Algebra II, SoSe 2012 – Lösung Blatt 8

8.1. • Wir verifizieren eine Richtung direkt:

Gelte $(a,b,c) = (2nm, n^2-m^2, n^2+m^2)$. Dann:

$$\begin{aligned} a^2+b^2 &= 4n^2m^2 + n^4 - 2n^2m^2 + m^4 \\ &= n^4 + 2n^2m^2 + m^4 \\ &= (n^2+m^2)^2 \\ &= c^2 \qquad \text{ok.} \end{aligned}$$

• Für die andere Richtung müssen wir geeignete $n,m \in \mathbb{N}$ konstruieren.

Zunächst folgt wegen $(a,b,c)=1$ aus $a^2+b^2=c^2$:

$$(a,b) = (a,c) = (b,c) = 1 \qquad (*)$$

(z.B. $\nexists\ (a,b) = n > 1 \Rightarrow a = n\cdot x,\ b = n\cdot y$
$\Rightarrow c^2 = a^2+b^2 = n^2(x^2+y^2)$ d.h. $n^2 \mid c^2$. Ist p irgendeine Primzahl, die in der Primfaktorzerlegung von n auftritt, so folgt: $p \mid n$, d.h. $p \mid a$ und $p \mid b$
sowie $p^2 \mid c^2$, also $p \mid c^2$ und damit $p \mid c$, da p Primzahl.
$\Rightarrow$ p ist gemeinsamer Teiler von a,b und c ↯)

• $a^2+b^2=c^2 \overset{a,b,c\in\mathbb{N}}{\Longrightarrow} \frac{a^2}{c^2} + \frac{b^2}{c^2} = 1$. Betrachte

$$z := \frac{b}{c} + i\frac{a}{c} \in \mathbb{C}$$

Für die Norm der Erweiterung $\mathbb{C}/\mathbb{R}$ gilt nach Vorlesung:

$$N_{\mathbb{C}/\mathbb{R}}(\zeta) = |\zeta|^2$$

$$\Rightarrow N_{\mathbb{C}/\mathbb{R}}(z) = |z|^2 = \frac{b^2}{c^2} + \frac{a^2}{c^2} = 1.$$

Bezeichnet $\tau: \mathbb{C} \to \mathbb{C}$ die Konjugation $\zeta \mapsto \overline{\zeta}$, so ist

$$Gal(\mathbb{C}/\mathbb{R}) = \{id, \tau\}$$

d.h. τ erzeugt $Gal(\mathbb{C}/\mathbb{R})$ und offenbar ist $\mathbb{C}/\mathbb{R}$ zyklisch. Mit Hilberts Satz 90 folgt also wegen $N_{\mathbb{C}/\mathbb{R}}(z) = 1$:

$$\exists\, w \in \mathbb{C}^* \text{ mit } z = w \cdot \tau(w)^{-1} = \frac{w}{\overline{w}}$$

Also ist

$$z = \frac{r+is}{r-is}$$ für gewisse $r, s \in \mathbb{R}$. Da $a, b, c \in \mathbb{N}$ gilt, muss sogar $r, s \in \mathbb{Q}$ gelten (direkt nachrechnen).

$$\Rightarrow \frac{b}{c} + i\frac{a}{c} = \frac{r+is}{r-is}$$ für gewisse $r, s \in \mathbb{Q}$. (**)

- Wir schreiben nun

$$r = \frac{r_1}{r_2} \text{ und } s = \frac{s_1}{s_2} \text{ mit } r_1, r_2, s_1, s_2 \in \mathbb{Z}$$

und OE gelte $(r_1, r_2) = (s_1, s_2) = 1$

(Brüche gekürzt).

