Einführung in die Algebra

Vorlesung im
Wintersemester 2006-2007
Technische Universität Berlin

gehalten von
Prof. Dr. M. Pohst

Contents

CHAPTER 4

Galoistheorie

4.1. Satz

Es seien $L, \tilde{L}$ zwei Körper und $\sigma_i : L \to \tilde{L} \quad (1 \leq i \leq n)$ verschiedene Isomorphismen.

Dann sind $\sigma_1, \ldots, \sigma_n$ im folgenden Sinn linear unabhängig:
$\sum_{i=1}^{n} \alpha_i \sigma_i(\beta) = 0$ für feste $\alpha_1, \ldots, \alpha_n \in \tilde{L}$ und alle $\beta \in L$ impliziert $\alpha_i = 0 \qquad (1 \leq i \leq n)$.

Beweis:
Mittels Induktion über n!
$n = 1$: trivial (speziell ist $\sigma_1(1) = 1$!).
$n - 1 \Rightarrow n$: Es sei $\sum_{i=1}^{n} \alpha_i \sigma_i(\beta) = 0 \ \ \forall \beta \in L$ vorgegeben.
Es sind σ_1 und σ_n verschieden, also existiert $\gamma \in L \backslash \{0, 1\}$ mit $\sigma_1(\gamma) \neq \sigma_n(\gamma)$.
Hierfür gilt: $\sigma_n(\gamma^{-1}) \ \sum_{i=1}^{n} \alpha_i \sigma_i(\gamma\beta) = 0 \ \ \forall \beta \in L$,
und wir subtrahieren hiervon $\sum_{i=1}^{n} \alpha_i \sigma_i(\beta) = 0 \ \ \forall \beta \in L$.
Dies liefert $\sum_{i=1}^{n-1} \alpha_i \left(\sigma_n(\gamma^{-1}) \, \sigma_i(\gamma) \ - 1\right) \sigma_i(\beta) = 0 \ \ \forall \beta \in L$.
Nach Induktionsannahme gilt dann $\alpha_i \left(\sigma_n(\gamma^{-1}) \, \sigma_i(\gamma) - 1\right) = 0 \qquad (1 \leq i \leq n-1)$,
also $\alpha_1 = 0$.
Wiederum nach Induktionsannahme folgt dann auch $\alpha_2 = \ldots = \alpha_n = 0$.

□

4.2. Hilfssatz

Es seien $L, \tilde{L}$ zwei Körper und $\sigma_i : \ L \to \tilde{L} \qquad (1 \leq i \leq n)$ verschiedene Isomorphismen.

Dann ist $K := \{\alpha \in L \mid \sigma_1(\alpha) = \ldots = \sigma_n(\alpha)\}$ ein Unterkörper von L mit $[L : K] \geq n$.

Beweis:
K Teilkörper ist klar, es bleibt die Gradaussage zu zeigen. Indirekt!

Wir nehmen $[L : K] = r < n$ an. Dann existiert eine K -Basis $\omega_1, \ldots, \omega_r$ von L/K.

Danach hat das lineare Gleichungssystem $\sum_{j=1}^{n} \sigma_j(\omega_i) X_j = 0 \qquad (1 \leq i \leq r)$

eine nicht triviale Lösung $X_1, \ldots, X_n$ in $\tilde{L}$.

Für beliebiges $\alpha \in L,\ \alpha = \sum_{i=1}^{r} \alpha_i \omega_i \qquad (\alpha_i \in K,\ 1 \leq i \leq r),$

liefert dies $\sum_{j=1}^{n} \sigma_j(\alpha_i \omega_i) X_j = 0 \qquad (1 \leq i \leq r)$

(mittels Multiplikation der i -ten Gleichung mit $\sigma_1(\alpha_i) = \sigma_2(\alpha_i) = \ldots = \sigma_n(\alpha_i)$).

Addition aller Gleichungen ergibt $\sum_{j=1}^{n} \sigma_j(\alpha) X_j = 0 \ \ \forall \alpha \in L$, Widerspruch!

□

Anwendung:

Es sei L eine endliche K-Erweiterung, $G(L/K)$ bezeichne die Gruppe aller K -Automorphismen von L.

Ferner sei H eine Untergruppe von $G(L/K)$ und $F(H) := \{\alpha \in L \mid \sigma(\alpha) = \alpha \ \ \forall \sigma \in H\}$.

Dann ist $F(H)$ ein Teilkörper von L, der K enthält, und es gilt $[L : F(H)] \geq (H : 1)$.

$F(H)$ heißt Fixkörper bzgl. H (Bezeichnung: $Fix\ (H)$).

Beispiel:

Es sei $L = K(t)$.

L besitzt u.a. folgende 6 Automorphismen σ_i,

welche durch $\sigma_1(t) = t,\ \sigma_2(t) = 1 - t,\ \sigma_3(t) = \frac{1}{t},\ \sigma_4(t) = 1 - \frac{1}{t},\ \sigma_5(t) = \frac{1}{1-t},\ \sigma_6(t) = \frac{t}{t-1}$ festgelegt sind. (Beachte:

$$\begin{array}{lcl} \sigma_5 & = & \sigma_4^2, \\ \sigma_1 & = & \sigma_4^3, \\ ord(\sigma_i) & = & 2 \\ \text{für } i & = & 2, 3, 6.) \end{array}$$

Es sei F derjenige Teilkörper von L, der von allen 6 Automorphismen elementweise invariant gelassen wird.

Hierfür gilt $[L : F] \geq 6$.

Es steht sogar das Gleichheitszeichen: Denn $g(t) := \frac{(t^2 - t + 1)^3}{t^2 (t-1)^2}$ liegt in F.

Also ist $F_1 := K(g(t))$ ein Teilkörper von F, d.h. $[L : F_1] \geq 6$.

Wegen $(t^2-t+1)^3 - g(t)t^2(t-1)^2 = 0$ in $F_1[t]$ ist t Wurzel eines Polynoms vom Grad 6 aus $F_1[t]$,
also $[F_1[t] : F_1] \leq 6$ und damit $F = K(g(t))$.

4.3. Satz

Es sei G eine endliche Gruppe von Automorphismen
eines Körpers L und $F = \{\alpha \in L \mid \sigma(\alpha) = \alpha \ \ \forall \alpha \in G\}$.
Dann ist F ein Körper, sog. Fixkörper $F(G)$, und es gilt: $[L : F] = (G : 1)$.

Beweis:
Gemäß (4.2) ist F Teilkörper von L mit $[L : F] \geq (G : 1) =: n$.
Wir nehmen an, daß L über F $n+1$ linear unabhängige Elemente $\omega_1, \ldots, \omega_{n+1}$ enthält.
Für $G = \{\sigma_1, \ldots, \sigma_n\}$ betrachten wir das homogene lineare Gleichungssystem

$$\sum_{j=1}^{n+1} \sigma_i(\omega_j) X_j = 0 \qquad (1 \leq i \leq n).$$

Hierfür sei $X_1, \ldots, X_{n+1}$ eine nicht triviale Lösung in L.
Unter allen Lösungen des Gleichungssystems wählen wir nun eine aus, bei der minimal viele X_i von Null verschieden sind.
Durch Umordnung der Basis erreichen wir also etwa

$$\sum_{j=1}^{r} \sigma_i(\omega_j) X_j = 0 \qquad (1 \leq i \leq n,\ r \leq n+1,\ X_1 \cdot \ldots \cdot X_r \neq 0).$$

Offenbar muß $r \geq 2$ sein.
Außerdem normieren wir X_r zu 1 und nehmen noch $X_1 \notin F$ an (alle $X_i \in F \Rightarrow \omega_1, \ldots, \omega_r$ linear abhängig), d.h. es existiert $h \in \{1, \ldots, n\}$ mit $\sigma_h(X_1) \neq X_1$.

