Galois-Gruppen

Clemens Adelmann

Braunschweig, Sommer 2005

Inhalt

Kapitel 1

Körpertheorie

1.1 Zerfällungskörper und normale Erweiterungen

Definition: Seien E_1, E_2 Erweiterungen des Körpers K.
$\sigma : E_1 \to E_2$ heißt K-*Homomorphismus* $:\iff$ σ ist Homomorphismus von K-Algebren, speziell $\sigma|_K = \mathrm{Id}_K$.

Schreibweise:

(a) E/K (Körpererweiterung) $:\iff$ E, K sind Körper mit $K \subseteq E$.

(b) $\sigma : E_1/K \to E_2/K :\iff$ $\sigma : E_1 \to E_2$ ist K-Homomorphismus.

(1.1) Bemerkung: Seien K, K' Körper, $\sigma : K \to K'$ Homomorphismus.

(a) σ ist injektiv.

(b) σ induziert den Ringhomomorphismus
$$\begin{array}{rcl} \tilde{\sigma} : K[X] & \to & K'[X] \\ f & \mapsto & f^\sigma \\ \sum_{\nu=0}^n a_\nu X^\nu & \mapsto & \sum_{\nu=0}^n \sigma(a_\nu) X^\nu \end{array}$$

(1.2) Satz: Seien K, K' Körper, $\sigma : K \to K'$ Homomorphismus, $f \in K[X]$. Seien $E/K, E'/K'$ Erweiterungen, $\alpha \in E$ mit $f(\alpha) = 0$, $\alpha' \in E'$ mit $f^\sigma(\alpha') = 0$.

(a) Sei $\tau : E \to E'$ Homomorphismus, $\tau|_K = \sigma$. Dann gilt $f^\sigma(\tau(\alpha)) = 0$.
(Jede Fortsetzung von σ bildet Nullstellen von f auf Nullstellen von f^σ ab.)

(b) Sei σ Isomorphismus, f irreduzibel über K. Dann gibt es einen eindeutigen Isomorphismus $\tau : K(\alpha) \to K'(\alpha')$ mit $\tau|_K = \sigma$ und $\tau(\alpha) = \alpha'$.
(Es gibt eine Fortsetzung von σ, die eine vorgegebene Nullstelle von f auf eine vorgegebene Nullstelle von f^σ abbildet.)

Beweis:

(a) Sei $f(X) = \sum_{\nu=0}^n a_\nu X^\nu$.
$0 = \tau(f(\alpha)) = \tau(\sum_{\nu=0}^n a_\nu \alpha^\nu) = \sum_{\nu=0}^n \sigma(a_\nu)\tau(\alpha)^\nu = f^\sigma(\tau(\alpha))$.

(b) Für $g \in K[X]$ definiere $\tau : K(\alpha) \to K'(\alpha')$ durch $\tau(g(\alpha)) = g^\sigma(\alpha')$.
τ ist wohldefiniert: Gelte $g_1(\alpha) = g_2(\alpha)$. Dann ist $(g_1 - g_2)(\alpha) = 0$.
Da f irreduzibel ist, gibt es $h \in K[X]$ mit $g_1 - g_2 = h \cdot f$.
Es ist $g_1^\sigma(\alpha') - g_2^\sigma(\alpha') = h^\sigma(\alpha')f^\sigma(\alpha') = 0$, also $\tau(g_1(\alpha)) = \tau(g_2(\alpha))$.
τ ist Homomorphismus, da σ nach (1.1)(b) einen Ringhomomorphismus $\tilde{\sigma} : K[X] \to K'[X]$ induziert.

τ ist injektiv: Gelte $0 = \tau(g(\alpha)) = g^\sigma(\alpha')$.
Da f irreduzibel über K ist, ist auch f^σ irreduzibel über K'.
Also gibt es $h \in K'[X]$ mit $g^\sigma = h \cdot f^\sigma$. Dann ist $g(\alpha) = h^{\sigma^{-1}}(\alpha) f(\alpha) = 0$.
$\tau|K = \sigma$ und τ ist surjektiv: Ist $g(X) = c$, dann folgt $\sigma(c) = \tau(c)$ und $K' \subseteq \mathrm{Im}(\tau)$. Ist $g(X) = X$, dann folgt $\alpha' \in \mathrm{Im}(\tau)$, also $\mathrm{Im}(\tau) = K'(\alpha')$.$\Diamond$

(1.3) Satz: Für alle $i \in I$ seien E_i/K Erweiterungen.
Dann gibt es einen Körper E/K und Homomorphismen $\tau_i : E_i/K \to E/K$, so dass $E = K\left(\bigcup_{i\in I} \tau_i(E_i)\right)$ gilt.

Beweis: Das Tensorprodukt $A = \bigotimes_{i\in I} E_i$ der K-Algebren E_i ist K-Algebra mit $1_A \neq 0$ und Einbettungen $\begin{array}{rcl} \sigma_i : E_i & \to & A \\ a & \mapsto & \bigotimes\limits_{j\in I} a_j \end{array}$ mit $a_j = \begin{cases} a & \text{für } j = i, \\ 1_{E_j} & \text{für } j \neq i. \end{cases}$
Nach dem Lemma von Zorn gibt es in A ein maximales Ideal M.
$E = A/M$ ist ein Körper und $\tau_i : E_i \xrightarrow{\sigma_i} A \to A/M$ ein K-Homomorphismus. $\Diamond$

Definition: Sei C ein Körper. C heißt *algebraisch algeschlossen* $:\Longleftrightarrow$
Jedes nicht konstante Polynom besitzt eine Nullstelle in C.

(1.4) Bemerkung: Sei C ein Körper. Äquivalent sind:

(1) C ist algebraisch abgeschlossen.
(2) Jedes irreduzible Polynom aus $C[X]$ hat den Grad 1.
(3) Ist E/C algebraisch, so gilt $E = C$.

(1.5) Satz: (Fortsetzungssatz) Sei $\sigma : K \to K'$ Isomorphismus, L/K algebraisch, C/K' mit C algebraisch abgeschlossen.
Dann gibt es $\tau : L \to C$ mit $\tau|_K = \sigma$.

Beweis: Setze $S = \{(F, \tau) | F \text{ Körper}, K \subseteq F \subseteq L, \tau : F \to C \text{ Hom.}, \tau|_K = \sigma\}$.
Wegen $(K, \sigma) \in S$ ist $S \neq \emptyset$. Auf S ist eine partielle Ordnung gegeben durch
$(F, \tau) \leq (F', \tau') :\Longleftrightarrow\ F \subseteq F'$ und $\tau'|_F = \tau$.
Sei $\mathcal{K} = \{(F_i, \tau_i) \,|\, i \in I\}$ eine Kette in S.
$F = \cup_{i\in I} F_i$ ist ein Körper mit $F \subseteq L$, sei $\varrho : F \to C$ gegeben durch $\varrho|_{F_i} = \tau_i$.
Dann ist (F, ϱ) eine obere Schranke für $\mathcal{K}$.
Nach dem Lemma von Zorn gibt es ein maximales $(E, \tau) \in S$.
Noch zu zeigen ist $E = L$:
Sei $\alpha \in L$. α ist algebraisch über E, sei $f = \mathrm{Mipo}_E(\alpha)$.
C ist algebraisch abgeschlossen, also gibt es $\alpha' \in C$ mit $f^\tau(\alpha') = 0$.
Nach (1.2)(b) ist τ fortsetzbar zu $\tau' : E(\alpha) \to C$ mit $\tau'(\alpha) = \alpha'$. Es folgt dann $(E(\alpha), \tau') \in S$, also $E = E(\alpha)$ und $\alpha \in E$ wegen der Maximalität von (E, τ). $\Diamond$

Definition: Sei K ein Körper. Eine algebraische Erweiterung C/K, so dass C algebraisch abgeschlossen ist, heißt *algebraischer Abschluss* von K.

(1.6) Satz: (Steinitz) Sei K ein Körper.

(a) Es gibt einen algebraischen Abschluss C von K.
(b) Seien C_1, C_2 algebraische Abschlüsse von K.
Dann gibt es einen Isomorphismus $C_1/K \xrightarrow{\cong} C_2/K$.

Beweis:

(a) Setze $I = \{M \mid \text{es gibt } m \in \mathbb{N}, \text{ so dass } M \subseteq K[X_1, \ldots, X_m] \text{ max. Ideal}\}$.
Für $M \in I$ ist $E_M = K[X_1, \ldots, X_m]/M$ ein Körper.
$K \subseteq E_M$, denn es gilt $K \cap M = \{0\}$, da M keine Einheiten enthält.
Anwenden von (1.3) auf $(E_M)_{M \in I}$:
Es gibt E/K und $\sigma_M : E_M/K \to E/K$ mit $E = \left(\bigcup_{M \in I} \sigma_M(E_M)\right)$.
Für jedes endliche L/K gibt es einen Homomorphismus $L/K \to E/K$,
denn ist $L = K(\alpha_1, \ldots, \alpha_m)$, so ist der Kern von $\varphi : K[X_1, \ldots, X_m] \to L$, gegeben durch $X_i \mapsto \alpha_i$, ein maximales Ideal M, und nach dem ersten Isomorphiesatz erhält man $L \overset{\cong}{\to} K[X_1, \ldots, X_m]/M = E_M \overset{\sigma_M}{\to} E$.
Sei $C = \{\alpha \in E \mid \alpha \text{ algebraisch über } K\}$.
C ist algebraisch abgeschlossen:
Annahme: Es gibt F/C algebraisch mit $F \neq C$.
Sei $\alpha \in F - C$. Dann ist α algebraisch über K. Sei $f = \mathrm{Mipo}_K(\alpha)$.
Seien $\beta_1, \ldots, \beta_r$ die verschiedenen Nullstellen von f in C.
Setze $L = K(\alpha, \beta_1, \ldots, \beta_r)$. Es ist $L \subseteq F$.
Da L/K endlich ist, gibt es einen K-Homomorphismus $\varphi : L \to E$.
φ ist injektiv und erfüllt $\varphi(L) \subseteq C$, also sind $\varphi(\alpha), \varphi(\beta_1), \ldots, \varphi(\beta_r)$ insgesamt $r + 1$ verschiedene Nullstellen von f in C. Widerspruch.

(b) Nach (1.5) gibt es einen Homomorphismus $\tau : C_1/K \to C_2/K$.
$C_2/\tau(C_1)$ ist algebraisch, und $\tau(C_1) \subseteq C_2$ ist algebraisch abgeschlossen.
Daher ist $C_2 = \tau(C_1)$, also ist τ ein Isomorphismus. ◊

Schreibweise: Sei E/K eine Körpererweiterung, $P \subseteq K[X]$.
$N_P(E) = \{\alpha \in E \mid \text{ es gibt } f \in P \text{ mit } f(\alpha) = 0\}$ ist die Nullstellenmenge von P in E. Statt $N_{\{f\}}(E)$ schreibe $N_f(E)$.

(1.7) Satz: Sei E/K algebraisch.
Dann ist jeder K-Endomorphismus von E ein Automorphismus.

Beweis: Sei $\sigma : E/K \to E/K$ ein Endomorphismus. Zu zeigen ist $\sigma(E) = E$.
Sei $\alpha \in E$, $f = \mathrm{Mipo}_K(\alpha)$. Es gilt $\sigma(N_f(E)) \subseteq N_f(E)$, und σ ist injektiv.
Damit ist σ surjektiv auf $N_f(E)$, und es gibt $\beta \in N_f(E)$ mit $\sigma(\beta) = \alpha$. ◊

Beispiel: Setze $K = \mathbb{Q}$.
Der $\mathbb{Q}$-Endomorphismus $\sigma : \mathbb{Q}(\pi)/\mathbb{Q} \to \mathbb{Q}(\pi)/\mathbb{Q}$ sei gegeben durch $\pi \mapsto \pi^2$.
Dann ist σ nicht surjektiv.

Definition: K sei Körper, $P \subseteq K[X] - K$ Menge nicht konstanter Polynome.
E/K heißt *Zerfällungskörper* von P über $K :\iff$

(i) Jedes $f \in P$ zerfällt über E in Linearfaktoren.

(ii) E wird über K von den Nullstellen aller $f \in P$ erzeugt.

Bei $P = \{f\}$ nennt man E auch *Zerfällungskörper* von f über K.

(1.8) Satz: Sei K ein Körper, $P \subseteq K[X] - K$.

(a) P besitzt einen Zerfällungskörper über K.

(b) Sind $E/K, E'/K$ Zerfällungskörper von P über K, dann gibt es einen Isomorphismus $E/K \overset{\cong}{\to} E'/K$.

Beweis:

(a) Sei C ein algebraischer Abschluss von K.
$E = K(N_P(C))$ ist ein Zerfällungskörper von P.

(b) Sei C' ein algebraischer Abschluss von E'.
Nach (1.5) gibt es einen K-Homomorphismus $\tau : E \to C'$.
$\tau(E)$ ist Zerfällungskörper von P über K'.
$\tau(E)$ und E' sind Teilkörper von C', also gilt $\tau(E) = E'$.
Damit ist $\tau : E \to E'$ ein K-Isomorphismus. ◊

Definition: Sei E/K algebraisch. E/K heißt *normal* $:\Longleftrightarrow$ Hat ein irreduzibles $f \in K[X]$ eine Nullstelle in E, dann zerfällt f in E in Linearfaktoren.

(1.9) Satz: Sei E/K algebraisch, C algebraischer Abschluss von E (und K). Äquivalent sind:

(1) E/K ist normal.

(2) Ist $\sigma : E/K \to C/K$ ein Homomorphismus, dann gilt $\sigma(E) = E$.

(3) Ist $\tau : C/K \to C/K$ ein Automorphismus, dann ist $\tau|_E$ ein Automorphismus von E/K.

(4) E ist ein Zerfällungskörper von Polynomen über K.

Beweis:
(1) $\Rightarrow$ (4): Setze $P = \{\mathrm{Mipo}_K(\alpha) \mid \alpha \in E\}$. Da E/K normal ist, gilt $N_P(C) \subseteq E$.
Also ist $N_P(C) = E$ und $E = K(N_P(C))$.
(4) $\Rightarrow$ (3): Sei $P \subseteq K[X] - K$, so dass $E = K(N_P(C))$ ist.
Ist $\tau : C/K \to C/K$ Automorphismus, dann gilt $\tau(N_P(C)) \subseteq N_P(C)$.
Also ist $\tau(E) \subseteq E$, und nach (1.7) ist $\tau|_E$ Automorphismus von E/K.
(3) $\Rightarrow$ (2): $\sigma : E/K \to C/K$ ist nach (1.5) fortsetzbar zu $\tau : C/K \to C/K$.
Nach (3) ist $\sigma = \tau|_E : E/K \to E/K$ ein Automorphismus, also gilt $\sigma(E) \subseteq E$.
(2) $\Rightarrow$ (1): Sei $f \in K[X]$ irreduzibel. Sei $\alpha \in E$ mit $f(\alpha) = 0$. Zeige $N_f(C) \subseteq E$.
Sei $\beta \in N_f(C)$. Nach (1.2)(b) gibt es $\sigma : K(\alpha)/K \to K(\beta)/K$ mit $\sigma(\alpha) = \beta$.
Nach (1.5) ist σ fortsetzbar zu $\tau : E/K \to C/K$.
Nach (2) gilt $\tau(E) = E$, also gilt $\beta = \tau(\alpha) \in E$. ◊

(1.10) Korollar: Sei K ein Körper, $P \subseteq K[X] - K$.
Ist E Zerfällungskörper von P über K, dann ist E/K normal.

Definition: Sei E/K algebraisch. Sei N/E Erweiterung mit:

(i) N/K ist normal.

(ii) Ist L Zwischenkörper von N/E, so dass L/K normal ist, so gilt $L = N$.

Dann heißt N/K *normale Hülle* von E/K.

(1.11) Satz: Sei E/K algebraisch.

(a) Es gibt eine normale Hülle N/K von E/K.

(b) Seien $N_1/K, N_2/K$ normale Hüllen von E/K.
Dann gibt es einen Isomorphismus $N_1/K \overset{\cong}{\to} N_2/K$.

(c) Ist E/K endlich, dann ist auch die normale Hülle N/K von E/K endlich.

Beweis: C sei algebraischer Abschluss von E.

(a) Sei $N = \prod_{\sigma: E/K \to C/K} \sigma(E)$ das Kompositum der Körper $\sigma(E)$ in C.
Setze $P = \{\mathrm{Mipo}_K(\alpha) \mid \alpha \in E\} \subseteq K[X]$. Zeige $N = K(N_P(C))$.
Sei $\beta \in N_P(C)$. Dann gibt es $\alpha \in E$ mit $f = \mathrm{Mipo}_K(\alpha)$ und $f(\beta) = 0$.
Nach (1.2)(b) gibt es $\sigma' : K(\alpha)/K \to K(\beta)/K$ mit $\sigma'(\alpha) = \beta$.
Nach (1.5) gibt es zu σ' eine Fortsetzung $\sigma : E/K \to C/K$, also $\beta \in \sigma(E)$.
Insgesamt folgt $N_P(C) \subseteq N$.
Für $\sigma : E/K \to C/K$ gilt $\sigma(E) \subseteq K(N_P(C))$, also $N \subseteq K(N_P(C))$.

(b) Seien C_1 bzw. C_2 algebraische Abschlüsse von N_1 bzw. N_2.
Nach (1.6)(b) gibt es einen Isomorphismus $\tau : C_1 \to C_2$.
Dann ist $\tau(N_1) = K(N_P(C_2)) = N_2$, also ist N_1 K-isomorph zu N_2.

(c) Sei $E = K(\alpha_1, \ldots, \alpha_r)$. Setze $P = \{\mathrm{Mipo}_K(\alpha_i) \mid i = 1, \ldots, r\}$.
Dann ist $N_P(C)$ endlich und $N \subseteq K(N_P(C))$. ◊

1.2 Separable Erweiterungen

Definition: Sei K Körper, C ein algebraischer Abschluss von K.
$\alpha, \beta \in C$ heißen *K-konjugiert* $:\Longleftrightarrow \mathrm{Mipo}_K(\alpha) = \mathrm{Mipo}_K(\beta)$.

(1.12) Bemerkung: Sei K Körper, C ein algebraischer Abschluss von K, $\alpha, \beta \in C$. Nach (1.2) und (1.5) sind äquivalent:

(1) α, β sind K-konjugiert.
(2) Es gibt einen Isomorphismus $\tau : K(\alpha)/K \to K(\beta)/K$ mit $\tau(\alpha) = \beta$.
(3) Es gibt einen Automorphismus $\sigma : C/K \to C/K$ mit $\sigma(\alpha) = \beta$.

(1.13) Lemma: Sei K Körper, C algebraischer Abschluss von K, $\alpha \in C$.
α besitzt höchstens $(K(\alpha) : K)$ verschiedene K-Konjugierte.

Beweis: Die Anzahl K-Konjugierter von α ist gleich der Anzahl der Nullstellen von $\mathrm{Mipo}_K(\alpha)$, und diese ist höchstens gleich dem Grad von $\mathrm{Mipo}_K(\alpha)$. ◊

Schreibweise: Seien $E/K, E'/K$ Körpererweiterungen.
$$\begin{aligned} G(E/K, E'/K) &= \{\sigma | \sigma : E/K \to E'/K\}, \\ G(E/K) &= G(E/K, E/K). \end{aligned}$$

(1.14) Bemerkung: Ist E/K algebraisch, dann ist $G(E/K)$ eine Gruppe bezüglich der Komposition von Abbildungen.

Definition: Sei E/K algebraisch, C algebraischer Abschluss von E.

(a) $G(E/K)$ heißt *Automorphismengruppe* oder *Galois-Gruppe* von E/K.
(b) $(E : K)_s = |G(E/K, C/K)|$ heißt *Separabilitätsgrad* von E/K.

(1.15) Bemerkung: Sei K Körper, C algebraischer Abschluss von K, $\alpha \in C$. Dann gilt $(K(\alpha) : K)_s \leq (K(\alpha) : K)$.

(1.16) Lemma: Sei E/K algebraisch, F ein Zwischenkörper von E/K. Sei C ein algebraischer Abschluss von E. Dann gibt es eine bijektive Abbildung $G(E/K, C/K) \tilde{\to} G(F/K, C/K) \times G(E/F, C/F)$.

Beweis: Nach (1.5) gibt es eine Abbildung $\begin{array}{ccc} G(F/K, C/K) & \to & G(C/K) \\ \sigma & \mapsto & \tilde{\sigma} \end{array}$.

Zeige: $\begin{array}{ccc} s : G(F/K, C/K) \times G(E/F, C/F) & \to & G(E/K, C/K) \\ (\sigma, \tau) & \mapsto & \tilde{\sigma} \circ \tau \end{array}$ ist bijektiv.

s ist injektiv: Gelte $\tilde{\sigma_1} \circ \tau_1 = \tilde{\sigma_2} \circ \tau_2$. Restriktion auf F liefert $\sigma_1 = \sigma_2$.
Da $\tilde{\sigma_1}$ ein K-Automorphismus ist, folgt $\tau_1 = \tau_2$.
s ist surjektiv: Sei $\varphi \in G(E/K, C/K)$. Setze $\sigma = \varphi|_F$ und $\tau = \tilde{\sigma}^{-1} \circ \varphi$.
Dann ist $\tau|_F = \mathrm{Id}_F$, also $\tau \in G(E/F, C/F)$ und $s(\sigma, \tau) = \varphi$. ◊

(1.17) Satz: Sei E/K algebraisch, C algebraischer Abschluss von E.