Dann berechnen wir:

$$\frac{b}{c}+i\frac{a}{c}=\frac{r+is}{r-is}=\frac{(r+is)^2}{r^2+s^2}=\frac{\frac{r_1^2}{r_2^2}-\frac{s_1^2}{s_2^2}+2i\frac{r_1s_1}{r_2s_2}}{\frac{r_1^2}{r_2^2}+\frac{s_1^2}{s_2^2}}$$

Wir können also $\mathbb{E}\ (r_1,s_1)=(r_2,s_2)=1$ annehmen (Ansonsten können wir oben im Zähler und Nenner den Bruch

$$\frac{(r_1,s_1)^2}{(r_2,s_2)^2}$$

ausklammern und wegkürzen, d.h. indem wir ggf. r_1,s_1,r_2,s_2 abändern, erhalten wir $(r_1,s_1)=(r_2,s_2)=1$ bei gleichem Wert obigen Bruchs (d.h. (**) bleibt gültig). Da wir bei dieser Modifikation höchstens Faktoren aus r_1,s_1,r_2,s_2 entfernen bleibt auch $(r_1,r_2)=(s_1,s_2)=1$ gültig.)

Wir rechnen weiter:

$$\frac{b}{c}+i\frac{a}{c}=\left(\frac{r_1^2s_2^2-r_2^2s_1^2}{r_1^2s_2^2+r_2^2s_1^2}\right)+2i\left(\frac{r_1s_1r_2s_2}{r_1^2s_2^2+r_2^2s_1^2}\right)$$

Ein Koeffizientenvergleich liefert:

$$\frac{b}{c}=\frac{r_1^2s_2^2-r_2^2s_1^2}{r_1^2s_2^2+r_2^2s_1^2}\quad\text{und}\quad\frac{a}{c}=\frac{2r_1s_1r_2s_2}{r_1^2s_2^2+r_2^2s_1^2}\qquad(***)$$

- Zwischenüberlegung: Sind $\alpha,\beta,\gamma,\delta\in\mathbb{N}$ mit $(\alpha,\beta)=1$ und $\frac{\alpha}{\beta}=\frac{\gamma}{\delta}$, dann folgt: $t\cdot\alpha=\gamma$, $t\cdot\beta=\delta$ für ein $t\in\mathbb{Z}$ (#)

Dazu: Ist $\alpha = 1$ oder $\beta = 1$, so folgt die Aussage direkt.
(z.B. $\alpha = 1$: $\frac{1}{\beta} = \frac{\gamma}{\delta} \Rightarrow \delta = \gamma \cdot \beta$ und $\gamma = \gamma \cdot 1$ ok.)

Seien also $\alpha, \beta > 1$.

$$(\alpha, \beta) = 1 \Rightarrow \gamma > 1$$

$$\beta > 1,\ (\alpha, \beta) = 1 \Rightarrow \frac{\alpha}{\beta} \notin \mathbb{Z} \Rightarrow \delta > 1$$

Wir betrachten also die Primfaktorzerlegungen

$$\alpha = p_{\alpha,1}^{j_{\alpha,1}} \cdot \ldots \cdot p_{\alpha,q}^{j_{\alpha,q}} \qquad \beta = p_{\beta,1}^{j_{\beta,1}} \cdot \ldots \cdot p_{\beta,r}^{j_{\beta,r}}$$

$$\gamma = p_{\gamma,1}^{j_{\gamma,1}} \cdot \ldots \cdot p_{\gamma,s}^{j_{\gamma,s}} \qquad \delta = p_{\delta,1}^{j_{\delta,1}} \cdot \ldots \cdot p_{\delta,t}^{j_{\delta,t}}.$$

$$\frac{\alpha}{\beta} = \frac{\gamma}{\delta} \Leftrightarrow \alpha\delta = \beta\gamma \qquad \text{Also:}$$

$$\underbrace{p_{\alpha,1}^{j_{\alpha,1}} \cdot \ldots \cdot p_{\alpha,q}^{j_{\alpha,q}}} \cdot p_{\delta,1}^{j_{\delta,1}} \cdot \ldots \cdot p_{\delta,t}^{j_{\delta,t}} = \underbrace{p_{\beta,1}^{j_{\beta,1}} \cdot \ldots \cdot p_{\beta,r}^{j_{\beta,r}}} \cdot p_{\gamma,1}^{j_{\gamma,1}} \cdot \ldots \cdot p_{\gamma,s}^{j_{\gamma,s}}$$

haben keine gem. Faktoren wg. $(\alpha, \beta) = 1$.