Anwendung von σ_h auf alle n Gleichungen ergibt

$$\begin{aligned} \sum_{j=1}^{r} \sigma_h(X_j)\sigma_h\sigma_i(\omega_j) &= 0 \quad (1 \leq i \leq n), \text{ also} \\ \sum_{j=1}^{r} \sigma_h(X_j)\sigma_k(\omega_j) &= 0 \quad (1 \leq k \leq n). \end{aligned}$$

Subtraktion vom Ausgangssystem liefert:

$$\sum_{j=1}^{r-1} \sigma_k(\omega_j)(X_j - \sigma_h(X_j)) = 0 \quad (1 \leq k \leq n).$$

Wegen $X_1 \neq \sigma_h(X_1)$ steht dies jedoch im Widerspruch zur Minimalität von r.

□

Es sei L/K normal, endlich, und F sei der Fixkörper von $G(L/K)$.

Wir haben gesehen, daß F/K rein inseparabel ist (Bem. (iii) nach 3.43).

Offenbar ist $G(L/F) = G(L/K)$, also nach (4.3):

$$[L : F] = \sharp G(L/F) =_{3.43} [L : F]_{sep}.$$

Folglich ist L/F separabel.

Wir merken noch an, dass $F = \{\alpha \in L | \alpha/K$ rein iseparabel $\}$ gilt.

4.4. Definition

Eine algebraische Erweiterung L/K heißt Galoiserweiterung, falls K der Fixkörper von $G(L/K)$ ist. In diesem Fall heißt $G = G(L/K)$ Galoisgruppe von L/K.

4.5. Satz

L/K endlich: L/K galoissch $\Leftrightarrow L/K$ normal und separabel.

Beweis:

" $\Leftarrow$" Es sei $F = Fix\,(G(L/K))$ der Fixkörper zu $G(L/K)$.
Hierfür ist $[F : K] = [L : K]_i = 1$, also $F = K$.
" $\Rightarrow$" Es sei $\alpha \in L$.
Betrachte $\alpha_j := \sigma_j(\alpha)$ für $G(L/K) = \{\sigma_1, \ldots, \sigma_n\}$, hierunter seien - evtl. Umnummerieren - $\alpha_1, \ldots, \alpha_r$ paarweise verschieden. G permutiert $\{\alpha_1, \ldots, \alpha_r\}$.

Alle symmetrischen Funktionen in $\alpha_1, \ldots, \alpha_r$ bleiben demnach G-invariant,

speziell ist $g_\alpha(t) := \prod_{i=1}^{r} (t - \alpha_i)$ demnach aus $K = Fix\,(G)$.

Ein irreduzibler Teiler $\tilde{g}(t)$ von $g(t)$ in $K[t]$ hat dann mit einer Nullstelle α_j alle α_i als Nullstellen, also ist $g_\alpha(t) = m_\alpha(t)$. Damit ist L/K normal.
Ferner ist Fix $(G(L/K)) = K$, also nach dem Vorangehenden L/K separabel.

□

Bemerkung:
L/K galoissch und $K \subset E \subset L \to L/E$ galoissch.

4.6. Satz

(Hauptsatz der Galoistheorie)

Es sei L/K eine endliche Galoiserweiterung.

Dann gibt es eine Bijektion zwischen den Zwischenkörpern $K \subset E \subset L$ und den Untergruppen von $G(L/K)$ mittels $E \longleftrightarrow G(L/E)$.

Dabei ist E/K genau dann galoissch, wenn $G(L/E)$ Normalteiler in $G(L/K)$ ist, und in diesem Fall gilt:
$G(E/K) \cong G(L/K) \,/\, G(L/E)$.

Beweis:

(i) Zunächst ist $E \to G(L/E)$ eine injektive Abbildung (vgl. Beweis zu (3.44)).

Es bleibt die Surjektivität zu zeigen.

Dazu sei H eine Untergruppe von $G(L/K)$ und $F(H)$ der zugehörige Fixkörper. Dann ist $L/F(H)$ normal und separabel, also galoissch mit Galoisgruppe $G(L/F(H))$.

Also gilt $H < G(L/F(H))$.

Gemäß (4.3) ist $[L : F(H)] = (H : 1)$ und nach (3.42) $[L : F(H)] = (G(L/F(H)) : 1)$,

also $H = G(L/F(H))$.

(ii) Sei nun $K \subset E \subset L$.

Wir nehmen zunächst E/K als galoissch, d.h. normal und separabel, an.

Ferner seien $\sigma \in G(L/K)$ und $\tau \in G(L/E)$.

Für $\alpha \in E$ ist $\sigma(\alpha) \in E$, also $\sigma^{-1}\tau\sigma(\alpha) = \sigma^{-1}\sigma(\alpha) = \alpha$, und damit $\sigma^{-1}\tau\sigma \in G(L/E)$. Damit ist $G(L/E)$ Normalteiler.

Umgekehrt sei $G(L/E) \lhd G(L/K)$.

Trivialerweise ist E/K separabel, es bleibt E/K normal zu zeigen.

Dazu sei $f \in K[t]$ irreduzibel mit Nullstelle $\alpha \in E$.

In $L[t]$ zerfällt f in Linearfaktoren,

alle Nullstellen sind dabei von der Form $\sigma(\alpha)$ $(\sigma \in G(L/K))$.

Für alle $\tau \in G(L/E)$ existiert nun $\rho \in G(L/E)$ mit $\tau = \sigma\rho\sigma^{-1}$, d.h. $\tau(\sigma(\alpha)) = \sigma\rho\sigma^{-1}(\sigma(\alpha)) = \sigma\rho(\alpha) = \sigma(\alpha)$,

d.h. $\sigma(\alpha) \in F(G(L/E)) = E$.

Also zerfällt f bereits in $E[t]$ in Linearfaktoren, und E/K ist normal.

(iii) Definiere $\phi : G(L/K) \to G(E/K) : \sigma \mapsto \sigma \mid_E$.

ϕ ist Homomorphismus wegen $\sigma \mid_E$ Automorphismus und gemäß (3.40) surjektiv.

$Ker\ \phi = \{\sigma \in G(L/K) \mid \sigma \mid_E = id_E\} = G(L/E)$.

Damit folgt die behauptete Isomorphie aus dem Homorphiesatz für Gruppen.

□

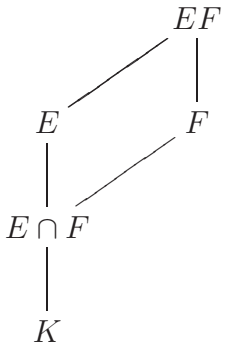
4.7. Korollar

Es sei L/K galoissch, E, F seien Zwischenkörper. Dann gilt: $E \subseteq F \iff G(L/E) \supseteq G(L/F)$.

4.8. Satz

Es sei L/K eine Körpererweiterung mit Zwischenkörpern E, F. Ist dann E/K eine endliche
Galoiserweiterung, so ist EF eine Galoiserweiterung von F mit $G(EF/F) \cong$

$G(E/E \cap F)$.



Beweis:

E/K ist Zerfällungskörper eines Polynoms $f \in K[t]$, dessen Faktoren lauter einfache Nullstellen besitzen.

Dann ist auch EF Zerfällungskörper von $f \in F[t]$, d.h. EF/F ist normal und separabel, also galoissch.

Es seien nun $\sigma \in G(EF/F)$ und $\alpha_1, \ldots, \alpha_n$ die verschiedenen Nullstellen von f. Dann induziert σ eine Permutation dieser Nullstellen, die einem Element $\tilde{\sigma} \in G(E/K)$ entspricht. Verschiedene σ induzieren so verschiedene $\tilde{\sigma}$, die Zuordnung $\sigma \mapsto \tilde{\sigma}$ liefert einen Isomorphismus von $G(EF/F)$ auf eine Untergruppe von $G(E/K)$. σ (und damit $\tilde{\sigma}$) läßt jedes Element von $F \cap E$ invariant, d. h. $\tilde{\sigma} \in G(E/E \cap F)$.

Jedes Element $\tilde{\sigma} \in G(E/E \cap F)$ permutiert $\alpha_1, \ldots, \alpha_n$ und ist daher als Bild eines $\sigma \in G(EF/F)$ erhältlich.

Also folgt die behauptete Isomorphie.

□

4.9. Definition

Es sei L/K galoissch.