(a) F sei Zwischenkörper von E/K. Dann gilt $(E : K)_s = (E : F)_s (F : K)_s$.

(b) E/K sei endlich. Dann gilt $(E : K)_s \leq (E : K)$.

Beweis:

(a) Die Aussage folgt direkt aus (1.16).

(b) Es gilt $E = K(\alpha_1, \ldots, \alpha_r)$ für geeignete $\alpha_i \in C$.
Es gibt eine Kette von Zwischenkörpern $K \subset K_1 \subset \ldots \subset K_r = E$ mit $K_i = K(\alpha_1, \ldots, \alpha_i)$. Es gilt $(K_{i-1}(\alpha_i) : K_{i-1})_s \leq (K_{i-1}(\alpha_i) : K_{i-1})$ nach (1.15), also folgt die Aussage mit (a). ◊

Definition: Sei E/K algebraisch.

(a) $\alpha \in E$ heißt *separabel* über $K :\iff (K(\alpha) : K) = (K(\alpha) : K)_s$.

(b) E/K heißt *separabel* $:\iff$ jedes $\alpha \in E$ ist separabel über K.

(1.18) Bemerkung: Sei $f \in K[X] - K$, E Zerfällungskörper von f über K. Die Primfaktorzerlegung von f in $E[X]$ hat die Form

$$f(X) = c(X - \alpha_1)^{e_1} \cdot \ldots \cdot (X - \alpha_r)^{e_r}.$$

e_ν heißt die *Vielfachheit* der Nullstelle α_ν, α_ν heißt *e_ν-fache Nullstelle* von f.

Definition: Sei K ein Körper, $f \in K[X]$ mit $n = \mathrm{grad}(f) \geq 1$.
f heißt *separabel* $:\iff$ f hat in einem Zerfällungskörper genau n paarweise verschiedene Nullstellen.

(1.19) Bemerkung: Sei K ein Körper, $f \in K[X]$ mit $\mathrm{grad}(f) \geq 1$.
f separabel $\iff$ f hat in einem Zerfällungskörper nur einfache Nullstellen.

(1.20) Bemerkung: Sei L/K Erweiterung, $\alpha \in L$ algebraisch über K.

(a) $(K(\alpha) : K)_s$ ist die Anzahl verschiedener Nullstellen von $\mathrm{Mipo}_K(\alpha)$.

(b) α ist separabel über $K \iff \mathrm{Mipo}_K(\alpha)$ ist separabel.

(c) Sei α separabel über K, E/K Erweiterung. Dann ist α separabel über E.

(1.21) Satz: Sei E/K endliche Erweiterung. Äquivalent sind:

(1) E/K ist separabel.

(2) $(E : K) = (E : K)_s$.

(3) Es gibt über K separable $\alpha_1, \ldots, \alpha_r \in E$ mit $E = K(\alpha_1, \ldots, \alpha_r)$.

Beweis:
(1) $\Rightarrow$ (3): E/K ist endlich erzeugt, und alle Erzeuger sind nach (1) separabel.

(3) $\Rightarrow$ (2): Es gibt eine Kette von Körpern $K \subset K_1 \subset \ldots \subset K_r = E$ mit $K_i = K(\alpha_1, \ldots, \alpha_i)$. Nach (1.20)(c) ist α_{i+1} separabel über K_i, also folgt aus $(K_i(\alpha_{i+1}) : K_i) = (K_i(\alpha_{i+1}) : K_i)_s$ mit (1.17)(a), dass $(E : K) = (E : K)_s$ gilt.
(2) $\Rightarrow$ (1): Sei $\alpha \in E$. Nach (1.17) gilt für den Zwischenkörper $K(\alpha)$ von E/K die Gleichheit $(K(\alpha) : K)_s = (K(\alpha) : K)$, also ist α separabel über K. $\Diamond$

(1.22) Satz: (Transitivität der Eigenschaft *separabel*)
Sei E/K algebraisch, L ein Zwischenkörper von E/K.
Sind E/L und L/K separabel, dann ist E/K separabel.

Beweis: Sei $\beta \in E$, setze $f = \mathrm{Mipo}_L(\beta) = X^n + \alpha_{n-1}X^{n-1} + \ldots + \alpha_0$.
Setze $F = K(\alpha_0, \ldots, \alpha_{n-1})$, dann ist $f = \mathrm{Mipo}_F(\beta)$.
Da β separabel über L ist, ist f separabel, also ist $F(\beta)/F$ separabel.
$\alpha_0, \ldots, \alpha_{n-1} \in L$ sind separabel über K, also ist F/K separabel nach (1.21).
Nach (1.17)(a) ist $F(\beta)/K$ separabel, also ist β separabel über K. $\Diamond$

Definition: Sei K ein Körper, $f \in K[X]$, $f = \sum_{\nu=0}^{n} a_\nu X^\nu$.
$f'(X) = \sum_{\nu=1}^{n} \nu a_\nu X^{\nu-1}$ heißt (formale) *Ableitung* von f.

(1.23) Bemerkung: Für $f, g \in K[X]$ und $c \in K$ gelten die Ableitungsregeln

$$\begin{aligned} (f+g)' &= f' + g', \\ (c \cdot f)' &= c \cdot f', \\ (fg)' &= f'g + fg'. \end{aligned}$$

(1.24) Bemerkung: Sei L/K Erweiterung, $\alpha \in L$ algebraisch über K.

(a) α ist mehrfache Nullstelle von $f \in K[X] \iff f(\alpha) = 0$ und $f'(\alpha) = 0$.
(b) $f \in K[X]$ ist separabel $\iff f, f'$ sind teilerfremd in $K[X]$.
(c) Sei $f \in K[X]$ irreduzibel. f ist separabel $\iff f' \neq 0$.

(1.25) Lemma: Sei K ein Körper mit $\mathrm{char}(K) = p > 0$, $f \in K[X]$.
Dann gilt: $f' = 0 \iff f \in K[X^p]$.

Beweis: Sei $f = \sum_{\nu=0}^{n} a_\nu X^\nu$. $f' = 0$ ist äquivalent zu $\nu a_\nu = 0$ für alle ν.
Dies ist äquivalent zu $a_\nu = 0$ für $\nu \not\equiv 0 \bmod p$. $\Diamond$

(1.26) Satz: Sei K ein Körper, E/K Erweiterung, $\alpha \in E$ algebraisch über K.

(a) Bei $\mathrm{char}(K) = 0$ ist α separabel über K.
(b) Bei $\mathrm{char}(K) = p > 0$ gibt es $m \in \mathbb{N}_0$, so dass α^{p^m} separabel über K ist. Dann gilt $(K(\alpha) : K) = p^m (K(\alpha) : K)_s$.

Beweis: Sei $f = \mathrm{Mipo}_K(\alpha) \in K[X]$.

(a) Es gilt $f' \neq 0$, nach (1.24)(c) ist also f und damit α separabel über K.
(b) Es gibt ein $m \in \mathbb{N}_0$ mit $f \in K[X^{p^m}]$ und $f \notin K[X^{p^{m+1}}]$.
Also gilt $f(X) = g(X^{p^m})$ mit $g \notin K[X^p]$.
g ist irreduzibel, denn aus einer Zerlegung $g(X) = h_1(X)h_2(X)$ folgt eine Zerlegung $f(X) = h_1(X^{p^m})h_2(X^{p^m})$, aber f ist irreduzibel.
Es ist $g(\alpha^{p^m}) = f(\alpha) = 0$, also ist $g = \mathrm{Mipo}_K(\alpha^{p^m})$.
Nach (1.25) und (1.24)(c) ist g separabel, also α^{p^m} separabel über K.
Alle Nullstellen von f haben die Vielfachheit p^m, also gilt nach (1.20)(a), dass $(K(\alpha) : K) = p^m (K(\alpha) : K)_s$ ist. $\Diamond$

(1.27) Korollar: Sei E/K endlich. Dann gilt: $(E:K)_s$ teilt $(E:K)$.

Definition: Sei E/K endliche Erweiterung.
$(E:K)_i = (E:K)/(E:K)_s$ heißt *Inseparabilitätsgrad* von E/K.

Beispiel: Setze $K = \mathbb{F}_2(t)$, $E = K(\sqrt{t})$. Dann ist $(E:K) = 2$.
Sei $f = X^2 + t \in K[X]$. f ist irreduzibel über K, in $E[X]$ gilt $f = (X + \sqrt{t})^2$.
Es folgt $G(E/K) = \{\mathrm{Id}_E\}$.

Definition: Sei E/K algebraisch.

(a) $\alpha \in E$ heißt *rein inseparabel* über $K :\iff (K(\alpha):K)_s = 1$.

(b) E/K heißt *rein inseparabel*: $\iff$ jedes $\alpha \in E$ ist rein inseparabel über K.

(1.28) Satz: Sei K ein Körper mit $\mathrm{char}(K) = p > 0$, E/K algebraisch.

(a) $\alpha \in E$ ist rein inseparabel über $K \iff$ es gibt $m \in \mathbb{N}_0$ mit $\alpha^{p^m} \in K$.

(b) E/K ist rein inseparabel $\iff (E:K)_s = 1$.

Beweis:

(a) Setze $a = \alpha^{p^m}$. $\mathrm{Mipo}_K(\alpha)$ teilt $X^{p^m} - a = (X-\alpha)^{p^m}$, was über $E[X]$ die einzige Nullstelle α hat. Nach (1.20)(a) ist α rein inseparabel über K.
Sei umgekehrt $\alpha \in E$ rein inseparabel über K. $\mathrm{Mipo}_K(\alpha)$ hat über E nur eine Nullstelle, also gibt es $n \in \mathbb{N}$ mit $\mathrm{Mipo}_K(\alpha) = (X-\alpha)^n$.
Nach (1.26)(b) gibt es $m \in \mathbb{N}_0$, so dass α^{p^m} separabel über K ist.
Sei m wie eben kleinstmöglich. Dann ist $f(X) = \mathrm{Mipo}_K(\alpha^{p^m})$ separabel, und über E gilt $\mathrm{Mipo}_K(\alpha) = f(X^{p^m}) = f(X)^{p^m} = (X-\alpha)^n$.
Aus der Separabilität von f und der eindeutigen Faktorzerlegung in $E[X]$ folgt $\mathrm{Mipo}_K(\alpha) = (X-\alpha)^{p^m} = X^{p^m} - \alpha^{p^m}$, also $\alpha^{p^m} \in K$.

(b) Gilt $(E:K)_s = 1$, so ist für jedes $\alpha \in E$ auch $(K(\alpha):K)_s = 1$.
Also ist E/K rein inseparabel.
Sei E/K rein inseparabel und C ein algebraischer Abschluss von E.
Nach (1.20)(a) hat jedes $\alpha \in E$ nur ein K-Konjugiertes in C.
Ist also $\sigma : E/K \to C/K$ ein Homomorphismus, so gilt nach (1.2) für alle $\alpha \in E$, dass $\sigma(\alpha) = \alpha$ ist. Also ist $(E:K)_s = |G(E/K, C/K)| = 1$. ◊

Definition: Sei E/K algebraisch.
$E_s = \{\alpha \in E \mid \alpha \text{ separabel über } K\}$ heißt der *separable Abschluss* von K in E.

(1.29) Satz: Sei E/K algebraisch.

(a) E_s ist ein Zwischenkörper von E/K.

(b) E_s/K ist separabel, und es gilt $(E_s:K) = (E:K)_s$.

(c) E/E_s ist rein inseparabel, und es gilt $(E:E_s) = (E:K)_i$.

Beweis: Für jedes $\alpha \in E_s$ ist $K(\alpha)/K$ separabel, also ist $K(\alpha) \subseteq E_s$.
E_s ist Körper als Vereinigung aller $K(\alpha)$ mit $\alpha \in E_s$.
E_s/K ist nach Definition separabel.
E/E_s ist rein inseparabel:
Sei $\alpha \in E$. Nach (1.26)(b) gibt es $m \in \mathbb{N}_0$, so dass α^{p^m} separabel über K ist.
Dann ist $\alpha^{p^m} \in E_s$, also ist α rein inseparabel über E_s.
Die Formeln für die Grade folgen aus (1.17) und (1.21). ◊

1.3 Galois-Erweiterungen

Definition: Sei E Körper, $G \leq \mathrm{Aut}(E)$ Gruppe von Automorphismen von E.
$E^G = \{\alpha \in E \mid \text{für alle } \sigma \in G \text{ gilt } \sigma(\alpha) = \alpha\}$ heißt *Fixkörper* von G.

(1.30) Lemma: Sei E ein Körper, $G \leq \mathrm{Aut}(E)$, $K = E^G$.
Für $\alpha \in E$ sei $G\alpha = \{\sigma(\alpha) \mid \sigma \in G\}$ die Bahn von α unter der Operation von G.

(a) $G\alpha$ ist endlich $\iff$ α ist algebraisch über K.

(b) Sei $G\alpha = \{\alpha_1, \ldots, \alpha_n\}$ endlich. Dann gilt $\mathrm{Mipo}_K(\alpha) = \prod_{i=1}^{n}(X - \alpha_i)$.

Beweis: Sei $G\alpha = \{\alpha_1, \ldots, \alpha_n\}$ endlich. Setze $f(X) = \prod_{i=1}^{n}(X - \alpha_i)$.
$f \in E[X]$ ist normiert und separabel, da die α_i paarweise verschieden sind.
Jedes $\tau \in G$ permutiert $G\alpha$, also gilt $f^\tau(X) = f(X)$ für alle $\tau \in G$.
Durch Koeffizientenvergleich folgt $f \in E^G[X] = K[X]$.
Jedes α_i ist nach (1.12) Nullstelle von $\mathrm{Mipo}_K(\alpha)$, d.h. f teilt $\mathrm{Mipo}_K(\alpha)$.
Insgesamt gilt $f = \mathrm{Mipo}_K(\alpha)$. Insbesondere ist α algebraisch über K.
Ist umgekehrt α algebraisch über K, dann hat α nach (1.13) nur endlich viele K-Konjugierte. Nach (1.12) sind die Elemente von $G\alpha$ K-konjugiert.
Also ist $G\alpha$ endlich. ◊

Definition: Sei E/K algebraische Erweiterung.
E/K heißt *Galois-Erweiterung* (oder *galoissch*) : $\iff$ $K = E^{G(E/K)}$.

(1.31) Bemerkung: Sei E/K eine Körpererweiterung.

(a) $K \subseteq E^{G(E/K)}$.

(b) Sei $G \leq \mathrm{Aut}(E)$ und $K = E^G$.
Ist E/K algebraisch, dann ist E/K galoissch.

(1.32) Satz: Sei E/K algebraische Erweiterung. Äquivalent sind:

(1) E/K ist galoissch.

(2) E/K ist normal und separabel.

Beweis:
(1) $\Rightarrow$ (2): Setze $G = G(E/K)$. Es gelte $K = E^G$.
Sei $\alpha \in E$. Die Menge $G\alpha = \{\sigma(\alpha) \mid \alpha \in G\}$ ist endlich und in E enthalten.
Nach (1.30) ist $\mathrm{Mipo}_K(\alpha)$ separabel und zerfällt über E in Linearfaktoren.
Da dies für alle $\alpha \in E$ gilt, ist E/K normal und separabel.
(2) $\Rightarrow$ (1): Sei $\alpha \in E$, setze $f = \mathrm{Mipo}_K(\alpha)$. Nach Voraussetzung und (1.20)(b) ist f separabel und zerfällt über E in Linearfaktoren.
Bei $\alpha \in E - K$ ist $\mathrm{grad}(f) \geq 2$, und es gibt $\beta \in E$, $\beta \neq \alpha$, mit $f(\beta) = 0$.
Nach (1.2)(b), (1.5) und (1.9) gibt es $\sigma \in G(E/K)$ mit $\sigma(\alpha) = \beta \neq \alpha$.
Also gilt $E^{G(E/K)} \subseteq K$. ◊

(1.33) Bemerkung: Sei $f \in K[X]$ separabel, sei E ein Zerfällungskörper von f über K. Dann ist E/K eine endliche Galois-Erweiterung.

(1.34) Satz: Sei E/K galoissch, F sei Zwischenkörper von E/K.
Dann ist E/F galoissch.

Beweis:
Mit E/K ist auch E/F normal und separabel, also nach (1.32) galoissch. ◊

Beispiel: Setze $K = \mathbb{Q}$, $F = \mathbb{Q}(\sqrt[3]{2})$, $E = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$.
E/K ist normal, aber F/K ist nicht normal.

(1.35) Satz: Sei E/K galoissch, F sei Zwischenkörper von E/K.

(a) Für $\sigma \in G(E/K)$ gilt $G(E/\sigma(F)) = \sigma G(E/F)\sigma^{-1}$.

(b) F/K ist galoissch $\iff$ $G(E/F)$ ist Normalteiler von $G(E/K)$.

(c) Ist F/K galoissch, dann induziert die Restriktion $\begin{array}{ccc} G(E/K) & \to & G(F/K) \\ \sigma & \mapsto & \sigma|_F \end{array}$
einen Isomorphismus $G(E/K)/G(E/F) \xrightarrow{\cong} G(F/K)$.

Beweis:

(a) Sei $\tau \in G(E/\sigma(F))$. Für alle $\alpha \in F$ gilt $\tau\sigma(\alpha) = \sigma(\alpha)$, also $\sigma^{-1}\tau\sigma(\alpha) = \alpha$.
Dies ist äquivalent zu $\tau \in \sigma G(E/F)\sigma^{-1}$.

(b) Sei F/K galoissch. Dann ist $G(E/F)$ Normalteiler in $G(E/K)$, denn für alle $\sigma \in G(E/K)$ gilt $\sigma(F) = F$, also $G(E/F) = \sigma G(E/F)\sigma^{-1}$.
Sei F/K nicht galoissch.
Nach (1.5) und (1.9) gibt es $\sigma \in G(E/K)$ mit $\sigma(F) \neq F$.
Dann ist $G(E/\sigma(F)) \neq G(E/F)$, also $G(E/F) \neq \sigma G(E/F)\sigma^{-1}$.
Also ist $G(E/F)$ kein Normalteiler von $G(E/K)$.

(c) Ist F/K galoissch, dann ist die Restriktion $G(E/K) \to G(F/K)$ ein Gruppenhomomorphismus, der nach dem Fortsetzungssatz (1.5) surjektiv ist.
Der Kern ist $\{\sigma \in G(E/K) \mid \sigma|_F = \mathrm{Id}_F\} = G(E/F)$. ◊

(1.36) Lemma: Sei E/K algebraisch und N/K die normale Hülle von E/K.
Ist E/K separabel, dann ist auch N/K separabel.

Beweis: Sei C ein algebraischer Abschluss von N.
Zu jedem $\beta \in N$ gibt es $\alpha \in E$ und $\sigma : E/K \to C/K$ mit $\sigma(\alpha) = \beta$.
$\mathrm{Mipo}_K(\beta) = \mathrm{Mipo}_K(\alpha)$ ist separabel, also ist β separabel über K. ◊

(1.37) Lemma: Sei E/K endliche galoissche Erweiterung.
Dann ist $G(E/K)$ endlich, und es gilt $|G(E/K)| = (E : K)$.

Beweis:
Sei C ein algebraischer Abschluss von E.
E/K ist separabel, also gilt $(E : K) = (E : K)_s = |G(E/K, C/K)|$.
Da E/K normal ist, gilt $\sigma(E) = E$ für jedes $\sigma \in G(E/K, C/K)$.
Also ist $G(E/K) = G(E/K, C/K)$. ◊

(1.38) Satz: (Satz vom primitiven Element) Sei E/K endlich und separabel.
Dann ist E/K einfach.

Beweis:
Zeige: E/K hat nur endlich viele Zwischenkörper F.
Ist N/K die normale Hülle von E/K und hat N/K nur endlich viele Zwischenkörper, dann gilt dies auch für die Teilerweiterung E/K.
N/K ist galoissch nach (1.36) und endlich nach (1.11)(c).
$G(N/K)$ ist endlich nach (1.37), hat also nur endlich viele Untergruppen.
Nach (1.34) gibt es daher höchstens endlich viele Zwischenkörper F. ◊

(1.39) Satz: (Artin)
Sei E ein Körper, $G \leq \mathrm{Aut}(E)$ endliche Untergruppe, $K = E^G$.
Dann ist E/K eine endliche galoissche Erweiterung, und es ist $G = G(E/K)$.

