Definition der n-ten Wurzeln

Definition (22.5)

Sei K ein Körper, $a \in K$ und $n \in \mathbb{N}$. Ein Element $\alpha \in K$ wird eine n-te Wurzel von a genannt, falls $\alpha^n = a$ gilt. Im Fall $n = 2$ spricht man von Quadrat-, im Fall $n = 3$ von Kubikwurzeln.

Ein Element α ist also genau dann n-te Wurzel von a, wenn es die Gleichung $x^n - a = 0$ löst. Eine solche Gleichung wird als reine Gleichung bezeichnet.

Die Galoisgruppe der reinen Gleichung

Satz (22.6)

Sei $n \in \mathbb{N}$ mit $n \geq 2$ und K ein Körper mit $\mathrm{char}(K) \nmid n$, was $\mathrm{char}(K) = 0$ einschließt. Wir setzen voraus, dass K eine primitive n-te Einheitswurzel ζ enthält. Weiter sei $a \in K^\times$, L ein Erweiterungskörper von K und $\alpha \in L$ eine n-te Wurzel von a.

(i) Die Erweiterung $K(\alpha)|K$ ist eine Galois-Erweiterung.

(ii) Sei G die Galoisgruppe von $K(\alpha)|K$. Dann gibt es einen Teiler d von n mit der Eigenschaft, dass G isomorph zu $\mathbb{Z}/d\mathbb{Z}$ ist.

(iii) Es gilt $G \cong \mathbb{Z}/n\mathbb{Z}$ genau dann, wenn das Polynom $f = x^n - a$ in $K[x]$ irreduzibel ist.

Beweis von Satz 22.6

$n \in \mathbb{N}$, $n \geq 2$, K Körper mit $\mathrm{char}(K) \nmid n$

$a \in K^*$, $f = x^n - a$, $L | K$ Erw., α n-te Wurzel von a

ζ primitive n-te EW in K (d.h. $\mathrm{ord}(\zeta) = n$ in K^*)

zu (i) z.Zg. $K(\alpha) | K$ ist galoissch

$\alpha^n = a \Rightarrow f(\alpha) = 0$ $\quad \mathrm{ord}(\zeta) = n \Rightarrow 1, \zeta, \ldots \zeta^{n-1}$

sind paarw. verschiedene Elemente $a \neq 0$, $x^n = a$

$\Rightarrow \alpha \neq 0 \Rightarrow \zeta^k \alpha$, $0 \leq k < n$ sind n verschiedene

Elemente außerdem: $f(\zeta^k \alpha) = (\zeta^k \alpha)^n - a =$

$(\zeta^n)^k x^n - a = 1^k \cdot a - a = 0 \Rightarrow f$ zerfällt über $K(x)$ in linearfaktoren Außerdem wird $K(x)$ über K von $\{\zeta^k x \mid 0 \le k \le n\}$ erzeugt (da bereits $\{x\}$ Erz.-system) $\Rightarrow K(x)$ ist Zerf.-körp von f über $K \Rightarrow K(x)|K$ ist normal

$f' = n x^{n-1} \neq 0$ da $\mathrm{char}(K) \nmid n$, $x \neq 0$ (wegen $a \neq 0$)
$\Rightarrow ggT(f, f') = 1 \rightarrow f$ hat keine mehrfachen Nullst. in einer Erw von $K \Rightarrow$ Die irred. Faktoren von f sind separabel $\Rightarrow \alpha$ ist separabel über $K \rightarrow K(x)|K$ ist separable Erw.

zu (ii) zeige: $G = Gal(K(x)|K)$ ist isomorph zu einer Untergruppe von $\mathbb{Z}/n\mathbb{Z}$ (Daraus folgt, dass G zyklisch und $d = |G|$ Teiler von n, da Untergr. zyklischer Gruppen zyklisch sind, und auf Grund des Satzes von Lagrange.)

Sei $\sigma \in G$. Da α Nullst. von f ist, muss dasselbe für $\sigma(\alpha)$ gelten, d.h. es gibt ein $j \in \{0, 1, \ldots, n-1\}$ mit $\sigma(\alpha) = \alpha_j$, wobei $\alpha_j = f^j \alpha$ für $0 \leq j \leq n-1$. Dieses Element α_j (und somit auch j) legt σ eindeutig fest (weil α die Erw. $K(\alpha)|K$ erzeugt).

Notation: Für $0 \leq j < n$ sei $\sigma_j \in G$ das eindeutig bestimmte Element mit $\sigma_j(\alpha) = \alpha_j$, sofern es existiert.