Ist dann $G(L/K)$ abelsch, zyklisch etc., so heißt auch die Erweiterung L/K abelsch, zyklisch etc..

Beispiel:

Für $f(t) = t^3 - 2 \in \mathbb{Q}[t]$ ist der Zerfällungskörper $K = \mathbb{Q}(\sqrt[3]{2},\ \sqrt{-3})$.

Demnach ist $[K : \mathbb{Q}] = 6$ und $K/\mathbb{Q}$ normal und separabel, also galoissch.

Alle 6 $\mathbb{Q}$ -Automorphismen von K sind durch ihre Wirkung auf $\sqrt[3]{2}$ und $\sqrt{-3}$ eindeutig bestimmt.

Wir setzen $\xi := \dfrac{-1 + \sqrt{-3}}{2}$ und

$$\sigma \ : \ K \to K \text{ mittels } \sqrt[3]{2} \mapsto \sqrt[3]{2},\ \sqrt{-3} \mapsto -\sqrt{-3} \qquad (\xi \mapsto \xi^2),$$
$$\tau \ : \ K \to K \text{ mittels } \sqrt[3]{2} \mapsto \xi\sqrt[3]{2},\ \sqrt{-3} \mapsto +\sqrt{-3} \qquad (\xi \mapsto \xi)$$

und erhalten folgende Tabelle:

	id	τ	τ^2	σ	$\sigma\tau$	$\sigma\tau^2$
$\sqrt[3]{2}$	$\sqrt[3]{2}$	$\xi\sqrt[3]{2}$	$\xi^2\sqrt[3]{2}$	$\sqrt[3]{2}$	$\xi^2\sqrt[3]{2}$	$\xi\sqrt[3]{2}$
$\sqrt{-3}$	$\sqrt{-3}$	$\sqrt{-3}$	$\sqrt{-3}$	$-\sqrt{-3}$	$-\sqrt{-3}$	$-\sqrt{-3}$

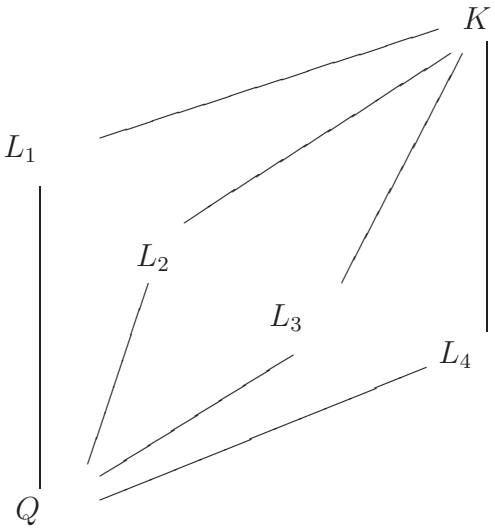
Die Untergruppen von $G(K/\mathbb{Q}) \cong S_3$ sind:

$$H_1 = \{id,\ \sigma\},\ H_2 = \{id,\ \sigma\tau\},\ H_3 = \{id,\ \sigma\tau^2\},\ H_4 = \{id,\ \tau,\ \tau^2\}.$$

Diesen entsprechen die Fixkörper

$$L_1 = \mathbb{Q}(\sqrt[3]{2}),\ L_2 = \mathbb{Q}(\xi\sqrt[3]{2}),\ L_3 = \mathbb{Q}(\xi^2\sqrt[3]{2}), L_4 = \mathbb{Q}(\sqrt{-3}).$$

Also ist $L_4/\mathbb{Q}$ galoissch, jedoch $L_i/\mathbb{Q}$ nicht normal $(1 \leq i \leq 3)$.



Wir haben dabei
$L_1 = \mathbb{Q}(\sqrt[3]{2})$
$L_2 = \mathbb{Q}(\xi\sqrt[3]{2})$
$L_3 = \mathbb{Q}(\xi^2\sqrt[3]{2})$
und $L_4 = \mathbb{Q}(\sqrt{-3})$.

Beispiel:
Gleichungen dritten Grades und ihre Diskriminanten.
Es sei $f[t] \in \mathbb{Z}[t]$ mit $deg\ (f) = 3$ irreduzibel.
Dann hat der Zerfällungskörper von f über $\mathbb{Q}$ genau dann den Grad 3, falls die Diskriminante der Nullstellen von f ein Quadrat in $\mathbb{Z}$ ist.
Dazu seien ρ_1, ρ_2, ρ_3 die Nullstellen von f in $\mathbb{C}$.
Dann ist $D(\rho_1, \rho_2, \rho_3) = \prod_{1 \leq i < j \leq 3} (\rho_1 - \rho_j)^2$,
also $D(\rho_1, \rho_2, \rho_3) \in \mathbb{Z}$ wegen $D(\rho_1, \rho_2, \rho_3) = \det\left(S_{i+j-2}(\rho_1, \rho_2, \rho_3)\right) \in \mathbb{Z}$.

Für Zerfällungskörper M von f über $\mathbb{Q}$ gibt es nun genau zwei Möglichkeiten:

(i) $[M : \mathbb{Q}] = 3 \Rightarrow M = \mathbb{Q}(\rho_1) \Rightarrow G(M/\mathbb{Q}) \cong C_3 \Rightarrow \tilde{D} = \sqrt{D}$ invariant unter $G(M/\mathbb{Q})$
$\Rightarrow \tilde{D} \in Fix(G(M/\mathbb{Q})) = \mathbb{Q}$;

(ii) $[M : \mathbb{Q}] = 6 \Rightarrow G(M/\mathbb{Q}) \cong S_3 \Rightarrow G(M/\mathbb{Q})$ enthält Transposition, etwa (23),
d.h. $\sigma(\tilde{D}) = -\tilde{D}$ für ein $\sigma \in G(M/\mathbb{Q}) \Rightarrow \tilde{D} = \sqrt{D} \notin Fix(G(M/\mathbb{Q})) = \mathbb{Q}$ wegen $\tilde{D} \neq 0$.

4.10. Satz

Es sei K eine endliche Erweiterung von $\mathbb{F}_p$ vom Grad n.
Dann ist $K/\mathbb{F}_p$ galoissch mit $G(K/\mathbb{F}_p) = \langle\sigma\rangle$,
wobei σ der Frobenius-Automorphismus von K ist, $\sharp\langle\sigma\rangle = n$.
Ist L eine Erweiterung von K vom Grad m, so ist auch L/K galoissch
mit Galoisgruppe $G(L/K) = \langle\psi\rangle$, wobei ψ durch $x \mapsto x^{p^n}$ gegeben ist, $\sharp\langle\psi\rangle = m$.

Beweis:

(i) Die Erweiterung $K/\mathbb{F}_p$ ist normal als Zerfällungskörper von $t^{p^n} - t$;
sie ist separabel, weil $\mathbb{F}_p$ vollkommen ist.
Die Abbildung $\sigma : K \to K : x \mapsto x^p$ ist - wie früher gezeigt - ein Monomorphismus, der wegen $\sharp K < \infty$ surjektiv ist.
Da für $x \in \mathbb{F}_p$ zudem $x^p = x$ gilt, ist $\sigma \in G(K/\mathbb{F}_p)$.
Wir betrachten die zyklische Untergruppe $\langle\sigma\rangle =: U$ von $G = G(K/\mathbb{F}_p)$.
Es gilt: $\sigma^\upsilon : K \to K : x \mapsto x^{p^\upsilon}$, d.h. $\sigma^\upsilon = id_k$ erstmalig für $\upsilon = n$.
Also ist $\sharp U = n = \sharp G$ und damit $U = G$.

(ii) L/K ist galoissch (vgl. (i)).
Wegen (4.3) gilt: $\sharp G(L/K) = m$.
Als Untergruppe von $G(L/\mathbb{F}_p)$ ist $G(L/K)$ zyklisch.
Die Gruppe wird erzeugt durch $\psi : L \to L : x \mapsto x^{p^n}$.

□

4.11. Definition

Es sei K ein Primkörper.
Jede Wurzel des Polynoms $t^n - 1 \in K[t]$ heißt n-te Einheitswurzel über K.
Der Zerfällungskörper K_n von $t^n - 1$ heißt n-ter Kreisteilungskörper über K.