Beweis: Sei $n = |G|$. Nach (1.30) ist jedes $\alpha \in E$ Nullstelle eines separablen Polynoms vom Grad $\leq n$, das über E in Linearfaktoren zerfällt.
E/K ist daher algebraisch, separabel und normal, also nach (1.32) galoissch.
Aus (1.38) folgt $(E : K) \leq n$. Nach Definition von K ist $G \leq G(E/K)$, und mit (1.37) gilt $n = |G| \leq |G(E/K)| = (E : K) \leq n$, also ist $G = G(E/K)$. ◊

Schreibweise: Sei E/K eine Körpererweiterung, G eine Gruppe.
$\mathcal{F}(E/K) = \{F \mid F \text{ Körper mit } K \subseteq F \subseteq E\}$,
$\mathcal{U}(G) = \{H \mid H \text{ Untergruppe von } G\}$.

(1.40) Satz: (Hauptsatz der Galois-Theorie)
Sei E/K endlich und galoissch.

(a) Die Abbildung $\begin{array}{ccc} \mathcal{F}(E/K) & \to & \mathcal{U}(G(E/K)) \\ F & \mapsto & G(E/F) \end{array}$ ist bijektiv.
Die Umkehrabbildung ist $\begin{array}{ccc} \mathcal{U}(G(E/K)) & \to & \mathcal{F}(E/K) \\ H & \mapsto & E^H \end{array}$.

(b) Die Abbildungen sind antiton:
Für $F_1, F_2 \in \mathcal{F}(E/K)$ gilt: $F_1 \subseteq F_2 \iff G(E/F_2) \subseteq G(E/F_1)$,
für $H_1, H_2 \in \mathcal{U}(G(E/K))$ gilt: $H_1 \subseteq H_2 \iff E^{H_2} \subseteq E^{H_1}$.

Beweis: Seien $\varphi : \mathcal{F}(E/K) \to \mathcal{U}(G(E/K))$ und $\psi : \mathcal{U}(G(E/K)) \to \mathcal{F}(E/K)$ die obigen Abbildungen.
φ ist injektiv: Für jeden Zwischenkörper F von E/K ist $E^{G(E/F)} = F$.
Für Zwischenkörper $F_1 \neq F_2$ gilt also $G(E/F_1) \neq G(E/F_2)$.
φ ist surjektiv: Zeige $\varphi \circ \psi = \mathrm{Id}_{\mathcal{U}(G(E/K))}$.
Da E/K endlich ist, ist $G(E/K)$ endlich nach (1.37).
Also ist auch jede Untergruppe $H \leq G(E/K)$ endlich.
Nach (1.39) gilt $\varphi \circ \psi(H) = G(E/E^H) = H$.
Die Inklusionen in (b) folgen aus den Definitionen. ◊

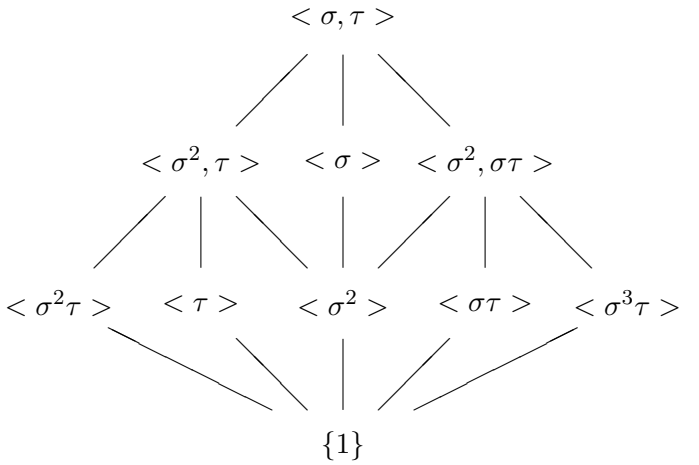
(1.41) Satz: (Translationssatz)
Sei E/K eine endliche Galois-Erweiterung, F/K eine beliebige Erweiterung.
Dann ist EF/F galoissch, und die Restriktion $\begin{array}{ccc} r : G(EF/F) & \to & G(E/K) \\ \sigma & \mapsto & \sigma|_E \end{array}$
induziert einen Isomorphismus $G(EF/F) \xrightarrow{\cong} G(E/E \cap F)$.

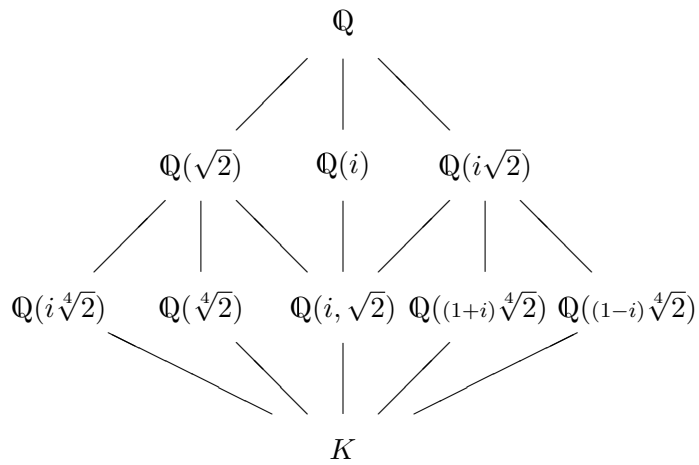
Beweis:
Mit E/K ist auch EF/F algebraisch, separabel und normal, denn ist E Zerfällungskörper von $P \subseteq K[X]$, dann ist EF Zerfällungskörper von $P \subseteq F[X]$.
r ist Gruppenhomomorphismus, denn Restriktion vertauscht mit Komposition.
r ist injektiv: Gilt $\sigma|_E = \mathrm{Id}_E$, dann ist σ trivial auf E und F, also $\sigma = \mathrm{Id}_{EF}$.
Setze $H = r(G(EF/F))$. Dann ist $H \leq G(E/K)$.
H lässt alle Elemente von $E \cap F$ fest, also gilt $E \cap F \subseteq E^H$.
Sei $\alpha \in E^H$, dann bleibt $\alpha \in EF$ unter $G(EF/F)$ fest, also gilt $\alpha \in F$.
Insgesamt gilt $E^H = E \cap F$. Nach (1.39) gilt $H = G(E/E \cap F)$. ◊

(1.42) Satz: Seien E_1/K, E_2/K endliche Galois-Erweiterungen.
Dann ist das Kompositum E_1E_2/K galoissch, und der Homomorphismus
$h : G(E_1E_2/K) \to G(E_1/K) \times G(E_2/K)$ ist injektiv.
$\sigma \mapsto (\sigma|_{E_1}, \sigma|_{E_2})$
Gilt $E_1 \cap E_2 = K$, dann ist h ein Isomorphismus.

Beweis: Nach (1.41) ist E_1E_2/K galoissch. h ist Gruppenhomomorphismus.
h ist injektiv: Für $\sigma \in G(E_1E_2/K)$ mit $\sigma|_{E_i} = \mathrm{Id}_{E_i}$ für $i = 1, 2$ gilt $\sigma = \mathrm{Id}_{E_1E_2}$.
Bei $E_1 \cap E_2 = K$ ist h surjektiv: Sei $(\sigma_1, \sigma_2) \in G(E_1/K) \times G(E_2/K)$. Nach (1.41) gibt es $\tau_1 \in G(E_1E_2/E_2)$ mit $\tau_1|_{E_1} = \sigma_1$ und $\tau_2 \in G(E_1E_2/E_1)$ mit $\tau_2|_{E_2} = \sigma_2$. Dann ist $h(\tau_1\tau_2) = (\sigma_1, \sigma_2)$. ◊

Beispiel: Sei K der Zerfällungskörper von $X^4 - 2$ über $\mathbb{Q}$. Es ist $K = \mathbb{Q}(i, \sqrt[4]{2})$ mit $(K : \mathbb{Q}) = 8$. Die Automorphismen $\sigma, \tau \in G(K/\mathbb{Q})$ seien gegeben durch
$\sigma : \begin{cases} i \mapsto i, \\ \sqrt[4]{2} \mapsto i\sqrt[4]{2}, \end{cases}$ und $\tau : \begin{cases} i \mapsto -i, \\ \sqrt[4]{2} \mapsto \sqrt[4]{2}. \end{cases}$
Dann ist $G(K/\mathbb{Q}) = < \sigma, \tau \,|\, \sigma^4 = 1, \tau^2 = 1, \tau^{-1}\sigma\tau = \sigma^{-1} >$.
Die Korrespondenz zwischen Untergruppen von $G(K/\mathbb{Q})$ und Zwischenkörpern von $K/\mathbb{Q}$ wird durch folgende Diagramme veranschaulicht:





Definition: Sei K Körper, $f \in K[X]$ separabel. Sei E Zerfällungskörper von f.
$G_f = G(E/K)$ heißt die *Galois-Gruppe* von f über K.
G_f heißt auch die *Galois-Gruppe* der Gleichung $f(X) = 0$ über K.

(1.43) Bemerkung: Sei $f \in K[X]$ separabel, $n = \text{grad}(f) \geq 1$.
Dann gibt es eine Einbettung $G_f \to S_n$ in die symmetrische Gruppe S_n.
Die Elemente von G_f werden als Permutationen der Nullstellen von f in einem Zerfällungskörper von f gedeutet.
Das Bild von G_f in S_n ist nur bis auf Konjugation eindeutig bestimmt.

(1.44) Satz: Sei $f \in K[X]$ separabel, E ein Zerfällungskörper von f.
Äquivalent sind:

(1) f ist irreduzibel.
(2) G_f operiert transitiv auf $N_f(E)$.

Beweis:
(1) $\Rightarrow$ (2): Seien $\alpha, \beta \in N_f(E)$.
Nach (1.5) und (1.9) gibt es $\sigma \in G(E/K)$ mit $\sigma(\alpha) = \beta$.
(2) $\Rightarrow$ (1): Sei $\alpha \in N_f(E)$. Setze $g = \text{Mipo}_K(\alpha)$. g teilt f.
Zu jedem $\beta \in N_f(E)$ gibt es $\sigma \in G(E/K)$ mit $\sigma(\alpha) = \beta$.
Dann ist $g(\beta) = g(\sigma(\alpha)) = 0$. Da f separabel ist, ist f ein Teiler von g. $\Diamond$

1.4 Zusammenfassung: Die Galois-Korrespondenz

Idee: Sei E/K eine algebraische Körpererweiterung, $G(E/K)$ die Gruppe der Automorphismen von E, die K elementweise fest lassen.

Die Zuordnung von Fixgruppen und Fixkörpern soll dann eine bijektive und antitone Abbildung vom Verband der Zwischenkörper von E/K zum Verband der Untergruppen von $G(E/K)$ liefern.

Probleme:

(a) $G(E/K)$ ist zu „klein“.
Dies tritt auf, falls E/K nicht normal oder E/K nicht separabel ist.
(b) $G(E/K)$ ist zu „groß“.
Dies tritt auf, falls $(E : K) = \infty$.

Beispiel zu (b): C sei algebraischer Abschluss von $\mathbb{F}_p$, setze $G = G(C/\mathbb{F}_p)$.
$\varphi_p : C \to C$ ist ein Automorphismus von $C/\mathbb{F}_p$.
$x \mapsto x^p$
φ_p wird der *Frobenius-Automorphismus* genannt.
Für die Fixkörper gilt $C^{<\varphi_p>} = \mathbb{F}_p = C^G$.
Es gilt $G \neq <\varphi_p>$, denn: Setze $F = \cup_{m\in\mathbb{N}} \mathbb{F}_{p^{2^m}}$. Es ist $(F : \mathbb{F}_p) = \infty$.
Dann ist $F \neq C$, und es gibt $\tau \in G(C/F)$ mit $\tau \neq \mathrm{Id}_C$.
Angenommen, es gälte $\tau = \varphi_p^n$ für ein $n \in \mathbb{Z} - \{0\}$, so folgte $F \subseteq C^{<\varphi_p^n>} = \mathbb{F}_{p^n}$, also $(F : \mathbb{F}_p) \leq n$. Widerspruch.

Lösung:

(a) Man fordert zusätzlich, dass E/K normal und separabel ist.

(b) Man führt eine Topologie auf $G(E/K)$ ein, so dass „maximale“ Fixgruppen eines Zwischenkörpers den abgeschlossenen Untergruppen von $G(E/K)$ entsprechen.

Definition: Eine Gruppe G heißt *topologische Gruppe*, wenn G ein topologischer Raum ist und die Gruppenverknüpfung $\cdot : G \times G \to G$ sowie die Inversenbildung $^{-1} : G \to G$ stetig sind.

Bemerkung: Die Topologie auf einer topologischen Gruppe ist durch Angabe einer Umgebungsbasis des neutralen Elements eindeutig bestimmt.
Dazu reicht es zu erklären, welche Untergruppen offen sind.

Definition: Sei E/K eine Galois-Erweiterung.
Die *Krull-Topologie* auf $G(E/K)$ ist wie folgt definiert:
Eine Untergruppe ist genau dann offen, wenn sie von endlichem Index ist.

Bemerkung: Sei E/K eine Galois-Erweiterung.

(a) Es gilt $E/K = \bigcup_{\alpha\in E} K(\alpha)$, wobei stets $(K(\alpha) : K) < \infty$ gilt.

(b) Ist F ein Zwischenkörper von E/K, dann ist $G(E/F)$ abgeschlossen.

(c) Für $H \leq G(E/K)$ gilt $G(E/E^H) = \overline{H}$, wobei $\overline{H}$ die abgeschlossene Hülle von H bezeichnet.

Definition: Eine topologische Gruppe G heißt *proendlich*, wenn sie kompakt und hausdorffsch ist und das neutrale Element von G eine Umgebungsbasis aus Normalteilern besitzt.

Bemerkung: Eine proendliche Gruppe G ist projektiver Limes der endlichen Gruppen G/N, wobei N die offenen Normalteiler von G durchläuft.

Bemerkung: Sei E/K eine Galois-Erweiterung.
Dann ist $G(E/K)$ eine proendliche Gruppe.

Kapitel 2

Arithmetik endlicher Erweiterungen

2.1 Invariante Polynome

Schreibweise: Sei K ein Körper.
$M_n(K)$ ist die K-Algebra der $n \times n$-Matrizen mit Einträgen aus K.

Definition: Sei K ein Körper, $f, g \in K[X] - \{0\}$.
Sei $f = \sum_{i=0}^{n} a_i X^i$ mit $a_n \neq 0$ und $g = \sum_{i=0}^{m} b_i X^i$ mit $b_m \neq 0$.

(a) Die Matrix $S(f,g) = (s_{i,j})_{0 \leq i,j \leq m+n-1} \in M_{m+n}(K)$ mit

$$s_{i,j} = \begin{cases} a_{n+i-j} & \text{für } 0 \leq i \leq m-1, \quad i \leq j \leq i+n, \\ b_{i-j} & \text{für } m \leq i \leq m+n-1, \quad i-m \leq j \leq i, \\ 0 & \text{sonst,} \end{cases}$$

heißt *Sylvester-Matrix* von f und g.

$$S(f,g) = \left(\begin{array}{ccccccc} a_n & a_{n-1} & \cdots & a_0 & & & \\ & a_n & a_{n-1} & \cdots & a_0 & & \\ & & \ddots & & & \ddots & \\ & & & a_n & a_{n-1} & \cdots & a_0 \\ b_m & b_{m-1} & \cdots & b_0 & & & \\ & b_m & b_{m-1} & \cdots & b_0 & & \\ & & \ddots & & & \ddots & \\ & & & b_m & b_{m-1} & \cdots & b_0 \end{array} \right) \begin{array}{l} \left. \vphantom{\begin{array}{c} a \\ a \\ a \\ a \end{array}} \right\} m \text{ Zeilen,} \\ \left. \vphantom{\begin{array}{c} a \\ a \\ a \\ a \end{array}} \right\} n \text{ Zeilen.} \end{array}$$

(b) $\mathrm{Res}(f,g) = \det(S(f,g))$ heißt *Resultante* von f und g.

(2.1) Satz: Sei K ein Körper. $f, g \in K[X] - \{0\}$ haben über K die Zerlegungen

$$\begin{aligned} f(X) &= a_n(X-\alpha_1) \cdot \ldots \cdot (X-\alpha_n), \\ g(X) &= b_m(X-\beta_1) \cdot \ldots \cdot (X-\beta_m). \end{aligned}$$

Dann gilt:
$$\begin{aligned} \mathrm{Res}(f,g) &= a_n^m b_m^n \prod_{i=1}^{n} \prod_{j=1}^{m} (\alpha_i - \beta_j) \\ &= a_n^m \prod_{i=1}^{n} g(\alpha_i) = (-1)^{mn} b_m^n \prod_{j=1}^{m} f(\beta_j). \end{aligned}$$

Beweis: Die Gleichheit der letzten drei Ausdrücke ist klar.
Man schreibe $S_{n,m}(f,g)$ für $S(f,g)$, um die Grade von f und g hervorzuheben.
Wegen $\mathrm{Res}(f,g) = (-1)^{nm}\,\mathrm{Res}(g,f)$ darf man $n \le m$ annehmen.
Sei $h = q \cdot f + g$ mit $q = \sum_{i=0}^{m-n} q_i X^i$ und $\mathrm{grad}(h) = m - p$.
Dann gilt $\mathrm{Res}(f,g) = a_n^p\,\mathrm{Res}(f,h)$*:*
Sei $M = (m_{i,j}) \in M_{m+n}(K)$ gegeben durch

$$m_{i,j} = \begin{cases} \delta_{i,j} & \text{für } i \le m \text{ oder } i-j > m \text{ oder } i-j < n, \\ q_{i-j-n} & \text{für } i > m \text{ und } n \le i-j \le m, \end{cases}$$

also

$$M = \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ q_{m-n} & \cdots\, q_0 & & 1 & & \\ & \ddots & & \ddots & & \ddots \\ & & q_{m-n} & \cdots\, q_0 & & 1 \end{pmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\\a\\a\end{matrix}}\right\} m \text{ Zeilen,} \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\\a\\a\end{matrix}}\right\} n \text{ Zeilen.} \end{matrix}$$

Dann ist $S_{n,m}(f,h) = M \cdot S_{n,m}(f,g)$.
$S_{n,m}(f,h)$ hat die Gestalt $\left(\begin{smallmatrix} A & * \\ 0 & B \end{smallmatrix}\right)$, wobei $A \in M_p(K)$ obere Dreiecksmatrix mit Diagonaleinträgen a_n und $B = S_{n,m-p}(f,h) = S(f,h)$ ist.
Wegen $\det(M) = 1$ folgt $\mathrm{Res}(f,g) = a_n^p\,\mathrm{Res}(f,h)$.

Das Ergebnis wird nun durch Induktion über $\min(m,n)$ bewiesen.
Es gelte wie oben $n \le m$.
Ist $n = 0$, so ist $\mathrm{Res}(f,g) = a_n^m$, und die Aussage des Satzes gilt.
Sei also $n > 0$. Da $K[X]$ ein euklidischer Ring ist, erhält man durch Polynomdivision $q, h \in K[X]$ mit $g = q \cdot f + h$ und $\mathrm{grad}(h) < n$.
Ist $h = 0$, so gilt $\mathrm{Res}(f,g) = 0$, und die Aussage des Satzes gilt.
Ist $h \neq 0$, so gilt bei $\mathrm{grad}(h) = m - p$ nach oben $\mathrm{Res}(f,g) = a_n^p\,\mathrm{Res}(f,h)$.
Für jede Nullstelle α_i von f gilt $h(\alpha_i) = g(\alpha_i)$.
Nach Induktionsannahme gilt die Aussage des Satzes für $\mathrm{Res}(f,h)$.
Also gilt sie auch für $\mathrm{Res}(f,g)$. ◊

(2.2) Korollar: Sei K ein Körper, $f, g \in K[X] - K$.
f und g sind teilerfremd $\iff \mathrm{Res}(f,g) \neq 0$.

