

## Algebra II, SoSe 2012 - Lösung Blatt 7

7.1. (i)  $E/K$  endliche Galoiserweiterung.

$$\Rightarrow \# \text{Gal}(E/K) < \infty \Rightarrow \# U < \infty \quad (\Rightarrow S_{p_0}(\alpha) \text{ wohldefiniert}).$$

Wir schreiben

$$U = \{\sigma_1, \dots, \sigma_n\}.$$

Als Körperhomomorphismen induzieren die  $\sigma_i: E \rightarrow E$  insbesondere Gruppenhomomorphismen

$$\sigma_i|_{E^*}: E^* \rightarrow E^*,$$

d.h. wir können die  $\sigma_i|_{E^*}$  als  $E$ -wertige Charaktere der Gruppe  $E^*$  auffassen. Da die  $\sigma_i|_{E^*}$  alle verschieden sind, folgt mit dem Satz von Artin:

$\{\sigma_1|_{E^*}, \dots, \sigma_n|_{E^*}\}$  ist eine linear unabhängige Teilmenge des  $E$ -Vektorraums  $\text{Abb}(E^*, E)$ .

$\Rightarrow$  Insbesondere ist  $\sigma_1|_{E^*} + \dots + \sigma_n|_{E^*} \neq 0$  (Nullabbildung).

$\Rightarrow \exists \alpha \in E$  mit  $(\sigma_1|_{E^*} + \dots + \sigma_n|_{E^*})(\alpha) \neq 0$ .

Damit:

$$S_{p_0}(\alpha) = \sigma_1(\alpha) + \dots + \sigma_n(\alpha) = (\sigma_1|_{E^*} + \dots + \sigma_n|_{E^*})(\alpha) \neq 0.$$

(iii) Vorüberlegung: Für  $\sigma \in U$  und  $e \in E$  berechnen wir:

$$\begin{aligned}\sigma(Sp_U(e)) &= \sigma(\sigma_1(e) + \dots + \sigma_n(e)) \\ &= \sigma \circ \sigma_1(e) + \dots + \sigma \circ \sigma_n(e) \\ &\stackrel{(*)}{=} \sigma_1(e) + \dots + \sigma_n(e) \\ &= Sp_U(e)\end{aligned}$$

Dabei haben wir in der Umformung  $(*)$  benutzt, dass die Linkstranslation mit  $\sigma \in U$  bijektiv ist, da  $U$  eine Gruppe ist.

Damit berechnen wir für  $\sigma \in U$ :

$$\begin{aligned}\sigma(\gamma) &= \sigma\left(\frac{\alpha}{Sp_U(\alpha)} \cdot \beta\right) = \frac{\sigma(\alpha)}{\sigma(Sp_U(\alpha))} \cdot \underbrace{\sigma(\beta)}_{=\beta, \text{ da } \beta \in E^U} \\ &= \frac{\sigma(\alpha)}{Sp_U(\alpha)} \cdot \beta\end{aligned}$$

Also erhalten wir:

$$\begin{aligned}Sp_U(\gamma) &= \sum_{\sigma \in U} \sigma(\gamma) = \sum_{\sigma \in U} \frac{\sigma(\alpha)}{Sp_U(\alpha)} \cdot \beta \\ &= \frac{\beta}{Sp_U(\alpha)} \cdot \sum_{\sigma \in U} \sigma(\alpha) = \frac{\beta}{Sp_U(\alpha)} \cdot Sp_U(\alpha) \\ &= \beta.\end{aligned}$$

(iii) • Zunächst gilt  $\forall \sigma \in U$  und  $m \in M \subset E$ :

$$\sigma(Sp_U(m)) = Sp_U(m) \quad (\text{vgl. Lösung von (ii)})$$

$$\Rightarrow Sp_U(M) \subset E^U.$$

• Sei nun  $\alpha \in E$  wie in Teil (i) und  $\beta \in E^U$  beliebig.

Wir müssen  $\beta$  als Linearkombination (über  $K$ ) der Elemente aus  $Sp_U(M)$  schreiben.

