Algebra II, SoSe 2012 - Lösung Blatt 6

6.1. Sei $[K:\mathbb{Q}] =: n < \infty$. Sei E_ℓ die Gruppe der ℓ-ten Einheitswurzeln ($E_\ell \subset \mathbb{C}^*$).

- Zeigen zunächst: Ist p Primzahl und $\alpha \in \mathbb{N}$, dann folgt aus $E_{p^\alpha} \subset K$, dass $p^\alpha \leq 2n$ gilt. Dazu: (*)

  Gelte $E_{p^\alpha} \subset K$. Sei $L \subset \mathbb{C}$ der Zerfällungskörper von $X^{p^\alpha} - 1$ über $\mathbb{Q}$. $\overset{E_{p^\alpha} \subset K}{\Longrightarrow} \mathbb{Q} \subset L \subset K$.

  Nach Vorlesung ist $[L:\mathbb{Q}] = \varphi(p^\alpha)$ also folgt wegen

  $$n = [K:\mathbb{Q}] = [K:L] \cdot [L:\mathbb{Q}],$$

  dass $\varphi(p^\alpha) \mid n$ gilt. Insbesondere gilt also

  $$\varphi(p^\alpha) \leq n.$$

  Damit:

  $$n \geq \varphi(p^\alpha) = (p-1)p^{\alpha-1} = (1 - \underbrace{\tfrac{1}{p}}_{\leq \frac{1}{2}})\, p^\alpha \geq \tfrac{1}{2} p^\alpha$$

  $\Rightarrow 2n \geq p^\alpha$ also ist (*) gezeigt.

- Nun zeigen wir allgemeiner: Ist $E_\ell \subset K$ für $\ell \in \mathbb{N}$, so folgt: $\ell \leq (2n)^{2n}$. Dazu: (**)

  Schreibe $\ell = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$ (Primfaktorzerlegung)

Für alle $j \in \{1, \dots, r\}$ ist $E_{p_j^{\alpha_j}} \subset E_\ell \subset K$.

$\overset{(*)}{\Rightarrow}$ $p_j^{\alpha_j} \leq 2n \quad \forall j \in \{1, \dots, r\}$

Damit folgt zunächst:

$$\ell = p_1^{\alpha_1} \cdot \dots \cdot p_r^{\alpha_r} \leq (2n)^r.$$

Da die p_j und die α_j aus $\mathbb{N}$ sind haben wir aber auch:

$$p_j \leq p_j^{\alpha_j} \leq 2n \qquad \forall j \in \{1, \dots, r\}.$$

$\Rightarrow$ $p_j \in \{1, \dots, 2n\} \quad \forall j \in \{1, \dots, r\}$ (optimistische Angabe...)

Da die p_j nach Konstruktion paarweise verschieden sind, erhalten wir also $r \leq 2n$ und damit:

$$\ell \leq (2n)^r \leq (2n)^{2n},$$

d.h. $(**)$ ist gezeigt.

- Damit zur Aufgabe. Sei $\alpha \in K$ eine Einheitswurzel, also

$$\alpha^m = 1 \quad \text{für ein } m \in \mathbb{N}$$

Schreibe $\ell := \operatorname{ord} \alpha \in \mathbb{N}$ (da Teiler von m), dann ist α primitive ℓ-te Einheitswurzel, d.h. $E_\ell \subset K$.

$\overset{(**)}{\Rightarrow}$ $\operatorname{ord} \alpha = \ell \leq (2n)^{2n}$. Also folgt:

$$\{\alpha \in K \mid \alpha \text{ Einheitswurzel}\} \subset \bigcup_{\ell=1}^{(2n)^{2n}} E_\ell \subset \mathbb{C}.$$

↖ endliche Menge!

6.2. (i) Nach Vorlesung ist $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ eine Galoiserweiterung mit

$$\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \simeq \left(\mathbb{Z}/p\mathbb{Z}\right)^*.$$

p ist Primzahl $\Rightarrow$ $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ ist Körper

$\Rightarrow$ $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$ zyklisch von der Ordnung $p-1$.

p ungerade $\Rightarrow$ $p-1$ gerade

$\Rightarrow (p-1) = 2 \cdot \underbrace{\frac{p-1}{2}}_{\in \mathbb{N}}$, d.h. $\frac{p-1}{2} \mid (p-1)$

$\overset{\text{Algebra I}}{\Rightarrow}$ $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$ besitzt genau eine Untergruppe U der Ordnung $\frac{p-1}{2}$.