Im folgenden seien stets die Voraussetzungen von (4.11) gegeben.

In K_n zerfällt $t^n - 1$ in Linearfaktoren. Für die Nullstellenmenge E_n von $t^n - 1$ in K_n gilt dabei:

4.12. Satz

Es sei $t^n - 1 \in K[t]$, K Primkörper.

Im Zerfällungskörper K_n von $t^n - 1$ bezeichne E_n die Nullstellenmenge von $t^n - 1$ ($\sharp E_n \leq n$).

Dann gilt:

(i) E_n ist zyklische Untergruppe von $K_n^\times$.
(ii) Für $\chi(K) = p$ mit $p|n$ gilt $E_n = E_{n/p}$.
(iii) Für $\chi(K) \not| n$ gilt $\sharp E_n = n$.
(iv) $\forall m \in \mathbb{N}$ gilt $E_n \subseteq E_{mn}$, also $K_n \subseteq K_{mn}$.

Beweis:

(i) Gemäß (3.9), denn mit $x, y \in K_n$ und $x^n = y^n = 1$ folgt $(xy)^n = (xy^{-1})^n = 1$,
also $E_n < K^\times$.
(ii) Es sei $n = pm$; es folgt $t^n - 1 = (t^m)^p - 1 = (t^m - 1)^p$.
(iii) $t^n - 1$ besitzt n Nullstellen in K_n, die wegen $\mathrm{ggT}\,(t^n - 1, (t^n - 1)') = \mathrm{ggT}\,(t^n - 1, nt^{n-1}) = 1$ alle verschieden sind. (Beachte: $n \neq 0$ in K_n).
(iv) $x^n = 1 \Rightarrow x^{nm} = 1 \forall m \in \mathbb{N}$.

□

Wegen (ii) können wir im weiteren stets $\chi(K) \nmid n$ annehmen!

Dann gilt $E_n = <\xi>$, $\sharp E_n = n$, also $E_n = \{1, \xi, \ldots, \xi^{n-1}\}$.

Jedes erzeugende Element der zyklischen Gruppe E_n heißt dann primitive $n - te$ Einheitswurzel.

Ist $E_n = <\xi>$, so gilt $K_n = K[\xi]$.

Wegen $\mathrm{ord}(\xi^m) = \dfrac{n}{ggT(m,n)}$ gibt es genau $\varphi(n)$ primitive $n - te$ Einheitswurzeln.

Hierbei mißt die Eulersche Funktion φ die Anzahl der zu n teilerfremden Zahlen in $\{1, 2, \ldots, n\}$.

Es bezeichne F_n die Menge der primitiven $n - ten$ Einheitswurzeln, dann gilt $F_n \subseteq E_n$, $\sharp F_n = \varphi(n)$.

4.13. Hilfssatz

(i) Für $m \neq n, m, n \in \mathbb{N}$ ist $F_m \cap F_n = \emptyset$.
(ii) $E_n = \dot{\bigcup\limits_{d|n}} F_d$.
(iii) $n = \sum\limits_{d|n} \varphi(d)$.

Beweis:

(i) Trivial.

(ii) Klar ist zunächst $E_n \supseteq \bigcup_{d|n} F_d$.

Die Vereinigung ist wegen (i) zudem disjunkt.

Ist andererseits $\xi \in E_n$, so existiert ein minimaler Exponent $m \in N$ mit $\xi^m = 1$ und $m|n$.

Hierfür ist ξ eine primitive $m - te$ Einheitswurzel.

(iii) Folgt sofort aus (ii).

□

4.14. Definition

$\Phi_n(t) := \prod_{\xi \in F_n} (t - \xi) \in K_n[t]$ heißt n-tes Kreisteilungspolynom über K.

Bemerkungen:

Offensichtlich ist $\deg(\Phi_n) = \varphi(n)$.

Ist ξ irgendeine primitive $n - te$ Einheitswurzel, so gilt $\Phi_n(t) = \prod_{\substack{i=1 \\ \text{ggT}\,(i,n)=1}}^{n} (t - \xi^i)$.

Damit folgt aus (4.13)(ii) unmittelbar $t^n - 1 = \prod_{d|n} \Phi_d(t)$ in $K_n[t]$.

4.15. Satz

Es ist $\Phi_n(t) \in K[t]$; speziell für $K = \mathbb{Q}$ gilt sogar $\Phi_n(t) \in \mathbb{Z}[t]$.

Beweis:

Mittels Induktion nach n!

$n = 1 : \Phi_1(t) = t - 1$

$1, \ldots, n-1 \to n :$

Wegen

$$t^n - 1 = \prod_{d|n} \Phi_d(t) \text{ ist } \Phi_n(t) = (t^n - 1)/ \underbrace{\left(\prod_{\substack{d|n \\ d<n}} (\Phi_d(t))\right)}_{=:g_n(t) \in K[t] \text{ bzw. } \mathbb{Z}[t]} \quad \text{in } K_n(t)$$

nach Induktionsannahme.

Also existieren Polynome $h_n(t)$, $r_n(t)$ aus $K[t]$ bzw. $\mathbb{Z}[t]$ mit $t^n - 1 = h_n(t)g_n(t) + r_n(t)$

und $\deg(r_n) < n - \varphi(n)$.

Da diese Zerlegung auch in $K_n(t)$ Gültigkeit besitzt, folgt $r_n(t) = 0$ und $h_n(t) = \Phi_n(t)$.

□

4.16. Satz

Es gilt $[K_n : K] = \varphi(n)$ für $K = \mathbb{Q}$; speziell ist $\Phi_n(t)$ in $\mathbb{Z}[t]$ irreduzibel, $K_n/\mathbb{Q}$ galoissch.

Beweis:

Offenbar ist $[K_n : K] \leq \varphi(n)$, da $\Phi_n(t)$ in K_n in Linearfaktoren zerfällt und

$K_n = K(\xi)$ mit ξ Nullstelle von Φ_n ist. Wir zeigen also noch $[K_n : K] \geq \varphi(n)$.

Dazu sei ξ eine Nullstelle von $\Phi_n(t)$ mit Minimalpolynom $m_\xi(t) \in K[t]$.

Hierfür gilt $m_\xi(t) | \Phi_n(t)$, d.h. es existiert $h(t) \in K[t]$ (nominiert!) mit $\Phi_n = m_\xi h$. Nach Gauß besteht diese Faktorisierung sogar in $\mathbb{Z}[t]$.

Wir zeigen: Ist nun x Nullstelle von m_ξ, so auch x^p für alle Primzahlen p, die n nicht teilen.

Daraus folgt dann sofort, daß jede primitive $n - te$ Einheitswurzel Nullstelle von m_ξ ist, also $m_\xi(t) = \Phi_n(t)$ gilt.

Annahme: x^p ist keine Nullstelle von m_ξ. Dies bedeutet wegen $\Phi_n(x^p) = 0$ jedoch $h(x^p) = 0$,

d.h. x Nullstelle von $h(t^p)$ bzw. $m_\xi(t) | h(t^p)$ oder $h(t^p) = m_\xi(t) g(t)$ in $\mathbb{Z}[t]$.

Also folgt wegen $h(t^p) \equiv h(t)^p \ mod\, p\mathbb{Z}[t]$ auch $h(t)^p \equiv m_\xi(t) g(t)$ $mod\ p\mathbb{Z}[t]$,

d.h. in $\mathbb{F}_p[t]$ gilt: $\mathrm{ggT}\,(\bar{h}, \bar{m}_\xi) \neq 1$,

was dann bedingt, daß $t^n - 1$ mehrfache Nullstellen in $\mathbb{F}_p[t]$ besitzt.

Dies ist jedoch ein Widerspruch zu $p \nmid n$.