Sei dazu

$$\gamma := \frac{\alpha}{Sp_U(\alpha)} \cdot \beta \in E.$$

$$\stackrel{(ii)}{\Rightarrow} Sp_U(\gamma) = \beta.$$

Da  $M$  ein Erzeugendensystem des  $K$ -Vektorraums  $E$  ist,  $\exists m_1, \dots, m_\ell \in M$  und  $\mu_1, \dots, \mu_\ell \in K$  mit

$$\gamma = \sum_{j=1}^{\ell} \mu_j m_j.$$

Wir berechnen:

$$\begin{aligned} \beta = Sp_U(\gamma) &= \sum_{i=1}^n \sigma_i(\gamma) = \sum_{i=1}^n \sigma_i\left(\sum_{j=1}^{\ell} \mu_j m_j\right) \\ &= \sum_{i=1}^n \sum_{j=1}^{\ell} \mu_j \cdot \sigma_i(m_j) = \sum_{j=1}^{\ell} \mu_j \cdot \sum_{i=1}^n \sigma_i(m_j) \end{aligned}$$



$$= \sum_{j=1}^l \mu_j \cdot \underbrace{Sp_v(m_j)}_{\in Sp_v(M)}$$

Dies ist wegen  $\mu_j \in K$  die gesuchte Darstellung von  $\beta$  als Linearkombination (über  $K$ ) von Elementen aus  $Sp_v(M)$ .



7.2. (i) Elemente von  $G'$  sind genau die Gruppenhomomorphismen  $G \rightarrow K^*$ .

- Zeigen:  $\sigma, \tau \in G' \Rightarrow \sigma \cdot \tau \in G'$ .

Seien dazu  $g_1, g_2 \in G$ . Dann:

$$(\sigma \cdot \tau)(g_1 g_2) = \sigma(g_1 g_2) \tau(g_1 g_2) = \sigma(g_1) \sigma(g_2) \tau(g_1) \tau(g_2)$$

$$\begin{aligned} & \overset{\substack{\text{Mult. in } K \\ \text{kommutativ}}}{=} \sigma(g_1) \tau(g_1) \sigma(g_2) \tau(g_2) \\ &= (\sigma \cdot \tau)(g_1) \cdot (\sigma \cdot \tau)(g_2) \end{aligned}$$

$$\Rightarrow \sigma \cdot \tau \in G'.$$

- Wegen der Assoziativität der Multiplikation in  $K$ , ist die Verknüpfung auf  $G'$  sicherlich assoziativ.
- Neutrales Element ist offenbar der triviale Charakter

$$1: G \rightarrow K^*, g \mapsto 1 \quad (1 \text{ in } K).$$

- Invers zu  $\sigma \in G'$  ist  $\tilde{\sigma}: G \rightarrow K^*, g \mapsto \sigma(g)^{-1}$ .  
 $\tilde{\sigma}$  ist ein Charakter, denn

$$\begin{aligned} \tilde{\sigma}(g_1 g_2) &= \sigma(g_1 g_2)^{-1} = (\sigma(g_1) \sigma(g_2))^{-1} \\ &= \sigma(g_1)^{-1} \cdot \sigma(g_2)^{-1} \\ &= \tilde{\sigma}(g_1) \cdot \tilde{\sigma}(g_2). \end{aligned}$$

Insgesamt:  $(G', \cdot)$  ist eine Gruppe.

(ii) • Sei zunächst  $G$  zyklisch mit  $\text{ord } G = n$  und sei  $g \in G$  erzeugendes Element, d.h.

$$G = \{g^0, \dots, g^{n-1}\}.$$

Wegen  $\sigma(g^i) = \sigma(g)^i$  für  $\sigma \in G'$  ist jeder Charakter  $\sigma \in G'$  durch seinen Wert  $\sigma(g)$  von  $g$  bereits eindeutig bestimmt.

Andererseits berechnen wir:

$$1 = \sigma(g^0) = \sigma(g^n) = \sigma(g)^n$$

$\Rightarrow \sigma(g)$  ist stets eine  $n$ -te Einheitswurzel.

Sei nun  $\zeta_n$  eine primitive  $n$ -te Einheitswurzel in  $K$ .

