Algebra II, SoSe 2012 – Lösung Blatt 12

12.1. Sei $f(X) = X^3 + 2X + 2 \in \mathbb{Q}[X]$

sowie $g(X) = X^3 + 3X^2 + 6X + 6 \in \mathbb{Q}[X]$.

Beide Polynome können völlig analog behandelt werden:

- f ist irreduzibel nach Eisenstein mit $p = 2$.
  g ist irreduzibel nach Eisenstein mit $p = 3$.

- Grad f = Grad g = 3
  $\overset{\text{Analysis}}{\Rightarrow}$ Beide Polynome besitzen mindestens eine reelle Nullstelle.

- Es ist
  $$f'(X) = 3x^2 + 2 > 0 \quad \forall x \in \mathbb{R}.$$
  $$g'(X) = 3x^2 + 6X + 6 = 3(x^2 + 2x + 2)$$
  $$= 3(x^2 + 2x + 1) + 3 = 3(x+1)^2 + 3 > 0 \quad \forall x \in \mathbb{R}.$$

  $\Rightarrow$ f und g sind streng monoton wachsend
  $\Rightarrow$ f und g besitzen genau eine reelle Nullstelle
  $\Rightarrow$ f und g besitzen genau zwei nicht reelle Nullstellen

- Mit Übungsaufgabe 11.1 folgt, dass sowohl f als auch g die Galoisgruppe $\mathfrak{S}_3$ besitzen.

12.2. (i) Es ist

$$X^4 - 4 = (X^2+2)(X^2-2)$$

$\Rightarrow$ Die Nullstellen sind $\pm i\sqrt{2}$ und $\pm\sqrt{2}$.

$\Rightarrow$ Der Zerfällungskörper des Polynoms ist

$$E = \mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\sqrt{2}) \cdot \mathbb{Q}(i)$$

Es ist $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(i) : \mathbb{Q}] = 2$ d.h.

$$Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \simeq Gal(\mathbb{Q}(i)/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}.$$

und damit wegen $\mathbb{Q}(\sqrt{2}) \cap \mathbb{Q}(i) = \mathbb{Q}$:

$$Gal(E/\mathbb{Q}) \simeq Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \times Gal(\mathbb{Q}(i)/\mathbb{Q})$$
$$\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Konkret ist $Gal(E/\mathbb{Q}) = \{id, \sigma, \tau, \sigma\tau\}$ mit

σ: $\sqrt{2} \mapsto -\sqrt{2}$ $\quad i \mapsto i$

τ: $\sqrt{2} \mapsto \sqrt{2}$ $\quad i \mapsto -i$

$\sigma\tau$: $\sqrt{2} \mapsto -\sqrt{2}$ $\quad i \mapsto -i$.

(ii) Es ist:

$$X^4 - 6X^2 + 5 = (X^2-1)(X^2-5)$$

$\Rightarrow$ Die Nullstellen sind ± 1 $(\in \mathbb{Q})$ und $\pm\sqrt{5}$.

$\Rightarrow$ Der Zerfällungskörper ist $E = \mathbb{Q}(\sqrt{5})$ und damit

$$Gal(E/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$$ (da Grad gleich 2!)

12.3. (i) • Behauptung: $\mathbb{Q}(i+\sqrt{2}) = \mathbb{Q}(i,\sqrt{2})$

Dazu: Da $i+\sqrt{2} \in \mathbb{Q}(i,\sqrt{2})$ ist, gilt sicherlich

$$\mathbb{Q}(i+\sqrt{2}) \subset \mathbb{Q}(i,\sqrt{2})$$

Für die umgekehrte Inklusion genügt es zu zeigen, dass

$$i \in \mathbb{Q}(i+\sqrt{2}) \qquad (*)$$

gilt, denn dann ist auch $i(i+\sqrt{2}) = -1+i\sqrt{2}$ und damit $i\sqrt{2}$ ein Element von $\mathbb{Q}(i+\sqrt{2})$. Dann muss aber auch $\sqrt{2} = -i(i\sqrt{2})$ in $\mathbb{Q}(i+\sqrt{2})$ liegen und wir sind fertig. Wir zeigen also $(*)$:

$$1+2i\sqrt{2} = (i+\sqrt{2})^2 \in \mathbb{Q}(i+\sqrt{2})$$

$$\Rightarrow i\sqrt{2} \in \mathbb{Q}(i+\sqrt{2})$$

$$\Rightarrow 1+i\sqrt{2} \in \mathbb{Q}(i+\sqrt{2})$$

$$\Rightarrow 3i = (1+i\sqrt{2})(i+\sqrt{2}) \in \mathbb{Q}(i+\sqrt{2})$$

$$\Rightarrow i \in \mathbb{Q}(i+\sqrt{2}).$$

ok.

• Wegen $K = \mathbb{Q}(i,\sqrt{2})$ ist K der Zerfällungskörper der Polynome X^2+1 und X^2-2 über $\mathbb{Q}$.

$\Rightarrow K/\mathbb{Q}$ ist normale Erweiterung.

Wegen $\chi(\mathbb{Q}) = 0$ ist $K/\mathbb{Q}$ separable Erweiterung.

$\Rightarrow K/\mathbb{Q}$ ist Galoiserweiterung.

(ii) Die Galoisgruppe von $\mathbb{Q}(\sqrt{2}, i)$ über $\mathbb{Q}$ wurde bereits mit Aufgabe 12.2 (i) ausgerechnet:

$$\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

12.4. (i) • $\widetilde{E}/\widetilde{K}$ ist nach 19.7. (i) normal:

E/K ist als Zerfällungskörper von f über K normal und $\widetilde{K}/K$ ist Körpererweiterung

$\Rightarrow$ $E\cdot\widetilde{K}/\widetilde{K}$ ist normal

Wegen $E\cdot\widetilde{K}=\widetilde{E}$ ist die Erweiterung $\widetilde{E}/\widetilde{K}$ also normal.

• Außerdem ist $\widetilde{E}/\widetilde{K}$ separabel da

$$\widetilde{E}=\widetilde{K}(\alpha_1,\dots,\alpha_n)$$

gilt, und die $\alpha_1,\dots,\alpha_n$ separabel sind. (vgl. 20.14 (ii)).

$\Rightarrow$ $\widetilde{E}/\widetilde{K}$ ist eine Galoiserweiterung

(ii) Mit Folgerung 21.5 berechnen wir:

$$\mathrm{Gal}(\widetilde{E}/\widetilde{K}) = \mathrm{Gal}(E\widetilde{K}/\widetilde{K}) \overset{21.5.}{\cong} \mathrm{Gal}(E/E\cap\widetilde{K})$$

$$E\cap\widetilde{K}=K \;\curvearrowright\; = \mathrm{Gal}(E/K).$$

(iii) Die Elemente $\sigma\in\mathrm{Gal}(\widetilde{E}/\widetilde{K})$ induzieren eine Permutation der Nullstellen $\alpha_1,\dots,\alpha_n$ von f und lassen die $X_1,\dots,X_n$ fest (da $X_i\in\widetilde{K}$ gilt).

$\Rightarrow$ Nur die Identität lässt alle α_i simultan fest

$\Rightarrow$ Nur für $\sigma=\mathrm{id}_{\widetilde{E}}$ gilt $\sigma(h)=h$.

(wg. $\sigma(h)=\sigma\left(\sum_{i=1}^{n}\alpha_i X_i\right)=\sum_{i=1}^{n}\sigma(\alpha_i)X_i$.)

