Definition (21.3)

Sei R ein Ring, $n \in \mathbb{N}$ und $R[x_1, \dots, x_n]$ der Polynomring über R in n Variablen. Dann bezeichnet man für $1 \leq k \leq n$ das Polynom

$$\varepsilon_k = \sum_{1 \leq i_1 < \dots < i_k \leq n} \prod_{j=1}^k x_{i_j}$$

als k -tes elementarsymmetrisches Polynom in $R[x_1, \dots, x_n]$.

Satz (21.4)

Sei R ein beliebiger Ring, $n \in \mathbb{N}$ und $f \in R[x]$ ein normiertes Polynom n -ten Grades, $f = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$. Wir nehmen an, dass f über R in Linearfaktoren zerfällt, also

$$f = (x - \alpha_1) \cdot \dots \cdot (x - \alpha_n)$$

mit geeigneten $\alpha_1, \dots, \alpha_n \in R$ erfüllt ist. Dann gilt

$$a_k = (-1)^{n-k} \varepsilon_{n-k}(\alpha_1, \dots, \alpha_n) \text{ für } 0 \leq k < n.$$

Definition (21.5)

Sei R ein beliebiger Ring und $n \in \mathbb{N}$. Wir bezeichnen ein Polynom $f \in R[x_1, \dots, x_n]$ als **symmetrisch**, wenn $\sigma(f) = f$ für alle $\sigma \in S_n$ erfüllt ist.

Der Hauptsatz über symmetrische Polynome

Satz (21.6)

Sei K ein Körper. Ein Polynom $f \in K[x_1, \dots, x_n]$ ist genau dann symmetrisch, wenn ein Polynom $g \in K[x_1, \dots, x_n]$ mit

$$f = g(\varepsilon_1, \dots, \varepsilon_n) \quad \text{existiert.}$$

Proposition (21.8)

Sei K ein Körper. Dann sind die elementarsymmetrischen Polynome $\varepsilon_1, \dots, \varepsilon_n \in K[x_1, \dots, x_n]$ **algebraisch unabhängig**. Das bedeutet: Ist $h \in K[x_1, \dots, x_n]$ ein Polynom mit $h(\varepsilon_1, \dots, \varepsilon_n) = 0$, dann folgt $h = 0_K$.

Beweisskizze: Sei $h = \sum_{g \in \Lambda} c_g g$ eine Darstellung des Polynoms h als Summe seiner Terme. Laut Annahme gilt

$$\sum_g c_g g(\varepsilon_1, \dots, \varepsilon_n) = 0.$$

Für verschiedene $g \in \Lambda$ haben $g(\varepsilon_1, \dots, \varepsilon_n)$ verschiedene Leitterme. Daraus folgt, dass zumindest ein Term der Summe durch die anderen nicht aufgehoben werden kann.

Operation der symmetrischen Gruppe auf Polynomen

- Die symmetrische Gruppe S_n operiert auf natürliche Weise auf dem Polynomring $K[x_1, \dots, x_n]$ über einem beliebigen Grundkörper K .
- Diese Operation kann auf den Quotientenkörper $K(x_1, \dots, x_n)$ fortgesetzt werden. Auf diese Weise wird jedem $\sigma \in S_n$ ein **Automorphismus** des Körpers $K(x_1, \dots, x_n)$ zugeordnet.
- Ist nun U eine beliebige Untergruppe von S_n , dann wird

$$K(x_1, \dots, x_n)^U = \{f \in K(x_1, \dots, x_n) \mid \sigma(f) = f \text{ für alle } \sigma \in U\}$$

als **Fixkörper** von U bezeichnet.

- Die Elemente des Polynomrings $K[x_1, \dots, x_n]$, die zugleich im Fixkörper $K(x_1, \dots, x_n)^{S_n}$ liegen, sind genau die **symmetrischen Polynome**.

Definition (21.9)

Sei K ein Körper und $K[s_0, \dots, s_{n-1}]$ ein Polynomring über K , dessen n Variablen mit $s_0, \dots, s_{n-1}$ bezeichnet sind. Es sei $F = K(s_0, \dots, s_{n-1})$ der Quotientenkörper dieses Polynomrings. Dann bezeichnet man

$$f = x^n + s_{n-1}x^{n-1} + \dots + s_1x + s_0 \in F[x]$$

als **allgemeines Polynom** und die Gleichung $f = 0$ als **allgemeine Gleichung n -ten Grades** über dem Körper K .