Für  $j \in \{1, \dots, n\}$  sei  $\sigma_j \in G'$  definiert durch

$$\sigma_j(g) = \zeta_n^j$$

Da  $\zeta_n^j$  für  $j \in \{1, \dots, n\}$  alle  $n$ -ten Einheitswurzeln durchläuft erhalten wir auf diese Weise alle Charaktere, d.h.

$$G' = \{\sigma_1, \dots, \sigma_n\}.$$

Wegen  $\sigma_j(g) = \zeta_n^j = \sigma_1(g)^j$  erhalten wir stets

$$\sigma_j = \sigma_1^j$$



Also ist  $\sigma_1$  ein Erzeuger von  $G'$ .

$\Rightarrow G'$  ist zyklisch und offenbar ebenfalls von der Ordnung  $n$ .

$$\Rightarrow G \cong \mathbb{Z}/n\mathbb{Z} \cong G'.$$

• Wir zeigen nun: Ist  $G = G_1 \times G_2$ , so folgt:

$$G' \cong G'_1 \times G'_2. \quad (*)$$

Dazu definieren wir:

$$\begin{aligned} \phi: G'_1 \times G'_2 &\longrightarrow G' \\ (\sigma_1, \sigma_2) &\longmapsto \left( (g_1, g_2) \longmapsto \sigma_1(g_1) \cdot \sigma_2(g_2) \right) \end{aligned}$$

- Wohldefiniertheit:

$$\begin{aligned} \phi(\sigma_1, \sigma_2) \left( (g_1, g_2) \cdot (h_1, h_2) \right) &= \phi(\sigma_1, \sigma_2) \left( (g_1 h_1, g_2 h_2) \right) \\ &= \sigma_1(g_1 h_1) \cdot \sigma_2(g_2 h_2) = \sigma_1(g_1) \sigma_1(h_1) \sigma_2(g_2) \sigma_2(h_2) \\ &= \sigma_1(g_1) \sigma_2(g_2) \sigma_1(h_1) \sigma_2(h_2) \\ &= \phi(\sigma_1, \sigma_2) \left( (g_1, g_2) \right) \cdot \phi(\sigma_1, \sigma_2) \left( (h_1, h_2) \right). \end{aligned}$$

$$\Rightarrow \phi(\sigma_1, \sigma_2) \in G'.$$

-  $\phi$  ist ein Gruppenhomomorphismus, denn:

$$\begin{aligned}
\phi((\sigma_1, \sigma_2) \cdot (\tau_1, \tau_2))((g_1, g_2)) &= \phi((\sigma_1 \cdot \tau_1, \sigma_2 \cdot \tau_2))((g_1, g_2)) \\
&= \sigma_1 \cdot \tau_1(g_1) \cdot \sigma_2 \cdot \tau_2(g_2) = \sigma_1(g_1) \tau_1(g_1) \sigma_2(g_2) \tau_2(g_2) \\
&= \sigma_1(g_1) \sigma_2(g_2) \tau_1(g_1) \tau_2(g_2) \\
&= \phi(\sigma_1, \sigma_2)((g_1, g_2)) \cdot \phi(\tau_1, \tau_2)((g_1, g_2)).
\end{aligned}$$

Def. von.  
 $\Rightarrow$  in  $G'$   $\phi((\sigma_1, \sigma_2) \cdot (\tau_1, \tau_2)) = \phi(\sigma_1, \sigma_2) \cdot \phi(\tau_1, \tau_2)$

$\Rightarrow \phi$  Gruppenhomomorphismus.

-  $\phi$  ist bijektiv. Definiere Umkehrabbildung:  
 Zunächst definieren wir für  $\psi \in G'$  Abbildungen

$$\psi_1: G_1 \rightarrow K^*, \quad g_1 \mapsto \psi(g_1, 1)$$

$$\psi_2: G_2 \rightarrow K^*, \quad g_2 \mapsto \psi(1, g_2)$$

$\Rightarrow$  Offenbar ist  $\psi_1 \in G'_1$  und  $\psi_2 \in G'_2$ . Damit:

$$\begin{aligned}
\Omega: G' &\longrightarrow G'_1 \times G'_2 && \text{ist wohldefiniert.} \\
\psi &\longmapsto (\psi_1, \psi_2)
\end{aligned}$$

