = [\langle \sigma^n \rangle : \langle \sigma^{nd} \rangle] = \frac{m}{d'} = d.$$

Es folgt $E \cong \mathbb{F}_{p^{nd}}$.

(b) Jede quadratische Erweiterung $K \subset L$ ist normal. Denn für $x \in L \backslash K$ gilt $L = K(x)$. Ist $f = X^2 + \alpha X + \beta \in K[X]$ das Minimalpolynom von x, dann $f = X^2 + \alpha X + \beta - x^2 - \alpha x - \beta = (X - x)(X + x + \alpha)$. Also ist L/K Zerfällungskörper von f. Insbesondere ist jede separabel quadratische Erweiterung $K \subset L$ Galoiserweiterung.

(c) Das Polynom $f = X^3 - 2 \in \mathbb{Q}[X]$ ist irreduzibel und separabel. Der Körper $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$ mit $\omega = \frac{1}{2}(-1 + \sqrt{-3})$ ist Zerfällungskörper von f. Also ist $K/\mathbb{Q}$ Galois'sch. Wir wissen, daß $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathfrak{S}_3$ ist. Die Körper zwischen $\mathbb{Q}$ und K sind



Die Unterkörper vom Grad 3 sind die Fixkörper der drei Untergruppen der Ordnung 2 von $\mathrm{Gal}(K/\mathbb{Q})$, der Unterkörper vom Grad 2 ist der Fixkörper von A_3. Die Körper vom Grad 3 sind zueinander konjugiert. Nur K und $\mathbb{Q}(\omega)$ sind Galois'sch über $\mathbb{Q}$.

Beispiele: EInheitswurzeln

(a) Die n^{ten} Einheitswurzeln in $\mathbb{C}$ sind $e^{\frac{2\pi ik}{n}}$, $1 \leqslant k \leqslant n$. Die primitiven sind dabei diejenigen, für die n und k teilerfremd sind.

(b) Sei p Primzahl, $n \in \mathbb{N}$. Alle Elemente in $\mathbb{F}_{p^n}^*$ sind $(p^n - 1)^{\text{te}}$ Einheitswurzeln.

Beispiele: Kreisteilungspolynome

Sei $\mathrm{char}(K) = 0$. Es ist $\phi_1 = X - 1$. Ist p Primzahl, so ist $X^p - 1 = \phi_1\phi_p$. Also ist

$$\phi_p = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + X + 1.$$

Ist außerdem $k \in \mathbb{N}$, dann $X^{p^k} - 1 = \phi_1\phi_p \cdots \phi_{p^{k-1}}\phi_{p^k} = (X^{p^{k-1}} - 1)\phi_{p^k}$. Also

$$\phi_{p^k} = \frac{X^{p^k} - 1}{X^{p^{k-1}} - 1} = X^{p^{k-1}(p-1)} + \cdots + X^{p^k - 1} + 1 = \phi_p(X^{p^{k-1}}).$$

Die ersten zehn Kreisteilungspolynome sind:

$$\begin{aligned}
\phi_1 &= X - 1 \\
\phi_2 &= X + 1 \\
\phi_3 &= X^2 + X + 1 \\
\phi_4 &= X^2 + 1 \\
\phi_5 &= X^4 + X^3 + X^2 + X + 1 \\
\phi_6 &= X^2 - X + 1 \\
\phi_7 &= X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 \\
\phi_8 &= X^4 + 1 \\
\phi_9 &= X^6 + X^3 + 1 \\
\phi_{10} &= X^4 + X^3 + X^2 - X + 1
\end{aligned}$$

Beispiele Diskriminante

(a) Ist $f = X^2 + bX + c \in K[X]$, $f = (X - x_1)(X - x_2) = X^2 - (x_1 + x_2)X + x_1x_2$, dann $D = (x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1x_2 = b^2 - 4ac$.

(b) Sei $f = X^3 + bX^2 + cX + d \in K[X]$. Wir werden sehen: $D = b^2c^2 + 18bcd - 4b^3d - 4c^3 - 27d^2$.

Beispiele: Polynome vom Grad 3

(a) Sei K Unterkörper von $\mathbb{R}$, $f \in K[X]$ normiert und irreduzibel vom Grad 3, und sei $G = G(f)$. Dann gilt:

(i) Hat f nur eine reelle Nullstelle, dann ist $D < 0$ und $G \cong \mathfrak{S}_3$.

(ii) Hat f lauter reelle Nullstellen, dann ist $D > 0$. Genau dann ist $G \cong A_3$, wenn D Quadrat in K ist.

(b) Das Polynom $f = X^3 - 2 \in \mathbb{Q}[X]$ ist irreduzibel, seine Diskriminante ist $D = -27(-2)^2 = -27 \cdot 4 < 0$. Also hat f genau eine reelle Nullstelle und es gilt $G(f) \cong \mathfrak{S}_3$.