□

Schreibt man die Möbiusche Umkehrformel multiplikativ, so erhält man:

$$\forall\, n \in \mathbb{N} : f(n) = \prod_{d|n} g(d) \Longleftrightarrow \forall\, n \in \mathbb{N} : g(n) = \prod_{d|n} f(d)^{\mu(n/d)}.$$

Wir wenden dies auf $f(n) = t^n - 1,\ g(d) = \Phi_d(t)$ an und erhalten

(1)
$$\Phi_n(t) = \prod_{d|n} (t^d - 1)^{\mu(n/d)}.$$

Hiermit lässt sich $\Phi_n(t)$ leicht berechnen. Wir erhalten für $n = 12$:

$$\Phi_{12}(t) = \frac{(t^2 - 1)(t^{12} - 1)}{(t^4 - 1)(t^6 - 1)} = t^4 - t^2 + 1.$$

Beispiel:
Über $\mathbb{F}_5$ gilt:
$\Phi_{12}(t) = t^4 - t^2 + 1 = (t^2 - 2t - 1)(t^2 + 2t - 1) = (t - \xi)(t - \xi^5) \cdot (t - \xi^7)(t - \xi^{11})$
(4.16) wird falsch!

Bemerkung:
Über $\mathbb{F}_p$ mit $p \not| n$ ist $[K_n : K] = \min\{m \in \mathbb{N} | p^m - 1 \equiv 0 \bmod n\}$.

4.17. Satz

Für $n \in \mathbb{N}$ ist $G(K_n/\mathbb{Q}) \cong U(\mathbb{Z}/n\mathbb{Z})$.

Beweis:
Es seien ξ eine (feste) primitive $n - te$ Einheitswurzel,
$K_n = \mathbb{Q}(\xi)$, und $h \in \mathbb{N}$ mit $1 \leq h \leq n$, ggT $(h, n) = 1$.
Dann sind ξ und ξ^h beide Nullstellen des irreduziblen Polynoms $\Phi_n(t) \in \mathbb{Z}[t]$,
welches in $K_n[t]$ in Linearfaktoren zerfällt, und es gilt $K_n(\xi) = K_n(\xi^h)$.
Wir definieren $\varphi : U(\mathbb{Z}/n\mathbb{Z}) \to G(K_n/\mathbb{Q}) : h + n\,\mathbb{Z} \mapsto \sigma_h$,
wobei $\sigma_h : K_n \to K_n$ mittels $\xi \mapsto \xi^h$ gegeben ist.
Offensichtlich ist σ_h ein Element aus $G(K_n/\mathbb{Q})$, vgl. (3.17).
φ ist wohldefiniert wegen $\xi^n = 1$, injektiv (und damit surjektiv).
Zur Homomorphie: $\varphi(hk + n\,\mathbb{Z}) = \sigma_{hk} = \sigma_h\sigma_k = \varphi(h + n\,\mathbb{Z})\varphi(k + n\,\mathbb{Z})$.

□

4.18. Korollar

Der n-te Kreiskörper K_n ist abelsch über $\mathbb{Q}$.
Alle Zwischenkörper F mit $\mathbb{Q} \subset F \subset K_n$ sind über $\mathbb{Q}$ galoissch.

Konstruktion mit Zirkel und Lineal

Gegeben sei eine zweidimensionale affine Ebene mit kartesischem Koordinatensystem sowie dem Punkt (1,0) auf der x-Achse.

Konstruktionsregeln

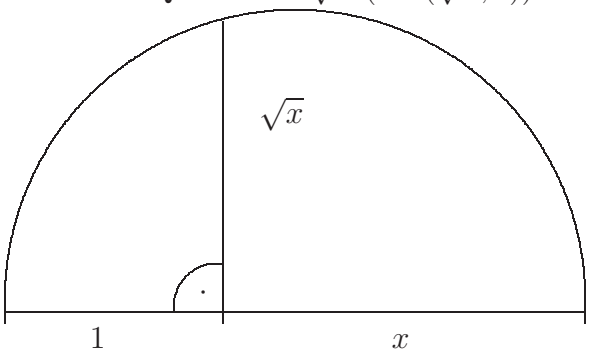
(i) Durch zwei gegebene Punkte läßt sich (eindeutig) eine Gerade zeichnen.
(ii) Um einen gegebenen Punkt läßt sich (eindeutig) ein Kreis zeichnen, dessen Radius gleich dem Abstand zweier gegebener Punkte ist.
(iii) Neue Punkte entstehen als Schnittpunkte von zwei Geraden, zwei Kreisen oder einer Geraden mit einem Kreis.

Konstruierbar sind dann (in endlich vielen Schritten!!!):

I. Alle Punkte (x,0) mit $x \in \mathbb{Q}, (0, y)$ mit $y \in \mathbb{Q}, (x, y) \in \mathbb{Q}^2$.

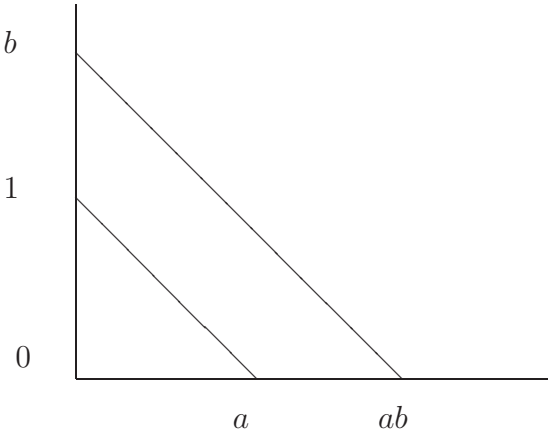
(Eine Strecke läßt sich in n gleiche Stücke teilen, da man zu einer Geraden und einem Punkt P außerhalb eine Parallele durch P konstruieren kann).

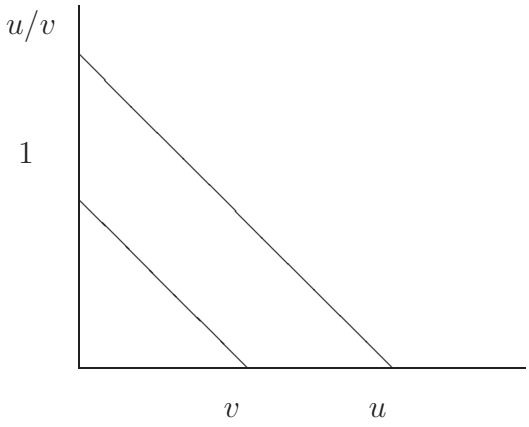
II. Zu $x \in \mathbb{Q}$ läßt sich $\sqrt{x}$ (als $(\sqrt{x}, 0)$) konstruieren.



Betrachte die Menge L der konstruierbaren reellen Zahlen x.

III. Mit u, v ist $u \pm v$ konstruierbar, sowie $uv, \frac{u}{v}$ $(v \neq 0)$.





Also gilt: $\mathbb{Q} \subset L \subset \mathbb{R}$, L Körper.

Es seien nun die bisher konstruierten Punkte im Körper $K \supseteq \mathbb{Q}$ enthalten.

(i) Schneide die Geraden durch $(x_1, y_1) \neq (x_2, y_2)$ bzw. $(u_1, v_1) \neq (u_2, v_2)$:

$$\frac{y - y_1}{x - x_1} = \frac{(y_2 - y_1)}{(x_2 - x_1)} =: r_1, \quad \frac{y - v_1}{x - u_1} = \frac{v_2 - v_1}{u_2 - u_1} =: r_2, \ \ r_1 \neq r_2,$$

$$y = r_1 x \underbrace{- x_1 r_1 + y_1}_{s_1} = r_2 x - u_1 r_2 + v_1, \quad x = \frac{x_1 r_1 - y_1 - u_1 r_2 + v_1}{r_1 - r_2}, \ \ (x, y) \in K.$$

(ii) Schneide Gerade durch $(x_1, y_1) \neq (x_2, y_2)$ mit Kreis um (u, v) vom Radius $r : y = r_1 x + s_1$, $(x-u)^2 + (y-v)^2 = r^2$
$\Rightarrow x$ genügt quadratischer Gleichung,
eine Lösung liegt in Erweiterung $\tilde{K}$ von K vom Grad ≤ 2 ($\tilde{K}/K$ galoissch).

(iii) Schneide Kreis um (u_1, v_1) vom Radius r_1, mit dem um (u_2, v_2) vom Radius r_2.