Erinnerung Galois-Erweiterungen

Galois-Erweiterung = Körpererweiterung $L|K$, die normal und separabel ist

($L|K$ endliche normale Erweiterung $\Rightarrow \exists f \in K[x] \setminus K$, so dass L Zerf.-Körper von f über K ist)

(das $K = 0$ oder K endlich $\Rightarrow$ Jede alg. Ers. von K ist separabel.)

Ist $L|K$ eine Galois-Erweiterung, dann haben wir
 $\text{Gal}(L|K) = \text{Aut}_K(L) = \{ \sigma \in \text{Aut}(L) \mid \sigma(a) = a \forall a \in K \}$
die Galoisgruppe von $L|K$ genannt.

Satz (21.10)

Sei E ein Zerfällungskörper des allgemeinen Polynoms f über F .
Dann ist $E|F$ eine Galois-Erweiterung, mit $\text{Gal}(E|F) \cong S_n$.

Beweis von Satz 2.10:

geg. $F = K(s_0, \dots, s_{n-1})$, $f \in F[x]$ allgemeines Polynom
 E Zerfällungskörper von f über F , $\alpha_1, \dots, \alpha_n \in E$ mit
 $f = (x - \alpha_1) \cdot \dots \cdot (x - \alpha_n)$, $E = F(\alpha_1, \dots, \alpha_n)$

Beh. $E|F$ ist galois'sch, $\text{Gal}(E|F) \cong S_n$

Sei $K[x_1, \dots, x_n]$ ein weiterer Polynomring, $\tilde{E} = K(x_1, \dots, x_n)$

Quotientenkörper von $K[x_1, \dots, x_n]$, überprüfe:

Es gilt $\tilde{E}^{S_n} = K(\varepsilon_1, \dots, \varepsilon_n)$, wobei ε_k jeweils das k -te
elementarsymm. Polynom bezeichnet "offensichtlich"

"S" siehe Skript

Setze $\tilde{F} = \tilde{E}^{S_n}$ Betrachte in
 $K[x_1, \dots, x_n][x]$ das Pol $f = (x - x_1)(x - x_2) \dots (x - x_n)$

Betrachte den Auswertungshom.

$$\Phi: K[s_0, \dots, s_{n-1}] \rightarrow K[x_1, \dots, x_n]$$

geg. durch $s_k \mapsto (-1)^{n-k} \varepsilon_{n-k}$

$$\Phi(f) = x^n + \sum_{k=0}^{n-1} \Phi(s_k) x^k =$$

$$\sum_{k=0}^{n-1} (-1)^{n-k} \varepsilon_{n-k} x^k = (x-x_1)(x-x_2) \cdots (x-x_n)$$

$\Rightarrow \Phi(f) = \tilde{f}$ Bem. Das Bild von Φ

ist in $K(x_1, \dots, x_n) = \tilde{F}$ enthalten, d.h.

Φ ist ein Ringhom. $K[s_0, \dots, s_{n-1}] \rightarrow \tilde{F}$

$\varepsilon_1, \dots, \varepsilon_n$ algebraisch unabh. $\rightarrow \ker \Phi = \{0\}$

$\rightarrow \Phi$ kann fortgesetzt werden auf den Quot.korp.
 F von $K[s_0, \dots, s_{n-1}]$, erhalte also einen Körperhom.

$\Phi: F \rightarrow \tilde{K}$. Auf Grund des Hauptsatzes über elem.
symm. Fkt. ist dieser surjektiv $\rightarrow \Phi$ ist Isom von
Körpern, bezeichne die Umkehrabb. $\tilde{K} \rightarrow F$ mit $\tilde{\Phi}$.

$$\begin{array}{ccc} \tilde{E} & \xrightarrow{\quad} & E = K(x_1, \dots, x_n) \\ | & & | \\ \tilde{K} & \xrightleftharpoons[\tilde{\Phi}]{\Phi} & F = K(s_0, \dots, s_{n-1}) \end{array}$$

Aus der Galoisstheorie wird sich ergeben.
Die Erweiterung $\tilde{E} | \tilde{F}$, also die Fort-
 $\tilde{E} | \tilde{E}^{S_n}$ ist galois'sch, mit $\text{Gal}(\tilde{E} | \tilde{E}^{S_n})$
 $\cong S_n$, und es ist $[\tilde{E} : \tilde{F}] = |S_n| = n!$.