Definiere $\phi : G \to \mathbb{Z}/n\mathbb{Z}$ durch $\phi(\sigma_j)$

$= j + n\mathbb{Z}$ für $j \in \{0, 1, \ldots, n-1\}$, sofern σ_j tatsächlich existiert. Da jedes $\sigma \in G$ durch die Zahl j eindeutig festgelegt ist, ist ϕ injektiv. Beh: ϕ ist ein Gruppenhomomorphismus. ($\Rightarrow G$ ist isomorph zu Untergruppe $U = \phi(G)$ von $(\mathbb{Z}/n\mathbb{Z}, +)$)

Seien $\sigma, \tau \in G$. z.Zg: $\phi(\sigma \circ \tau) = \phi(\sigma) + \phi(\tau)$

s.o. $\Rightarrow \exists j, k \in \{0, \ldots, n-1\}$ mit $\sigma = \sigma_j$ und $\tau = \tau_k$. Sei $l \in \{0, \ldots, n-1\}$ das eindeutig bestimmte Element mit $l \equiv j + k \bmod n$. Es genügt z.Zg., dass σ_l in G existiert und $\sigma_j \circ \sigma_k = \sigma_l$ gilt, denn dann folgt

$\phi(\sigma_j \circ \sigma_k) = \phi(\sigma_l) = l + n\mathbb{Z} = (j + n\mathbb{Z}) +$

$(k + n\mathbb{Z}) = \phi(\sigma_j) + \phi(\sigma_k) = \phi(\beta) + \phi(\tau)$

Tatsächlich gilt $(\sigma_j \circ \sigma_k)(\alpha) = \sigma_j(\sigma_k(\alpha)) =$

$\sigma_j(\beta^k \alpha) = \sigma_j(\beta)^k \sigma_j(\alpha) = \beta^k \sigma_j(\alpha) = \beta^k \cdot \beta^j \alpha$

$= \beta^{j+k} \alpha = \beta^l \alpha$ Es gibt also ein $\rho \in G$ mit

$\rho(\alpha) = \beta^l \alpha$, nämlich $\sigma_j \circ \sigma_k$, und aus $(\sigma_j \circ \sigma_k)(\alpha)$

$= \sigma_l(\alpha)$ folgt $\sigma_j \circ \sigma_k = \sigma_l$.

$\beta^k = \beta^j$ $\quad l \equiv j + k$ $\quad \operatorname{ord}(\beta) = n$

zu (iii) z.Zg.: $|G| = n \iff f$ irred. über K

Sei $\beta = \mu_{\alpha, K}$. $f(\alpha) = 0 \longrightarrow \beta \mid f$

$\Longrightarrow$ $[K(\alpha) : K] = |G| = n = \operatorname{grad}(f)$

$g = \mu_{\alpha,K} \Rightarrow \operatorname{grad}(g) = [K(\alpha):K] = \operatorname{grad}(f)$

$g \mid f \Longrightarrow g = f \overset{g \text{ irred.}}{\Longrightarrow} f$ irred.

beide normiert

„$\Longleftarrow$" $g \mid f$, f irred. $\Rightarrow g = f \Rightarrow |G| = [K(\alpha):K]$

$= \operatorname{grad}(g) = \operatorname{grad}(f) = n$

Da G isomorph zu einer Untergr. von $\mathbb{Z}/n\mathbb{Z}$, ist $|G| = n$ äquivalent zu $G \cong \mathbb{Z}/n\mathbb{Z}$. □

Das Dedekindsche Lemma

Satz (22.7)

Sei H eine Halbgruppe und K ein Körper. Dann ist jede endliche Menge von Halbgruppen-Homomorphismen $H \to K^\times$ im K-Vektorraum $\mathrm{Abb}(H, K)$ der Abbildungen $H \to K$ linear unabhängig.

Beweis von Satz 22.7

geg.: Halbgruppe H, Körper K

zeige für alle $n \in \mathbb{N}$: Je n Halbgruppen-Hom. $H \to K^*$ sind im K-Vektorraum $\mathrm{Abb}(H, K)$ linear unabh.