Betrachte den zugehörigen Fixkörper $Z := \mathbb{Q}(\zeta_p)^U \subset \mathbb{Q}(\zeta_p)$.
Nach dem Hauptsatz der Galoistheorie ist

$$\mathrm{Gal}(\mathbb{Q}(\zeta_p)/Z) \simeq U \quad \text{und damit:}$$

$$[\mathbb{Q}(\zeta_p) : Z] = \#\,\mathrm{Gal}(\mathbb{Q}(\zeta_p)/Z) = \#U = \frac{p-1}{2}.$$

Damit erhalten wir:

$$2 \cdot \frac{p-1}{2} = p-1 = \#\,\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) = [\mathbb{Q}(\zeta_p) : \mathbb{Q}]$$

$$= [\mathbb{Q}(\zeta_p) : Z] \cdot [Z : \mathbb{Q}] = \frac{p-1}{2} \cdot [Z : \mathbb{Q}].$$

$\Rightarrow [Z : \mathbb{Q}] = 2$.

Die Eindeutigkeit von Z folgt mit obigen Überlegungen wegen des Hauptsatzes der Galoistheorie aus der Eindeutigkeit der Untergruppe $U \subset Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ mit $\#U = \frac{p-1}{2}$.

(ii) • Zunächst: $\zeta_p \notin \mathbb{R}$, denn alle Einheitswurzeln in $\mathbb{C}$ liegen auf der Einheitskreislinie $\Rightarrow$ In $\mathbb{R}$ kommen nur 1 und -1 in Frage. Wegen $p > 2$ sind diese aber nicht primitiv.

$\Rightarrow \mathbb{Q}(\zeta_p) \not\subset \mathbb{R}$, d.h. für die Komplexe Konjugation

$$\tau : \mathbb{Q}(\zeta_p) \longrightarrow \mathbb{Q}(\zeta_p), \; z \longmapsto \overline{z} \qquad (*)$$

gilt: $\tau \in Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ und $\tau \neq id$.

• Für die Untergruppe U aus Teil (i) gilt:

$$U = \{\sigma \in Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \mid ord\,\sigma \mid \tfrac{p-1}{2}\}. \qquad (**)$$

Denn: Wegen $ord\,U = \frac{p-1}{2}$ ist „$\subset$" Klar.
Haben wir umgekehrt ein σ mit $ord\,\sigma \mid \frac{p-1}{2}$, so betrachten wir $V_1 := \langle \sigma \rangle$.
U ist als Untergruppe einer zyklischen Gruppe selbst zyklisch und besitzt daher wegen $ord\,\sigma \mid \frac{p-1}{2} = ord\,U$ eine Untergruppe V_2 mit $ord\,V_2 = ord\,\sigma = ord\,V_1$.
Da $Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ zyklisch ist, besitzt sie nur eine Untergruppe der Ordnung $ord\,\sigma$. $\Rightarrow V_1 = V_2$, also $\sigma \in U$.

- Wir betrachten nun den Isomorphismus

$$\psi: \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \xrightarrow{\simeq} \left(\mathbb{Z}/p\mathbb{Z}\right)^* = \{\overline{1}, \dots, \overline{p-1}\}.$$

$\Rightarrow$ Zu jedem $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ existiert ein eindeutig bestimmtes Element $r(\sigma) \in \{1, \dots, p-1\}$ mit

$$\psi(\sigma) = \overline{r(\sigma)}.$$

Wegen (**) entsprechen den $\sigma \in U$ gerade die Restklassen in $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$ mit $\overline{r(\sigma)}^{\frac{p-1}{2}} = \overline{1}$.

- Wegen $\tau^2 = \mathrm{id}$ entspricht τ in $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$ gerade $\overline{-1}$, also

$$\overline{r(\tau)} = \overline{-1}.$$

Damit:

$$Z \subset \mathbb{R} \overset{\text{Bezug zw. Z und U!}}{\Longleftrightarrow} \tau \in U \overset{\text{s.o.}}{\Longleftrightarrow} \overline{(-1)}^{\frac{p-1}{2}} = \overline{1}$$

$$\Longleftrightarrow (-1)^{\frac{p-1}{2}} = 1$$

$$\Longleftrightarrow \tfrac{p-1}{2} \text{ gerade also } \tfrac{p-1}{2} = 2 \cdot q \text{ für ein } q \in \mathbb{Z}$$

$$\Longleftrightarrow p-1 = 4 \cdot q \text{ für ein } q \in \mathbb{Z}$$

$$\Longleftrightarrow p-1 \equiv 0 \bmod 4$$

$$\Longleftrightarrow p \equiv 1 \bmod 4.$$

6.3. (i) Sei ζ_{p^r} primitive p^r-te Einheitswurzel.