Es ist:

$$\begin{aligned}
\phi \circ \Omega(\psi)(g_1, g_2) &= \phi(\psi_1, \psi_2)(g_1, g_2) = \psi_1(g_1) \cdot \psi_2(g_2) \\
&= \psi(g_1, 1) \cdot \psi(1, g_2) = \psi((g_1, 1) \cdot (1, g_2)) \\
&= \psi(g_1, g_2)
\end{aligned}$$



$$\Rightarrow \phi \circ \Omega = \text{id}$$

Andererseits:  $\Omega \circ \phi(\sigma_1, \sigma_2) = (\phi(\sigma_1, \sigma_2)_1, \phi(\sigma_1, \sigma_2)_2)$

Dabei ist

$$\phi(\sigma_1, \sigma_2)_1(g_1) = \phi(\sigma_1, \sigma_2)(g_1, 1) = \sigma_1(g_1) \sigma_2(1) = \sigma_1(g_1)$$

$$\text{d.h. } \phi(\sigma_1, \sigma_2)_1 = \sigma_1$$

$$\phi(\sigma_1, \sigma_2)_2(g_2) = \phi(\sigma_1, \sigma_2)(1, g_2) = \sigma_1(1) \sigma_2(g_2) = \sigma_2(g_2)$$

$$\text{d.h. } \phi(\sigma_1, \sigma_2)_2 = \sigma_2$$

Also:  $\Omega \circ \phi(\sigma_1, \sigma_2) = (\sigma_1, \sigma_2)$ , d.h.  $\Omega \circ \phi = \text{id}$

$\Rightarrow \phi$  ist bijektiv.

$\phi$  ist also ein Gruppenisomorphismus, d.h. (\*) ist gezeigt.

• Sei nun allgemein  $G$  endlich und abelsch.

Mit dem Hauptsatz über endlich erzeugte abelsche Gruppen

folgt:

$$G \cong \frac{\mathbb{Z}}{m_1} \mathbb{Z} \times \frac{\mathbb{Z}}{m_2} \mathbb{Z} \times \dots \times \frac{\mathbb{Z}}{m_k} \mathbb{Z}$$

für gewisse  $m_1, \dots, m_k \in \mathbb{N}$ . Mit (\*) folgt nun:

$$G' \cong G' \left( \frac{\mathbb{Z}}{m_1} \mathbb{Z} \right) \times \dots \times G' \left( \frac{\mathbb{Z}}{m_k} \mathbb{Z} \right) \leftarrow \text{suggestive Notation!}$$

Fall zu Beginn  $\curvearrowright \cong \frac{\mathbb{Z}}{m_1} \mathbb{Z} \times \dots \times \frac{\mathbb{Z}}{m_k} \mathbb{Z}$

$$\cong G.$$



7.3. (i) • Analog zu 7.1. (i) Können wir die  $\sigma \in \text{Gal}(E/K)$

nach Einschränken auf  $E^*$  als  $E$ -wertige Charaktere von  $E^*$  auffassen. Mit dem Satz von Artin sind dann alle  $\sigma$  aus  $\text{Gal}(E/K)$  linear unabhängig.

$$\Rightarrow \exists a \in E \text{ mit } \sum_{\sigma \in G} \chi(\sigma) \cdot \sigma(a) \neq 0 \quad (*)$$

$\uparrow$   
 $\neq 0$ , d.h. nichttriviale Linearkombination  
der  $\sigma \in G$ .

Mit diesem  $a$  definieren wir  $\alpha$  wie in der Aufgabe:

$$\alpha := \sum_{\sigma \in G} \chi(\sigma) \cdot \sigma(a)$$

• Ist nun  $\tau \in G$  beliebig, so berechnen wir:

$$\tau(\alpha) = \tau\left(\sum_{\sigma \in G} \underbrace{\chi(\sigma)}_{\in K} \cdot \sigma(a)\right) = \sum_{\sigma \in G} \chi(\sigma) \cdot (\tau \circ \sigma)(a)$$

Also gilt  $\forall \tau \in G$ :

$$\chi(\tau) \cdot \tau(\alpha) = \chi(\tau) \cdot \sum_{\sigma \in G} \chi(\sigma) \cdot (\tau \circ \sigma)(a)$$

$$= \sum_{\sigma \in G} \chi(\tau) \cdot \chi(\sigma) \cdot (\tau \circ \sigma)(a)$$

