Bereits in § 9 haben wir die Begriffe „Teilkörper“, „Erweiterungskörper“ und „Körpererweiterung“ eingeführt.

Definition (15.1)

Sei $L|K$ eine Körererweiterung. Ein Zwischenkörper von $L|K$ ein Teilkörper von L, der zugleich Erweiterungskörper von K ist.

Erzeugendensysteme von Teilkörpern

Satz (15.2)

Sei $\tilde{L}|K$ eine Körpererweiterung und $S \subseteq \tilde{L}$ eine Teilmenge. Dann gibt es einen eindeutig bestimmten Zwischenkörper L von $\tilde{L}|K$ mit den Eigenschaften

(i) $L \supseteq S$

(ii) Für jeden weiteren Zwischenkörper L' von $\tilde{L}|K$ mit $L' \supseteq S$ gilt $L' \supseteq L$.

Insgesamt ist L also der kleinste Zwischenkörper von $L|K$ mit der Eigenschaft $L \supseteq S$.

Wir bezeichnen den Körper L mit $K(S)$ und nennen ihn den von der Teilmenge S über K erzeugten Teilkörper von $\tilde{L}$.

Eigenschaften erzeugter Teilkörper

Proposition (15.3)

Sei $\tilde{L}|K$ eine Körpererweiterung, und seien S und T beliebige Teilmengen von $\tilde{L}$. Dann gilt

$$K(S \cup T) \quad = \quad K(S)(T).$$

Proposition (15.4)

Sei $\tilde{L}|K$ eine Körpererweiterung und $a \in \tilde{L}$. Dann gilt

$$K(a) \quad = \quad \left\{ \frac{f(a)}{g(a)} \;\middle|\; f, g \in K[x], g(a) \neq 0 \right\}.$$

Ziel der Körpertheorie: Studium algebraischer Gleichungen

- „Mitternachtsformel“

  Lösungen der Gleichung $x^2 + px + q = 0$

  $$x_{1,2} \quad = \quad -\tfrac{1}{2}p \pm \tfrac{1}{2}\sqrt{p^2 - 4q}$$

- Cardano / Tartaglia (1545)

  Lösungen der Gleichung $x^3 + px + q = 0$

  definiere $\alpha = \sqrt[3]{-\tfrac{1}{2}q + \sqrt{(\tfrac{1}{2}q)^2 + (\tfrac{1}{3}p)^3}}$ und $\zeta = \tfrac{1}{2} + \tfrac{1}{2}\sqrt{-3}$,

  dann sind die drei komplexen Lösungen gegeben durch

  $$x_1 = \alpha - \tfrac{1}{3}p\alpha^{-1} \quad , \quad x_2 = \zeta\alpha - \tfrac{1}{3}p\zeta^2\alpha^{-1} \quad , \quad x_3 = \zeta^2\alpha - \tfrac{1}{3}p\zeta\alpha^{-1}.$$

Lösungsformel für Gleichungen vierten Grades

- Ferrari (1545)

  Lösungen der Gleichung $x^4 + px^2 + qx + r = 0$
  Bilde die kubische Resolvente $g = x^3 - px^2 - 4rx + (4rp - q^2)$
  und berechne eine Nullstelle $\gamma \in \mathbb{C}$ mit der Cardanischen Formel. Dann sind die vier Lösungen gegeben durch

$$x_1 = -\tfrac{1}{2}\sqrt{\gamma - p} + \tfrac{1}{2}\sqrt{\gamma - p - 2\sqrt{\gamma^2 - 4r}}$$

$$x_2 = -\tfrac{1}{2}\sqrt{\gamma - p} + \tfrac{1}{2}\sqrt{\gamma - p + 2\sqrt{\gamma^2 - 4r}}$$

$$x_3 = -\tfrac{1}{2}\sqrt{\gamma - p} - \tfrac{1}{2}\sqrt{\gamma - p - 2\sqrt{\gamma^2 - 4r}}$$

$$x_4 = -\tfrac{1}{2}\sqrt{\gamma - p} - \tfrac{1}{2}\sqrt{\gamma - p + 2\sqrt{\gamma^2 - 4r}}.$$

Gleichungen höheren Grades

Durch die Arbeiten von Abel, Ruffini und Galois zu Anfang des 19. Jahrhunderts (ca. 1820-1830) ist bekannt, dass für Gleichungen fünften, sechsten und höheren Grades keine Lösungsformeln existieren können.