Ind-Anf. Sei $\lambda_1 \in K$ und $\tau : H \to K^*$ ein Halbgruppen-Hom. mit $\lambda_1 \tau = 0_{\mathrm{Abb}(H,K)}$ Sei $h \in H$ bel. gew. $\Rightarrow \lambda_1 \tau(h) = 0_K$

$\tau(h) \in K^*$ $\Longrightarrow \lambda_1 = 0$

Ind-Schritt. Seien $\tau_1, \dots, \tau_{n+1} : H \to K^*$ verschiedene Halbgruppen-Hom. und $\lambda_1, \dots, \lambda_{n+1} \in K$ mit $\sum_{j=1}^{n+1} \lambda_j \tau_j \overset{(*)}{=} 0_{\mathrm{Abb}(H,K)}$ z.zg.: $\lambda_j = 0_K$ für $1 \le j \le n+1$

Ind-V. $\Rightarrow \tau_1, \dots, \tau_n$ sind linear unabh.

ebenso $\tau_2, \dots, \tau_{n+1}$

$\tau_1 \neq \tau_{n+1} \Rightarrow \tau_1(a) \neq \tau_{n+1}(a)$ für ein $a \in H$

Beh.: $\sum_{k=2}^{n+1} \lambda_k (\tau_k(a) - \tau_1(a))\, \tau_k = 0$ Sei $G \in H$

$$\sum_{k=2}^{n+1} \lambda_k (\tau_k(a) - \tau_1(a)) \tau_k(G) = \sum_{k=1}^{n+1} \lambda_k (\tau_k(a) - \tau_1(a))\, \tau_k(G)$$

$$= \sum_{k=1}^{n+1} \lambda_k \tau_k(a) \tau_k(G) - \sum_{k=1}^{n} \lambda_k \tau_1(a)\, \tau_k(G) =$$

$$\sum_{k=1}^{n+1} \lambda_k \tau_k(aG) - \tau_1(a) \sum_{k=1}^{n} \lambda_k \tau_k(G) = 0 - \tau_1(a) \cdot 0 = 0$$

($\Rightarrow$ Beh.) $\tau_2, \dots \tau_{n+1}$ lin. unabh. $\Rightarrow \lambda_k (\tau_k(a) - \tau_1(a)) = 0$

für $2 \leq k \leq n+1$ $\overset{\tau_1(a) \neq \tau_{n+1}(a)}{\Longrightarrow}$ $\lambda_{n+1} = 0$ $\overset{(*)}{\Rightarrow}$ $\sum_{k=1}^{n} \lambda_k \tau_k = 0$ $_{\text{Ang}(H,K)}$

$\tau_1, \dots \tau_n$ linear unabh. $\Longrightarrow$ $\lambda_1 = \dots = \lambda_n = 0$ $\square$

Definition der Lagrangeschen Resolventen

Definition (22.8)

Sei $L|K$ eine endliche Galois-Erweiterung mit einer zyklischen Galoisgruppe G der Ordnung n, wobei K ein primtive n-te Einheitswurzel ζ enthält. Sei $\sigma \in G$ ein Element mit $G = \langle \sigma \rangle$. Dann nennt man für beliebiges $\alpha \in L$ das Element