(iv) Wegen $h \in \widetilde{E}$ ist

$$\widetilde{K} \subset \widetilde{K}(h) \subset \widetilde{E}$$

ein Zwischenkörper der Galoiserweiterung $\widetilde{E}/\widetilde{K}$. Nach (iii) wird h nur von $\mathrm{id}_{\widetilde{E}} \in \mathrm{Gal}(\widetilde{E}/\widetilde{K})$ festgelassen.

$$\Rightarrow \quad \widetilde{K}(h) = \widetilde{E}^{\{\mathrm{id}_{\widetilde{E}}\}} = \widetilde{E} \qquad \text{(Hauptsatz der Galoistheorie).}$$

$\{\mathrm{id}_{\widetilde{E}}\}$: Untergruppe von $\mathrm{Gal}(\widetilde{E}/\widetilde{K})$

12.5. (i) • f kann wegen

$$f(\overline{0}) = \overline{0} + \overline{0} + \overline{1} = \overline{1} \neq \overline{0}$$

$$f(\overline{1}) = \overline{1} + \overline{1} + \overline{1} = \overline{1} \neq \overline{0}$$

in $\mathbb{F}_2[X]$ keinen Faktor vom Grad 1 abspalten.

$\Rightarrow$ Ist f reduzibel, dann müssen die Faktoren wegen Grad f = 4 irreduzible Polynome vom Grad 2 sein.

• Die Polynome vom Grad 2 in $\mathbb{F}_2[X]$ sind:

$$X^2,\ X^2+\overline{1},\ X^2+X \text{ und } X^2+X+\overline{1}$$

Wegen

$$X^2 = X \cdot X,\quad X^2+\overline{1} = (X+\overline{1})(X+\overline{1})$$

$$X^2+X = X(X+\overline{1})$$

Kommt also nur $X^2+X+\overline{1}$ als Faktor in Frage.

• Wir dividieren $X^4+X^3+\overline{1}$ mit Rest durch $X^2+X+\overline{1}$:

$$X^4+X^3+\overline{1} = (X^2+X+\overline{1})(X^2+\overline{1}) + X$$

$\Rightarrow (X^2+X+\overline{1}) \nmid (X^4+X^3+\overline{1})$

$\Rightarrow f(X) = X^4+X^3+\overline{1}$ ist in $\mathbb{F}_2[X]$ irreduzibel.

(ii) und (iii).

- Wegen (i) erzeugt jede Nullstelle von f einen Erweiterungskörper von $\mathbb{F}_2$ vom Grad 4, d.h. (VL)

$$\mathbb{F}_{2^4} = \mathbb{F}_{16}.$$

$\Rightarrow$ $\mathbb{F}_{16}$ ist der Zerfällungskörper von f über $\mathbb{F}_2$ und nach Vorlesung ist $\mathrm{Gal}(\mathbb{F}_{16}/\mathbb{F}_2)$ zyklisch von der Ordnung 4, d.h.

$$\mathrm{Gal}(\mathbb{F}_{16}/\mathbb{F}_2) \simeq \mathbb{Z}/4\mathbb{Z}.$$

($\Rightarrow$ (iii)).

- Nach Vorlesung ist $\mathbb{F}_{16}$ der Zerfällungskörper von

$$X^{16} - X \in \mathbb{F}_2[X]$$

und seine Elemente sind genau die Nullstellen von $X^{16} - X$.

$\Rightarrow$ Die Elemente von $\mathbb{F}_{16}^*$ sind genau die Nullstellen von $X^{15} - \overline{1} \in \mathbb{F}_2[X]$ also genau die 15-ten Einheitswurzeln.

- Wir müssen noch zeigen, dass jede Nullstelle $\alpha \in \mathbb{F}_{16}^*$ von f sogar eine primitive 15-te Einheitswurzel ist. Dazu: Ist $\eta \in \mathbb{F}_{16}^*$, dann gilt $\mathrm{ord}\,\eta \in \{1, 3, 5, 15\}$ (vrg. $\#\mathbb{F}_{16}^* = 15$) und η ist primitive 15-te Einheitswurzel

genau dann, wenn

$$\operatorname{ord} \eta = 15$$

gilt. Sei $\alpha \in \mathbb{F}_{16}^*$ Nullstelle von f.