Exakte Lösung einer Gleichung fünften Grades

Ziel: Darstellung der komplexen Lösungen der Gleichung

$$x^5 + 15x + 12 = 0$$

durch verschachtelte Wurzelausdrücke

Vorgehensweise

- Zerfällungskörper und Ordnung der Galoisgruppe
- Galoisgruppe als Untergruppe von S_5
- Auflösbarkeit der Galoisgruppe
- Bestimmung der Lagrange-Resolventen
- Bestimmung der Lösungen

Zerfällungskörper und Ordnung der Galoisgruppe

- Durch numerische Rechnung (z.B. Newton-Iteration) sieht man, dass das Polynom $f = x^5 + 15x + 12 \in \mathbb{Q}[x]$ genau eine reelle Nullstelle $\alpha \approx -0,781$ besitzt.

- Über dem Körper $\mathbb{Q}(\alpha)$ zerfällt das Polynom f in $(x - \alpha)g$ mit $g \in \mathbb{Q}(\alpha)[x]$ gegeben durch

$$g = x^4 + \alpha x^3 + \alpha^2 x^2 + \alpha^3 x + \alpha^4 + 15.$$

- Das Polynom g besitzt eine komplexe Nullstelle $\beta \approx 1,559 + 1,413i$.

Zerfällungskörper und Ordnung der Galoisgruppe

- Über dem Körper $\mathbb{Q}(\alpha, \beta)$ zerfällt f in Linearfaktoren, neben $\alpha_1 = \alpha$ und $\alpha_2 = \beta$ mit den weiteren Nullstellen

$$\begin{aligned}\alpha_3 &= \tfrac{1}{60}(\alpha^3 + 3\alpha^2 + 6)\beta^3 + \tfrac{1}{20}(\alpha^3 + 3\alpha - 6)\beta^2 \\ &+ \tfrac{1}{20}(3\alpha^2 - 13\alpha - 18)\beta + \tfrac{1}{10}(\alpha^3 - 3\alpha^2 - 9\alpha - 3) \\ &\approx -1,169 - 1,451i \quad ,\end{aligned}$$

$$\begin{aligned}\alpha_4 = \overline{\alpha_3} &= \tfrac{1}{120}(-3\alpha^4 - 2\alpha^3 - 3\alpha^2 + 6\alpha - 24)\beta^3 \\ &+ \tfrac{1}{60}(-\alpha^4 + 3\alpha + 12)\beta^2 + \tfrac{1}{40}(\alpha^4 - 2\alpha^3 + 7\alpha^2 + 24\alpha + 8)\beta \\ &+ \tfrac{1}{10}(\alpha^3 + 4\alpha^2 - \alpha) \approx -1,169 + 1,451i \quad ,\end{aligned}$$

$$\begin{aligned}\alpha_5 = \overline{\alpha_2} &= \tfrac{1}{40}(\alpha^4 - \alpha^2 - 2\alpha + 4)\beta^3 + \tfrac{1}{60}(\alpha^4 - 3\alpha^3 - 12\alpha + 6)\beta^2 \\ &+ \tfrac{1}{40}(-\alpha^4 + 2\alpha^3 - 13\alpha^2 + 2\alpha - 12)\beta + \tfrac{1}{10}(-2\alpha - \alpha^2 + 3) \\ &\approx 1,559 - 1,413i\end{aligned}$$

Zerfällungskörper und Ordnung der Galoisgruppe

- Weil alle fünf Nullstellen von f in $\mathbb{Q}(\alpha, \beta)$ liegen, ist dies der Zerfällungskörper von f über $\mathbb{Q}$.

- Für die Ordnung der Galoisgruppe

$$G \quad = \quad \mathrm{Gal}(f|\mathbb{Q}) \quad = \quad \mathrm{Aut}(\mathbb{Q}(\alpha, \beta))$$

folgt daraus $$|G| \quad = \quad [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] \quad =$$

$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] \quad =$$

$$\mathrm{grad}(g) \cdot \mathrm{grad}(f) \quad = \quad 4 \cdot 5 \quad = \quad 20.$$

- Laut Galoistheorie ist G also isomorph zu einer Untergruppe der Ordnung 20 der symmetrischen Gruppe S_5.

- Frage: Welche Untergruppe ist das?