Definition: Sei K ein Körper, $f \in K[X] - K$, $f = a_n(X-\alpha_1)\cdot\ldots\cdot(X-\alpha_n)$.
Die *Diskriminante* von f ist

$$D(f) = a_n^{2n-2} \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2.$$

Beispiel: Spezialfall $n = 2$ über algebraisch abgeschlossenem Körper K:

$$f(X) = a_2X^2 + a_1X + a_0 \text{ mit } a_2 \neq 0.$$

$$f(X) = a_2\left(X + \frac{a_1}{2a_2} + \sqrt{(\frac{a_1}{2a_2})^2 - \frac{a_0}{a_2}}\right)\left(X + \frac{a_1}{2a_2} - \sqrt{(\frac{a_1}{2a_2})^2 - \frac{a_0}{a_2}}\right).$$

$$D(f) = a_2^2(4((\frac{a_1}{2a_2})^2 - \frac{a_0}{a_2})) = a_1^2 - 4a_0a_2.$$

(2.3) Satz: Sei K ein Körper, $f \in K[X] - K$, $f = \sum_{i=0}^{n} a_i X^i$ mit $a_n \neq 0$.

$$\mathrm{Res}(f, f') = (-1)^{\frac{n(n-1)}{2}} a_n D(f).$$

Beweis: Es gelte $f = a_n(X - \alpha_1) \cdot \ldots \cdot (X - \alpha_n)$ in einem Zerfällungskörper von f über K. Dann gilt nach Anwendung der Produktregel für Ableitungen

$$f'(\alpha_i) = a_n \prod_{j=1, j\neq i}^{n} (\alpha_i - \alpha_j).$$

Nach (2.1) ist

$$\begin{aligned} \mathrm{Res}(f, f') &= a_n^n \prod_{i=1}^{n} f'(\alpha_i) = a_n^{2n-1} \prod_{i=1}^{n} \prod_{j\neq i} (\alpha_i - \alpha_j) \\ &= a_n^{2n-1} (-1)^{\sum_{j=1}^{n-1} j} \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 = (-1)^{\frac{n(n-1)}{2}} a_n D(f). \end{aligned}$$

$\Diamond$

Beispiel: $f = a_2X^2 + a_1X + a_0$. Dann ist $f' = 2a_2X + a_1$.

$$S(f, f') = \begin{pmatrix} a_2 & a_1 & a_0 \\ 2a_2 & a_1 & 0 \\ 0 & 2a_2 & a_1 \end{pmatrix}.$$

$$\mathrm{Res}(f, f') = a_2a_1^2 + 4a_0a_2^2 - a_1^2 2a_2 = 4a_0a_2^2 - a_1^2a_2.$$

Beispiel: Sei K ein Körper. $f, g \in K[X] - \{0\}$ haben über K die Zerlegungen

$$\begin{aligned} f(X) &= (X - \alpha_1) \cdot \ldots \cdot (X - \alpha_n), \\ g(X) &= (X - \beta_1) \cdot \ldots \cdot (X - \beta_m). \end{aligned}$$

Gesucht ist ein Polynom $h(X)$, das als Nullstellen genau alle Werte $\alpha_i - \beta_j$ mit $1 \leq i \leq n, 1 \leq j \leq m$ hat.
Idee zur Lösung ist, über $K(Y)$ statt über K zu rechnen.

$$f(X + Y) = (X + Y - \alpha_1) \cdot \ldots \cdot (X + Y - \alpha_n).$$

$$\mathrm{Res}(f(X + Y), g(X)) = \prod_{i=1}^{n} \prod_{j=1}^{m} (-Y + \alpha_i - \beta_j).$$

Man schreibe Res_Z für die über dem Polynomring in Z gebildete Resultante. Dann lautet das gesuchte Ergebnis:

$$h(X) = (-1)^{nm} \mathrm{Res}_Y(f(Y + X), g(Y)).$$

Schreibweise: Sei K ein Körper. $A_n = K[x_1, \ldots, x_n]$.

(2.4) Bemerkung: Die symmetrische Gruppe S_n der Permutationen von $\{1, \ldots, n\}$ operiert auf A_n durch Permutation der Indizes der Unbestimmten, also durch $\begin{array}{ccc} S_n & \to & \mathrm{Aut}(A_n) \\ \pi & \mapsto & (P \mapsto P^\pi) \end{array}$, wobei $P^\pi(x_1, \ldots, x_n) = P(x_{\pi(1)}, \ldots, x_{\pi(n)})$.

Definition: Sei $U \leq S_n$.

(a) $P \in A_n$ heißt *U-invariant* $:\Longleftrightarrow$ für alle $\pi \in U$ gilt $P^\pi = P$.

(b) $P \in A_n$ heißt *symmetrisch* $:\Longleftrightarrow$ P ist S_n-invariant.

Schreibweise: Sei $U \leq S_n$.
$A_n^U = \{P \in A_n \mid \text{für alle } \pi \in U \text{ gilt } P^\pi = P\}$ K-Algebra der U-invarianten Polynome.

Beispiel:

(a) Für $1 \leq k \leq n$ ist $s_k = \sum\limits_{\substack{I \subseteq \{1,\ldots,n\} \\ |I|=k}} \prod\limits_{i \in I} x_i$ ein symmetrisches Polynom.
Setze $s_0 = 1$ und $s_k = 0$ für $k > n$.
s_k heißt das *k-te elementarsymmetrische* Polynom aus A_n.

(b) Für $k \in \mathbb{N}_0$ ist $p_k = \sum\limits_{i=1}^{n} x_i^k$ ein symmetrisches Polynom.
p_k heißt die *k-te Potenzsumme* aus A_n.

(2.5) Bemerkung: Sei K ein Körper.
$f \in K[X]$ habe in $K[X]$ die Zerlegung $f = (X - \alpha_1) \cdot \ldots \cdot (X - \alpha_n)$. Dann gilt

$$f = X^n - s_1 X^{n-1} + s_2 X^{n-2} - \ldots + (-1)^{n-1} s_{n-1} X + (-1)^n s_n,$$

wobei $s_k = s_k(\alpha_1, \ldots, \alpha_n)$ das k-te elementarsymmetrische Polynom in den Nullstellen von f ist.

(2.6) Satz: (Newton)
In A_n gilt für $k \in \mathbb{N}$

$$k\, s_k = \sum_{i=1}^{k} (-1)^{i-1} p_i s_{k-i}.$$

Beweis: Im Ring $A_n[[Y]]$ der formalen Potenzreihen in Y über A_n gelten folgende Identitäten

$$S(Y) = \sum_{k \geq 0} (-1)^k s_k Y^k = \prod_{i=1}^{n} (1 - x_i Y),$$

$$S'(Y) = \sum_{k \geq 1} (-1)^k k s_k Y^{k-1} = \prod_{i=1}^{n} (1 - x_i Y) \left(\sum_{i=1}^{n} \frac{-x_i}{1 - x_i Y} \right),$$

$$P(Y) = \sum_{k \geq 1} p_k Y^k = \sum_{i=1}^{n} \sum_{k \geq 1} (x_i Y)^k = \sum_{i=1}^{n} \frac{x_i Y}{1 - x_i Y}.$$

Daraus folgt die Identität

$$\frac{S'(Y)}{S(Y)} = -Y P(Y).$$

Das Ergebnis folgt dann durch Koeffizientenvergleich bei Y^k in der Identität $S'(Y) = -Y S(Y) P(Y)$. $\Diamond$

Beispiel: Berechnung der Potenzsummen $p_k(\alpha_i)$ der Nullstellen eines normierten $f \in K[X]$ mit $\text{grad}(f) = 3$.

$$f(X) = X^3 + a_1X^2 + a_2X + a_3 = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3).$$

$$\begin{array}{lll} s_1 = -a_1 & p_1 = s_1 & = -a_1 \\ s_2 = a_2 & p_2 = s_1p_1 - 2s_2 & = a_1^2 - 2a_2 \\ s_3 = -a_3 & p_3 = s_1p_2 - s_2p_1 + 3s_3 & = -a_1^3 + 3a_1a_2 - 3a_3 \\ & p_4 = s_1p_3 - s_2p_2 + s_3p_1 & = a_1^4 - 4a_1^2a_2 + 4a_1a_3 + 2a_2^2 \\ & \vdots & \end{array}$$

(2.7) Satz: (Hauptsatz über elementarsymmetrische Polynome)
Sei K ein Körper, $A_n = K[x_1, \ldots, x_n]$. Dann gelten:

(a) $s_1, \ldots, s_n \in A_n$ sind über K algebraisch unabhängig.
(b) $A_n^{S_n} = K[s_1, \ldots, s_n]$.

Beweis: Auf der Folge der Exponenten der Monome $ax_1^{a_1} \cdot \ldots \cdot x_n^{a_n}$ aus A_n wird wie folgt eine Ordnungsrelation erklärt, die *graduiert lexikographische* Ordnung: $(a_1, \ldots, a_n) > (b_1, \ldots, b_n) : \Longleftrightarrow$ $(\sum_{i=1}^n a_i > \sum_{i=1}^n b_i)$ oder $(\sum_{i=1}^n a_i = \sum_{i=1}^n b_i$ und es gibt i, $1 \leq i \leq n$, mit $a_i > b_i$ und $(a_1, \ldots, a_{i-1}) = (b_1, \ldots, b_{i-1}))$.
Durch die Gradbedingung gibt es zu gebener Exponentenfolge $(a_1, \ldots, a_n)$ nur endlich viele kleinere Folgen. Daher kann der Beweis durch Induktion über die Exponentenfolgen geführt werden.
Sei $f \in A_n^{S_n}$, die Monome seien absteigend angeordnet.
Wegen der Symmetrie enthält f mit jedem Monom $ax_1^{a_1} \cdot \ldots \cdot x_n^{a_n}$ auch eines, dessen Exponentenfolge $a_1 \geq \ldots \geq a_n$ erfüllt, und diese Folge ist in der Ordnung größer als alle anderen, die aus Permutationen von $a_1, \ldots, a_n$ resultieren.
Sei also $ax_1^{a_1} \cdot \ldots \cdot x_n^{a_n}$ mit $a_1 \geq \ldots \geq a_n$ das größte auftretende Monom in f.
Im symmetrischen Polynom $g = s_1^{a_1-a_2} \cdot s_2^{a_2-a_3} \cdot \ldots \cdot s_{n-1}^{a_{n-1}-a_n} \cdot s_n^{a_n}$ tritt als größter Exponent $(a_1, \ldots, a_n)$ mit $a_1 \geq \ldots \geq a_n$ auf.
In $h = f - a \cdot g$ tritt dann die Exponentenfolge $(a_1, \ldots, a_n)$ nicht mehr auf, sondern nur noch Monome mit kleineren Exponentenfolgen.
Nach Induktionsannahme ist h als Polynom in $s_1, \ldots, s_n$ darstellbar. Also gilt dasselbe auch für f.
Die Eindeutigkeit der Darstellung ergibt sich wie folgt.
Der Ausdruck $s_1^{c_1} \cdot \ldots \cdot s_n^{c_n}$ besitzt in $x_1, \ldots, x_n$ die größte Exponentenfolge $(c_1 + \ldots + c_n, c_2 + \ldots + c_n, \ldots, c_{n-1} + c_n, c_n)$. Die Exponentenfolgen verschiedener derartiger Ausdrücke sind paarweise verschieden, da die Abbildung $(c_1, \ldots, c_n) \mapsto (c_1 + \ldots + c_n, \ldots, c_{n-1} + c_n, c_n)$ injektiv ist.
Sei $f \in A_n^{S_n}$. Gilt $f = g_1(s_1, \ldots, s_n) = g_2(s_1, \ldots, s_n)$ für $g_1, g_2 \in K[y_1, \ldots, y_n]$, dann setze $g = g_1 - g_2$. Es gilt dann $g(s_1, \ldots, s_n) = 0$.
Zu zeigen ist dann $g = 0$.
Angenommen, es gelte $g \neq 0$. Dann sei $ay_1^{c_1} \cdot \ldots \cdot y_n^{c_n}$ das Monom von g, für das $(c_1 + \ldots + c_n, \ldots, c_{n-1} + c_n, c_n)$ die größte Exponentenfolge aller in g auftretenden Monome ist.
Dann kann der Term $as_1^{c_1} \cdot \ldots \cdot s_n^{c_n}$ durch keinen anderen Monomausdruck fortgehoben werden. Also ist $g(s_1, \ldots, s_n) \neq 0$. Widerspruch. $\Diamond$

Definition: Sei K ein Körper.

(a) Eine K-Algebra A heißt *graduiert* $:\Longleftrightarrow$ A besitzt eine Zerlegung $A = \bigoplus_{d\geq 0} A_d$ mit $A_0 = K$ und $A_i \cdot A_j \subseteq A_{i+j}$.
Die Elemente aus A_d nennt man *homogen* vom Grad d.

(b) Sei A eine graduierte K-Algebra mit $\dim_K(A_d) < \infty$ für alle $d \geq 0$.
Die *Hilbert-Reihe* von A ist $\Phi_A(z) = \sum_{d\geq 0} \dim_K(A_d) z^d$.

(2.8) Bemerkung: Sei $U \leq S_n$.

(a) Es gibt homogene Elemente $u_1, \ldots, u_n, r_1, \ldots, r_t \in A_n^U$ mit
  (i) $u_1, \ldots, u_n$ sind algebraisch unabhängig,
  (ii) A_n^U besitzt als K-Modul die Zerlegung $A_n^U = \bigoplus_{i=1}^{t} r_i K[u_1, \ldots, u_n]$.

(b) Die Hilbert-Reihe von A_n^U ist

$$\Phi_{A_n^U}(z) = \frac{z^{\mathrm{grad}(r_1)} + \ldots + z^{\mathrm{grad}(r_t)}}{(1 - z^{\mathrm{grad}(u_1)}) \cdot \ldots \cdot (1 - z^{\mathrm{grad}(u_n)})}.$$

Beispiel:

(a) Sei $U = \{1\}$. Dann gilt (2.8) mit $u_1 = x_1, \ldots, u_n = x_n$ und $t = 1, r_1 = 1$.

$$\Phi_{A_n}(z) = \frac{1}{(1-z)^n} = \sum_{d\geq 0} \binom{n+d-1}{d} z^d.$$

Speziell gilt $\dim_K((A_n)_d) = \binom{n+d-1}{d}$.

(b) Sei $U = S_n$. Nach (2.7) ist $A_n^{S_n} = K[s_1, \ldots, s_n]$.
Dann gilt (2.8) mit $u_1 = s_1, \ldots, u_n = s_n$ und $t = 1, r_1 = 1$.

$$\Phi_{A_n^{S_n}}(z) = \frac{1}{(1-z)(1-z^2) \cdot \ldots \cdot (1-z^n)}.$$

(2.9) Bemerkung: (Molien)
Sei K ein Körper der Charakteristik 0, $U \leq S_n$.
Zu $\pi \in S_n$ bezeichne $M(\pi) \in M_n(K)$ die Permutationsmatrix $M(\pi) = (\delta_{\pi(i),j})$.
Dann gilt

$$\Phi_{A_n^U}(z) = \frac{1}{|U|} \sum_{\pi \in U} \frac{1}{\det(I_n - z \cdot M(\pi))}.$$

(2.10) Bemerkung: $\pi \in S_n$ sei Produkt zifferndisjunkter Zyklen der Längen $\ell_1, \ldots, \ell_r$. Dann gilt mit den Bezeichnungen aus (2.9)

$$\det(I_n - z \cdot M(\pi)) = \prod_{i=1}^{r} (1 - z^{\ell_i}).$$

Definition: Sei $U \leq S_n$, $P \in A_n$. Setze $W_P = \mathrm{Stab}_U(P) = \{\pi \in U \mid P^\pi = P\}$.

$$R_P(X) = \prod_{\pi \in U/W_P} (X - P^\pi)$$

heißt das *Resolventenpolynom* von P bezüglich U.

(2.11) Bemerkung: Seien $U \leq S_n$ und $P \in A_n$. Dann gilt $R_P(X) \in A_n^U[X]$.

2.2 Norm und Spur

(2.12) Satz: (Dedekind)
Sei E/K endliche separable Körpererweiterung, $n = (E : K)$. C sei algebraisch abgeschlossener Körper mit $E \subseteq C$. Seien $\sigma_1, \ldots, \sigma_n \in G(E/K, C/K)$.
Dann sind $\sigma_1, \ldots, \sigma_n$ über C linear unabhängig.

Beweis:
Zeige: Für $c_1, \ldots, c_n \in C$ gilt: Aus $\sum_{i=1}^{n} c_i\sigma_i = 0$ folgt $(c_1, \ldots, c_n) = (0, \ldots, 0)$.
Es reicht dazu, die Aussage für eine K-Basis $(\beta_1, \ldots, \beta_n)$ von E zu betrachten.
Die Aussage ist dann äquivalent zu $\det((\sigma_i(\beta_j))_{1\le i,j\le n}) \neq 0$.
Nach dem Satz (1.38) vom primitiven Element gibt es $\alpha \in E$ mit $E = K(\alpha)$.
Dann ist $(1, \alpha, \ldots, \alpha^{n-1})$ eine K-Basis von E, und die n Werte $\alpha_i = \sigma_i(\alpha)$ sind paarweise verschieden. Die Matrix $A = (\sigma_i(\alpha^{j-1}))_{1\le i,j\le n} = (\alpha_i^{j-1})_{1\le i,j\le n}$ ist eine Vandermonde-Matrix, also gilt $\det(A) = \prod_{1\le i<j\le n}(\alpha_j - \alpha_i) \neq 0$. ♢

Definition: Sei E/K endliche Körpererweiterung, setze $r = (E : K)_s$.
Sei C ein algebraischer Abschluss von E, sei $G(E/K, C/K) = \{\sigma_1, \ldots, \sigma_r\}$.
Für $\alpha \in E$ heißt

(a) $N_{E/K}(\alpha) = \left(\prod_{\nu=1}^{r} \sigma_\nu(\alpha)\right)^{(E:K)_i}$ die *Norm* von α in K.

(b) $T_{E/K}(\alpha) = (E : K)_i \sum_{\nu=1}^{r} \sigma_\nu(\alpha)$ die *Spur* von α in K.

(2.13) Bemerkung: Sei E/K endliche Körpererweiterung.

(a) $N_{E/K} : E^* \to K^*$ ist ein multiplikativer Gruppenhomomorphismus.

(b) $T_{E/K} : E \to K$ ist ein additiver Gruppenhomomorphismus.

(2.14) Satz: Sei E/K endliche Körpererweiterung.

(a) Ist E/K separabel, dann ist $T_{E/K}$ surjektiv.

(b) Ist E/K nicht separabel, dann ist $T_{E/K} = 0$.

Beweis: Setze $n = (E : K)$.
C sei algebraischer Abschluss von E und $G(E/K, C/K) = \{\sigma_1, \ldots, \sigma_r\}$.
(a): Es ist $r = n$. Gilt für alle $\alpha \in E$, dass $0 = T_{E/K}(\alpha) = \sum_{j=1}^{n} \sigma_j(\alpha)$ ist, dann sind die σ_j über K linear abhängig. Widerspruch zu (2.12).
Als K-lineare Abbildung ist $T_{E/K}$ dann surjektiv.
(b): Ist $\mathrm{char}(K) = p > 0$, dann ist $(E : K)_i = p^m$ nach (1.26)(b), und es ist $m > 0$, da E/K nicht separabel ist. Für alle $\alpha \in E$ ist dann $T_{E/K}(\alpha) = 0$. ♢

(2.15) Satz: (Transitivität von Norm und Spur)
Sei E/K endliche Erweiterung, F Zwischenkörper von E/K.
Dann gelten $N_{E/K} = N_{F/K} \circ N_{E/F}$ und $T_{E/K} = T_{F/K} \circ T_{E/F}$.

Beweis: Sei C ein algebraischer Abschluss von E. Nach (1.16) gibt es eine Bijektion $\begin{array}{ccc} G(F/K, C/K) \times G(E/F, C/F) & \tilde{\to} & G(E/K, C/K) \\ (\tau, \varrho) & \mapsto & \tilde{\tau} \circ \varrho \end{array}$, wenn $\tilde{\tau}$ eine Fortsetzung von τ auf E bezeichnet. Seien also $\tilde{\tau}_1, \ldots, \tilde{\tau}_{(F:K)_s}$ fest gewählte Fortsetzungen der Elemente von $G(F/K, C/K)$ auf E.
Aus (1.17)(a) folgt $(E : K)_i = (E : F)_i(F : K)_i$.

Ist $G(E/K, C/K) = \{\sigma_1, \ldots, \sigma_{(E:K)_s}\}$ und $G(E/F, C/F) = \{\varrho_1, \ldots, \varrho_{(E:F)_s}\}$, dann gelten für alle $\alpha \in E$

$$\begin{aligned} N_{E/K}(\alpha) &= \prod_{\ell=1}^{(E:K)_s} \sigma_\ell(\alpha)^{(E:K)_i} = \prod_{j=1}^{(F:K)_s} \tilde{\tau}_j \left(\prod_{k=1}^{(E:F)_s} \varrho_k(\alpha)^{(E:F)_i} \right)^{(F:K)_i} \\ &= N_{F/K}(N_{E/F}(\alpha)), \\ T_{E/K}(\alpha) &= (E:K)_i \sum_{\ell=1}^{(E:K)_s} \sigma_\ell(\alpha) = (F:K)_i \sum_{j=1}^{(F:K)_s} \tilde{\tau}_j \left((E:F)_i \sum_{k=1}^{(E:F)_s} \varrho_k(\alpha) \right) \\ &= T_{F/K}(T_{E/F}(\alpha)). \end{aligned}$$ ◊

(2.16) Satz:
Sei $E = K(\alpha)$ mit $\alpha \in E$ und $\mathrm{Mipo}_K(\alpha) = X^n + a_{n-1}X^{n-1} + \ldots + a_0$.
Dann ist $N_{E/K}(\alpha) = (-1)^n a_0$ und $T_{E/K}(\alpha) = -a_{n-1}$.

Beweis: Sei C ein algebraischer Abschluss von E. Mit $r = (E : K)_s$ sei $G(E/K, C/K) = \{\sigma_1, \ldots, \sigma_r\}$. Für $1 \le j \le r$ setze man $\alpha_j = \sigma_j(\alpha)$.
Dann ist $N_{\mathrm{Mipo}_K(\alpha)}(C) = \{\alpha_1, \ldots, \alpha_r\}$, und über $C[X]$ gilt

$$\mathrm{Mipo}_K(\alpha) = ((X - \alpha_1) \cdot \ldots \cdot (X - \alpha_r))^{(E:K)_i}.$$

Koeffizientenvergleiche bei X^{n-1} und bei X^0 liefern die Behauptungen. ◊

(2.17) Satz: Sei E/K endliche separable Körpererweiterung.