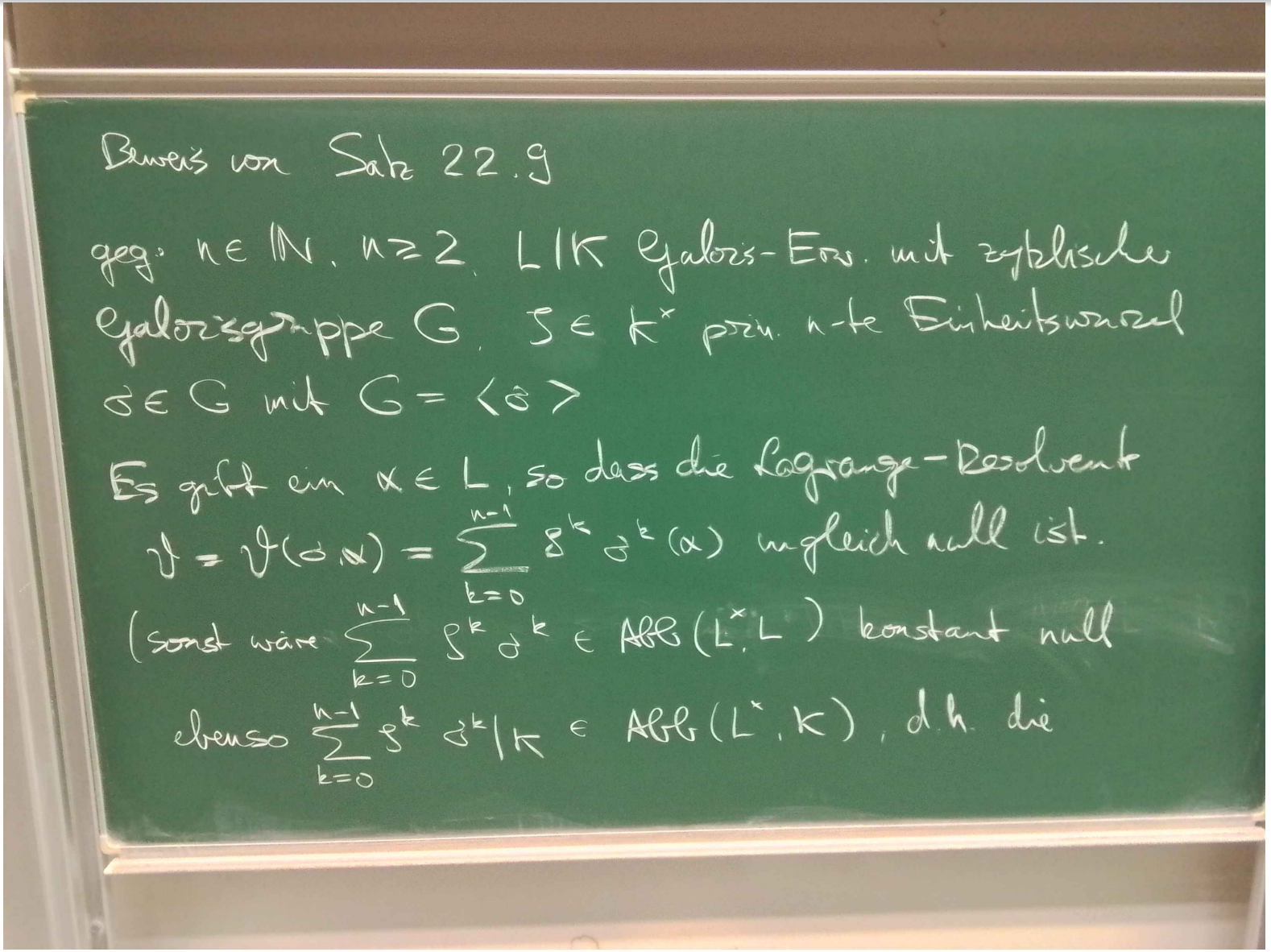
$$\vartheta(\sigma, \alpha) \quad = \quad \alpha + \zeta\sigma(\alpha) + \zeta^2\sigma^2(\alpha) + ... + \zeta^{n-1}\sigma^{n-1}(\alpha)$$

die Lagrangesche Resolvente von α bezüglich σ.

Zyklische Galois-Erweiterungen und Wurzeln

Satz (22.9)

Sei $n \in \mathbb{N}$, K ein Körper, der eine primitive n-te Einheitswurzel ζ enthält, und $L|K$ eine Galois-Erweiterung vom Grad n mit zyklischer Galoisgruppe G. Dann gibt es ein Element $\vartheta \in L$ mit $L = K(\vartheta)$ und $\vartheta^n \in K$.



Korrektur: Die Abbildungen σ^k müssen auf $K^\times$ (statt K) eingeschränkt werden, und man erhält dann Elemente aus $\mathrm{Abb}(K^\times, K)$ (statt aus $\mathrm{Abb}(L^\times, K)$).

Elemente σ^k / k $(0 \leq k \leq n-1)$ waren linear abhängig,
im Widerspruch zum Dedekindschen Lemma)

Zeige: $L = K(\vartheta)$ und $\vartheta^n \in K$

$$\sigma(\vartheta) = \sum_{k=0}^{n-1} \sigma(\rho^k \sigma^k(\alpha)) = \sum_{k=0}^{n-1} \sigma(\rho^k)\, \sigma(\sigma^k(\alpha)) = \quad \rho^k \in K$$

$$= \sum_{k=0}^{n-1} \rho^k \sigma^{k+1}(\alpha) = \rho^{-1} \sum_{k=0}^{n-1} \rho^{k+1} \sigma^{k+1}(\alpha) = \rho^{-1} \sum_{k=1}^{n} \rho^k \sigma^k(\alpha)$$

$$= \rho^{-1} \sum_{k=0}^{n-1} \rho^k \sigma^k(\alpha) = \rho^{-1} \cdot \vartheta \Rightarrow \sigma(\vartheta^n) = \sigma(\vartheta)^n =$$