Galoisgruppe als Untergruppe von S_5

- Laut Körpertheorie ist jedes Element $\sigma \in \mathrm{Aut}(\mathbb{Q}(\alpha, \beta)|\mathbb{Q})$ durch die Bilder von α und β eindeutig festgelegt.
- Dabei muss $\sigma(\alpha)$ eine Nullstelle von f und $\sigma(\beta)$ eine Nullstelle von $\sigma(g) \in \mathbb{Q}(\sigma(\alpha))[x]$ sein.
- Insbesondere gibt es ein eindeutiges $\sigma \in G$ mit $\sigma(\alpha) = \beta$ und $\sigma(\beta) = \alpha_5$.
- Dieses Element erfüllt die Gleichungen $\sigma(\alpha_1) = \alpha_2$, $\sigma(\alpha_2) = \alpha_5$, $\sigma(\alpha_3) = \alpha_4$, $\sigma(\alpha_4) = \alpha_1$ und $\sigma(\alpha_5) = \alpha_3$. Es entspricht also in S_5 dem Element

$$\sigma \quad = \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 1 & 3 \end{pmatrix} \quad = \quad (1\ \ 2\ \ 5\ \ 3\ \ 4).$$

Galoisgruppe als Untergruppe von S_5

- Genau sieht man, dass es in G ein Element τ mit $\tau(\alpha_1) = \alpha_1$, $\tau(\alpha_2) = \alpha_3$, $\tau(\alpha_3) = \alpha_4$, $\tau(\alpha_4) = \alpha_5$ und $\tau(\alpha_5) = \alpha_2$ gibt. Dieses entspricht in S_5 dem Element

$$\tau \quad = \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 5 & 2 \end{pmatrix} \quad = \quad (2 \;\; 3 \;\; 4 \;\; 5).$$

- Man kann leicht nachrechnen, dass die Untergruppe $\langle \sigma, \tau \rangle$ von S_5 aus genau 20 Elementen besteht. Also ist dies bereits die gesamte Galoisgruppe.

Auflösbarkeit der Galoisgruppe

- In der Galoisgruppe $G \leq S_5$ existiert eine Kette von Untergruppen

$$\{\mathrm{id}\} = U_3 \quad \subsetneq \quad U_2 \quad \subsetneq \quad U_1 \quad \subsetneq \quad U_0 = G$$

  bestehend aus Untergruppen der Ordnungen 1, 5, 10 und 20 mit $U_1 = \langle \sigma, \tau^2 \rangle$ und $U_2 = \langle \sigma \rangle$.

- Dabei ist U_{i+1} jeweils ein Normalteiler von U_i, und die Faktorgruppe U_i/U_{i+1} ist zyklisch, von Ordnung 2, 2 bzw. 5 für $i = 0, 1, 2$. Dies zeigt, dass G eine auflösbare Gruppe ist.

- Laut Galoistheorie ist dies gleichbedeutend damit, dass die Nullstellen $\alpha_1, ..., \alpha_5$ als verschachtelte Wurzeln darstellbar sind!

Bestimmung der Lagrange-Resolventen

- Sei $L = \mathbb{Q}(\alpha, \beta)$. Laut Galoistheorie entspricht die Untergruppenkette von oben einer Zwischenkörperkette der Erweiterung $L|\mathbb{Q}$ der Form

$$L = L^{\mathrm{id}} = L^{U_3} \quad \supsetneq \quad L^{U_2} \quad \supsetneq \quad L^{U_1} \quad \supsetneq \quad L^{U_0} = L^{G} = \mathbb{Q}.$$

- Weil U_2/U_3 zyklisch von Ordnung 5 ist, können die Elemente von L laut Galoistheorie als fünfte Wurzeln von gewissen Elementen aus L^{U_2} dargestellt werden.

- Diese Elemente wiederum genügen algebraischen Gleichungen, die leichter gelöst werden können (weil die Erweiterung $L^{U_2}|\mathbb{Q}$ „einfacher“ als die Erweiterung $L|\mathbb{Q}$ ist).