$(x-u_1)^2 + (y-v_1)^2 = {r_1}^2$, $(x-u_2)^2 + (y-v_2)^2 = {r_2}^2$,
$(x-u_2)^2 = (x-u_1)^2 - 2u_1 x + \delta^2$ ($\delta = u_2 - u_1$),
$(y-v_2)^2 = (y-v_1)^2 - 2v_1 y + \gamma^2$ ($\gamma = v_2 - v_1$),
${r_2}^2 = {r_1}^2 - 2u_1 x - 2v_1 y + \gamma^2 + \delta^2$ usw.
$\Rightarrow x$ genügt quadratischer Gleichung, fahre fort wie in (ii).

4.19. Satz

$x \in \mathbb{R}$ ist genau dann konstruierbar, wenn es einen endlichen Körperturm
$\mathbb{Q} = K_0 \subset K_1 \subset K_2 \subset \ldots \subset K_n \subset \mathbb{R}$ mit $x \in K_n$ gibt,
wo stets $K_i = K_{i-1}(\sqrt{\beta_i})$ mit $\beta_i \in K_{i-1}$, $\beta_i > 0$, $\sqrt{\beta_i} \notin K_{i-1}$ ($1 \leq i \leq n$) gilt.
$K_n = \mathbb{Q}(\sqrt{\beta_1} \ldots, \sqrt{\beta_n})$.

Beweis:
x konstruierbar $\Rightarrow x$ liegt in solchem K_n.
Jede Zahl aus K_n ist konstruierbar: $x \in K_n \Rightarrow x = a + b\sqrt{\beta_n}$ mit $a, b, \beta_n \in K_{n-1}$,
dann wende Induktion über n an und beachte Konstruktionsregeln II und III.

□

4.20. Korollar

(i) $x \in \mathbb{R}$ konstruierbar $\Rightarrow x$ liegt in Körper K mit $\mathbb{Q} \subset K \subset \mathbb{R}$ und $[K : \mathbb{Q}] = 2^n$ ($n \in \mathbb{Z}^{\geq 0}$).

(ii) Transzendente Zahlen aus $\mathbb{R}$ sind nicht konstruierbar.

(iii) $x \in \mathbb{R}$ algebraisch über $\mathbb{Q}$ mit $[\mathbb{Q}(x) : \mathbb{Q}] = n$ und n keine Potenz von 2 ist nicht konstruierbar.

Anwendungen:

(i) *Delisches Problem*: Verdoppelung eines Würfels gegebener Kantenlänge x.
Die zu konstruierende Kantenlänge ist $\sqrt[3]{2}x$. Dies ist genau dann möglich, falls $\sqrt[3]{2}$ konstruierbar ist.
Wegen $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ ist dies über $\mathbb{Q}$ unmöglich.
Dagegen ist $t^2 - 2$ reduzibel in $\mathbb{Q}(\sqrt{2})$, $\sqrt{2}$ ist konstruierbar.

(ii) *Quadratur des Kreises*: $\pi r^2 = x^2$. Dies geht nur, falls $\sqrt{\pi}$ konstruierbar ist.

Da π bzw. $\sqrt{\pi}$ transzendent sind, ist dies unmöglich.

(iii) *Winkeldreiteilung*: Winkel α konstruierbar $\Leftrightarrow$ $\cos\alpha, \sin\alpha$ konstruierbar!

$\cos 3x + i\sin 3x = e^{2\pi i 3x} = (e^{2\pi i x})^3 = (cosx + i\sin x)^3 =$

$\cos^3 x - 3\cos x \sin^2 x + i(3\cos^2 x \sin x - \sin^3 x)$

impliziert (mit $\sin^2 x = 1 - \cos^2 x$) :

$\cos 3x = 4\cos^3 x - 3\cos x$.

Also ist der Winkel $3x$ "drittelbar" $\Leftrightarrow 4t^3 - 3t - \cos 3x$ in $K = \mathbb{Q}(\cos 3x)$

reduzibel und $K/\mathbb{Q}$ konstruierbar. Dies ist jedoch i.a. falsch!

$x = 20^0 : 4t^3 - 3t - \frac{1}{2} = 0 \Leftrightarrow (2t)^3 - 3(2t) - 1 = 0.$

Jedoch ist $u^3 - 3u - 1$ irreduzibel.

$x = 15^0 : 4t^3 - 3t - \frac{\sqrt{2}}{2} = 0 \Leftrightarrow u^3 - 3u - \sqrt{2} = 0.$

Dies ist reduzibel in $\mathbb{Q}(\sqrt{2})$, x ist konstruierbar.

(iv) *Reguläre $n-Ecke$* : Konstruierbar $\Leftrightarrow \deg(\Phi_n) = \varphi(n)$ Potenz von 2.

(Für "$\Leftarrow$" beachte, daß die Galoisgruppe eines Kreiskörpers abelsch ist.)

Für $n = 2^{m_0} p_1^{m_1} \dots p_r^{m_r}$ (p_i paarweise verschiedene ungerade Primzahlen)

ist $\Phi(n) = 2^{max(0,m_o-1)} p_1^{m_1-1}(p_1-1)\dots p_r^{m_r-1}(p_r-1)$.

Dies ist genau dann eine Potenz von 2, falls $m_1 = \dots = m_r = 1$ und $p_i := 2^{k_i} + 1 (k_i \in \mathbb{N})$ ist. D.h. die p_i sind sog. *Fermatsche Primzahlen*.

(Beachte : $k_i = 2^{l_i}$, denn für $k_i = \varphi_i \gamma_i$, γ_i ungerade, ist $2^{k_i}+1$ durch $2^{\varphi_i}+1$ teilbar).

l_i	0	1	2	3	4
p_i	3	5	17	257	65537

(Für $l_5 = 5$ ist p_5 keine Primzahl.)

Das reguläre n-Eck ist genau dann konstruierbar, falls $n = 2^{m_0} p_1 \dots p_r$ mit paarweise verschiedenen Fermatschen Primzahlen p_i ist ($m_0 \in \mathbb{Z}^{\geq 0}$).

Beispiel: $n = 17$.

Zyklische Erweiterungen

4.21. Satz

Es sei K ein Körper, $n \in \mathbb{N}$ mit $\chi(K) \nmid n$, K enthalte eine primitive $n-te$ Einheitswurzel ζ.

(i) Ist α Nullstelle von $t^n - a \in K[t]$, so ist $K(\alpha)$ zyklisch über K.

(ii) Ist L/K zyklisch vom Grad n, so ist L Zerfällungskörper eines Polynoms $t^n - a \in K[t]$.

Beweis:

(i) Ist α Nullstelle von $t^n - a$ und ζ eine primitive $n - te$ Einheitswurzel,

so gilt $t^n - a = \prod_{i=0}^{n-1}(t - \alpha\zeta^i)$ in $K(\alpha)[t]$.

$K(\alpha)$ ist also Zerfällungskörper eines separablen Polynoms über K.

Wir zeigen im Anschluß an diesen Beweis, daß dann $K(\alpha)/K$ separabel ist.

Also ist $K(\alpha)/K$ galoissch.

Gemäß (...Nr.?) enthält $G(K(\alpha)/K)$ Automorphismen σ_i gegeben durch $\alpha \mapsto \alpha\zeta^i$

(für $\alpha\zeta^i$ Nullstelle von $m_\alpha(t)$).

Analog zum Beweis von (...Nr.?) erhält man einen Gruppenepimorphismus

$$\psi : (\mathbb{Z}/n\mathbb{Z}, +) \to G(K(\alpha)/K) : k + n\mathbb{Z} \mapsto \sigma_k,$$

also ist $G(K(\alpha)/K)$ isomorph zu einer Faktorgruppe von $(\mathbb{Z}/n\mathbb{Z}, +)$, also zyklisch.

(ii) Gemäß (...Nr.?) sind die Automorphismen $\sigma_i := \sigma^i \qquad (0 \leq i < n)$ für $G(L/K) = <\sigma>$

linear unabhängig.