$\rho^0 = \rho^n$, $\sigma^0 = \sigma^n$, $k=0$

$$(\rho^{-1}\vartheta)^n = (\rho^n)^{-1} \vartheta^n = 1^{-1} \vartheta^n = \vartheta^n \Rightarrow \vartheta^n \text{ liegt im}$$

Fixkörper von $G = \langle \sigma \rangle$ Galoistheorie

$\Rightarrow L^G = K \rightarrow \vartheta^n \in K$

Das Element ϑ ist also Nullstelle des Polynoms $f = x^n - a \in K[x]$ mit $a = \vartheta^n$. Sei $g = Mi.K$ $f(\vartheta) = 0 \rightarrow g \mid f$ $g(\vartheta) = 0$.

σ^k $(0 \leq k \leq n-1)$ bildet die Nullstelle ϑ von g auf eine weitere Nullstelle von g ab $\rightarrow$ $\sigma^{-k} f = \sigma^k(\vartheta)$ sind n verschiedene Nullstellen von g $\rightarrow$ $\operatorname{grad}(g) = n \Rightarrow [K(\vartheta) : K] = \operatorname{grad}(g) = n = [L : K]$

Gradformel $\Rightarrow$ $n = [L:k] = [L:k(\vartheta)] \cdot [k(\vartheta):k]$

$= [L:k(\vartheta)] \cdot n \Rightarrow [L:k(\vartheta)] = 1 \Rightarrow L = k(\vartheta)$

□

Das Kompositum von Körpern

Proposition (23.1)

Ist $\tilde{K}$ ein Körper mit Teilkörpern L und M, dann gilt

$$L(M) \quad = \quad M(L).$$

Man bezeichnet $L \cdot M = L(M) = M(L)$ als das Kompositum der Körper L und M in $\tilde{K}$. Es handelt sich dabei um den kleinsten Teilkörper von $\tilde{K}$, der $L \cup M$ enthält.

Der Verschiebungssatz der Galoistheorie

Satz (23.2)

Sei $L|K$ eine endliche Galois-Erweiterung und $M|K$ eine weitere Körpererweiterung mit der Eigenschaft, dass L und M in einem gemeinsamen Erweiterungskörper $\tilde{K}$ enthalten sind. Dann sind auch $L \cdot M|M$ und $L|L \cap M$ Galois-Erweiterungen, und es gibt einen Isomorphismus

$$\phi : \mathrm{Gal}(L \cdot M|M) \longrightarrow \mathrm{Gal}(L|L \cap M)$$

von Gruppen mit $\phi(\tau) = \tau|_L$ für alle $\tau \in \mathrm{Gal}(L \cdot M|M)$.

Beweis von Satz 23.2

$L|K$ endl. Galois-Erw., $M|K$ bel. Erw.

$\tilde{K} \supseteq L \cup M$ gem. Erweiterungskörper

klar: Mit $L|K$ ist auch $L|L \cap M$ eine Galois-Erweiterung

zeige: $L \cdot M | M$ ist galoissch

Satz vom prim. Element $\Rightarrow \exists \alpha \in L$ mit $L = K(\alpha)$ Beh.: $L \cdot M = M(\alpha)$

„$\supseteq$" offensichtlich, da $M \cup \{\alpha\} \subseteq L \cup M \subseteq L \cdot M$

„$\subseteq$" klar: $M \subseteq M(\alpha)$, außerdem: $\alpha \in M(\alpha)$

$[K(\vartheta):K]$

$= K(\vartheta)$

□

$K \subseteq M \Rightarrow K \cup \{x\} \subseteq M \Rightarrow L = K(x) \subseteq M(x)$

$L \subseteq M(x),\ M \subseteq M(x) \xrightarrow[\text{Kompositums}]{\text{Def. des}} LM \subseteq M(x)$

($\Rightarrow$ Beh) Es genügt also z.zg., dass $M(x)/M$ galoissch ist.

- x ist separabel über $K \Rightarrow x$ ist separabel über M
  $\Rightarrow M(x)/M$ ist separabel
- $\mu_{x,M}$ teilt $\mu_{x,K} \Rightarrow$ Mit $\mu_{x,K}$ zerfällt auch $\mu_{x,M}$ über $K(x)$ in Linearfaktoren, ist recht über $M(x) \Rightarrow M(x)$ ist Zerf.körper von $\mu_{x,M}$ über M
  $\Rightarrow M(x)/M$ ist normale Erweiterung