$\Rightarrow$ Die $p_{\alpha,\cdot}$ müssen unter den $p_{\gamma,\cdot}$ auftauchen, die $p_{\beta,\cdot}$ unter den $p_{\delta,\cdot}$

$\Rightarrow \delta = \beta \cdot r_1, \quad \gamma = \alpha \cdot r_2$ für gewisse $r_1, r_2 \in \mathbb{Z}$.

$$\alpha\delta = \beta\gamma \Rightarrow \alpha\beta r_1 = \beta\alpha r_2 \Rightarrow r_1 = r_2$$

Also mit $t := r_1 \ (= r_2)$:

$t \cdot \alpha = \gamma$ sowie $t \cdot \beta = \delta \Rightarrow$ (#) gezeigt.

- Indem wir (#) auf beide Brüche in (***) anwenden erhalten wir unter Berücksichtigung, dass die „Nennergleichungen" gleich sind:

$\exists\, t \in \mathbb{Z}$ (sogar: $t \in \mathbb{N}$) mit:

$$t \cdot b = r_1^2 s_2^2 - r_2^2 s_1^2 \quad , \quad t \cdot a = 2 r_1 s_1 r_2 s_2$$

$$t \cdot c = r_1^2 s_2^2 + r_2^2 s_1^2 \qquad (\#\#).$$

Insbesondere gilt also: (addiere entsprechende Relationen!)

$$t \mid 2 r_1^2 s_2^2 \quad , \quad t \mid 2 s_1^2 r_2^2 \quad , \quad t \mid 2 r_1 s_1 r_2 s_2$$

- Wegen $(r_1, r_2) = (s_1, s_2) = (r_1, s_1) = (r_2, s_2) = 1$ erhalten wir:

$$(r_1 s_2, r_2 s_1) = 1 \quad \text{und damit}$$

$$(r_1^2 s_2^2, r_2^2 s_1^2) = 1$$

(betrachte wieder Primfaktorzerlegungen der r_i und s_i!)

- Wegen der Teilbarkeitsrelationen aus (##) liefern diese ggT's: $\nearrow\!\!\!/\ t > 2 \Rightarrow t$ gemeinsamer Teiler von $r_1^2 s_2^2$ und $s_1^2 r_2^2$ ↯

$$\Rightarrow \quad t \in \{1, 2\}.$$

- Wir schließen den Fall $t = 2$ aus:

$\nearrow\!\!\!/\ t = 2$. Wir wenden (##) wiederholt an:

Zunächst ist

$$r_1 s_2 \equiv s_1 r_2 \equiv 0 \mod 2 \quad \text{wegen } (r_1 s_2, s_1 r_2) = 1$$

ausgeschlossen (es können nicht beide Zahlen gerade sein).

Nach (##) ist nun $2 \mid r_1^2 s_2^2 - s_1^2 r_2^2$.

$$\Rightarrow r_1^2 s_2^2 - s_1^2 r_2^2 \equiv 0 \mod 2$$

$$\Rightarrow r_1^2 s_2^2 \equiv s_1^2 r_2^2 \mod 2$$

Wäre $r_1 s_2 \not\equiv s_1 r_2 \mod 2$, so würden wir also einen Widerspruch erhalten (da wir in $\mathbb{Z}/2\mathbb{Z}$ rechnen!).

$$\Rightarrow r_1 s_2 \equiv s_1 r_2 \mod 2.$$

Damit müssen also beide Zahlen ungerade sein, d.h.

$$r_1 s_2 \equiv s_1 r_2 \equiv 1 \mod 2.$$

Mit (##) folgt aber:

$$2 \cdot a = t \cdot a = 2 r_1 s_1 r_2 s_2$$

$$\Rightarrow a = r_1 s_1 r_2 s_2 \quad \Rightarrow a \equiv 1 \mod 2,$$

d.h. a ist ungerade ↯ a ist nach Vor. gerade.

$\Rightarrow$ Es gilt $t = 1$.

- Wähle $n := r_1 s_2$ und $m := s_1 r_2$ $(\in \mathbb{N})$, dann folgt aus (##):

$$a = t \cdot a = 2 r_1 s_1 r_2 s_2 = 2nm,$$
$$b = t \cdot b = r_1^2 s_2^2 - r_2^2 s_1^2 = n^2 - m^2$$
$$c = t \cdot c = r_1^2 s_2^2 + r_2^2 s_1^2 = n^2 + m^2.$$

8.2. $X^n - c$ ist nach Voraussetzung irreduzibel.