$\Rightarrow \operatorname{ord} \zeta_{p^r} = p^r$

$\Rightarrow \operatorname{ord}\left((\zeta_{p^r})^{p^{r-1}}\right) \overset{\text{Algebra I}}{=} \frac{p^r}{ggT(p^r, p^{r-1})} = \frac{p^r}{p^{r-1}} = p$

$\Rightarrow (\zeta_{p^r})^{p^{r-1}}$ ist primitive p-te Einheitswurzel

$\Rightarrow (\zeta_{p^r})^{p^{r-1}}$ ist Nullstelle von $\Phi_p(X)$

$\Rightarrow \zeta_{p^r}$ ist Nullstelle von $\Phi_p(X^{p^{r-1}})$

Andererseits ist $\Phi_{p^r}(X)$ das Minimalpolynom von ζ_{p^r} über $\mathbb{Q}$

$\Rightarrow \Phi_{p^r}(X) \mid \Phi_p(X^{p^{r-1}})$ (*)

Es ist nach Vorlesung:

$\operatorname{Grad} \Phi_{p^r}(X) = \varphi(p^r) = (p-1)p^{r-1}$

$\operatorname{Grad} \Phi_p(X) = \varphi(p) = p-1 \Rightarrow \operatorname{Grad} \Phi_p(X^{p^{r-1}}) = (p-1)p^{r-1}$

Beide Polynome haben also denselben Grad und sind offenbar normiert.

$\overset{(*)}{\Rightarrow} \Phi_{p^r}(X) = \Phi_p(X^{p^{r-1}})$.

(ii) Völlig analog zu (i): Sei α primitive n-te Einheitswurzel. $\Rightarrow \operatorname{ord}(\alpha) = n = p_1^{r_1} \cdot \ldots \cdot p_s^{r_s}$.

$$\Rightarrow \quad \operatorname{ord}\left(\alpha^{p_1^{r_1-1}\cdot\ldots\cdot p_s^{r_s-1}}\right) = \frac{p_1^{r_1}\cdot\ldots\cdot p_s^{r_s}}{ggT\left(p_1^{r_1}\cdot\ldots\cdot p_s^{r_s},\, p_1^{r_1-1}\cdot\ldots\cdot p_s^{r_s-1}\right)}$$

$$= \frac{p_1^{r_1}\cdot\ldots\cdot p_s^{r_s}}{p_1^{r_1-1}\cdot\ldots\cdot p_s^{r_s-1}} = p_1\cdot\ldots\cdot p_s$$

$\Rightarrow$ $\alpha^{p_1^{r_1-1}\cdot\ldots\cdot p_s^{r_s-1}}$ ist primitive $(p_1\cdot\ldots\cdot p_s)$-te Einheitswurzel, also eine Nullstelle von $\Phi_{p_1\cdot\ldots\cdot p_s}(X)$

$\Rightarrow$ α ist Nullstelle von $\Phi_{p_1\cdot\ldots\cdot p_s}\left(X^{p_1^{r_1-1}\cdot\ldots\cdot p_s^{r_s-1}}\right)$

Da $\Phi_n(X)$ das Minimalpolynom von α über $\mathbb{Q}$ ist, folgt:

$$\Phi_n(X) \mid \Phi_{p_1\cdot\ldots\cdot p_s}\left(X^{p_1^{r_1-1}\cdot\ldots\cdot p_s^{r_s-1}}\right) \qquad (*)$$

Es ist:

$$\text{Grad } \Phi_n(X) = \varphi(n) = (p_1-1)\cdot p_1^{r_1-1}\cdot\ldots\cdot(p_s-1)\cdot p_s^{r_s-1}.$$

$$\text{Grad } \Phi_{p_1\cdot\ldots\cdot p_s}(X) = \varphi(p_1\cdot\ldots\cdot p_s) = (p_1-1)\cdot\ldots\cdot(p_s-1).$$

$$\Rightarrow \text{Grad } \Phi_{p_1\cdot\ldots\cdot p_s}\left(X^{p_1^{r_1-1}\cdot\ldots\cdot p_s^{r_s-1}}\right) = (p_1-1)\cdot\ldots\cdot(p_s-1)\cdot p_1^{r_1-1}\cdot\ldots\cdot p_s^{r_s-1}$$

$$= \text{Grad } \Phi_n(X).$$

Die Polynome haben also denselben Grad und sind normiert.

$$\overset{(*)}{\Rightarrow} \quad \Phi_n(X) = \Phi_{p_1\cdot\ldots\cdot p_s}\left(X^{p_1^{r_1-1}\cdot\ldots\cdot p_s^{r_s-1}}\right).$$

(Damit ist auch erneut Teil (i) gezeigt, für $n = p^r$).