Bestimmung der Lagrange-Resolventen

- konkret: Sei $\zeta = e^{2\pi i/5} = \frac{1}{4}(\sqrt{5}-1) + i\sqrt{\frac{1}{8}(\sqrt{5}+5)}$, eine sog. primitive fünfte Einheitswurzel. Dann sind die fünften Potenzen der Lagrange-Resolventen bezüglich $U_2 = \langle\sigma\rangle$ gegeben durch

$$\begin{aligned}
\rho_1 &= \alpha_1 + \zeta^1\alpha_2 + \zeta^2\alpha_5 + \zeta^3\alpha_3 + \zeta^4\alpha_4 \\
\rho_2 &= \alpha_1 + \zeta^2\alpha_2 + \zeta^4\alpha_5 + \zeta^1\alpha_3 + \zeta^3\alpha_4 \\
\rho_3 &= \alpha_1 + \zeta^3\alpha_2 + \zeta^1\alpha_5 + \zeta^4\alpha_3 + \zeta^2\alpha_4 \\
\rho_4 &= \alpha_1 + \zeta^4\alpha_2 + \zeta^3\alpha_5 + \zeta^2\alpha_3 + \zeta^1\alpha_4
\end{aligned}$$

  im Körper L^{U_2} enthalten.

Bestimmung der Lagrange-Resolventen

- Die Galoisgruppe G permutiert die Lagrange-Resolventen $\rho_1, \rho_2, \rho_3, \rho_4$. Daraus folgt, dass das Polynom

$$h \quad = \quad (x - \rho_1^5)(x - \rho_2^5)(x - \rho_3^5)(x - \rho_4^5)$$

  in $\mathbb{Q}[x]$ liegt.

- Weil wir die Nullstellen $\alpha_1, ..., \alpha_5$ numerisch bestimmt haben, können wir auch $\rho_1, ..., \rho_4$ und damit das Polynom $h \in \mathbb{Q}[x]$ numerisch berechnen. Heraus kommt

$$h \quad = \quad (x^2 - 11250x - 759375)(x^2 + 3750x + 759375).$$

- Durch eine algebraische Rechnung lässt sich überprüfen, dass diese Gleichung auch exakt gilt.

Bestimmung der Lösungen

- Die Nullstellen des Polynoms h lassen sich durch die „Mitternachtsformel“ exakt bestimmen. Es sind

$$\gamma_{1,2} = 5625 \pm \sqrt{23400000} \text{ und } \gamma_{3,4} = -1875 \pm \sqrt{2756250}.$$

- Durch numerische Rechnung ordnet man die Zahlen $\rho_1^5, \rho_2^5, \rho_3^5, \rho_4^5$ den Werten $\gamma_1, \gamma_2, \gamma_3, \gamma_4$ zu. Weil $\gamma_1, ..., \gamma_4$ reelle Zahlen sind, kann man auch leicht feststellen, welche fünfte Wurzel aus diesen Zahlen jeweils dem zugehörigen ρ_j entspricht. Auf diese Weise erhält man

$$\rho_1 = \sqrt[5]{5625 + \sqrt{23400000}} \quad , \quad \rho_2 = \zeta^2 \sqrt[5]{-1875 - \sqrt{2756250}} \quad ,$$

$$\rho_3 = \zeta^2 \sqrt[5]{-1875 + \sqrt{2756250}} \quad , \quad \rho_4 = \zeta^2 \sqrt[5]{5625 - \sqrt{23400000}}$$

Bestimmung der Lösungen

- Das Gleichungssystem zwischen $\alpha_1, ..., \alpha_5$ und $\rho_1, ..., \rho_4$ kann zu den α_j hin aufgelöst werden. Es gilt

$$\begin{aligned}
\alpha_1 &= \tfrac{1}{5}(\rho_1 + \rho_2 + \rho_3 + \rho_4) \\
\alpha_2 &= \tfrac{1}{5}(\zeta^4\rho_1 + \zeta^3\rho_2 + \zeta^2\rho_3 + \zeta^1\rho_4) \\
\alpha_3 &= \tfrac{1}{5}(\zeta^3\rho_1 + \zeta^1\rho_2 + \zeta^4\rho_3 + \zeta^2\rho_4) \\
\alpha_4 &= \tfrac{1}{5}(\zeta^2\rho_1 + \zeta^4\rho_2 + \zeta^1\rho_3 + \zeta^3\rho_4) \\
\alpha_5 &= \tfrac{1}{5}(\zeta^1\rho_1 + \zeta^2\rho_2 + \zeta^3\rho_3 + \zeta^4\rho_4)
\end{aligned}$$

- Setzen wir die oben gefundenen Darstellungen von $\rho_1, ..., \rho_4$ ein, so haben wir eine Darstellung der Nullstellen von f als verschachtelte Wurzeln gefunden!