$\overset{\text{Satz 25.3}}{\Rightarrow}$ E/K ist zyklische Erweiterung vom Grad n.

Sei $\zeta_n \in K$ primitive n-te Einheitswurzel (liegt nach Voraussetzung in K).

$\Rightarrow$ $\alpha, \zeta_n\alpha, \zeta_n^2\alpha, \ldots, \zeta_n^{n-1}\alpha \in E$ sind alle Nullstellen von $X^n - c$.

Da $\zeta_n \in K$ ist, folgt also $E = K(\alpha)$.

$\Rightarrow$ $Gal(E/K)$ wird von dem $\sigma \in Gal(E/K)$ erzeugt, welches $\sigma(\alpha) = \zeta_n\alpha$ erfüllt.

(Die Elemente aus $Gal(E/K)$ sind wegen $E = K(\alpha)$ durch ihre Werte auf α eindeutig bestimmt und zu jeder Nullstelle β von $X^n - c$ gibt es genau ein $\tau \in Gal(E/K)$ mit

$$\tau(\alpha) = \beta.$$

Die Aussage gilt also wegen $\sigma^k(\alpha) = \zeta_n^k\alpha$.)

Wegen $\operatorname{ord}\sigma = n$ ist

$$\operatorname{ord}(\sigma^{n_2}) = \frac{\operatorname{ord}(\sigma)}{(n_2, \operatorname{ord}(\sigma))} = \frac{n}{n_2} = n_1.$$

$\Rightarrow$ σ^{n_2} erzeugt eine eindeutig bestimmte Untergruppe $U < Gal(E/K)$ der Ordnung n_1. (beachte: Galoisgruppe zyklisch)

Hauptsatz d. Galoistheorie $\Rightarrow$ Es gibt genau einen Zwischenkörper

$$K \subset Z \subset E$$

mit $[E:Z] = n_1$, d.h. (Gradsatz) $[Z:K] = n_2$.

Wir zeigen nun, dass $[K(\alpha^{n_1}):K] = n_2$ gilt, dann ist die Behauptung wegen obiger Eindeutigkeit gezeigt.

α^{n_1} ist Nullstelle von $X^{n_2} - c \in K[X]$

$$\Rightarrow [K(\alpha^{n_1}):K] \leq n_2.$$

α ist Nullstelle von $X^{n_1} - \alpha^{n_1} \in K(\alpha^{n_1})$

$$\Rightarrow [K(\alpha):K(\alpha^{n_1})] \leq n_1.$$

Mit dem Gradsatz erhalten wir also:

$$n_1 \cdot n_2 = [E:K] = [K(\alpha):K] = [K(\alpha):K(\alpha^{n_1})] \cdot [K(\alpha^{n_1}):K]$$

$$\leq n_1 \cdot n_2.$$

$\Rightarrow$ In allen Ungleichungen muss Gleichheit gelten, d.h. insbesondere

$$[K(\alpha^{n_1}):K] = n_2.$$

$\blacksquare$

8.3. Wir zeigen (i) und (ii) gleichzeitig.

Für $\rho \in \{1, \dots, r\}$ bezeichne K_ρ den Zerfällungskörper von $X^n - c_\rho$ über K.

$\overset{25.3\,(ii)}{\Rightarrow}$ $\exists\, d_\rho$ mit $d_\rho \mid n$ so dass für eine Nullstelle γ_ρ von $X^n - c_\rho$ gilt:

$\gamma_\rho^{d_\rho} \in K$ und $X^{d_\rho} - \gamma_\rho^{d_\rho} \in K[X]$ ist das Minimalpolynom von γ_ρ über K.

Da die n-ten (und damit die d_ρ-ten) Einheitswurzeln nach Voraussetzung in K liegen, ist $K_\rho = K(\gamma_\rho)$ und aus demselben Satz folgt, dass $K(\gamma_\rho)$ und damit K_ρ über K eine zyklische Erweiterung vom Grad d_ρ ist.

Sei $G_\rho := \mathrm{Gal}(K_\rho / K)$.