Durch diesen Erweiterungsgrad ist gewähr-
leistet, dass $\Phi : \tilde{F} \rightarrow F$ mit dem
Fortsetzungssatz aus § 16 subzessive
auf $\tilde{F}(x_1), \tilde{F}(x_1, x_2), \dots$ und schließlich
auf $\tilde{F}(x_1, \dots, x_n) = \tilde{E} \rightarrow E$ mit $x_k \mapsto \alpha_k$ erhalten einen Isom.
Daraus folgt $\text{Gal}(E | F) \subseteq \text{Gal}(\tilde{E} | \tilde{F}) = S_n$ (Details siehe Skript)

... und schließlich auf $\tilde{F}(x_1, \dots, x_n) = \tilde{E}$ fortgesetzt werden kann.

- (1) Sei $L|K$ eine endliche Galois-Erweiterung und $G = \text{Gal}(L|K)$ die zugehörige Galoisgruppe. Genau wie wir es oben mit den Untergruppen von S_n getan haben, kann man auch jeder Untergruppe $U \leq G$ einen Fixkörper

$$L^U = \{\alpha \in L \mid \sigma(\alpha) = \alpha \forall \sigma \in U\}$$

zuordnen. Es handelt sich dabei um eine Zwischenkörper von $L|K$. Der **Hauptsatz der Galoistheorie** besagt, dass durch $U \mapsto L^U$ eine **bijektive Korrespondenz** zwischen den Untergruppen von G und den Zwischenkörpern von $L|K$ besteht.

- (2) Die Untergruppenstruktur von G enthält die gesamte Information über die **Zwischenkörperstruktur** von $L|K$. Insbesondere gilt: Sind $U \subseteq V$ beides Untergruppen von G , dann ist $L^U|L^V$ eine Teilerweiterung von $L|K$. Dabei gilt $(V : U) = [L^U : L^V]$, und es gilt $U \trianglelefteq V$ genau dann, wenn $L^U|L^V$ eine normale Erweiterung ist.

- (3) Besonders interessant ist für uns der Fall, dass $U \trianglelefteq V$ gilt, $(V : U)$ gleich einer Primzahl p ist und der Körper K eine primitive p -te Einheitswurzel enthält. Dann entsteht die Erweiterung $L^U | L^V$ durch **Adjunktion einer p -ten Wurzel**. Es gibt also ein Element $\gamma \in L^U$ mit der Eigenschaft, dass $L^U = L^V(\gamma)$ und $\gamma^p \in L^V$ gilt. Ein solches Element α kann **explizit bestimmt** werden.

Aus diesen Ergebnissen werden wir ableiten, dass sich genau dann alle Elemente von L als **Wurzelausdrücke** in geeigneten Elementen des Grundkörpers K darstellen lassen, wenn die Gruppe G **auflösbar** ist.

Erinnerung: Eine endliche Gruppe G ist auflosbar,
wenn eine Kette von Untergruppen existiert der Form

$$G = U_0 \supseteq U_1 \supseteq \dots \supseteq U_r = \{e\} \quad \text{wobei}$$

$$U_{j+1} \trianglelefteq U_j \quad \text{für } 0 \leq j < r \text{ gilt und } p_j = (U_j : U_{j+1})$$

jeweils eine Primzahl ist.

Sei nun L/K eine endliche Galois-Erweiterung haben,
mit endlicher auflosbarer Galoisgruppe $G = \text{Gal}(L/K)$

Sei eine Untergruppenkette wie oben gegeben

Galustheorie $\Rightarrow$ erhalte eine Körperkette

mit endlicher auflösbarer Galoisgruppe $G = \text{Gal}(L|K)$

$$K = L^{U_0} = L^G \subsetneq L^{U_1} \subsetneq L^{U_2} \subsetneq \dots \subsetneq L^{U_r} = L^{\text{id}} = L$$

Dabei gilt jeweils $[L^{U_{j+1}} : L^{U_j}] = (U_j : U_{j+1}) = p_j$
ist eine Primzahl p_j . Setze voraus, dass K für $j=0, \dots, r-1$
jeweils eine p_j -te Einheitswurzel enthält. Dann entsteht

$L^{U_{j+1}} | L^{U_j}$ durch Adjunktion einer p_j -ten Wurzel,
d.h. jedes Element in $L^{U_{j+1}}$ kann über L^{U_j} durch diese Wurzel
dargestellt werden

Daraus folgt insgesamt, dass jedes Element aus L als
verschachtelter Wurzel Ausdruck über K dargestellt werden kann.