(a) Die Abbildung $\begin{array}{rcl} E \times E & \to & K \\ (\alpha, \beta) & \mapsto & T_{E/K}(\alpha\beta) \end{array}$ ist eine nicht ausgeartete symmetrische Bilinearform.

(b) Sei $E = K(\alpha)$ mit $f(X) = \mathrm{Mipo}_K(\alpha)$.
Sei $\dfrac{f(X)}{X - \alpha} = \beta_0 + \beta_1 X + \ldots + \beta_{n-1}X^{n-1}$ mit $\beta_0, \ldots, \beta_{n-1} \in E$.
Dann ist die Dualbasis von $(1, \alpha, \ldots, \alpha^{n-1})$ gleich $(\frac{\beta_0}{f'(\alpha)}, \ldots, \frac{\beta_{n-1}}{f'(\alpha)})$.

Beweis: Sei C ein algebraischer Abschluss von E.
(a): Symmetrie und Bilinearität folgen aus Symmetrie und Linearität von $T_{E/K}$.
Gilt $T_{E/K}(\alpha\beta) = 0$ für alle $\beta \in E$, so folgt nach (2.14)(a), dass $\alpha = 0$ ist.
(b): Mit $n = (E : K) = (E : K)_s$ sei $G(E/K, C/K) = \{\sigma_1, \ldots, \sigma_n\}$.
Setze $\alpha_i = \sigma_i(\alpha)$ für $1 \le i \le n$. Dann ist $N_f(C) = \{\alpha_1, \ldots, \alpha_n\}$.
Für $0 \le r \le n-1$ gilt die Identität

$$X^r = \sum_{i=1}^{n} \frac{f(X)}{(X - \alpha_i)} \frac{\alpha_i^r}{f'(\alpha_i)}.$$

Denn $g(X) = X^r - \sum_{i=1}^n \frac{f(X)}{(X-\alpha_i)} \frac{\alpha_i^r}{f'(\alpha_i)}$ ist ein Polynom mit $\mathrm{grad}(g) \le n-1$, das die n Nullstellen $\alpha_1, \ldots, \alpha_n$ hat. Daher gilt $g = 0$.
Setzt man die σ_i wie in (1.1)(b) auf $E(X)$ fort, dann gilt mit (1.41)

$$T_{E(X)/K(X)} \left(\frac{f(X)}{(X - \alpha)} \frac{\alpha^r}{f'(\alpha)} \right) = \sum_{i=1}^{n} \frac{f(X)}{(X - \alpha_i)} \frac{\alpha_i^r}{f'(\alpha_i)} = X^r.$$

Koeffizientenvergleich ergibt dann $T_{E/K}(\alpha^i \frac{\beta_j}{f'(\alpha)}) = \delta_{i,j}$ für $0 \le i, j \le n-1$. ◊

(2.18) Bemerkung: Sei E/K endliche Körpererweiterung, $n = (E : K)$.
Die Multiplikation mit $\beta \in E$ definiert eine K-lineare Abbildung

$$\begin{array}{rcl} m_\beta : E & \to & E, \\ x & \mapsto & \beta x. \end{array}$$

m_β wird bezüglich einer K-Basis $B = (b_1, \ldots, b_n)$ von E beschrieben durch eine Matrix $A_\beta \in M_n(K)$, deren i-te Spalte das Bild $m_\beta(b_i)$ bezüglich B ist.

Definition: Die Abbildung $\begin{array}{rcccc} m : E & \to & \mathrm{End}_K(E) & \to & M_n(K) \\ \beta & \mapsto & m_\beta & \mapsto & A_\beta \end{array}$
ist ein injektiver Homomorphismus von K-Algebren, genannt die *reguläre Darstellung* der K-Algebra E.

Beispiel: Sei $E = K(\alpha)$ mit $\mathrm{Mipo}_K(\alpha) = X^n + a_{n-1}X^{n-1} + \ldots + a_0$.
Sei $B = (1, \alpha, \ldots, \alpha^{n-1})$ und $m_\alpha : x \mapsto \alpha x$. Dann gilt

$$A_\alpha = \begin{pmatrix} 0 & \cdots & \cdots & -a_{n-1} \\ 1 & \ddots & & \vdots \\ \vdots & \ddots & 0 & \vdots \\ 0 & \cdots & 1 & -a_0 \end{pmatrix}.$$

(2.19) Bemerkung: Sei E/K endliche Erweiterung, $\alpha \in E$.
Es bezeichne $\mathrm{Mipo}_K(m_\alpha)$ das Minimalpolynom des K-Endomorphismus m_α.
Dann gilt $\mathrm{Mipo}_K(\alpha) = \mathrm{Mipo}_K(m_\alpha)$.
Speziell folgt:

(a) $T_{E/K}(\alpha) = T(m_\alpha)$ und $N_{E/K}(\alpha) = \det(m_\alpha)$.
(b) Die Eigenwerte von m_α sind genau die Konjugierten von α.

(2.20) Bemerkung: Sei $E = K(\alpha)$ endliche Erweiterung, $n = (E : K)$.
Sei $\beta \in E$. Den Übergang von $\mathrm{Mipo}_K(\alpha)$ zum charakteristischen Polynom von β bzw. m_β, $\chi_K(m_\beta) = \det(m_\beta - X\,\mathrm{Id}_E)$, nennt man *Tschirnhaus-Transformation*.
Es gilt $\chi_K(m_\beta) = \mathrm{Mipo}_K(\beta)^r$ für ein $r \in \mathbb{N}$.

2.3 Normalbasen

Definition: Sei E/K endliche Galois-Erweiterung, $\alpha \in E$.
Ist das System $B(\alpha) = (\sigma(\alpha) | \sigma \in G(E/K))$ über K linear unabhängig, dann ist $B(\alpha)$ eine K-Basis von E, die *Normalbasis* von E/K genannt wird.

(2.21) Bemerkung: Sei E/K endliche Galois-Erweiterung.
Sei $\alpha \in E$, so dass $B(\alpha)$ eine Normalbasis von E/K ist.

(a) α ist primitives Element von E/K, also gilt $E = K(\alpha)$.
(b) Jedes $\tau \in G(E/K)$ permutiert die Elemente von $B(\alpha)$, und τ ist durch Angabe der Permutation der Elemente von $B(\alpha)$ eindeutig bestimmt.

(2.22) Satz: (Existenz einer Normalbasis)
Sei E/K endliche Galois-Erweiterung.
Dann gibt es $\alpha \in E$, so dass $(\sigma(\alpha) | \sigma \in G(E/K))$ eine Normalbasis von E/K ist.

Beweis: Mit $n = (E : K)$ sei $G(E/K) = \{\sigma_1, \ldots, \sigma_n\}$.
(a) K enthalte unendlich viele Elemente.
Gilt für ein $\alpha \in E$ eine Relation $\sum_{i=1}^n a_i \sigma_i(\alpha) = 0$ mit $a_i \in K$, dann gilt für alle j mit $1 \le j \le n$ auch $\sum_{i=1}^n a_i \sigma_j^{-1}\sigma_i(\alpha) = 0$.
Also ist zu zeigen: Es gibt $\alpha \in E$ mit $\det((\sigma_j^{-1}\sigma_i(\alpha))_{ij}) \neq 0$.
Nach dem Satz (1.38) vom primitiven Element gibt es $\beta \in E$ mit $E = K(\beta)$.
Setze $f(X) = \mathrm{Mipo}_K(\beta) = \prod_{i=1}^n (X - \sigma_i(\beta))$.
Setze $g(X) = \frac{f(X)}{X-\beta} \in E[X]$, dann gilt $g^{\sigma_i}(\beta) \begin{cases} = 0 & \text{für } \sigma_i \neq \mathrm{Id}_E, \\ \neq 0 & \text{für } \sigma_i = \mathrm{Id}_E\,. \end{cases}$
Setze $A = (g^{\sigma_i^{-1}\sigma_j}(X))_{1\le i,j\le n} \in M_n(E[X])$ und $d(X) = \det(A) \in E[X]$.
Dann ist $d(X) \neq 0$, denn $d(\beta) = \det((g^{\sigma_i^{-1}\sigma_j}(\beta))_{i,j}) = g(\beta)^n \neq 0$.
Da K unendlich viele Elemente enthält, gibt es $\gamma \in K$ mit $d(\gamma) \neq 0$.
Dann gilt $\det((\sigma_i^{-1}\sigma_j(\frac{f(\gamma)}{\gamma-\beta}))_{i,j}) = \det((\frac{f(\gamma)}{\gamma-\sigma_i^{-1}\sigma_j(\beta)})_{i,j}) = d(\gamma) \neq 0$,
und $\alpha = \frac{f(\gamma)}{\gamma-\beta}$ erfüllt die gewünschte Bedingung.
(b) $G(E/K)$ sei zyklisch, erzeugt von σ. (Das ist bei endlichem K der Fall.)
Dann hat der K-Endomorphismus σ das Minimalpolynom $X^n - 1$, denn es gilt $\sigma^n = \mathrm{Id}_E$, und $1, \sigma, \ldots, \sigma^{n-1}$ sind nach (2.12) über K linear unabhängig.
Bezüglich einer geeigneten K-Basis B wird σ durch die Permutationsmatrix $(\delta_{i,(j+1) \bmod n})_{0\le i,j\le n-1}$ dargestellt. B ist dann eine Normalbasis von E/K. $\Diamond$

(2.23) Satz:
Sei E/K endliche Galois-Erweiterung, F Zwischenkörper von E/K.
Sei $\alpha \in E$, so dass $(\sigma(\alpha) | \sigma \in G(E/K))$ eine Normalbasis von E/K ist, seien $\sigma_1, \ldots, \sigma_m$ die Repräsentanten der Linksnebenklassen von $G(E/F)$ in $G(E/K)$.

(a) Es gilt $F = K(T_{E/F}(\alpha))$.
(b) $B = (\sigma_1^{-1}T_{E/\sigma_1(F)}(\alpha), \ldots, \sigma_m^{-1}T_{E/\sigma_m(F)}(\alpha))$ ist eine Basis von F/K.
(c) Ist F/K normal, dann ist B aus (b) eine Normalbasis von F/K.

Beweis: Setze $G = G(E/K)$ und $H = G(E/F)$, so dass $H \le G$ gilt.
(b): Jedes $x \in E$ hat eine eindeutige Darstellung $x = \sum_{\sigma\in G} a_\sigma \sigma(\alpha)$ mit $a_\sigma \in K$.
Für $\tau \in G$ gilt dann $\tau(x) = \sum_{\sigma\in G} a_\sigma \tau\sigma(\alpha) = \sum_{\sigma\in G} a_{\tau^{-1}\sigma}\sigma(\alpha)$.
Es gilt genau dann $x \in F$, wenn $a_{\tau^{-1}\sigma} = a_\sigma$ für alle $\tau \in H$ gilt, wenn also die Koeffizienten a_σ auf den Rechtsnebenklassen $H\sigma$ von H übereinstimmen.
$\sigma_1^{-1}, \ldots, \sigma_m^{-1}$ repräsentieren die Rechtsnebenklassen von H, und nach (1.35)(a) gilt $\sigma_i H \sigma_i^{-1} = G(E/\sigma_i(F))$, also hat jedes $x \in F$ eine eindeutige Darstellung

$$x = \sum_{i=1}^m a_i \left(\sum_{\tau\in H} \tau\sigma_i^{-1}(\alpha) \right) = \sum_{i=1}^m a_i \sigma_i^{-1} \left(T_{E/\sigma_i(F)}(\alpha) \right) \text{ mit } a_i \in K.$$

Wegen der Eindeutigkeit dieser Darstellung ist B eine Basis von F/K.
(c): Ist H ein Normalteiler von G, dann gilt $\sigma_i(F) = F$, und B enthält genau alle Konjugierten von $T_{E/F}(\alpha)$. Also ist B eine Normalbasis von F/K.
(a): Setze $t_\alpha = T_{E/F}(\alpha)$. Für $i \neq j$ gilt $\sigma_i(t_\alpha) \neq \sigma_j(t_\alpha)$ wegen der Eindeutigkeit der Basisdarstellung. Also hat t_α mindestens $m = (F : K)$ Konjugierte in E, so dass $\mathrm{grad}(\mathrm{Mipo}_K(t_\alpha)) \ge m$ gilt.
Dann sind $1, t_\alpha, \ldots, t_\alpha^{m-1}$ über K linear unabhängig, also gilt $F \subseteq K(t_\alpha)$. $\Diamond$

Kapitel 3

Ergebnisse der Galois-Theorie

3.1 Endliche Körper

(3.1) Satz: Sei p eine Primzahl und $n \in \mathbb{N}$.

(a) Es gibt einen endlichen Körper mit p^n Elementen.

(b) Je zwei endliche Körper mit p^n Elementen sind isomorph.

Beweis: $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ ist ein endlicher Körper mit p Elementen.
Setze $q = p^n$. Sei C ein algebraischer Abschluss von $\mathbb{F}_p$.

(a) $f(X) = X^q - X \in \mathbb{F}_p[X]$ ist separabel. Sei $F = \{\alpha \in C \mid f(\alpha) = 0\}$.
F ist ein Körper: Für $a, b \in F$ gelten $(a-b)^q = a^q - b^q = a - b$ und $(ab)^q = ab$, also $a - b, ab \in F$.
Für $a \in F^*$ gilt $(a^{-1})^q = (a^q)^{-1} = a^{-1}$, also $a^{-1} \in F$.
Also ist F der Zerfällungskörper von $X^q - X$, und es gilt $|F| = q$.

(b) Sei F ein Körper mit q Elementen. Wegen $\mathrm{char}(F) = p$ ist ein zu $\mathbb{F}_p$ isomorpher Körper in F enthalten. Also darf man $\mathbb{F}_p \subseteq F$ annehmen.
Die multiplikative Gruppe F^* hat $q-1$ Elemente. Jedes $\alpha \in F^*$ erfüllt $\alpha^{q-1} = 1$. Also ist F ein Zerfällungskörper von $X^q - X$ über $\mathbb{F}_p$.
Nach (1.8)(b) sind je zwei Zerfällungskörper isomorph. ◊

Definition: Sei K endlicher Körper mit $q = |K|$, E/K endliche Erweiterung.
$\sigma_q : \begin{array}{ccc} E & \to & E \\ x & \mapsto & x^q \end{array}$ heißt *Frobenius-Automorphismus* der Erweiterung E/K.

(3.2) Satz: Sei K endlicher Körper mit $q = |K|$, E/K endliche Erweiterung.

(a) E/K ist galoissch.

(b) $G(E/K) = <\sigma_q>$ ist zyklisch der Ordnung $(E : K)$.

Beweis: Setze $G = <\sigma_q> \leq \mathrm{Aut}(E)$.
Es gilt $K = E^G$, denn K enthält nach (3.1) genau alle $\alpha \in E$ mit $\alpha^q = \alpha$.
Nach (1.39) ist $E/K = E/E^G$ galoissch mit $G(E/K) = G$. ◊

3.2 Einheitswurzelkörper

Definition: Sei K ein Körper, $n \in \mathbb{N}$.

(a) Für $x \in K^*$ bezeichne $\operatorname{ord}(x)$ die Ordnung von x in der Gruppe K^*,
$$\operatorname{ord}(x) = \begin{cases} \min\{m \in \mathbb{N} | x^m = 1\}, & \text{falls es } m \in \mathbb{N} \text{ mit } x^m = 1 \text{ gibt,} \\ \infty & \text{sonst.} \end{cases}$$

(b) $W(K) = \{x \in K^* | \operatorname{ord}(x) < \infty\}$ heißt Gruppe der *Einheitswurzeln* in K.

(c) $W_n(K) = \{x \in K^* | x^n = 1\}$ heißt Gruppe der *n-ten Einheitswurzeln* in K.

(d) $x \in K^*$ heißt *primitive n-te Einheitswurzel* $:\iff \operatorname{ord}(x) = n$.

(3.3) Bemerkung: Sei K ein Körper, $n, m \in \mathbb{N}$.

(a) $W_n(K)$ ist endliche zyklische Gruppe, deren Ordnung n teilt.

(b) Bei $(n, m) = 1$ gilt $W_{nm}(K) \cong W_n(K) \times W_m(K)$.

(c) Bei $\operatorname{char}(K) = p > 0$ und $r \in \mathbb{N}$ gilt $W_{p^r}(K) = \{1\}$.

(3.4) Bemerkung: Sei $n \in \mathbb{N}$.

(a) $W_n(\mathbb{C}) = \{e^{\frac{2\pi i k}{n}} \mid k = 0, 1, \ldots, n-1\}$ enthält n Elemente.

(b) Sei C algebraisch abgeschlossener Körper mit $\operatorname{char}(C) = p > 0$.
Dann gilt $|W_n(C)| = n \cdot p^{-w_p(n)}$.

Definition: Sei K ein Körper, $n \in \mathbb{N}$.
Der Zerfällungskörper von $X^n - 1$ über K heißt der *Körper der n-ten Einheitswurzeln* über K oder der *n-te Kreisteilungskörper* über K.

Schreibweise: Sei K ein Körper, $n \in \mathbb{N}$.
$K_n = K(\sqrt[n]{1})$ sei der Körper der n-ten Einheitswurzeln über K.

(3.5) Satz: Sei K ein Körper, $n \in \mathbb{N}$.

(a) K_n/K ist endliche Galois-Erweiterung.

(b) Ist $\operatorname{char}(K)$ kein Teiler von n, dann gibt es einen injektiven Gruppenhomomorphismus $G(K_n/K) \to (\mathbb{Z}/n\mathbb{Z})^*$.

Beweis:
(a): Bei $\operatorname{char}(K) = p > 0$ gilt in einem algebraischen Abschluss C von K nach (3.3)(c) für alle $r \in \mathbb{N}$, dass $W_{p^r}(C) = \{1\}$ ist.
Also darf man nach (3.3)(b) annehmen, dass $(n, p) = 1$ gilt. Dann ist $X^n - 1$ über K separabel, und nach (1.33) ist K_n als Zerfällungskörper galoissch.
(b): Sei $\sigma \in G(K_n/K)$. Sei $\zeta_n \in K_n^*$ mit $\operatorname{ord}(\zeta_n) = n$.
Wegen $\operatorname{ord}(\sigma(\zeta_n)) = n$ und (3.3)(a) gibt es $k \in \mathbb{N}$ mit $(k, n) = 1$ und $\sigma(\zeta_n) = \zeta_n^k$.
k ist modulo n eindeutig bestimmt, und für alle $\zeta \in W_n(K_n)$ gilt $\sigma(\zeta) = \zeta^k$.
Damit die Abbildung $\begin{array}{ccc} \psi : G(K_n/K) & \to & (\mathbb{Z}/n\mathbb{Z})^* \\ \sigma & \mapsto & k \bmod n \end{array}$ wohldefiniert.
ψ ist ein Homomorphismus wegen $(\zeta_n^k)^\ell = \zeta_n^{k\ell}$.
ψ ist injektiv, da $\sigma \in G(K_n/K)$ bereits durch $\sigma(\zeta_n)$ eindeutig festgelegt ist. $\Diamond$

(3.6) Korollar: Sei K ein Körper, $n \in \mathbb{N}$. Dann ist $G(K_n/K)$ abelsch.

Definition: $\begin{array}{ccc} \varphi : \mathbb{N} & \to & \mathbb{N} \\ n & \mapsto & |(\mathbb{Z}/n\mathbb{Z})^*| \end{array}$ heißt *Eulersche φ-Funktion.*

(3.7) Bemerkung: Für $n \in \mathbb{N}$ gilt $\varphi(n) = n \prod_{p|n} (1 - \frac{1}{p})$.

Definition: Sei C algebraischer Abschluss von $\mathbb{Q}$, $n \in \mathbb{N}$.
$F_n(X) = \prod_{\substack{\zeta \in W_n(C) \\ \mathrm{ord}(\zeta) = n}} (X - \zeta)$ heißt das *n-te Kreisteilungspolynom.*

(3.8) Bemerkung: Sei $n \in \mathbb{N}$.

(a) $F_n(X) \in \mathbb{Z}[X]$ ist normiert vom Grad $\varphi(n)$.

(b) Es gilt $X^n - 1 = \prod_{d|n} F_d(X)$.

(3.9) Bemerkung: Sei C algebraischer Abschluss von $\mathbb{Q}$, seien $m, n \in \mathbb{N}$.

(a) $F_{mn}(X)$ teilt $F_n(X^m)$.

(b) Ist jeder Primteiler von m auch einer von n, dann gilt $F_{mn}(X) = F_n(X^m)$.

(c) Ist p eine Primzahl, die n nicht teilt, dann gilt $F_n(X)F_{np}(X) = F_n(X^p)$.

(d) Für $(m, n) = 1$ und $n > 1$ bei $m = 2$ gilt $F_{mn}(X) = \prod_{\substack{\zeta \in C^* \\ \mathrm{ord}(\zeta) = m}} F_n(\zeta X)$.