Mit $\zeta \in K$ bilden wir $\mu := \sigma_0 + \zeta\sigma_1 + \ldots + \zeta^{n-1}\sigma_{n-1}$.

Hierzu exististiert dann $\gamma \in L$ mit $0 \neq \beta := \mu(\gamma) = \sum_{i=0}^{n-1} \zeta^i\sigma_i(\gamma)$.

Also gilt auch $0 \neq \sigma(\beta) = \sum_{i=1}^{n} \zeta^{i-1}\sigma_i(\gamma) = \zeta^{-1}\mu(\gamma)$, sowie $\sigma(\beta^n) = \beta^n$,

und damit $a := \beta^n \in K = F(G(L/K)) = F(<\sigma>)$.

Folglich ist $\beta \in L$ Nullstelle von $t^n - a \in K[t]$.

Mit β sind auch $\sigma^{-i}(\beta) = \beta\zeta^i \qquad (0 \leq i < n)$ Nullstellen von $m_\beta(t) \in K[t]$,

diese sind jedoch paarweise verschieden, also folgt $\deg(m_\beta) \geq n$.

Wegen $m_\beta(t)|(t^n - a)$ folgt hier Gleichheit

und wegen $G(L/K) = n = [L : K] = [K(\beta) : K]$ dann auch $L = K(\beta)$.

□

Auflösung algebraischer Gleichungen durch Radikale

Im folgenden sei K ein Körper der Charkteristik 0.

4.22. Definition

Eine Körpererweiterung L/K heißt Radikalerweiterung,
wenn es einen Körperturm $K = K_0 \subset K_1 \subset \ldots \subset K_m = L$ gibt,
bei dem K_i aus K_{i-1} durch Adjunktion einer Wurzel von $t^{n_i} - a_i \in K_{i-1}[t]$ entsteht.

Eine Gleichung $f(x) = 0$ mit $f(t) \in K[t]$ heißt durch Radikale auflösbar,
falls es eine Radikalerweiterung L/K gibt, die einen Zerfällungskörper von f als Teilkörper enthält.

4.23. Satz

Zu jeder Radikalerweiterung L/K existiert eine Radikalerweiterung M/K mit $M \supseteq L$,
M/K galoissch.

Beweis:
Mittels Induktion nach $r = [L : K]$.
$r = 1$.
Es ist $L = K$, also nichts zu zeigen.
Sei also $r > 1$ und L/K Radikalerweiterung mit Körperturm $K = K_0 \subset K_1 \subset K_2 \subset \ldots \subset K_m = L$.

1. Fall: $m = 1$.
Dann ist $L = K(\alpha)$ mit $\alpha^n = a \in K$.
Ist dann ζ eine primitive $n-te$ Einheitswurzel, so setze $M = L(\zeta)$:
$K \subseteq L \subseteq M$ ist ebenfalls Radikalerweiterung.
Hierin ist nun M als Zerfällungskörper von $(t^n - a)(t^n - 1)$ galoissch über K.

2. Fall: $m \geq 2$.
Dann ist K_{m-1} Radikalerweiterung von K mit $[K_{m-1} : K] = [L : K] \,/\, [L : K_{m-1}] < [L : K] = r$.
Nach Induktionsvoraussetzung exisitiert eine galoissche Radikalerweiterung N über K,
die K_{m-1} umfaßt.
Wegen (...Nr.?) ist N Zerfällungskörper eines Polynoms $g \in K[t]$.
Nach Voraussetzung gilt $L = K_{m-1}(\gamma)$ mit $\gamma^n \in K_{m-1}$.
Hiermit bilden wir das Polynom $f(t) := \prod_{\sigma \in G(N/K)}(t^n - \sigma(\gamma^n)) = \sum a_i t^i$ in $N[t]$.
Nach Konstruktion ist f invariant unter allen $\sigma \in G(N/K)$,
d.h. $\sigma(a_i) = a_i \; \forall_i$, also $a_i \in F(G(N/K)) = K$.
Es sei M der Zerfällungskörper von f über N.
Nach Konstruktion von f ist M Radikalerweiterung von N, also auch von K.
Wegen $f(\gamma) = 0$ gilt $\gamma \in M$, also $L \subseteq M$.
Es bleibt zu zeigen, daß M/K galoissch ist.

Offenbar ist M Zerfällungskörper von gf über K (beachte $f \in K[t]$!),
also ist M/K normal (...Nr.?) und separabel ($\chi(K) = 0$).

□

4.24. Definition

Eine endliche Gruppe G heißt auflösbar,
falls eine Kette von Untergruppen $G = G_0 \supset G_1 \supset G_2 \supset \ldots \subset G_n = 1$ existiert,
so daß $G_{i+1} \triangleleft G_i$ gilt und G_i/G_{i+1} abelsch ist $(0 \leq i < n)$.

4.25. Hilfssatz

(i) Jede endliche abelsche Gruppe ist auflösbar mit zyklischen Faktorgruppen.
(ii) Eine endliche Gruppe ist genau dann auflösbar,
falls eine Untergruppenkette $G = G_0 \supset G_1 \supset \ldots \supset G_n = 1$ mit $G_{i+1} \triangleleft G_i$ und G_i/G_{i+1} zyklisch existiert.

Beweis:

(i) Induktion über $m = (G : 1)$. $m = 1$ ist trivial.
Sei also $m > 1$.
Ist G selbst zyklisch, so ist nichts zu zeigen.
Andernfalls sei $H =< x >$ zyklische Untergruppe von G mit $x \neq 1$.
Nach Induktionsvoraussetzung ist dann G/H auflösbar mit zyklischen Faktorgruppen,
d.h. es exististieren Untergruppen $G_i/H \quad (0 \leq i \leq r,\ G_0 = G,\ G_r = H)$
mit $G_i/H\ /G_{i+1}/H \cong G_i/G_{i+1}$ zyklisch.
Dann leistet $G = G_0 \supset G_1 \supset \ldots \supset G_{r-1} \supset G_r = H \supset 1$ das Gewünschte.
(ii) $\Leftarrow$ klar nach Definition;
$\Rightarrow$ gemäß (i).

□

4.26. Hilfssatz

Es sei G eine endliche Gruppe mit Untergruppe H.

(i) Ist G auflösbar, so auch H und im Fall $H \triangleleft G$ ist auch G/H auflösbar.
(ii) Ist H Normalteiler und sind H sowie G/H auflösbar, dann ist auch G auflösbar.

Beweis:

(i) Es sei $G = G_0 \supset G_1 \ldots \supset G_n = 1$ mit $G_{i+1} \triangleleft G_i, G_i/G_{i+1}$ abelsch.

Bilde $H_i := G_i \cap H \qquad (0 \leq i \leq n)$.

$H_{i+1} \triangleleft H_i$:

Für $x \in H_i$ gilt: $xH_{i+1}x^{-1} \subseteq xG_{i+1}x^{-1} \cap xHx^{-1} = G_{i+1} \cap H = H_{i+1}$.

Ferner ist $H_i/H_{i+1} = H_i/H_i \cap G_{i+1} \cong H_iG_{i+1}/G_{i+1} < G_i/G_{i+1}$, also abelsch.

Gilt außerdem $H \triangleleft G$,

so bilde mittels $\tilde{G}_i := G_iH < G \qquad (0 \leq i \leq n)$ Kette $\tilde{G}_0/H \supseteq \tilde{G}_1/H \subseteq \ldots \subseteq \tilde{G}_n/H = T$.

Betrachte Abbildung $\phi : \tilde{G}_i \to G_i/G_{i+1} : g_ih \mapsto g_iG_{i+1}$.

ϕ Homomorphismus:

$\phi(g_ih)\phi(\tilde{g}_i\tilde{h}) = (g_iG_{i+1})(\tilde{g}_iG_{i+1}) = g_i\tilde{g}_i\ G_{i+1} = \phi(g_i\tilde{g}_ik) = \phi(g_ih\tilde{g}_i\tilde{h})$,

da $k \in H$ bel..

ϕ surjektiv klar, $Ker\phi = \{g_ih \in \tilde{G}_i \mid g_i \in G_{i+1}\} = G_{i+1}H = \tilde{G}_{i+1}$.