$\overset{(i)}{\Rightarrow}$ α hat Grad 4 über $\mathbb{F}_2$.

- $\operatorname{ord} \alpha = 1$ kann wegen $\alpha \neq 1$ (vgl. (i)) nicht gelten.
- $\operatorname{ord} \alpha = 3$.
  $\Rightarrow$ α ist Nullstelle von $X^3 - \overline{1}$ $\lightning$ α hat Grad 4 über $\mathbb{F}_2$.
- $\operatorname{ord} \alpha = 5$.
  $\Rightarrow$ α ist Nullstelle von

$$X^5 - \overline{1} = (X - \overline{1})(X^4 + X^3 + X^2 + X + \overline{1})$$

$\overset{\alpha \neq 1}{\Rightarrow}$ α ist Nullstelle von

$$X^4 + X^3 + X^2 + X + \overline{1}$$

Andererseits ist α Nullstelle von

$$X^4 + X^3 \qquad + \overline{1}$$

$\overset{\text{Subtrahiere}}{\Rightarrow}$ α ist Nullstelle von $X^2 + X = X(X + \overline{1})$

$\Rightarrow$ $\alpha = \overline{0}$ oder $\alpha = \overline{1}$ $\lightning$

Also folgt: $\operatorname{ord} \alpha = 15$, d.h. α ist primitive 15-te Einheitswurzel.

($\Rightarrow$ (ii)).

12.6. OE dürfen wir $p < q$ annehmen.

Sei s_p die Anzahl der p-Sylowgruppen in G und s_q die Anzahl der q-Sylowgruppen.

- Behauptung: $s_q = 1$ oder $s_p = 1$. (*)

Dazu: Aus den Sylowsätzen folgt

$s_p \equiv 1 \mod p$ und $s_p \mid q$

$s_q \equiv 1 \mod q$ und $s_q \mid p$.

$s_p \mid q \overset{q \text{ Primzahl}}{\Rightarrow} s_p = 1$ oder $s_p = q$.

Falls $s_p = 1$ gilt, sind wir fertig. Gelte also $s_p = q$.

Wir müssen $s_q = 1$ zeigen.

$s_p \equiv 1 \mod p \Rightarrow p \mid (s_p - 1)$ d.h. $p \mid (q-1)$.

Andererseits:

$s_q \mid p \overset{p \text{ Primzahl}}{\Rightarrow} s_q \in \{1, p\}$.

$s_q = p$. Es ist $s_q \equiv 1 \mod q$, d.h. $q \mid (s_q - 1)$

also $q \mid (p-1)$. $\Rightarrow q \leq p-1$

Andererseits: $p \mid (q-1)$ d.h. $p \leq q-1$.

Damit folgt:

$q+1 \leq p \leq q-1$ ↯

$\Rightarrow$ Es gilt $s_q = 1$ also ist (*) gezeigt.

- Damit: G enthält eine p-Sylowgruppe, welche Normalteiler ist oder eine q-Sylowgruppe welche Normalteiler ist.

  O.E. sei U eine p-Sylowgruppe, welche Normalteiler ist

  Betrachte Normalreihe

  $$G \rhd U \rhd \{e\}.$$

  Es ist G/U eine Gruppe der Ordnung q und damit zyklisch (da q Primzahl ist).

  Außerdem ist $U/\{e\} = U$ eine Gruppe der Ordnung p und damit zyklisch (da p Primzahl ist)

  $\Rightarrow$ Wir haben eine Normalreihe mit abelschen Faktoren für G konstruiert.

  $\Rightarrow$ G ist auflösbar.

(Der Fall dass U eine q-Sylowgruppe ist, welche Normalteiler ist, kann völlig analog behandelt werden).

▨