Der Grad einer Körpererweiterung

Definition (15.5)

Ist $L|K$ eine Körpererweiterung, dann definieren die beiden Abbildungen

$$+ : L \times L \to L\,,\ (\alpha, \beta) \mapsto \alpha + \beta \quad \text{und} \quad \cdot : K \times L \to L\,,\ (a, \alpha) \mapsto a\alpha$$

eine K-Vektorraumstruktur auf L. Dabei bezeichnet man $[L : K] = \dim_K L$ als den Grad der Körpererweiterung. Ist $[L : K]$ endlich, dann nennt man $L|K$ eine endliche Körpererweiterung.

Beispiel: $[\mathbb{C} : \mathbb{R}] = 2$

Die Gradformel

Satz (15.6)

Seien $L|K$ und $M|L$ endliche Körpererweiterungen. Dann ist auch die Körpererweiterung $M|K$ endlich, und es gilt

$$[M : K] \quad = \quad [M : L] \cdot [L : K].$$

Ergänzungen:

- Ist $M|K$ eine endliche Erweiterung, dann sind auch $M|L$ und $L|K$ endlich.
- Für jede Körpererweiterung $L|K$ gilt offenbar $[L : K] = 1$ genau dann, wenn $L = K$ ist.
- Anwendung:
  Die Erweiterung $\mathbb{C}|\mathbb{R}$ besitzt keine echten Zwischenkörper.

Beweis von Satz 15.6

geg.: endliche Erweiterungen $L|K$, $M|L$

Sei $m = [L:K]$, $n = [M:L]$

z.Zg.: $mn = [M:K]$, d.h. M ist ein mn-dimensionaler K-Vektorraum

$m = [L:K] \rightarrow \exists$ m-elem. Basis $\{\alpha_1, \dots, \alpha_m\}$ von L als K-Vektorraum

$n = [M:L] \Rightarrow \exists$ n-elem. Basis $\{\beta_1, \dots, \beta_n\}$ von M als L-Vektorraum

Sei $B = \{\alpha_i \beta_j \mid 1 \leq i \leq m, 1 \leq j \leq n\}$ Beh.:

B ist eine mn-elementige Basis von M als K-Vektorraum

Zu überprüfen: (i) B ist Erz.-system von M als K-Vektorraum

(ii) B ist linear unabh. und $|B| = mn$

M | n | L | m | K

zu (i) Sei $\gamma \in M$ z.zg.: γ ist Linearkomb. von B

$\{\beta_1, \dots, \beta_n\}$ ist Erz.-system von M als L-Vektorraum

$\Rightarrow \exists b_1, \dots, b_n \in L$ mit $\gamma = \sum_{j=1}^{n} b_j \beta_j$

$\{\alpha_1, \dots, \alpha_m\}$ ist Erz.-system von L als K-Vektorraum

$\Rightarrow \exists a_{ij} \in K$ $(1 \le i \le m, 1 \le j \le n)$ mit $b_j = \sum_{i=1}^{m} a_{ij} \alpha_i$ für $1 \le j \le n$ einsetzen $\Rightarrow$ $\gamma = \sum_{j=1}^{n} \left(\sum_{i=1}^{m} a_{ij} \alpha_i \right) \beta_j = \sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij} \alpha_i \beta_j$

zu (ii) Seien $a_{ij} \in K$ $(1 \le i \le m, 1 \le j \le n)$ mit

$\sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij} \alpha_i \beta_j = 0$. z.zg.: $a_{ij} = 0 \ \forall i, j$ Vor. $\rightarrow$

$\sum_{j=1}^{n} \left(\sum_{i=1}^{m} a_{ij} \alpha_i \right) \beta_j = 0$ $\xrightarrow[\text{lin. unabh. im } L\text{-Vektorraum } M]{\beta_1, \dots, \beta_n}$ $\sum_{i=1}^{m} a_{ij} \alpha_i = 0$ für $1 \le j \le n$

$\xrightarrow[\text{lin. unabh. im } K\text{-Vektorraum } L]{\alpha_1, \dots, \alpha_m}$ $a_{ij} = 0$ für $1 \le i \le m$, $1 \le j \le n$. $\square$

Algebraische und transzendente Elemente

Definition (15.7)

Sei $L|K$ eine Körpererweiterung. Ein Element $\alpha \in L$ heißt algebraisch über K, wenn ein Polynom $f \neq 0$ in $K[x]$ mit der Eigenschaft existiert, dass α eine Nullstelle von f ist. Gibt es ein solches Polynom nicht, dann nennt man α transzendent über K.