Def. von  $\cdot$  in  $G$   $\rightarrow$

$$= \sum_{\sigma \in G} \chi(\tau \circ \sigma) \cdot (\tau \circ \sigma)(a)$$

Linkstranslation mit  $\tau$  in  $G$  bijektiv  $\rightarrow$

$$= \sum_{\sigma \in G} \chi(\sigma) \cdot \sigma(a)$$

$$= \alpha$$

Da  $\alpha \neq 0$  ist (vgl. (\*)), ist auch  $\tau(\alpha) \neq 0$  (denn  $\tau \in G = \text{Gal}(E/K)$ ). Also können wir diese Gleichung umformen:

$$\chi(\tau) = \frac{\alpha}{\tau(\alpha)} \quad \forall \tau \in G. \quad (**)$$

• Gelte nun  $\frac{\alpha}{\sigma(\alpha)} = \frac{\gamma}{\sigma(\gamma)} \quad \forall \sigma \in G.$

(Da  $\chi$  Charakter, ist  $\chi(\sigma)$  stets  $\neq 0$ , d.h.  $\alpha, \gamma \neq 0$ ).

$$\Rightarrow \frac{\alpha}{\gamma} = \frac{\sigma(\alpha)}{\sigma(\gamma)} = \sigma\left(\frac{\alpha}{\gamma}\right) \quad \forall \sigma \in G.$$

Da  $E^G = K$  gilt, folgt  $\frac{\alpha}{\gamma} \in K$  und damit sogar

$$\frac{\alpha}{\gamma} \in K^*, \text{ also } \frac{\alpha}{\gamma} = \beta \text{ für } \beta \in K^* \text{ geeignet.}$$

$$\Rightarrow \alpha = \beta \cdot \gamma \text{ für ein } \beta \in K^*.$$

Also: Durch (\*\*) wird  $\alpha$  bis auf einen Faktor  $\beta \in K^*$  eindeutig bestimmt.

(Bemerkung: Für  $\beta \in K^*$  ist natürlich

$$\frac{\beta\alpha}{\sigma(\beta\alpha)} = \frac{\beta\alpha}{\beta\sigma(\alpha)} = \frac{\alpha}{\sigma(\alpha)}$$

d.h. alle  $\beta \in K^*$  sind möglich! )



(ii) Wir rechnen direkt nach, dass

$$\chi: G \rightarrow K^*, \quad \sigma \mapsto \frac{\alpha}{\sigma(\alpha)}$$

ein Charakter ist. Dazu:

$$\begin{aligned}\chi(\sigma \circ \tau) &= \frac{\alpha}{(\sigma \circ \tau)(\alpha)} = \frac{\alpha}{\sigma(\tau(\alpha))} = \frac{\sigma(\alpha) \cdot \alpha}{\sigma(\alpha) \cdot \sigma(\tau(\alpha))} \\ &= \frac{\alpha}{\sigma(\alpha)} \cdot \frac{\sigma(\alpha)}{\sigma(\tau(\alpha))} = \frac{\alpha}{\sigma(\alpha)} \cdot \sigma\left(\frac{\alpha}{\tau(\alpha)}\right)\end{aligned}$$

$\frac{\alpha}{\tau(\alpha)} \in K$  nach  
Voraussetzung

$$\Rightarrow \frac{\alpha}{\sigma(\alpha)} \cdot \frac{\alpha}{\tau(\alpha)} = \chi(\sigma) \cdot \chi(\tau).$$

(iii) Es ist  $K^* \subset E^*$  Untergruppe, d.h.  $E^*/K^*$  ist eine Gruppe. Nach Teil (i) finden wir zu jedem  $\chi \in G'$  ein bis auf einen Faktor aus  $K^*$  eindeutiges Element  $\alpha(\chi) \in E^*$ .

$$\Rightarrow \psi: G' \rightarrow E^*/K^*, \quad \chi \mapsto \alpha(\chi) K^*$$

ist eine wohldefinierte, injektive Abbildung.