Beispiel:

(a) Ist p eine Primzahl, dann gilt $F_p(X) = \sum_{k=0}^{p-1} X^k$.

(b) Es gilt $F_{15}(X)F_3(X) = F_3(X^5)$.
Also ist $F_{15}(X) = \frac{X^{10}+X^5+1}{X^2+X+1} = X^8 - X^7 + X^5 - X^4 + X^3 - X + 1$.

(c) $F_{120}(X) = F_{2^3 \cdot 3 \cdot 5}(X) = F_{2 \cdot 3 \cdot 5}(X^4) = F_{3 \cdot 5}(-X^4) = F_{15}(-X^4)$.
Also ist $F_{120}(X) = X^{32} + X^{28} - X^{20} - X^{16} - X^{12} + X^4 + 1$.

Definition: Sei $f \in \mathbb{Z}[X]$, $f = \sum_{i=0}^{n} a_i X^i$ mit $a_i \in \mathbb{Z}$.
f heißt *primitiv* $:\Longleftrightarrow$ $(a_0, \ldots, a_n) = 1$.

(3.10) Lemma: (Gauß)
Seien $f, g \in \mathbb{Z}[X]$ primitiv. Dann ist fg primitiv.

Beweis: Seien $f = \sum_{i=0}^{n} a_i X^i$ und $g = \sum_{j=0}^{m} b_j X^j$ mit $(a_0, \ldots, a_n) = 1$ und $(b_0, \ldots, b_m) = 1$. Setze $fg = \sum_{k=0}^{n+m} c_k X^k$.
Sei p eine Primzahl. Setze $r = \max\{i \mid 0 \le i \le n,\ p \text{ teilt nicht } a_i\}$ und
$s = \max\{j \mid 0 \le j \le m,\ p \text{ teilt nicht } b_j\}$.
Der Koeffizient von X^{r+s} in fg ist $c_{r+s} = \sum_{k=0}^{r+s} a_k b_{r+s-k}$.
p teilt nicht $a_r b_s$, aber p teilt jeden weiteren Summanden in c_{r+s}.
Also ist p kein Teiler von $(c_0, \ldots, c_{m+n})$.
Dies gilt für alle Primzahlen p, also ist $(c_0, \ldots, c_{m+n}) = 1$. ◊

(3.11) Korollar: Ist $f \in \mathbb{Z}[X]$ reduzibel über $\mathbb{Q}$, dann ist f reduzibel über $\mathbb{Z}$.

(3.12) Satz: (Gauß) Sei $n \in \mathbb{N}$.

(a) $F_n(X)$ ist irreduzibel über $\mathbb{Q}$.

(b) Es gilt $G(\mathbb{Q}_n/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$.

Beweis:
(a): Sei C algebraischer Abschluss von $\mathbb{Q}$. Sei $\zeta \in W_n(C)$ mit $\mathrm{ord}(\zeta) = n$. Setze $f = \mathrm{Mipo}_{\mathbb{Q}}(\zeta)$. In $\mathbb{Q}[X]$ ist f ein Teiler von $X^n - 1$.
Also gilt $X^n - 1 = f(X)h(X)$, und nach (3.11) gilt $f, h \in \mathbb{Z}[X]$.

Zu zeigen ist $f(\zeta^k) = 0$ für alle k mit $0 < k < n$ und $(n, k) = 1$.
Dann folgt $\text{grad}(f) \geq \varphi(n)$, also $f = F_n$.
Da sich jedes der genannten k als Produkt von Primzahlen darstellen lässt, reicht es zu zeigen, dass für jede Primzahl p, die n nicht teilt, $f(\zeta^p) = 0$ gilt.
Annahme: ζ^p sei keine Nullstelle von f.
Dann ist $h(\zeta^p) = 0$, also ist ζ Nullstelle von $h(X^p)$. Als Minimalpolynom ist f ein Teiler von $h(X^p)$, nach (3.11) gilt also $h(X^p) = f(X)g(X)$ mit $g \in \mathbb{Z}[X]$.
Dann gilt $h(X^p) \equiv h(X)^p \equiv f(X)g(X) \bmod p$, also haben die modulo p reduzierten Polynome f und h einen gemeinsamen Faktor in $\mathbb{F}_p[X]$.
Damit hat $X^n - 1 \equiv f(X)h(X) \bmod p$ eine mehrfache Nullstelle in $\mathbb{F}_p[X]$.
Bei $(n, p) = 1$ ist aber $X^n - 1$ teilerfremd zur Ableitung nX^{n-1}. Widerspruch.
(b): Es bleibt zu zeigen, dass die in (3.5)(b) genannte Abbildung surjektiv ist.
Dies folgt nach (a), da $|G(\mathbb{Q}_n/\mathbb{Q})| = (\mathbb{Q}_n : \mathbb{Q}) = \varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$ ist. ◊

(3.13) Satz: Sei K endlicher Körper mit $q = |K|$. Sei $n \in \mathbb{N}$ mit $(n, q) = 1$. Dann gilt $(K_n : K) = \text{ord}(q \bmod n)$.

Beweis: Sei $\zeta \in W_n(K_n)$ mit $\text{ord}(\zeta) = n$. Es gilt $(K_n : K) = \text{ord}(\sigma_q)$ nach (3.2)(b). Es ist $\text{ord}(\sigma_q) = \min\{f \in \mathbb{N} \mid \zeta^{q^f} = \zeta\} = \min\{f \in \mathbb{N} \mid q^f \equiv 1 \bmod n\}$.
Dann ist $\text{ord}(\sigma_q) = \text{ord}(q \bmod n)$, also die Ordnung von q in $(\mathbb{Z}/n\mathbb{Z})^*$. ◊

(3.14) Bemerkung: (Kronecker, Weber)
Sei $K/\mathbb{Q}$ Galois-Erweiterung und $G(K/\mathbb{Q})$ abelsch.
Dann gibt es $n \in \mathbb{N}$ mit $K \subseteq \mathbb{Q}_n$.

(3.15) Bemerkung: (Gauß)
Das regelmäßige n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn

$$n = 2^e \cdot p_1 \cdot \ldots \cdot p_r$$

mit $e \geq 0$ und $r \geq 0$ verschiedenen Primzahlen p_i der Form $p_i = 2^{2^{k_i}} + 1$ gilt.

3.3 Zyklische Erweiterungen und reine Gleichungen

(3.16) Satz: Sei E/K endliche Galois-Erweiterung.

(a) $\text{Ker}(T_{E/K} : E \to K)$ besteht aus allen endlichen Summen von Elementen der Form $\tau(\alpha) - \alpha$ mit $\alpha \in E$ und $\tau \in G(E/K)$.

(b) Ist $G(E/K)$ zyklisch und σ ein Erzeugendes, dann gilt für $b \in E$:
$T_{E/K}(b) = 0 \iff$ Es gibt $\alpha \in E$ mit $b = \sigma(\alpha) - \alpha$.

Beweis:
(a): Nach (2.22) gibt es $\beta \in E$, so dass $(\tau(\beta) \mid \tau \in G(E/K))$ eine K-Basis von E ist. Jedes $b \in E$ hat dann die Gestalt $b = \sum_{\tau \in G(E/K)} a_\tau \tau(\beta)$ mit $a_\tau \in K$.
Dann ist $T_{E/K}(b) = \sum_\tau a_\tau T_{E/K}(\tau(\beta)) = T_{E/K}(\beta)(\sum_\tau a_\tau)$.
Da β eine Normalbasis definiert, ist $T_{E/K}(\beta) = \sum_\tau \tau(\beta) \neq 0$.
Also gilt $T_{E/K}(b) = 0 \iff \sum_\tau a_\tau = 0$.
Sei nun $b \in \text{Ker}(T_{E/K})$. Dann gilt
$b = \sum_\tau a_\tau \tau(\beta) = \sum_\tau a_\tau \tau(\beta) - (\sum_\tau a_\tau)\beta = \sum_\tau (\tau(a_\tau \beta) - a_\tau \beta)$ wie gewünscht.

(b): $M = \{\sigma(\alpha) - \alpha \,|\, \alpha \in E\}$ ist additive Untergruppe von E.
Zu zeigen ist, dass für $\tau = \sigma^k$ und $\alpha \in E$ stets $\tau(\alpha) - \alpha \in M$ gilt.
Sei $\alpha \in E$. Mit $\beta = \sum_{i=0}^{k-1} \sigma^i(\alpha)$ gilt $\sigma(\beta) - \beta = \sigma^k(\alpha) - \alpha$ wie gesucht. $\Diamond$

(3.17) Satz: (Satz 90 von Hilbert)
Sei E/K endliche Galois-Erweiterung, so dass $G(E/K) = < \sigma >$ zyklisch ist.
Für $\beta \in E^*$ gilt: $N_{E/K}(\beta) = 1 \iff$ Es gibt $\alpha \in E^*$ mit $\beta = \alpha/\sigma(\alpha)$.

Beweis:
$\Rightarrow$: Setze $n = (E : K)$. Sei $\gamma \in E$. Setze $\alpha = \sum_{i=0}^{n-1} \sigma^i(\gamma) \prod_{j=0}^{i-1} \sigma^j(\beta)$.
Dann ist $\beta\sigma(\alpha) = \sigma^n(\gamma)\beta \prod_{j=1}^{n-1} \sigma^j(\beta) + \sum_{i=1}^{n-1} \sigma^i(\gamma) \prod_{j=0}^{i-1} \sigma^j(\beta) = \alpha$.
Da $1, \sigma, \ldots, \sigma^{n-1}$ nach (2.12) über E linear unabhängig sind, kann durch geeignete Wahl von γ erreicht werden, dass $\alpha \neq 0$ gilt.
$\Leftarrow$: Es gilt $N_{E/K}(\beta) = N_{E/K}(\alpha)/N_{E/K}(\sigma(\alpha)) = 1$. $\Diamond$

Definition: Sei K Körper, C algebraischer Abschluss von K. Sei $n \in \mathbb{N}, b \in K$.
$\alpha \in C$ heißt *n-te Wurzel* von b, wenn α Nullstelle von $X^n - b$ ist.

(3.18) Satz: Sei K Körper, sei $n \in \mathbb{N}$ mit $|W_n(K)| = n$.
Für $b \in K$ sei E der Zerfällungskörper von $X^n - b$ über K.
$\alpha \in E$ sei n-te Wurzel von b. Sei $d \in \mathbb{N}$ minimal mit $\alpha^d \in K$.
Dann gelten:

(a) d teilt n und $\mathrm{Mipo}_K(\alpha) = X^d - \alpha^d$.
(b) Es ist $E = K(\alpha)$, und $K(\alpha)/K$ ist Galois-Erweiterung vom Grad d.
(c) $G(K(\alpha)/K)$ ist zyklisch.

Beweis: Wegen $|W_n(K)| = n$ haben alle Nullstellen von $X^n - b$ die Form $\zeta\alpha$ mit $\zeta \in W_n(K)$. Speziell gilt $E = K(\alpha)$.
Für $\sigma \in G(E/K)$ ist $\sigma(\alpha)$ Nullstelle von $X^n - b$, also gilt $\sigma(\alpha) = \zeta\alpha$ für ein $\zeta \in W_n(K)$, und σ ist durch ζ eindeutig festgelegt.
Die Abbildung $\begin{array}{rcl} \psi : G(K(\alpha)/K) & \to & W_n(K) \\ \sigma & \mapsto & \sigma(\alpha)/\alpha \end{array}$ ist dann ein injektiver Homomorphismus. $G(K(\alpha)/K)$ ist isomorph zu einer Untergruppe von $W_n(K)$, also ist $G(K(\alpha)/K)$ zyklisch einer Ordnung d', die n teilt.
Ist σ Erzeugendes von $G(K(\alpha)/K)$, dann hat σ die Ordnung d'.
$\zeta = \sigma(\alpha)/\alpha$ erfüllt dann $\mathrm{ord}(\zeta) = d'$, und es ist $\sigma(\alpha^{d'}) = \alpha^{d'}$, also $d' \geq d$.
$1, \alpha, \ldots, \alpha^{d'-1}$ sind über K linear unabhängig, und α ist Nullstelle des Polynoms $X^d - \alpha^d \in K[X]$, also folgt $d' \leq d$.
Insgesamt gilt $d = d'$ und $X^d - \alpha^d = \mathrm{Mipo}_K(\alpha)$. $\Diamond$

(3.19) Satz: Sei K Körper, sei $n \in \mathbb{N}$ mit $|W_n(K)| = n$.
Ist E/K eine Galois-Erweiterung mit $(E : K) = n$ und $G(E/K)$ zyklisch,
dann gibt es $\alpha \in E^*$ und $b \in K^*$ mit $E = K(\alpha)$ und $\mathrm{Mipo}_K(\alpha) = X^n - b$.

Beweis: Sei σ Erzeugendes von $G(E/K)$.
Sei $\zeta \in W_n(K)$ mit $\mathrm{ord}(\zeta) = n$. Da $\zeta \in K$ ist, gilt $N_{E/K}(\zeta) = \zeta^n = 1$.
Nach (3.17) gibt es $\alpha \in E^*$ mit $\sigma(\alpha)/\alpha = \zeta$.
Wegen $\sigma(\alpha^n) = \alpha^n$ gilt $\alpha^n \in K$, mit $b = \alpha^n$ ist also α Nullstelle von $X^n - b$.
Da $\sigma^i(\alpha) = \zeta^i\alpha$ gilt, besitzt α die n Konjugierten $\alpha, \zeta\alpha, \ldots, \zeta^{n-1}\alpha$ über K.
Damit ist $(K(\alpha) : K) = n = (E : K)$, also $E = K(\alpha)$. $\Diamond$

Schreibweise: Sei K ein Körper, $n \in \mathbb{N}$. $K^n = \{b^n \mid b \in K^*\}$.

(3.20) Satz: Sei K ein Körper, p eine Primzahl. Für $b \in K^*$ gilt:
$X^p - b$ ist irreduzibel über $K \iff b \notin K^p$.

Beweis:
$\Rightarrow$: Ist $b = \beta^p \in K^p$, dann ist $X - \beta$ ein echter Teiler von $X^p - b$ über K.
$\Leftarrow$: Sei E Zerfällungskörper von $X^p - b$ über K und $\alpha \in E$ Nullstelle von $X^p - b$.
Ist $\mathrm{char}(K) = p$, so ist $X^p - b = (X - \alpha)^p = \mathrm{Mipo}_K(\alpha)$ wegen $b \notin K^p$, und $E = K(\alpha)$ ist rein inseparabel über K.
Sei also $\mathrm{char}(K) \neq p$. Dann ist $X^p - b$ separabel.
Damit ist $|W_p(E)| = p$. Sei daher $\zeta \in W_p(E)$ mit $\mathrm{ord}(\zeta) = p$. Setze $F = K(\zeta)$.
F/K ist galoissch, und nach (3.5)(b) ist $G(F/K) = <\sigma>$ zyklisch.
Sei $X^p - b$ reduzibel über F. Dann zerfällt $X^p - b$ nach (3.18) in Linearfaktoren.
Damit ist $K(\alpha) \subseteq F$, und es gilt $\sigma(\alpha) = \eta\alpha$ mit $\eta \in W_p(F)$.
Es gibt dann k mit $0 \leq k \leq p-1$, so dass $\sigma(\eta^k\alpha) = \eta^k\alpha$ ist.
Das ist klar für $\eta = 1$, und bei $\eta \neq 1$ gelten $\alpha \notin K$ und $\eta \notin K$.
Dann ist $\sigma(\eta)/\eta$ primitive p-te Einheitswurzel, und es gibt k mit $1 \leq k \leq p-1$ und $(\sigma(\eta)/\eta)^k = \eta^{-1}$. Dies ist das gesuchte k.
Damit ist $\beta = \eta^k\alpha \in K$, und es gilt $\beta^p = (\eta^p)^k\alpha^p = \alpha^p = b$, also $b \in K^p$. $\Diamond$

(3.21) Satz: (Vahlen, Capelli) Sei K ein Körper. Sei $n \in \mathbb{N}$ und $b \in K^*$.
$X^n - b$ ist genau dann irreduzibel über K, wenn folgende Bedingungen gelten.

(i) Für jeden Primteiler p von n gilt $b \notin K^p$.

(ii) Ist n durch 4 teilbar, so gilt $b \notin -4K^4$.

Beweis:
$\Rightarrow$: Sei $X^n - b$ irreduzibel über K.
Sei p Primteiler von n, setze $m = n/p$. Gilt $b = \beta^p$ mit $\beta \in K$, dann ist $X^p - b$ reduzibel über K nach (3.20), also ist $(X^m)^p - b$ reduzibel über K.
Sei 4 Teiler von n und $m = n/4$. Ist $b = -4\beta^4$ mit $\beta \in K$, dann gilt über K
$X^4 - b = X^4 + 4\beta^4 = (X^2 - 2\beta X + 2\beta^2)(X^2 + 2\beta X + 2\beta^2)$.
Also ist $X^n - b = (X^m)^4 - b$ reduzibel über K.
$\Leftarrow$: Der Beweis erfolgt durch Induktion nach n, wobei $n = 1$ klar ist.
Sei E Zerfällungskörper von $X^n - b$, sei $\alpha \in E$ Nullstelle von $X^n - b$.
Sei p Primteiler von n, setze $m = n/p$. Dann ist α^p Nullstelle von $X^m - b$.
Nach Induktionsannahme ist $X^m - b$ irreduzibel, da (i) und (ii) gelten.
Setze $F = K(\alpha^p)$. Dann gilt $(F : K) = m$.
Ist $X^p - \alpha^p$ irreduzibel über F, gilt $(K(\alpha) : K) = (K(\alpha) : F)(F : K) = pm = n$, und $X^n - b$ ist irreduzibel über K.
Ist $X^p - \alpha^p$ reduzibel über F, dann ist $\alpha^p \in F^p$ nach (3.20), also $\alpha^p = \gamma^p$ mit $\gamma \in F$. Es gilt dann $N_{F/K}(\gamma)^p = N_{F/K}(\alpha^p) = (-1)^{m+1}b$.
Sind m und p nicht beide gerade, dann gilt $b \in K^p$ im Widerspruch zu (i).
Dieser Induktionsschritt ist stets ausführbar bei $n = 2$ oder falls n einen ungeraden Primteiler p besitzt. Also gilt die Behauptung für diese n.
Bei $n = 2^r$ mit $r \geq 2$ und $m = 2^{r-1}$ gilt jetzt $-b = \beta^2$ mit $\beta \in K^*$.
Wegen (i) gilt $b \notin K^2$, also gilt $-1 \notin K^2$.
Sei i primitive 4-te Einheitswurzel über K, also Nullstelle von $X^2 + 1$.
Über $K(i)$ gilt die Zerlegung $X^{2^r} - b = (X^{2^{r-1}} - i\beta)(X^{2^{r-1}} + i\beta)$.

Wäre $X^{2^{r-1}} - i\beta$ irreduzibel über $K(i)$, dann wäre auch $X^{2^{r-1}} + i\beta$ als konjugierter Faktor irreduzibel über $K(i)$, und wegen der Eindeutigkeit der Primfaktorzerlegungen in $K(i)[X]$ und $K[X]$ wäre $X^n - b$ irreduzibel über K, also wäre auch $X^2 - \alpha^2$ irreduzibel über F im Widerspruch zu obiger Annahme.
Also ist $X^{2^{r-1}} - i\beta$ reduzibel über $K(i)$, und aus (3.20) folgt $i\beta \in K(i)^2$.
Es gilt $i\beta = (c + id)^2 = c^2 - d^2 + 2icd$ mit $c, d \in K$, so dass $c^2 = d^2$ ist.
Dann folgt $b = -\beta^2 = -4c^4 \in -4K^4$ im Widerspruch zu (ii). ◊

(3.22) Satz: (Artin, Schreier) Sei K Körper mit $\mathrm{char}(K) = p > 0$.

(a) Sei E/K Galois-Erweiterung vom Grad p, und $G(E/K)$ sei zyklisch. Dann gibt es $\alpha \in E$ und $b \in K$ mit $E = K(\alpha)$ und $\mathrm{Mipo}_K(\alpha) = X^p - X - b$.

(b) Für $b \in K$ sei E der Zerfällungskörper von $X^p - X - b$ über K. Dann tritt einer der folgenden Fälle ein.
   (i) $X^p - X - b$ zerfällt über K in Linearfaktoren, und es ist $E = K$.
   (ii) $X^p - X - b$ ist über K irreduzibel. Dann ist E/K Galois-Erweiterung vom Grad p, und $G(E/K)$ ist zyklisch.