Beispiele zum Begriff des algebraischen Elements:

$L|K$ Körpererweiterung (z.B. $K = \mathbb{Q}$, $L = \mathbb{C}$)

$\alpha \in L$ <u>algebraisch über K</u> $\Leftrightarrow$ $\exists\, f \in K[x] \setminus \{0\}$ mit der Eig. $f(\alpha) = 0$

(i) $\alpha = \sqrt{2}$ ist algebraisch über $\mathbb{Q}$, da $\sqrt{2}$ Nullstelle von $x^2 - 2 \in \mathbb{Q}[x]$ ist

$\zeta = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$ ist alg. über $\mathbb{Q}$, da Nullstelle von $x^2 + x + 1 \in \mathbb{Q}[x]$

(ii) Jedes $a \in K$ ist algebraisch über K, da a Nullstelle von $x - a \in K[x]$.

(iii) Es gibt überabzählbar viele reelle bzw. komplexe Zahlen die transzendent über $\mathbb{Q}$ sind. (Man spricht dann auch von transzendenten Zahlen.)

Transzendenz von e: 1873 von C. Hermite
Transzendenz von π: 1882 von F. Lindemann
(Irrationalität von e: 1572 von L. Euler)

Das Minimalpolynom eines algebraischen Elements

Definition (15.8)

Sei $L|K$ eine Körpererweiterung, und sei $\alpha \in L$ algebraisch über K. Dann gibt es ein eindeutig bestimmtes, normiertes Polynom $f \in K[x]$, $f \neq 0$ minimalen Grades mit $f(\alpha) = 0$. Man nennt f das Minimalpolynom von α über K. Wir bezeichnen es mit $\mu_{\alpha,K}$.

Beispiel: $\mu_{\sqrt{2},\mathbb{Q}} = x^2 - 2$

zu Existenz und Eindeutigkeit von $M_{\alpha,K}$

(wobei $L|K$ Körpererw., $\alpha \in L$ alg. über K)

Existenz: klar: Da α algebraisch über K ist, existiert ein normiertes Polynom $\tilde{f} \in K[x]$ mit $\tilde{f}(\alpha) = 0$ (denn: Zu $f \in K[x] \setminus K$ mit $f(\alpha) = 0$ und $c \in K^*$ der Leitkoeff. von f, dann setze $\tilde{f} = c^{-1} f$.) Aus allen normierten Polynomen mit Nullstelle α kann eines mit minimalem Grad gewählt werden.

Eindeutigkeit: Ang., f, g sind beides normier-

zu (ii)

te Polynome von minimalem Grad mit $f(\alpha) = g(\alpha) = 0$. Sei $h = g - f$ und $\tilde{h}$ die Normierung von h. $\rightarrow h(\alpha) = g(\alpha) - f(\alpha) = 0 - 0 = 0$ und somit auch $\tilde{h}(\alpha) = 0$. außerdem f, g beide normiert, $\operatorname{grad}(f) = \operatorname{grad}(g) \Rightarrow \operatorname{grad}(\tilde{h}) = \operatorname{grad}(0) < \operatorname{grad}(f)$ $\lightning$ zur Minimalität von $\operatorname{grad}(f)$. $\square$

Eigenschaften des Minimalpolynoms

Proposition (15.9)

Sei $L|K$ eine Körpererweiterung, $\alpha \in L$ algebraisch über K und $f \in K[x]$ sein Minimalpolynom, also $f = \mu_{\alpha,K}$. Dann gilt

(i) Das Polynom f ist irreduzibel.

(ii) Ist $g \in K[x]$ mit $g(\alpha) = 0$, dann folgt $f \mid g$.

(iii) Ist $g \in K[x]$ ebenfalls normiert, irreduzibel, mit $g(\alpha) = 0_K$, dann folgt $f = g$.