Dann (analog zu 8.2):

G_ρ wird erzeugt von $\sigma_\rho \in G_\rho$ mit $\sigma_\rho(\gamma_\rho) = \zeta_{d_\rho} \gamma_\rho$

(ζ_{d_ρ} primitive d_ρ-te Einheitswurzel)

$\overset{\#G_\rho = d_\rho}{\Rightarrow}$ $G_\rho \cong \left\langle \left(\frac{n}{d_\rho}\right) \right\rangle < \mathbb{Z}/n\mathbb{Z}$, d.h. insbesondere

G_ρ ist isomorph zu Untergruppe von $\mathbb{Z}/n\mathbb{Z}$.

Der Zerfällungskörper E/K von f ist

$$E = K(\gamma_1) \cdot \ldots \cdot K(\gamma_r)$$

(Direkt wegen der Definition von $\cdot$ und Zerfällungskörper).

Mit Satz 21.6 ist also

$$\mathrm{Gal}(E/K) \text{ Untergruppe von } G_1 \times \ldots \times G_r.$$

Da alle G_ρ Untergruppen von $\mathbb{Z}/n\mathbb{Z}$ sind, erhalten wir (bis auf Isomorphie):

$$\mathrm{Gal}(E/K) < \underbrace{\mathbb{Z}/n\mathbb{Z} \times \ldots \times \mathbb{Z}/n\mathbb{Z}}_{r\text{-mal}}.$$

Damit ist (i) und (ii) gezeigt. ▨

8.4. Wir lösen wieder beide Teilaufgaben gleichzeitig.

- α ist Nullstelle von $X^n - a$.

$\Rightarrow$ $\zeta_n^i \alpha$ für $i \in \{0, \dots, n-1\}$ sind alle Nullstellen von $X^n - a$.

Wegen $\mathbb{Q}(\alpha, \zeta_n\alpha, \dots, \zeta_n^{n-1}\alpha) = \mathbb{Q}(\zeta_n, \alpha) = E$ ist E der Zerfällungskörper von $X^n - a$ über $\mathbb{Q}$.

Nach Vorlesung haben wir

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$$

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \left(\mathbb{Z}/n\mathbb{Z}\right)^*$$

Außerdem gibt es nach Satz 25.3 ein d mit $d \mid n$ und

$$[\mathbb{Q}(\zeta_n, \alpha) : \mathbb{Q}(\zeta_n)] = d.$$

$\Rightarrow$ $[E : \mathbb{Q}] = \varphi(n) \cdot d$ (Gradsatz)

Außerdem ist $E/\mathbb{Q}$ eine Galoiserweiterung (als Zerfällungskörper ist $E/\mathbb{Q}$ normal, Separabilität ist klar).

$\Rightarrow$ $G := \mathrm{Gal}(E/\mathbb{Q})$ hat Ordnung $\varphi(n) \cdot d$.

- Wir untersuchen nun diese Galoisgruppe genauer.

Zunächst enthält sie Abbildungen

σ_r für $r \in \{1, \dots, n-1\}$ mit $(r,n) = 1$, welche

$$\sigma_r(\zeta_n) = \zeta_n^r$$
$$\sigma_r(\alpha) = \alpha$$

erfüllen (sukzessive entlang der beiden einfachen Erweiterungen aus der Überlegung zu Beginn konstruieren).

Offenbar ist

$$U_8 = \{\sigma_r \mid r \in \{1, \dots, n-1\},\ (r,n) = 1\} < G$$

eine Untergruppe, welche zu $(\mathbb{Z}/n\mathbb{Z})^*$ isomorph ist.

Insbesondere ist $\operatorname{ord} U = \varphi(n)$.

Sei $\zeta_{d\,8} = \zeta_n^{\frac{n}{d}}$, so ist ζ_d primitive d-te Einheitswurzel.

G enthält dann für $i \in \{0, \dots, d\}$ Abbildungen τ_i mit

$$\tau(\zeta_n) = \zeta_n$$
$$\tau(\alpha) = \zeta_d^i \alpha.$$

Es ist bekannt: (Zahlentheorie)

$(\mathbb{Z}/n\mathbb{Z})^*$ zyklisch $\iff n \in \{2, 4, p^m, 2p^m \mid p$ prim, ungerade, $m \in \mathbb{N}\}$ (*)

- Setzen wir $E/\mathbb{Q}$ als zyklisch voraus, so ist G zyklisch, also wegen $U < G$ auch U.