(c) Das Polynom $f = X^3 - 3X - 1 \in \mathbb{Q}[X]$ ist irreduzibel, seine Diskriminante ist $D = -4(-3)^3 - 27(-1)^2 = 4 \cdot 27 - 27 = 9^2 > 0$. Also hat f drei reelle Nullstellen und es gilt $G(f) \cong A_3$.

(d) Das Polynom $f = X^3 - 4X - 1 \in \mathbb{Q}[X]$ ist irreduzibel, seine Diskriminante ist $D = -4(-4)^3 - 27(-1)^2 = 256 - 27 = 229 > 0$, kein Quadrat. Also hat f drei reelle Nullstellen, aber $G(f) \cong \mathfrak{S}_3$.

Beispiele: Auflösbare Erweiterungen

(a) Sei $K = \mathbb{Q}(\sqrt[3]{2})(\omega) = \mathbb{Q}(\sqrt[3]{2}, \omega)$ der Zerfällungskörper von $X^3 - 2 \in \mathbb{Q}[X]$, wobei $\omega = e^{\frac{2\pi i}{3}}$. Dann ist $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ Erweiterung vom Typ II und $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\sqrt[3]{2}, \omega)$ vom Typ I. Also ist $K/\mathbb{Q}$ Galois'sche Radikalerweiterung.

(b) Jede separabel Erweiterung $K \subset L$ vom Grad $\leqslant 4$ ist durch Radikale auflösbar.

(c) Sei $K \subset L$ eine endliche und separabel Erweiterung, $L \subset L'$ ein normaler Abschluß von L/K. Wenn $\mathrm{Gal}(L'/K)$ eine einfache nicht-abelsche Untergruppe enthält, dann ist L/K nicht durch Radikale auflösbar.

Beispiele: Konstruktionen mit Zirkel und Lineal

Würfelverdopplung *Gegeben sei ein Würfel der Kantenlänge $a > 0$. Ist ein Würfel doppelten Inhalts, nämlich $2a^3$, aus a mit Zirkel und Lineal konstruierbar?*
Sei speziell $a = 1$, ist $\sqrt[3]{2}$ aus $M = \{0, 1\}$ konstruierbar? Es gilt $K = \mathbb{Q}(M \cup \overline{M}) = \mathbb{Q}$. Das Minimalpolynom von $\sqrt[3]{2}$ über $\mathbb{Q}$ ist $f = X^3 - 2$, es gilt $G(f) \cong \mathfrak{S}_3$. Da $\mathfrak{S}_3$ keine Zweigruppe ist, ist $\sqrt[3]{2}$ nicht aus M konstruierbar.

Winkeldreiteilung *Gegeben ist ein Winkel φ. Ist $\frac{\varphi}{3}$ mit Zirkel und Lineal konstruierbar? Genauer: Ist $z = e^{i\frac{\varphi}{3}}$ aus $\{0, 1, w = e^{i\varphi}\}$ konstruierbar?*
Wir betrachten speziell $\varphi = \frac{\pi}{3}$, das heißt $w = e^{i\frac{\pi}{3}} = e^{2\pi i \frac{1}{6}} = \frac{1}{2}(1 + i\sqrt{-3})$. Sei $z = e^{i\frac{\pi}{9}} = x + iy$ mit $x = \cos\frac{\pi}{9}$ und $y = \sin\frac{\pi}{9}$. Der Punkt z ist genau dann konstruierbar, wenn x, y kontruierbar sind. Es gilt

$$w = z^3 = x^3 - 3xy^2 + (3x^2y - y^3)i = x^3 - 3x(1 - x^2) + (3(1 - y^2)y - y^3)i = 4x^3 - 3x + (3y - 4y^3)i.$$

Es folgt $4x^3 - 3x - \frac{1}{2} = 0$, also $(2x)^3 - 3(2x) - 1 = 0$. Das Polynom $X^3 - 3X - 1 \in \mathbb{Q}[X]$ ist irreduzibel, also hat $2x$ den Grad 3 über $\mathbb{Q}$. Damit sind $2x$, x und z nicht konstruierbar.

Einheitswurzeln *Ist $\zeta_{2019} = e^{\frac{2\pi i}{2019}}$ mit Zirkel und Lineal konstruierbar?*
Die Einheitswurzel ζ_{2019} ist konstruierbar, wenn $\varphi(2019)$ Zweierpotenz ist. Aber da $2019 = 3 \cdot 673$ prim ist und $\varphi(2019) = \varphi(3) \cdot \varphi(673) = 2 \cdot 672 = 2 \cdot 2^5 \cdot 3 \cdot 7$, ist dies nicht der Fall.