(iii) Sei ζ_n primitive n-te Einheitswurzel.

$\Rightarrow \Phi_n(\zeta_n) = 0 \Rightarrow -\zeta_n$ ist Nullstelle von $\Phi_n(-X)$.

Es ist $\operatorname{ord}(\zeta_n) = n$ und $\operatorname{ord}(-1) = 2$

$\overset{2 \nmid n}{\Rightarrow} \operatorname{ord}(-\zeta_n) = \operatorname{ord}((-1)\cdot\zeta_n) = 2n$

$\Rightarrow -\zeta_n$ ist primitive $2n$-te Einheitswurzel, d.h. Nullstelle von $\Phi_{2n}(X)$. Außerdem ist $\Phi_{2n}(X)$ das Minimalpolynom von $-\zeta_n$ über $\mathbb{Q}$.

$\Rightarrow \Phi_{2n}(X) \mid \Phi_n(-X)$. (*)

Wir berechnen die Grade:

$\operatorname{Grad} \Phi_{2n}(X) = \varphi(2n) = \underbrace{\varphi(2)}_{=1} \cdot \varphi(n) = \varphi(n)$

$\operatorname{Grad} \Phi_n(-X) = \varphi(n)$

Die Grade beider Polynome stimmen also überein. Da beide Polynome normiert sind, folgt aus (*):

$$\Phi_{2n}(X) = \Phi_n(-X).$$

∎

6.4. • Zeigen zunächst: $\mathbb{Q}(\zeta_m) \cdot \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{mn})$ (*)

Dazu: Wegen $\mathbb{Q}(\zeta_m) \subset \mathbb{Q}(\zeta_{mn})$ und $\mathbb{Q}(\zeta_n) \subset \mathbb{Q}(\zeta_{mn})$ gilt $\mathbb{Q}(\zeta_m) \cdot \mathbb{Q}(\zeta_n) \subset \mathbb{Q}(\zeta_{mn})$. (Definition des Körperkompositums!)

Da $\operatorname{ggT}(m,n) = 1$ gilt, ist (vgl. Vorlesung):

$$\operatorname{ord}(\zeta_m \cdot \zeta_n) = m \cdot n.$$

$\Rightarrow \zeta_m \cdot \zeta_n$ ist primitive mn-te Einheitswurzel

$\Rightarrow \mathbb{Q}(\zeta_{mn}) = \mathbb{Q}(\zeta_m \cdot \zeta_n) \subset \mathbb{Q}(\zeta_m) \cdot \mathbb{Q}(\zeta_n)$.

Insgesamt also: $\mathbb{Q}(\zeta_m) \cdot \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{mn})$.

• Nun zeigen wir: $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$ (**)

Nach Vorlesung gilt: $[\mathbb{Q}(\zeta_{mn}) : \mathbb{Q}] = \varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$ und $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$. Sei

$$L := \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n).$$

Wegen

$$\mathbb{Q}(\zeta_{mn}) \overset{(*)}{=} \mathbb{Q}(\zeta_m) \cdot \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_m, \zeta_n) = \mathbb{Q}(\zeta_n)(\zeta_m) \text{ ist}$$

$$\varphi(m) \cdot \varphi(n) = [\mathbb{Q}(\zeta_n)(\zeta_m) : \mathbb{Q}] = [\mathbb{Q}(\zeta_n)(\zeta_m) : \mathbb{Q}(\zeta_n)] \cdot \underbrace{[\mathbb{Q}(\zeta_n) : \mathbb{Q}]}_{\varphi(n).}$$

$\Rightarrow \zeta_m$ hat über $\mathbb{Q}(\zeta_n)$ den Grad $\varphi(m)$, also folgt wegen $L \subset \mathbb{Q}(\zeta_n)$:

ζ_m hat über L einen Grad $\geq \varphi(m)$.

Damit berechnen wir:

$$\varphi(m) = [\mathbb{Q}(\zeta_m) : \mathbb{Q}] = [\mathbb{Q}(\zeta_m) : L] \cdot [L : \mathbb{Q}]$$

$$\geq \varphi(m) \cdot [L : \mathbb{Q}]$$

$\Rightarrow [L : \mathbb{Q}] = 1 \Rightarrow L = \mathbb{Q}$. Also ist (**) gezeigt.

- Mit (*) und (**) sind die Voraussetzungen von Satz 21.6 erfüllt.

$\Rightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_{mn})/\mathbb{Q}) \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$.

□