$\Rightarrow (\mathbb{Z}/n\mathbb{Z})^*$ ist zyklisch, also muss n von obiger Form (*) sein.

Damit folgt, dass $E/\mathbb{Q}$ im Allgemeinen nicht zyklisch ist, d.h. Behauptung (ii) ist gezeigt.

- Wir berechnen nun für

  s mit $1 \leq s \leq n-1$, $(s,n)=1$

  und j mit $0 \leq j \leq d-1$:

$$\tau_j \sigma_s(\zeta_n) = \tau_j(\zeta_n^s) = \tau_j(\zeta_n)^s = \zeta_n^s$$

$$\tau_j \sigma_s(\alpha) = \tau_j(\alpha) = \zeta_n^{\frac{n}{d} \cdot j} \alpha$$

$\Rightarrow$ Die Abbildungen sind alle verschieden und da es insgesamt $\varphi(n) \cdot d$ Abbildungen aus G sind, und $\#G = \varphi(n) \cdot d$ gilt, folgt:

$$G = \{\tau_j \sigma_s \mid 1 \leq s \leq n-1,\ (s,n)=1,\ 0 \leq j \leq d-1\}.$$

Insbesondere sehen wir, dass jedes $\sigma \in G$ eindeutig durch das „zugehörige" s und j bestimmt ist.

$\Rightarrow$ Die Abbildung $\Psi: Gal(E/\mathbb{Q}) \longrightarrow M$ mit

$$\Psi(\tau_j \sigma_s) := \begin{pmatrix} \overline{s} & \overline{\frac{n}{d} \cdot j} \\ \overline{0} & \overline{1} \end{pmatrix}$$

ist wohldefiniert und injektiv. Wir rechnen nach, dass sie ein Gruppenhomomorphismus ist:

Zunächst berechnen wir:

$$\psi(\tau_j\sigma_s)\cdot\psi(\tau_k\sigma_t) = \begin{pmatrix} \overline{s} & \overline{\frac{n}{d}\cdot j} \\ \overline{0} & \overline{1} \end{pmatrix} \cdot \begin{pmatrix} \overline{t} & \overline{\frac{n}{d}\cdot k} \\ \overline{0} & \overline{1} \end{pmatrix}$$

$$= \begin{pmatrix} \overline{st} & \overline{\frac{n}{d}ks} + \overline{\frac{n}{d}j} \\ \overline{0} & \overline{1} \end{pmatrix}$$

Andererseits berechnen wir:

$$\tau_j\sigma_s\tau_k\sigma_t(\zeta_n) = \tau_j\sigma_s(\zeta_n^t) = (\tau_j\sigma_s(\zeta_n))^t = \zeta_n^{st}$$

$$\tau_j\sigma_s\tau_k\sigma_t(\alpha) = \tau_j\sigma_s(\zeta_n^{\frac{n}{d}\cdot k}\alpha) = \tau_j(\sigma_s(\zeta_n)^{\frac{n}{d}\cdot k}\sigma_s(\alpha))$$

$$= \tau_j(\zeta_n^{\frac{n}{d}\cdot ks}\alpha) = \zeta_n^{\frac{n}{d}\cdot k\cdot s}\cdot\zeta_n^{\frac{n}{d}\cdot j}\alpha$$

$$= \zeta_n^{\left(\frac{n}{d}ks+\frac{n}{d}\cdot j\right)}\alpha$$

$$\Rightarrow \psi(\tau_j\sigma_s\tau_k\sigma_t) = \begin{pmatrix} \overline{st} & \overline{\frac{n}{d}ks+\frac{n}{d}j} \\ \overline{0} & \overline{1} \end{pmatrix}$$

Also folgt:

$$\psi(\tau_j\sigma_s\tau_k\sigma_t) = \psi(\tau_j\sigma_s)\cdot\psi(\tau_k\sigma_t),$$

d.h. ψ ist ein Gruppenhomomorphismus. Damit ist auch die Behauptung (i) gezeigt.

∎