$\psi$  ist ein Gruppenhomomorphismus, denn gelte

$$\chi_1(\sigma) = \frac{\alpha_1}{\sigma(\alpha_1)}, \quad \chi_2(\sigma) = \frac{\alpha_2}{\sigma(\alpha_2)} \quad \forall \sigma \in G,$$

dann (nach (i)):  $\psi(\chi_1) = \alpha_1 K^*$ ,  $\psi(\chi_2) = \alpha_2 K^*$

und

$$(\chi_1 \cdot \chi_2)(\sigma) = \chi_1(\sigma) \cdot \chi_2(\sigma) = \frac{\alpha_1}{\sigma(\alpha_1)} \cdot \frac{\alpha_2}{\sigma(\alpha_2)} = \frac{\alpha_1 \alpha_2}{\sigma(\alpha_1 \alpha_2)}$$

$$\Rightarrow \psi(\chi_1 \cdot \chi_2) = (\alpha_1 \alpha_2) K^* = (\alpha_1 K^*) \cdot (\alpha_2 K^*) = \psi(\chi_1) \cdot \psi(\chi_2).$$

7.4. Wegen  $[E:K] = d$  und  $K = \mathbb{F}_{p^n}$  ist  $E$  als  $\mathbb{F}_{p^n}$ -Vektorraum isomorph zu  $(\mathbb{F}_{p^n})^d$ .

$$\Rightarrow \#E = p^{nd} \xRightarrow{VL} E = \mathbb{F}_{p^{nd}}.$$

(i) Nach Folgerung 22.5 gilt:

$\text{Gal}(E/K)$  ist zyklisch von der Ordnung  $d$  und erzeugendes Element ist  $\chi^n$ , wobei  $\chi$  den Frobenius-automorphismus bezeichne (d.h.  $\chi^n(e) = e^{p^n}$ ), d.h.

$$\text{Gal}(E/K) = \{\text{id}, \chi^n, \chi^{2n}, \dots, \chi^{(d-1)n}\}.$$

Nach Vorlesung (24.7) folgt daher:

$$\begin{aligned} N_{E/K}(\alpha) &= \text{id}(\alpha) \cdot \chi^n(\alpha) \cdot \chi^{2n}(\alpha) \cdot \dots \cdot \chi^{(d-1)n}(\alpha) \\ &= \alpha \cdot \alpha^{p^n} \cdot \alpha^{p^{2n}} \cdot \dots \cdot \alpha^{p^{(d-1)n}} \\ &= \alpha^{(1+p+p^2+\dots+p^{(d-1)})} \end{aligned}$$

Es ist

$$1 + q + q^2 + \dots + q^{(d-1)} \stackrel{\text{endl. geom. Reihe}}{=} \frac{1 - q^d}{1 - q} = \frac{q^d - 1}{q - 1} = m.$$

Also:

$$N_{E/K}(\alpha) = \alpha^m \quad \forall \alpha \in E.$$

(ii) Nach Teil (i) ist

$$N_{E/K} : E^* \rightarrow K^* \quad (\text{Einschränkung } \nabla)$$

gegeben durch den Homomorphismus  $\psi: \alpha \mapsto \alpha^m$ . Es ist

$$\begin{aligned} \text{Kern } \psi &= \{ \alpha \in E^* \mid \alpha^m = 1 \} \\ &= \{ \alpha \in E^* \mid \alpha \text{ Nullstelle von } X^m - 1 \}. \end{aligned}$$

Da  $X^m - 1$  in  $E$  höchstens  $m$  Nullstellen besitzt, folgt:

$$\# \text{Kern } \psi \leq m.$$

Nach dem Homomorphiesatz ist

$$\text{Bild } \psi \simeq E^* / \text{Kern } \psi.$$

$$\Rightarrow \# \text{Bild } \psi = \frac{\# E^*}{\# \text{Kern } \psi} \geq \frac{\# E^*}{m} = \frac{(q^d - 1)}{m} = q - 1.$$

Andererseits ist wegen  $\text{Bild } \psi \subset K^*$  und  $\# K^* = q - 1$ :

$$\# \text{Bild } \psi \leq q - 1.$$

$$\Rightarrow \# \text{Bild } \psi = q - 1 = \# K^*$$

$$\Rightarrow \text{Bild } \psi = K^*$$

$\Rightarrow \psi$  und damit  $N_{E/K}$  ist surjektiv.