Beweis:
(a): Sei E/K Galois-Erweiterung vom Grad p und $G(E/K) = <\sigma>$ zyklisch.
Es gilt $T_{E/K}(1) = (E : K) \cdot 1 = p = 0$.
Nach (3.16)(b) gibt es $\alpha \in E$ mit $1 = \sigma(\alpha) - \alpha$, also $\sigma(\alpha) = \alpha + 1$.
Für $0 \le j \le p-1$ ist dann $\sigma^j(\alpha) = \alpha + j$, insbesondere sind die p Werte $\sigma^j(\alpha)$ paarweise verschieden. Damit ist $(K(\alpha) : K) \ge p$, also $E = K(\alpha)$.
Es gilt $\sigma(\alpha^p - \alpha) = (\alpha + 1)^p - (\alpha + 1) = \alpha^p - \alpha$, also gilt $b = \alpha^p - \alpha \in K$ und $\mathrm{Mipo}_K(\alpha) = X^p - X - b$.
(b): Sei E Zerfällungskörper von $f(X) = X^p - X - b$.
Sei $\alpha \in E$ Nullstelle von f. Für $n \in \mathbb{F}_p$ gilt dann
$f(\alpha + n) = (\alpha + n)^p - (\alpha + n) - b = \alpha^p + n^p - \alpha - n - b = f(\alpha) + n^p - n = 0$.
Also hat f in E die Nullstellen $\alpha, \alpha + 1, \ldots, \alpha + (p-1)$.
f ist daher separabel, E/K ist galoissch, und es ist $E = K(\alpha)$.
Liegt eine Nullstelle von f in K, dann gilt das für alle Nullstellen, und (i) gilt.
Hat f keine Nullstelle in K, so gilt für $\sigma \in G(E/K)$, dass $\sigma(\alpha) = \alpha + n_\sigma$ mit $n_\sigma \in \mathbb{F}_p$ ist. Die Abbildung $\begin{array}{rcl} \psi : G(E/K) & \to & \mathbb{Z}/p\mathbb{Z} \\ \sigma & \mapsto & \sigma(\alpha) - \alpha \end{array}$ ist ein injektiver Gruppenhomomorphismus in die additive Gruppe $\mathbb{Z}/p\mathbb{Z}$. Wegen $E \neq K$ ist $G(E/K) \cong \mathbb{Z}/p\mathbb{Z}$ zyklisch. f ist irreduzibel, da $G(E/K)$ transitiv ist. ◊

3.4 Kummer-Theorie

Definition: Sei G eine abelsche Gruppe.
$G^\wedge = \mathrm{Hom}(G, \mathbb{C}^*)$ heißt die *Charaktergruppe* von G.

Schreibweise: Sei K ein Körper, C ein algebraischer Abschluss von K.
Sei $n \in \mathbb{N}$ mit $|W_n(K)| = n$. Für $A \subseteq K^*$ sei $\sqrt[n]{A} = \{\alpha \in C \mid \alpha^n \in A\}$.

(3.23) Bemerkung: Sei K ein Körper, sei $n \in \mathbb{N}$ mit $|W_n(K)| = n$.
Sei $A \subseteq K^*$. Bezeichnet $B = <A, K^n>$ die von A und K^n erzeugte multiplikative Untergruppe von K^*, dann gilt $K(\sqrt[n]{A}) = K(\sqrt[n]{B})$.

Definition: Sei K ein Körper, sei $n \in \mathbb{N}$ mit $|W_n(K)| = n$.
Eine Körpererweiterung E/K heißt *Kummer-Erweiterung vom Exponenten n*, wenn E/K galoissch und $G(E/K)$ abelsch vom Exponenten n ist.

(3.24) Satz: Sei K ein Körper. Sei $n \in \mathbb{N}$ mit $|W_n(K)| = n$.
Sei A multiplikative Gruppe mit $K^n \leq A \leq K^*$.

(a) $K(\sqrt[n]{A})/K$ ist Galois-Erweiterung.
Setze $G = G(K(\sqrt[n]{A})/K)$, dann ist G abelsch vom Exponenten n.

(b) Die Abbildung $\begin{array}{ccc} G \times A/K^n & \to & W_n(K) \\ (\sigma, aK^n) & \mapsto & \sigma(\alpha)/\alpha \end{array}$, wobei $\alpha \in \sqrt[n]{A}$ mit $\alpha^n = a$ gilt, ist eine nicht ausgeartete Paarung.

(c) $K(\sqrt[n]{A})/K$ ist genau dann endlich, wenn A/K^n endlich ist.
Ist A/K^n endlich, dann gilt $G^\wedge \cong A/K^n$.

Beweis: Setze $E = K(\sqrt[n]{A})$. Sei $a \in A$, $\alpha \in E$ mit $\alpha^n = a$.
Alle Nullstellen von $\mathrm{Mipo}_K(\alpha)$ haben die Form $\zeta\alpha$ mit $\zeta \in W_n(K)$. Also zerfällt $\mathrm{Mipo}_K(\alpha)$ über E in Linearfaktoren. Daher ist E/K galoissch.
Für $\sigma \in G$ gilt $(\sigma(\alpha))^n = a$, also ist $\zeta_{(\sigma,a)} = \frac{\sigma(\alpha)}{\alpha} \in W_n(K)$.
$\zeta_{(\sigma,a)}$ *ist wohldefiniert:* Ist $\gamma \in E$ mit $\gamma^n = a$, dann gibt es $\eta \in W_n(K)$ mit $\alpha = \eta\gamma$, und es gilt $\frac{\sigma(\alpha)}{\alpha} = \frac{\sigma(\eta)\sigma(\gamma)}{\eta\gamma} = \frac{\sigma(\gamma)}{\gamma}$.
Für $b \in K$ gilt $\frac{\sigma(\alpha b)}{\alpha b} = \frac{\sigma(\alpha)}{\alpha}$, also ist $\zeta_{(\sigma,ab^n)} = \zeta_{(\sigma,a)}$.
Die Abbildung $(\sigma, a) \mapsto \zeta_{(\sigma,a)}$ ist multiplikativ in beiden Komponenten:
Seien $\sigma, \varrho \in G$, $b \in A$ und $\beta \in E$ mit $\beta^n = b$. Dann gelten
$\zeta_{(\sigma\varrho,a)} = \frac{\sigma\varrho(\alpha)}{\alpha} = \zeta_{(\sigma,a)}\zeta_{(\varrho,a)}$ und $\zeta_{(\sigma,ab)} = \frac{\sigma(\alpha\beta)}{\alpha\beta} = \frac{\sigma(\alpha)}{\alpha} \cdot \frac{\sigma(\beta)}{\beta} = \zeta_{(\sigma,a)}\zeta_{(\sigma,b)}$.
Die Abbildung $(\sigma, a) \mapsto \zeta_{(\sigma,a)}$ ist nicht ausgeartet:
Ist $\sigma \in G$, so dass $\frac{\sigma(\alpha)}{\alpha} = 1$ für alle $\alpha \in E$ mit $\alpha^n \in A$ gilt, dann ist $\sigma = \mathrm{Id}_E$.
Sei $\alpha \in E$ mit $\alpha^n = a \in A$. Bei $\frac{\sigma(\alpha)}{\alpha} = 1$ für alle $\sigma \in G$ ist $\alpha \in K^*$ und $a \in K^n$.
Multiplikativität und Injektivität in der ersten Komponente liefern, dass G abelsch ist und den Exponenten n hat.
(c) folgt direkt aus der Existenz der Paarung in (b). Ein Isomorphismus ist gegeben durch $\begin{array}{ccc} A/K^n & \to & G^\wedge \\ aK^n & \mapsto & (\sigma \mapsto \frac{\sigma(\alpha)}{\alpha}) \end{array}$. ◊

Schreibweise: Sei K ein Körper.
Sei $n \in \mathbb{N}$ mit $|W_n(K)| = n$. Sei C algebraischer Abschluss von K.
$\mathcal{A}_n(K) = \{E \mid K \subseteq E \subseteq C, E/K \text{ Kummer-Erweiterung vom Exponenten } n\}$,
$\mathcal{U}_n(K) = \{A \mid K^n \leq A \leq K^*\}$.

(3.25) Satz: (Hauptsatz der Kummer-Theorie)
Sei K ein Körper. Sei $n \in \mathbb{N}$ mit $|W_n(K)| = n$.

(a) Die Abbildung $\begin{array}{ccc} \mathcal{U}_n(K) & \to & \mathcal{A}_n(K) \\ A & \mapsto & K(\sqrt[n]{A}) \end{array}$ ist bijektiv.
Die Umkehrabbildung ist $\begin{array}{ccc} \mathcal{A}_n(K) & \to & \mathcal{U}_n(K) \\ E & \mapsto & E^n \cap K^* \end{array}$.

(b) Die Abbildungen sind isoton:
Für $A_1, A_2 \in \mathcal{U}_n(K)$ gilt: $A_1 \subseteq A_2 \iff K(\sqrt[n]{A_1}) \subseteq K(\sqrt[n]{A_2})$,
für $E_1, E_2 \in \mathcal{A}_n(K)$ gilt: $E_1 \subseteq E_2 \iff E_1^n \cap K^* \subseteq E_2^n \cap K^*$.

Beweis: Seien $\varphi : \mathcal{U}_n(K) \to \mathcal{A}_n(K)$, $\psi : \mathcal{A}_n(K) \to \mathcal{U}_n(K)$ obige Abbildungen.
φ ist surjektiv: Zeige $\varphi \circ \psi = \mathrm{Id}_{\mathcal{A}_n(K)}$.
Sei E/K Galois-Erweiterung und $G(E/K)$ abelsch vom Exponenten n.
Setze $A = E^n \cap K^*$. Dann gilt $K^n \leq A \leq K^*$. Setze $E_A = K(\sqrt[n]{A})$.
Dann gilt $\varphi \circ \psi(E) = E_A$, und zu zeigen ist $E_A = E$.
$E_A \subseteq E$ ist klar wegen $\sqrt[n]{A} \subseteq E$.
Für $\alpha \in E$ ist $K(\alpha)/K$ endliche galoissche Teilerweiterung von E/K, und $G(K(\alpha)/K)$ ist abelsch, also ist $K(\alpha)/K$ das Kompositum endlich vieler galoisscher Teilerweiterungen von E/K mit zyklischer Galois-Gruppe.
Daher ist zu zeigen: Jede galoissche Erweiterung von K mit zyklischer Galois-Gruppe, die in E enthalten ist, ist auch in E_A enthalten.
Sei $F \subseteq E$ mit $G(F/K)$ zyklisch. Nach (3.19) gibt es $\beta \in F^*$ mit $F = K(\beta)$ und $\beta^n \in K^*$. Dann ist $\beta \in A$, also $F \subseteq E_A$.
φ ist injektiv: Zeige $\psi \circ \varphi = \mathrm{Id}_{\mathcal{U}_n(K)}$.
Sei A mit $K^n \leq A \leq K^*$ gegeben. Setze $E = K(\sqrt[n]{A})$ und $A_E = E^n \cap K^*$.
Dann gilt $\psi \circ \varphi(A) = A_E$, und zu zeigen ist $A = A_E$.
$A \subseteq A_E$ ist klar wegen $A \subseteq E^n$.
Sei $a \in A_E$. Wegen $K(\sqrt[n]{A}) = E$ gibt es zu $\alpha \in E$ mit $\alpha^n = a$ Elemente $\alpha_1, \ldots, \alpha_r \in E$ mit $\alpha_i^n = a_i \in A$ für $i = 1, \ldots, r$ und $\alpha \in K(\alpha_1, \ldots, \alpha_r)$.
Setze $B = < a_1, \ldots, a_r > K^n$, $F = K(\sqrt[n]{B})$ und $A_F = F^n \cap K^*$.
Dann gilt $a \in A_F$. Weiter ist $B \subseteq A_F$, und nach dem ersten Beweisabschnitt gilt $K(\sqrt[n]{B}) = K(\sqrt[n]{A_F})$. Da A_F/K^n endlich ist, folgt nach (3.24)(c), dass $(B : K^n) = (A_F : K^n)$ gilt. Daraus folgt $B = A_F$.
Aus $A_F = B \subseteq A$ folgt dann $a \in A$. Insgesamt gilt dann $A_E \subseteq A$.
Die Inklusionen in (b) folgen aus den Definitionen. ◊

Schreibweise: Sei K Körper mit $\mathrm{char}(K) = p > 0$, C algebraischer Abschluss von K. Es bezeichne $\wp$ die Abbildung $\begin{array}{ccc} \wp : K & \to & K \\ x & \mapsto & x^p - x \end{array}$.
Für $A \subseteq K$ sei $\wp^{-1}(A) = \{\alpha \in C \mid \alpha^p - \alpha \in A\}$.

(3.26) Bemerkung: Sei K Körper mit $\mathrm{char}(K) = p > 0$.
Sei $A \subseteq K$. Bezeichnet $B = < A, \wp(K) >$ die von A und $\wp(K)$ erzeugte additive Untergruppe von K, dann gilt $K(\wp^{-1}(A)) = K(\wp^{-1}(B))$.

(3.27) Bemerkung: Sei K Körper mit $\mathrm{char}(K) = p > 0$.
Sei A additive Gruppe mit $\wp(K) \leq A \leq K$.

(a) $K(\wp^{-1}(A))/K$ ist eine Galois-Erweiterung.
Setze $G = G(K(\wp^{-1}(A))/K)$, dann ist G abelsch vom Exponenten p.

(b) Die Abbildung $\begin{array}{ccc} G \times A/\wp(K) & \to & \mathbb{Z}/p\mathbb{Z} \\ (\sigma, a + \wp(K)) & \mapsto & \sigma(\alpha) - \alpha \end{array}$, wobei $\alpha \in \wp^{-1}(A)$ mit $\wp(\alpha) = a$ gilt, ist eine nicht ausgeartete Paarung.

(c) $K(\wp^{-1}(A))/K$ ist genau dann endlich, wenn $A/\wp(K)$ endlich ist.
Ist $A/\wp(K)$ endlich, dann gilt $(K(\wp^{-1}(A)) : K) = (A : \wp(K))$.

(d) Die Abbildung $A \mapsto K(\wp^{-1}(A))$ ist eine Bijektion zwischen Gruppen A mit $\wp(K) \leq A \leq K$ und Kummer-Erweiterungen E/K vom Exponenten p.

3.5 Auflösbare Erweiterungen

Definition: G sei endliche Gruppe. G heißt *auflösbar* (oder *metazyklisch*) $:\Longleftrightarrow$ es gibt eine Kette $G = H_0 > H_1 > \ldots > H_r = \{1\}$ mit

(i) für $i = 0, 1, \ldots, r$ ist H_i Untergruppe von G,

(ii) für $i = 1, \ldots, r$ ist H_i normal in H_{i-1}, und $(H_{i-1} : H_i) = p_i$ mit p_i prim.

(3.28) Bemerkung: Sei G eine endliche Gruppe.

(a) Sei G auflösbar. Dann ist jede Untergruppe von G und jede Faktorgruppe von G auflösbar.

(b) Sei N ein Normalteiler von G. Sind N und G/N auflösbar, dann ist G auflösbar.

Beispiel:

(a) Sei G eine endliche abelsche Gruppe. Dann ist G auflösbar.

(b) Sei p eine Primzahl und G eine p-Gruppe. Dann ist G auflösbar.

(c) Die symmetrische Gruppe S_n ist für $n \geq 5$ nicht auflösbar.

Definition: Sei F/K eine Körpererweiterung.

(a) F/K heißt eine *Radikalerweiterung* $:\Longleftrightarrow$ es gibt eine endliche Kette $K = K_0 \subset K_1 \subset \ldots \subset K_r = F$, so dass für $i = 1, \ldots, r$ die Erweiterung K_i/K_{i-1} von der Form $K_i = K_{i-1}(\alpha_i)$ ist, wobei es ein $a_i \in K_{i-1}^*$ und eine Primzahl p_i gibt, so dass α_i Nullstelle von $X^{p_i} - a_i$ ist.

(b) F/K heißt *durch Radikale auflösbar* $:\Longleftrightarrow$ es gibt eine Radikalerweiterung E/K mit $F \subseteq E$.

(c) $f \in K[X]$ heißt *durch Radikale auflösbar* $:\Longleftrightarrow$ es gibt einen Zerfällungskörper E von f, so dass E/K durch Radikale auflösbar ist.

(3.29) Bemerkung: Sei K ein Körper.

(a) Sind E_1/K und E_2/K Radikalerweiterungen, dann ist das Kompositum E_1E_2/K eine Radikalerweiterung.

(b) Ist E/K Radikalerweiterung und N/K normale Hülle von E/K, dann ist N/K Radikalerweiterung.

(c) Ist E/K rein inseparabel, dann ist E/K Radikalerweiterung.

(d) Ist $f \in K[X]$ irreduzibel, E/K durch Radikale auflösbar, und gibt es $\alpha \in E$ mit $f(\alpha) = 0$, dann ist f durch Radikale auflösbar.

(3.30) Satz: Sei E/K endliche separable Körpererweiterung, N/K normale Hülle von E/K.

(a) Ist E/K durch Radikale auflösbar, dann ist $G(N/K)$ auflösbar.

(b) Ist $G(N/K)$ auflösbar und teilt $\mathrm{char}(K)$ nicht die Ordnung von $G(N/K)$, dann ist E/K ist durch Radikale auflösbar.

Beweis: Sei C ein algebraischer Abschluss von N, setze $n = (N : K)$.
(a): *Es reicht, die Aussage für E/K normal und Radikalerweiterung zu zeigen:* Denn nach (3.29)(b) ist mit E/K auch N/K durch Radikale auflösbar, und

nach Definition gibt es eine Radikalerweiterung F/K mit $N \subseteq F$, wobei F nach (3.29)(b) als normal vorausgesetzt werden darf.
Mit $G(F/K)$ ist dann auch die Faktorgruppe $G(N/K)$ nach (3.28)(a) auflösbar.
Sei nun $K = K_0 \subset K_1 \subset \ldots \subset K_r = E$ eine Kette von Zwischenkörpern, die für $i = 1, \ldots, r$ nach Voraussetzung $K_i = K_{i-1}(\alpha_i)$ mit $\mathrm{Mipo}_{K_{i-1}}(\alpha_i) = X^{p_i} - a_i$ erfüllen, wobei die p_i Primzahlen sind, die wegen der Separabilität von E/K ungleich $\mathrm{char}(K)$ sind. Dann ist $n = p_1 \cdot \ldots \cdot p_r$.
Da $\mathrm{char}(K)$ nicht n teilt, gilt $|W_n(C)| = n$. Sei $\zeta \in W_n(C)$ mit $\mathrm{ord}(\zeta) = n$.
Es reicht zu zeigen, dass $G(E(\zeta)/K(\zeta))$ auflösbar ist:
Die Erweiterung $E(\zeta)/K$ ist normal als Kompositum von E/K und $K(\zeta)/K$.
Mit E/K ist auch $E(\zeta)/K(\zeta)$ Radikalerweiterung, denn für die Kette der Zwischenkörper $K(\zeta) = K_0(\zeta) \subseteq K_1(\zeta) \subseteq \ldots \subseteq K_r(\zeta) = E(\zeta)$ ist für $i = 1, \ldots, r$ der Grad $(K_i(\zeta) : K_{i-1}(\zeta))$ gleich 1 oder p_i.
Wenn $G(E(\zeta)/K(\zeta))$ auflösbar ist, dann ist nach (3.28)(b) auch $G(E/K)$ auflösbar, da auch $G(K(\zeta)/K)$ abelsch, also auflösbar ist.
Gelte nun $\zeta \in K$, also $|W_n(K)| = n$.
Wegen der Separabilität von E/K ist jede Teilerweiterung K_i/K_{i-1} galoissch, und $G(K_i/K_{i-1})$ ist zyklisch der Ordnung p_i nach (3.18).
Nach (1.40) korrespondiert zur Kette der Zwischenkörper K_i von E eine Kette $G = H_0 > H_1 > \ldots > H_r = \{1\}$ von Untergruppen $H_i = G(E/K_i)$ von $G = G(E/K)$, in der für $i = 1, \ldots, r$ die Untergruppe H_i Normalteiler in H_{i-1} und die Faktorgruppe H_{i-1}/H_i zyklisch der Ordnung p_i ist.
Also ist $G(E/K)$ auflösbar.
(b): *Es reicht, die Aussage für E/K normal zu zeigen:*
Denn ist N/K durch Radikale auflösbar, dann auch E als Teilkörper von N.
Da $\mathrm{char}(K)$ nicht n teilt, gilt $|W_n(C)| = n$. Sei $\zeta \in W_n(C)$ mit $\mathrm{ord}(\zeta) = n$.
Es reicht zu zeigen, dass $E(\zeta)/K(\zeta)$ durch Radikale auflösbar ist:
Denn da $K(\zeta)/K$ Radikalerweiterung ist, ist nach (3.29)(a) dann $E(\zeta)/K$ durch Radikale auflösbar. Damit ist auch E/K durch Radikale auflösbar.
Gelte nun $\zeta \in K$, also $|W_n(K)| = n$.
Nach Voraussetzung gibt es eine Kette $G = H_0 > H_1 > \ldots > H_r = \{1\}$ von Untergruppen H_i von G, wo H_i Normalteiler in H_{i-1} und die Faktorgruppe H_{i-1}/H_i zyklisch von Primzahlordnung p_i ist.
Nach (1.40) korrespondiert zu dieser Kette eine Kette von Zwischenkörpern $K = K_0 \subset K_1 \subset \ldots \subset K_r = E$, so dass für $i = 1, \ldots, r$ die Erweiterung K_i/K_{i-1} galoissch mit zu H_{i-1}/H_i isomorpher Galois-Gruppe ist. Also ist $G(K_i/K_{i-1})$ zyklisch der Ordnung p_i, und nach (3.19) gibt es $\alpha_i \in K_i^*$ mit $K_i = K_{i-1}(\alpha_i)$ und $\alpha_i^{p_i} \in K_{i-1}^*$.
Also ist E/K durch Radikale auflösbar. $\Diamond$

Beispiel: Sei $K = \mathbb{Q}$ und E der Zerfällungskörper von $X^3 - 3X + 1$ über $\mathbb{Q}$.
Es gilt $E \subseteq \mathbb{R}$, aber E ist über $\mathbb{R}$ nicht durch Radikale auflösbar.
Ist α eine Nullstelle von $X^3 - 3X + 1$, dann gilt über $\mathbb{C}$

$$\alpha = \sqrt[3]{-\frac{1}{2} + \frac{\sqrt{-3}}{2}} + \sqrt[3]{-\frac{1}{2} - \frac{\sqrt{-3}}{2}},$$

also ist E über $\mathbb{C}$ durch Radikale auflösbar.