Also gilt: $\tilde{G}_{i+1} \triangleleft \tilde{G}_i$ und $\tilde{G}_i/\tilde{G}_{i+1} \cong G_i/G_{i+1}$, also abelsch.

Wende nun (... Nr.?) an: $(\tilde{G}_i/H)/(\tilde{G}_{i+1}/H) \cong \tilde{G}_i/\tilde{G}_{i+1}$.

(ii) H auflösbar:

$H = H_0 \supset H_1 \supset \ldots \supset H_r = 1$ und H_i/H_{i+1} abelsch.

G/H auflösbar:

Existiert Untergruppe $G_0 = G \supset G, \supset \ldots \supset G_s = H$ von G mit $(G_i/H)/(G_{i+1}/H) \overset{(1.21)}{\cong} G_i/G_{i+1}$ abelsch.

Also ist $G = G_0 \supset G_1 \supset \ldots \supset G_s = H = H_0 \supset H_1 \supset \ldots \supset H_r = 1$, d.h. G auflösbar.

□

4.27. Satz

Es sei $f \in K[t]$ mit $deg(f) \geq 1$.

Dann ist f(x) = 0 genau dann durch Radikale auflösbar, wenn für einen Zerfällungskörper L von f über K die Galoisgruppe $G(L/K)$ (Galoisgruppe von f) auflösbar ist.

Beweis:

(i) Es sei L Zerfällungskörper von $f \in K[t]$ und $G(L/K)$ auflösbar.

Wir setzen $n = [L : K]$.

Zunächst nehmen wir an, daß K eine primitive $n-te$ Einheitswurzel ζ enthält.

Zu $G = G(L/K)$ gehöre die Kette $G = G_0 \supset G_1 \supset \ldots \supset G_r = 1$ mit G_i/G_{i+1} zyklisch (vgl.(3.15)(ii)).

Ferner sei $F_i = F(G_i)$ $(G_i := G(L/F_i))$ mit $F_0 = K \subset F_1 \subset \ldots \subset F_r = L$.

Für $n_i = [F_i : F_{i-1}]$ gilt $n_i \mid n$, also enthält $F_i - 1$ eine primitive $n_i - te$ Einheitswurzel.

Wegen $G_i \triangleleft G_{i-1}$ ist F_i/F_{i-1} galoissch (vgl. (3....Nr.?)):

die betreffende Galoisgruppe ist isomorph zu G_{i-1}/G_i, also zyklisch.

Nunmehr wenden wir (3.11) (ii) an und erhalten $F_i = F_{i-1}(\alpha_i)$,

α_i Wurzel eines Polynoms $t^{n_i} - \beta_i \in F_{i-1}[t]$.

Also ist L/K Radikalerweiterung für f.

Enthält K dagegen keine primitive $n - te$ Einheitswurzel,

so bilden wir den Zerfällungskörper M von $t^n - 1 \in L[t]$,

der dann eine primitive $n - te$ Einheitswurzel ζ enthält.

Damit setze $K_1 = K(\zeta)$ und $L_1 = K_1 L$.

Dann ist L_1 Zerfällungskörper von f über K_1 und $G(L_1/K_1)$ ist isomorph zu einer Untergruppe von $G = G(L/K)$ nach (... Nr.?).

Nach (3.16) (i) ist $G(L_1/K_1)$ auflösbar.

Für $m = [L_1 : K_1]$ gilt $m|n$,

also enthält K_1 auch eine primitive $m - te$ Einheitswurzel ξ.

Wie im ersten Teil des Beweises gezeigt,

existiert ein Körperturm $K_1 = F_0 \subset F_1 \subset \ldots \subset F_r = L_1$, also L_1/K_1 Radikalerweiterung.

Wegen $K_1 = K(\zeta)$ ist auch L_1/K Radikalerweiterung mit $L_1 \supseteq L$,

d.h.$f(x)$ ist durch Radikale auflösbar.

(ii) Sei umgekehrt $f(x)$ durch Radikale auflösbar.

Nach (3.13) exististiert ein Körperturm $K = K_0 \subset K_1 \subset \ldots \subset K_r =: M$,

M/K Radikalerweiterung,

M enthält Zerfällungskörper L von f über K,

M/K galoissch.

Für $i = 1, \ldots, r$ ist dabei $K_i = K_{i-1}(\alpha_i)$, α_i Wurzel von $t^{n_i} - \beta_i \in K_{i-1}[t]$.

Setze $n = n_1 \cdot \ldots \cdot n_r$

und bestimme primitive $n - te$ Einheitswurzel ζ in Erweiterung von M

(Zerfällungskörper von $t^n - 1 \in M[t]$).

Für $i = 1, \ldots, r$ setze $F_i = K_i(\zeta)$.

Dann ist $K(\zeta) =: F_0 \subset F_1 \subset \ldots \subset F_r$ eine normale Radikalerweiterung von $K(\zeta)$.

Hierbei ist jeweils $F_i = F_{i-1}(\alpha_i) = K_{i-1}(\alpha_i, \zeta)$,

und F_{i-1} enthält eine primitive n_i-te Einheitswurzel.

Nach (3.11) (i) ist F_i demnach über F_{i-1} zyklisch.

Mit $H_i := G(F_r/F_i) \qquad (0 \leq i \leq n)$ ist $H_0 \supset H_1 \supset H_2 \supset \ldots \supset H_r = 1$

und dabei $H_i/H_{i+1} = G(F_r/F_i)/G(F_r/F_{i+1}) \cong G(F_{i+1}/F_i)$ zyklisch.

Also ist $G(F_r/F_0)$ auflösbar.

Wegen $F_r = K_rK(\zeta) = K_rF_0$ erhalten wir mittles (... Nr.?)

$G(F_r/F_0) \cong G(K_r/K_r \cap F_0) =: \tilde{G}$, so daß auch $\tilde{G}$ auflösbar ist.

Schließlich ist F_0/K abelsch (... Nr.?),

also $K_r \cap F_0/K$ abelsch und insbesondere $G(K_r \cap F_0/K)$ auflösbar.

$K_r \cap F_0/K$ galoissch impliziert $G(K_r/K_r \cap F_0) \triangleleft G(K_r/K)$;

die Faktorgruppe ist dabei isomorph zu $G(K_r \cap F_0/K)$, also abelsch.

Damit ist dann auch $G(K_r/K)$ auflösbar nach (3.16) (ii)

$\Rightarrow G(L/K)$ auflösbar nach (3.16) (i).

□

Bibliography

[1] Bewersdorff, Jörg, *Algebra für Einsteiger*,Vieweg, 2002.
[2] Birkhoff, Bartee, *Modern Applied Algebra.*
[3] S. Bosch, *Algebra*, Springer, 1993.
[4] N. Bourbaki, *Algebre*, Hermann, Paris 1962.
[5] J. H. Davenport, Y. Siret, E. Tournier, *Computer algebra*, Acad. Press, 1989.
[6] I. N. Herstein, *Topics in Algebra*, Xerox Coll. Pub., 1964.
[7] Th. W. Hungerford, *Algebra*, 1974.
[8] N. Jacobson, *Lectures in Abstract Algebra*, Springer GTM, 1974.
[9] R. Kochendörffer, *Einführung in die Algebra*, Dt.Verl.d. Wissenschaften, 1974.
[10] S. Lang, *Algebra*, Addison-Wesley, 1971.
[11] A. Leutbecher, *Zahlentheorie*, Springer, 1996.
[12] F. Lorenz, *Algebra I, II*, BI Wissenschaftsverlag, 1987/90.
[13] K. Meyberg, *Algebra I, II*, Carl Hanser Verlag, 1975.
[14] Mignotte, *Mathematics for Computer Algebra*, Springer, 1992.
[15] E. Scholz, *Geschichte der Algebra*, BI Wissenschaftsverlag, 1990.
[16] G. Stroth, *Algebra*, de Gruyter, 1998.
[17] B. L. van der Waerden, *Algebra I, II*, Springer, 1966/87.
[18] Weber, *Lehrbuch der Algebra*, Vieweg, 1895.