Anwendung auf Gleichungen dritten Grades

geg. K_0 Körper mit $\text{char}(K_0) \neq 2, 3$

$F = K_0(s_0, s_1, s_2) = \text{Quotientenkörper des Polynomrings } K_0[s_0, s_1, s_2]$

allgemeine Gleichung $x^3 + s_2x^2 + s_1x + s_0 = 0$

$E = F(x_1, x_2, x_3)$ Zerf. Körper des allg. Pol.

bekannt: S_3 ist auflösbar, mit der

Subnormalreihe $\text{id} \triangleleft A_3 \triangleleft S_3$

$\uparrow$ Index 3

$\uparrow$ Index 2

$$\text{Galoisith.} \Rightarrow E = E^{\text{idf}} \supseteq E^{A_3} \supseteq E^{S_3} = F$$

$$\text{mit } [E : E^{A_3}] = (A_3 : \text{idf}) = 3$$

$$[E^{A_3} : F] = (S_3 : A_3) = 2$$

Führe das allg. Polynom durch $x \mapsto x - \frac{1}{3}s_2$
über in ein Pol. f der Form $f = x^3 + px + q$
 $\Rightarrow \alpha_j = \delta_j + \frac{1}{3}s_2$ sind Nullst.won f in E ($1 \leq j \leq 3$)

S.o. $\Rightarrow \text{Gal}(E|F) \cong S_3 \Rightarrow$ erhalte eine
Operation von S_3 auf E geg. durch

$$\sigma(\alpha_j) = \alpha_{\sigma(j)} \text{ für } \sigma \in S_3, j \in \{1, 2, 3\}$$

Setze voraus, dass $f \in K_0$ pzm. hatte EW.

s.o. $\Rightarrow$ Die Erweiterung $E|E^{A_3}$ entsteht durch Adjunktion einer dritten Wurzel. Diese kann bestimmt werden.

Betrachte die Elemente

$$\beta_1 = \alpha_1 + \zeta\alpha_2 + \zeta^2\alpha_3, \quad \beta_2 = \alpha_1 + \zeta\alpha_3 + \zeta^2\alpha_2$$

Sei $\sigma = (123) \in A_3$

$$\begin{aligned} \Rightarrow \sigma(\beta_1) &= \sigma(\alpha_1) + \zeta\sigma(\alpha_2) + \zeta^2\sigma(\alpha_3) \\ &= \alpha_2 + \zeta\alpha_3 + \zeta^2\alpha_1 = \zeta^2\beta_1 \end{aligned}$$

$$\Rightarrow \sigma(\beta_1^3) = (\zeta^2)^3 \beta_1^3 = \beta_1^3 \quad \begin{matrix} \zeta^3=1 \\ A_3 = \langle \sigma \rangle \end{matrix}$$

β_1^3 ist im Teilkörper E^{A_3} enthalten $\Rightarrow$
 β_1 ist dritte Wurzel eines Elements aus E^{A_3}

$$\beta_1 \in E \setminus E^{A_3} \quad [E : E^{A_3}] = 3 \quad E = E^{A_3}(\beta_1)$$

überprüfe genauso: β_2 ist dritte Wurzel eines Elements aus E^{A_3} , und $E = E^{A_3}(\beta_2)$

$\exists$ primitive dritte Einheitswurzel $\Rightarrow \zeta^2 = -1 - \zeta$

Damit kann nachgerechnet werden, dass $\alpha_1, \alpha_2, \alpha_3$ durch die Elemente β_1, β_2 darstellbar sind:

$$\alpha_1 = \beta_1 + \beta_2, \quad \alpha_2 = \frac{1}{3}\zeta^2\beta_1 + \frac{1}{3}\zeta\beta_2, \quad \alpha_3 = \frac{1}{3}\zeta\beta_1 + \frac{1}{3}\zeta^2\beta_2$$

Stelle nun β_1^3, β_2^3 als Wurzelausdrücke dar.

Sei $\tau = (23)$ Berö. $\tau(\beta_1) = \beta_2, \tau(\beta_2) = \beta_1$

Sei $\tau = (23)$ Berz. $\tau(\beta_1) = \beta_2, \tau_2(\beta_2) = \beta_1$

$\Rightarrow \beta_1^3, \beta_2^3$ werden durch τ vertauscht

$\Rightarrow$ Die Menge $\{\beta_1^3, \beta_2^3\}$ ist invariant unter $\langle \sigma, \tau \rangle = S_3$

$\Rightarrow$ Die Koeff. des Polynoms $(x - \beta_1^3)(x - \beta_2^3) =$
 $x^2 - (\beta_1^3 + \beta_2^3)x + \beta_1^3 \beta_2^3$ bleiben unter S_3 fest, sind

also symmetrisch in x_1, x_2, x_3

$\Rightarrow$ Die Koeff. lassen sich durch die Koeff. p. 9 des Polynoms f darstellen.