Beispiel: Setze $K = \mathbb{Q}$ und $f = X^5 - 6X + 3$.
Es gilt $G_f \cong S_5$, also ist f nicht durch Radikale auflösbar.

(3.31) Bemerkung:
Die Begriffe der Radikalerweiterung und der durch Radikale auflösbaren Erweiterung können auf eine Galois-Erweiterung F/K mit $\mathrm{char}(K) = p > 0$ und $(F : K) = p$ verallgemeinert werden, indem in der Definition für die Kette der Zwischenerweiterungen zusätzlich Erweiterungen der Form $K_i = K_{i-1}(\alpha_i)$ mit $\mathrm{Mipo}_{K_{i-1}}(\alpha_i) = X^p - X - a_i$ mit $a_i \in K_{i-1}^*$ zugelassen werden.
Die Verallgemeinerung von (3.30) hat dann folgende einfache Gestalt:

Sei E/K endliche Körpererweiterung, N/K normale Hülle von E/K.
E/K ist durch Radikale auflösbar $\iff$ $G(N/K)$ ist auflösbar.

Literatur

[1] Lang, Serge: *Algebra*, Addison-Wesley, Reading, Mass., 1971.

[2] Lorenz, Falko: *Einführung in die Algebra, Teil I*, BI-Wissenschaftsverlag, Zürich, 1987.

[3] Morandi, Patrick: *Field and Galois Theory*, Springer, New York, 1996.

[4] Stroth, Gernot: *Algebra*, De Gruyter, Berlin, 1998.

Aufgabenblätter

Technische Universität Braunschweig
Institut für Analysis und Algebra
Dr. C. Adelmann

20. April 2005
Blatt 1

Aufgaben zur Vorlesung „Galoisgruppen“

Aufgabe 1

(a) Berechne das Minimalpolynom von $\sqrt{2}+\sqrt{3}$ über $\mathbb{Q}$.

(b) Seien $a, b \in \mathbb{Z}$ keine Quadratzahlen, $p, q \in \mathbb{Z} - \{0\}$.
Berechne ein Polynom 4. Grades über $\mathbb{Q}$, das $p\sqrt{a} + q\sqrt{b}$ als Nullstelle hat.

Aufgabe 2

Sei $\alpha = \sqrt[3]{2}$. In $K = \mathbb{Q}(\alpha)$ ist die Multiplikation mit einem Element y eine lineare Abbildung, bezeichnet mit $m_y : K \to K$. Stelle diese in Matrixform bezüglich der Basis $\{1, \alpha, \alpha^2\}$ dar, d.h. bestimme eine Matrix M über $\mathbb{Q}$ mit $m_y(x) = M \cdot x$.

Aufgabe 3

Sei $K = \mathbb{F}_2$, $f(X) = X^3 + X + 1$.

(a) Bestimme einen Zerfällungskörper E von f über K.

(b) Berechne die Nullstellen von f in E, und stelle f als Produkt von Linearfaktoren über E dar.

Aufgabe 4

Zeige durch ein Gegenbeispiel, dass folgende Aussage falsch ist:
Sind E/F und F/K normal, dann ist auch E/K normal.
(Hinweis: Betrachte $K = \mathbb{Q}$ und $\alpha = \sqrt[4]{2}$.)

Technische Universität Braunschweig
Institut für Analysis und Algebra
Dr. C. Adelmann

27. April 2005
Blatt 2

Aufgaben zur Vorlesung „Galoisgruppen“

Aufgabe 5
Berechne in $\mathbb{Q}[X]$ für die Poynome

$$\begin{aligned} f(x) &= x^3 + x^2 - x - 1, \\ g(x) &= x^4 + x^3 + x + 1, \end{aligned}$$

den größten gemeinsamen Teiler von f, f' sowie den von f, g.

Aufgabe 6
Sei α algebraisch über $\mathbb{Q}$, $f(X)$ das Minimalpolynom von α über $\mathbb{Q}$.
Stelle das Minimalpolynom von α^2 über $\mathbb{Q}$ mit Hilfe von $f(X)$ dar.

Aufgabe 7
Gib ein Beispiel für eine endliche Erweiterung E/K an, die unendlich viele Zwischenkörper F besitzt.
(Hinweis: Betrachte $E = \mathbb{F}_p(X, Y)$, $K = \mathbb{F}_p(X^p, Y^p)$ und $F = K(X + cY)$.)

Aufgabe 8
Sei E/K eine beliebige Körpererweiterung mit $\mathrm{char}(K) = p > 0$. Sei $\alpha \in E$. Zeige:

$K(\alpha^p) = K(\alpha)$ gilt genau dann, wenn α algebraisch und separabel über K ist.

Technische Universität Braunschweig
Institut für Analysis und Algebra
Dr. C. Adelmann

4. Mai 2005
Blatt 3

Aufgaben zur Vorlesung „Galoisgruppen“

Aufgabe 9
Sei E/K algebraische Körpererweiterung, E_s der separable Abschluss von K in E. Zeige: Ist E/K normal, dann ist E_s/K normal.

Aufgabe 10
Sei $\omega = e^{2\pi i/9}$. Berechne das Minimalpolynom von $\omega + \omega^{-1}$ über $\mathbb{Q}$.

Aufgabe 11
Berechne ein primitives Element des Zerfällungskörpers von $X^3 - 2$ über $\mathbb{Q}$.

Aufgabe 12
Sei K ein Körper der Charakteristik $p > 0$. Schreibe $K^m = \{x^m \mid x \in K\}$.
Sei E/K rein inseparabel mit $(E : K)_i = p^r$. Zeige:
Gilt $E^{p^s} \neq K$ für alle s mit $1 \leq s < r$, dann ist E/K einfach.

Technische Universität Braunschweig
Institut für Analysis und Algebra
Dr. C. Adelmann

11. Mai 2005
Blatt 4

Aufgaben zur Vorlesung „Galoisgruppen“

Aufgabe 13
Berechne die Galois-Gruppe und die Zwischenkörper von $X^4 + X^2 - 6$ über $\mathbb{Q}$.

Aufgabe 14
Berechne die Galois-Gruppe und die Zwischenkörper von $X^4 + X^2 + X + 1$ über $\mathbb{Q}$.

Aufgabe 15
Sei $X^4 + aX^2 + b$ irreduzibel über $\mathbb{Q}$ mit Galois-Gruppe G. Zeige:

(a) Ist b ein Quadrat in $\mathbb{Q}$, so gilt $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(b) Ist b kein Quadrat in $\mathbb{Q}$, aber $b(a^2-4b)$ ein Quadrat in $\mathbb{Q}$, so gilt $G \cong \mathbb{Z}/4\mathbb{Z}$.

(c) Sind b und $b(a^2 - 4b)$ keine Quadrate in $\mathbb{Q}$, so gilt $G \cong D_8$, die Diedergruppe mit 8 Elementen.

Aufgabe 16
Sei E/K eine normale algebraische Erweiterung, $G = G(E/K)$. Zeige:

(a) E^G/K ist rein inseparabel, und E/E^G ist separabel.

(b) Sei E_s der separable Abschluss von E/K.
Dann gelten $E = E^G E_s$ und $E^G \cap E_s = K$.

Technische Universität Braunschweig
Institut für Analysis und Algebra
Dr. C. Adelmann

25. Mai 2005
Blatt 5

Aufgaben zur Vorlesung „Galoisgruppen“

Aufgabe 17
Berechne die Resultante von $f = 2X^2 + 3X + 1$ und $g = 7X^2 + X + 3$ in $\mathbb{Q}[X]$.

Aufgabe 18
Berechne die Diskriminante des Polynoms $a_3X^3 + a_2X^2 + a_1X + a_0$ über $\mathbb{Q}$.

Aufgabe 19
Die normierten separablen Polynome $f, g \in K[X]$ haben in einem algebraischen Abschluss von K die Nullstellen $\{\alpha_1, \ldots, \alpha_m\}$ bzw. $\{\beta_1, \ldots, \beta_n\}$.
Berechne mit Hilfe einer Resultante ein Polynom in $K[X]$, das als Nullstellen genau alle Produkte $\alpha_i\beta_j$ mit $1 \leq i \leq m$ und $1 \leq j \leq n$ hat.

Aufgabe 20
Seien K ein Körper, $f, g \in K[X] - K$. Zeige:
Es gibt $\varphi, \psi \in K[X]$ mit $\operatorname{grad}(\varphi) < \operatorname{grad}(g)$, $\operatorname{grad}(\psi) < \operatorname{grad}(f)$ und

$$\varphi f + \psi g = \operatorname{Res}(f, g).$$

Technische Universität Braunschweig
Institut für Analysis und Algebra
Dr. C. Adelmann

1. Juni 2005
Blatt 6

Aufgaben zur Vorlesung „Galoisgruppen“

Aufgabe 21
Berechne die Diskriminante des allgemeinen Polynoms vierten Grades

$$f(X) = a_4X^4 + a_3X^3 + a_2X^2 + a_1X + a_0.$$

Aufgabe 22
Stelle $f \in K[x_1, \ldots, x_5]^{S_5}$,

$$f = \sum_{i \neq j \neq k \neq i} x_i^2 x_j^2 x_k,$$

als Polynom in den elementarsymmetrischen Polynomen dar.

Aufgabe 23
Über dem Polynomring $K[x_1, \ldots, x_n]$ sei für $k \in \mathbb{N}_0$

$$h_k(x_1, \ldots, x_n) = \sum_{\substack{(a_1,\ldots,a_n) \in \mathbb{N}_0^n \\ a_1+\ldots+a_n=k}} x_1^{a_1} \cdot \ldots \cdot x_n^{a_n}$$

das k-te vollständige symmetrische Polynom vom Grad k. Zeige

$$\sum_{k=0}^{n} (-1)^k s_k h_{n-k} = 0.$$

Aufgabe 24
Sei K ein Körper. Zeige, dass $K[X]^*$ ein kommutativer Ring bezüglich der Verknüpfungen ist, die für $f, g \in K[X]^*$ wie folgt gegeben sind:

(a) *Addition* ist das gewöhnliche Produkt fg,
(b) *Multiplikation* ist $\mathrm{Res}_{(\mathrm{grad}(f),\mathrm{grad}(g)),Y}((-Y)^{\mathrm{grad}(f)} f(X/Y), g(Y))$, berechnet in $K[X][Y]$.

Gib das Null- und das Einselement an.

Man sagt, $K[X]^*$ hat die Struktur eines λ-Rings.

Technische Universität Braunschweig
Institut für Analysis und Algebra
Dr. C. Adelmann

8. Juni 2005
Blatt 7

Aufgaben zur Vorlesung „Galoisgruppen“

Aufgabe 25
Sei $f(X) = X^4 + a_3X^3 + a_2X^2 + a_1X + a_0$ ein normiertes Polynom vierten Grades. Berechne die Gleichung seiner kubischen Resolvente, die sich als Resolventenpolynom von $P = x_1x_2 + x_3x_4$ ergibt.

Aufgabe 26
Sei E der Zerfällungskörper von $X^3 - 2$ über $\mathbb{Q}$. Sei $a = \sqrt[3]{2}$, $b = \frac{-1+\sqrt{-3}}{2}$. Berechne für $\alpha = a+b$ die Matrix von $m_\alpha : E \to E$ zur Basis $(1, a, a^2, b, ab, a^2b)$.
$x \mapsto \alpha x$

Aufgabe 27
Sei α eine Nullstelle von $X^3 - 3X + 1$ über $\mathbb{Q}$.
Berechne das Minimalpolynom von $\alpha^3 + \alpha^2 + 2$.

Aufgabe 28
Sei K ein Körper und $G \leq \mathrm{Aut}(K)$ endliche Untergruppe.
Eine Abbildung $f : G \to K^*$ heißt *verschränkter Homomorphismus*, falls für alle $\sigma, \tau \in G$ gilt:

$$f(\sigma\tau) = \tau(f(\sigma))f(\tau).$$

Zeige: Ist f ein verschränkter Homomorphismus, dann gibt es ein $a \in K^*$ mit

$$\text{Für alle } \sigma \in G \text{ gilt } f(\sigma) = a\sigma(a)^{-1}.$$

Technische Universität Braunschweig
Institut für Analysis und Algebra
Dr. C. Adelmann

15. Juni 2005
Blatt 8

Aufgaben zur Vorlesung „Galoisgruppen“

Aufgabe 29
Sei K ein Körper, $\alpha_1, \ldots, \alpha_n \in K$. Berechne die Determinante der Vandermonde-Matrix

$$\begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{pmatrix}.$$

Aufgabe 30
Berechne in $\mathbb{Q}[X]$ eine Tschirnhaus-Transformation, die $X^4 + X^2 + X + 1$ in $X^4 + X^3 + 3X^2 + 2X + 1$ überführt.

Aufgabe 31
Sei E/K eine endliche Erweiterung endlicher Körper.
Zeige: Die Normabbildung $N_{E/K} : E^* \to K^*$ ist surjektiv.

Aufgabe 32
In einem endlichen Körper K nennt man ein erzeugendes Element der multiplikativen Gruppe K^* eine *primitive Wurzel* von K.

Bestimme für die Galois-Erweiterung $\mathbb{F}_{3^3}/\mathbb{F}_3$

(a) eine primitive Wurzel, deren Konjugierte keine Normalbasis bilden,

(b) eine Normalbasis, die nicht aus primitiven Wurzeln besteht.

Technische Universität Braunschweig
Institut für Analysis und Algebra
Dr. C. Adelmann

22. Juni 2005
Blatt 9

Aufgaben zur Vorlesung „Galoisgruppen“

Aufgabe 33
Sei K ein Körper, $f, g \in K[X]$ verschiedene normierte irreduzible Polynome vom Grad m bzw. n. Sei E/K eine Erweiterung, in der es α mit $f(\alpha) = 0$ und β mit $g(\beta) = 0$ gibt. Zeige das Reziprozitätsgesetz

$$N_{K(\alpha)/K}(g(\alpha)) \cdot N_{K(\beta)/K}(f(\beta))^{-1} = (-1)^{mn}.$$

Aufgabe 34
Sei K ein endlicher Körper mit q Elementen, sei $f \in K[X]$ irreduzibel. Zeige: f ist genau dann Teiler von $X^{q^n} - X$ in $K[X]$, wenn $\operatorname{grad}(f)$ Teiler von n ist.

Aufgabe 35

(a) Zeige für $p \neq 2$: $a \in \mathbb{F}_p^*$ ist genau dann ein Quadrat, wenn $a^{\frac{p-1}{2}} = 1$ gilt.
(b) In welchen endlichen Körpern $\mathbb{F}_q$ ist -1 ein Quadrat?

Aufgabe 36

(a) Bestimme für $f(X) = X^5 - X^4 - 6X^3 - 6X^2 - 3X + 3$ die Primfaktorzerlegungen über $\mathbb{Q}$, $\mathbb{F}_5$ und $\mathbb{F}_{13}$.
(b) Berechne die Ordnungen der zugehörigen Galois-Gruppen.

Technische Universität Braunschweig
Institut für Analysis und Algebra
Dr. C. Adelmann

29. Juni 2005
Blatt 10

Aufgaben zur Vorlesung „Galoisgruppen“

Aufgabe 37
Bestimme $W(K)$ für folgende Körper K:
$\mathbb{Q}(i), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{-5})$.

Aufgabe 38
Sei p eine Primzahl. Bestimme die $n \in \mathbb{N}$, für die $F_n(X)$ irreduzibel über $\mathbb{F}_p$ ist.

Aufgabe 39

(a) Zeige: Für Primzahlen $p \neq q$ hat $F_{pq}(X)$ nur Koeffizienten vom Betrag ≤ 1. Betrachte dazu $F_{pq}(X) = (1-X)[F_q(X^p)(1-X^q)^{-1}]$ als Identität von Potenzreihen.

(b) Zeige: $F_n(X)$ kann Koeffizienten beliebig hohen Betrags enthalten. Hinweis: Sei $n = p_1 \cdot \ldots \cdot p_r$ mit r ungerade, $p_1 < \ldots < p_r$, $p_1 + p_2 > p_r$. Berechne den Koeffizienten von X^{p_r} in $F_n(X)$.

Aufgabe 40
Sei $\zeta_n \in \mathbb{C}$ eine primitive n-te Einheitswurzel.
Für welche n bilden die Konjugierten von ζ_n eine Normalbasis von $\mathbb{Q}(\zeta_n)/\mathbb{Q}$?

Technische Universität Braunschweig
Institut für Analysis und Algebra
Dr. C. Adelmann

6. Juli 2005
Blatt 11

Aufgaben zur Vorlesung „Galoisgruppen“

Aufgabe 41
Sei K ein Körper, p eine Primzahl mit $\mathrm{char}(K) \neq p$. Sei ζ_p eine primitive p-te Einheitswurzel über K. Zeige, dass für $a \in K^*$ gilt:
Ist $a \in K(\zeta_p)^p$, so folgt $a \in K^p$.

Aufgabe 42
Sei $n \in \mathbb{N}$ nicht durch 4 teilbar.

(a) Ist $f(X) = X^n - a \in \mathbb{Q}[X]$ irreduzibel, so hat die Galois-Gruppe G_f von f die Ordnung $n\varphi(n)$ oder $n\varphi(n)/2$.

(b) Hat G_f die Ordnung $n\varphi(n)$, dann ist G_f isomorph zur multiplikativen Untergruppe von $\mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z})$ bestehend aus Matrizen der Form $\left(\begin{smallmatrix} i & j \\ 0 & 1 \end{smallmatrix}\right)$.

Aufgabe 43
Sei A eine endliche abelsche Gruppe. Zeige:
Es gibt $n \in \mathbb{N}$, so dass A isomorph zu einer Faktorgruppe von $(\mathbb{Z}/n\mathbb{Z})^*$ ist.

Aufgabe 44
Sei A eine endliche abelsche Gruppe. Zeige:
Es gibt eine Galois-Erweiterung $K/\mathbb{Q}$ mit $G(K/\mathbb{Q}) \cong A$.

Technische Universität Braunschweig
Institut für Analysis und Algebra
Dr. C. Adelmann

13. Juli 2005
Blatt 12

Aufgaben zur Vorlesung „Galoisgruppen“

Aufgabe 45
Sei K ein Körper mit $\mathrm{char}(K) = p > 0$, E/K eine Galois-Erweiterung mit $G(E/K) = <\sigma>$ zyklisch und $(E : K) = p^{m-1}$ für ein $m \geq 2$.
Sei $\beta \in E$ mit $T_{E/K}(\beta) = 1$. Zeige:

(a) Es gibt $\alpha \in E$ mit $\sigma(\alpha) - \alpha = \beta^p - \beta$.

(b) Das Polynom $X^p - X - \alpha$ ist über E irreduzibel.

(c) Ist θ eine Nullstelle von $X^p - X - \alpha$, dann ist $E(\theta)$ eine Galois-Erweiterung von K, die zyklisch vom Grad p^m über K ist.

(d) Es gilt $G(E(\theta)/K) = <\tau>$, wobei τ durch $\tau|_E = \sigma$ und $\tau(\theta) = \theta + \beta$ festgelegt ist.

Aufgabe 46
Bestimme mit der Kummer-Theorie alle Teilkörper von $\mathbb{Q}(\sqrt{-3}, \sqrt{5}, \sqrt{-7})/\mathbb{Q}$.

Aufgabe 47
Sei K ein Körper mit $\mathrm{char}(K) = 0$.
Für jedes $n \in \mathbb{N}$ und jede endliche Erweiterung E/K sei $(E^* : E^n) < \infty$.
Zeige: Für alle $n \in \mathbb{N}$ gibt es nur endlich viele Galois-Erweiterungen A/K mit $(A : K) = n$ und $G(A/K)$ abelsch.

Aufgabe 48
Sei E/K endliche Körpererweiterung und M eine multiplikative Gruppe mit $K^* \leq M \leq E^*$, so dass die Faktorgruppe M/K^* endlich ist. Zeige:

(a) Es gilt $(K(M) : K) \leq (M : K^*)$.

(b) $K(M)/K$ ist separabel $\iff$ $\mathrm{char}(K)$ ist kein Teiler von $(M : K^*)$.