Beweis von Prop. 15.9:

geg: Körpererweiterung $L|K$, $\alpha \in L$ algebraisch über K. $f = M_{\alpha,K}$ (Minimalpol.)

zu (i) Ang f ist reduzibel in $K[x]$. $\Rightarrow \exists g, h \in K[x]$ mit $1 \leq \operatorname{grad}(g), \operatorname{grad}(h) < \operatorname{grad}(f)$ und $f = gh$

$\Rightarrow g(\alpha) h(\alpha) = f(\alpha) = 0 \Rightarrow g(\alpha) = 0$ oder $h(\alpha) = 0$

Seien $\tilde{g}, \tilde{h}$ die Normierungen von g bzw. h. $\Rightarrow$ $\tilde{g}(\alpha) = 0$ oder $\tilde{h}(\alpha) = 0$. $\lightning$ zur Minimalität von $\operatorname{grad}(f)$

zu (ii) geg: $g \in K[x]$ mit $g(\alpha) = 0$ zzg: $f \mid g$

Division mit Rest $\Rightarrow \exists q, r \in K[x]$ mit

$g = qf + r$ und $r = 0$ oder $\operatorname{grad}(r) < \operatorname{grad}(f)$

Ang. $r \neq 0$ $\quad r = g - qf \Rightarrow r(x) = g(x) - q(x) f(x)$

$= 0 - q(x) \cdot 0 = 0$ Sei $\tilde{r}$ die Normierung von r.

$\Rightarrow \tilde{r}(x) = 0$, $\operatorname{grad}(\tilde{r}) = \operatorname{grad}(r) < \operatorname{grad}(f)$ ↯ zur Minimalität

zu iii) geg.: $g \in K[x]$ normiert, irreduzibel, $g(x) = 0$

Beh.: $g = f$ $\quad$ ii) $\overset{g(x)=0}{\Rightarrow}$ $f \mid g$ $\overset{g \text{ irred.}}{\Rightarrow}$

$f \in K^\times$ oder $f \sim g$ (assoziiert) $\overset{f(x)=0}{\Rightarrow}$ $f \sim g$

f, g normiert $\Rightarrow$ $f = g$ $\square$

Die Struktur einfacher algebraischer Erweiterungen

Satz (15.10)

Sei $L|K$ eine Körpererweiterung, $\alpha \in L$ algebraisch über K, $f = \mu_{\alpha,K}$ und $n = \mathrm{grad}(f)$. Dann bilden die Elemente

$$1, \alpha, \alpha^2, ..., \alpha^{n-1}$$

eine Basis von $K(\alpha)$ als K-Vektorraum. Insbesondere gilt $[K(\alpha) : K] = n$.

Beweis von Satz 15.10:

gegeben $L \mid K$ Körpererw., $\alpha \in L$ alg. über K, $f = \mu_{\alpha,K}$ und $n = \operatorname{grad}(f)$

z.zg: $B = \{1, \alpha, \ldots, \alpha^{n-1}\}$ ist eine n-elementige Basis von $K(\alpha)$ als K-Vektorraum

wichtigster Schritt: Die Menge der Linearkombinationen von B, also $U = \{a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} \mid a_0, \ldots, a_{n-1} \in K\}$
$= \{g(\alpha) \mid g \in K[x], g = 0 \text{ oder } \operatorname{grad}(g) < n\}$ ist ein Teilkörper von L

zu überprüfen: (0) $1_L \in U$ (1) $\alpha, \beta \in U \Rightarrow \alpha + \beta, \alpha\beta \in U$

(2) $\alpha \in U$, $\alpha \neq 0_L \Rightarrow \alpha^{-1} \in U$

zu (0) klar, da $1_L = 1_K \in K[x]$, $\operatorname{grad}(1_K) = 0 < n$ und $1_K(\alpha) = 1_K$

zu (1) Seien $\beta, \gamma \in U \Rightarrow \exists g, h \in K[x]$ mit $g = 0$ oder $\operatorname{grad}(g) < n$, gleiche Bed. für h, und $\beta = g(\alpha)$, $\gamma = h(\alpha)$

$\Rightarrow g + h = 0$ oder $\operatorname{grad}(g+h) < n \Rightarrow \beta + \gamma = g(\alpha) + h(\alpha)$

$= (g+h)(\alpha) \in U$

Division mit Rest $\Rightarrow \exists q, r \in K[x]$ mit $gh = qf + r$ und $r = 0$ oder $\operatorname{grad}(r) < n \Rightarrow r(\alpha) \in U$

außerdem: $r = gh - qf \Rightarrow r(\alpha) = g(\alpha)\,h(\alpha) - q(\alpha)\cdot f(\alpha)$

$= g(\alpha)\cdot h(\alpha) - q(\alpha)\cdot 0 = g(\alpha)\cdot h(\alpha) = \beta \cdot \gamma \Rightarrow \beta\gamma \in U$