Algebra II, SoSe 2012 - Lösung Blatt 11

11.1. (i) • f irreduzibel, Grad $f = p$

$\Rightarrow$ f hat p verschiedene Nullstellen

$$\alpha_1, \dots, \alpha_p \quad (\in \mathbb{C}).$$

Sei E der Zerfällungskörper von f über $\mathbb{Q}$. Wissen: Elemente $\varphi \in Gal(E/\mathbb{Q})$ sind durch ihre Werte

$$\varphi(\alpha_1), \dots, \varphi(\alpha_p)$$

eindeutig bestimmt und mit α ist stets auch $\varphi(\alpha)$ Nullstelle von f.

$\Rightarrow$ Jedes $\varphi \in Gal(E/\mathbb{Q})$ induziert eine Permutation $\pi_\varphi \in \mathcal{S}_p$. Dazu: $\varphi(\alpha_i) = \alpha_{i(\varphi)}$ für $i(\varphi)$ geeignet. Setze $\pi_\varphi(i) := i(\varphi)$. Da φ bijektiv ist, ist π Permutation von $\{1, \dots, p\}$.

Außerdem Klar: Die Abbildung

$$Gal(E/\mathbb{Q}) \longrightarrow \mathcal{S}_p, \quad \varphi \mapsto \pi_\varphi$$

ist injektiver Gruppenhomomorphismus.

$\Rightarrow$ $Gal(E/\mathbb{Q})$ ist zu einer Untergruppe von $\mathcal{S}_p$ isomorph.

- Grad $f = p \overset{VL}{\Rightarrow} p \leq [E:\mathbb{Q}] \leq p!$

Da z.B. $\mathbb{Q}(\alpha_i)$ für ein α_i mit $\alpha_i \notin \mathbb{R}$ ein Zwischen-Körper mit $[\mathbb{Q}(\alpha_i):\mathbb{Q}] = \deg f = p$ ist, haben wir

$$p \mid [E:\mathbb{Q}]$$

$\Rightarrow p \mid \operatorname{ord} \mathrm{Gal}(E/\mathbb{Q})$. Mit den Sylowsätzen folgt:

$\exists\ U < \mathrm{Gal}(E/\mathbb{Q})$ mit $\operatorname{ord} U = p$, d.h. U ist zyklisch.

Sei $\varphi \in U$ ein erzeugendes Element von U.

$\Rightarrow \operatorname{ord} \varphi = p$

$\Rightarrow \operatorname{ord} \pi_\varphi = p$ (in $\mathcal{S}_p$).

Mit Aufgabe 10.2 folgt: π_φ ist ein p-Zyklus, d.h.

$$\pi_\varphi = (i_1, i_2, \ldots, i_p) \text{ mit } \{i_1, \ldots, i_p\} = \{1, \ldots, p\}.$$

- Nach Voraussetzung hat f genau 2 nicht reelle Nullstellen, etwa α_{j_1} und α_{j_2} $(j_1, j_2 \in \{1, \ldots, p\},\ j_1 \neq j_2)$

Bezeichne K die Kpx. Konjugation.
$\Rightarrow K$ induziert Automorphismus von E über $\mathbb{Q}$, d.h.
$K \in \mathrm{Gal}(E/\mathbb{Q})$. Es gilt:

$$K(\alpha_{j_1}) = \alpha_{j_2} \text{ und } K(\alpha_{j_2}) = \alpha_{j_1}$$

(denn: mit α ist auch $\bar{\alpha}$ Nullstelle von f, $\alpha_{j_1}, \alpha_{j_2}$ sind

die einzigen nicht reellen Nullstellen von f.)

$\Rightarrow \forall i \in \{1,\dots,p\} \setminus \{j_1, j_2\}: \quad K(\alpha_i) = \alpha_i.$

$\Rightarrow \quad \pi_K = (j_1\, j_2) \qquad (\text{in } \mathcal{S}_p).$

- Wir können nun den p-Zyklus $\pi_c = (i_1,\dots,i_p)$ wegen

$$\{i_1,\dots,i_p\} = \{1,\dots,p\}$$

auch so umschreiben, dass er mit j_1 beginnt:

$$\pi_c = \{j_1,\dots\}$$

Mit Aufgabe 10.3 (ii) folgt dann aber

$$\langle \pi_K, \pi_c \rangle = \mathcal{S}_p$$

und da $K, c \in Gal(E/\mathbb{Q})$ erhalten wir

$$Gal(E/\mathbb{Q}) \simeq \mathcal{S}_p.$$

(ii) Nach Eisenstein mit $p=3$ ist

$$f(X) = X^5 - 6X + 3 \in \mathbb{Q}[X]$$

irreduzibel. Wir wollen (i) mit $p=5$ anwenden und müssen daher zeigen: f besitzt genau 3 reelle Nullstellen.

Es ist $f'(X) = 5X^4 - 6$.

$\overset{\text{2. Abl.}}{\Rightarrow}$ f hat in $-\sqrt[4]{\frac{6}{5}}$ lokales Maximum und in $+\sqrt[4]{\frac{6}{5}}$ lokales Minimum.

Für $|x| < \sqrt[4]{\frac{6}{5}}$ ist $f'(x) < 0$ und für

$|x| > \sqrt[4]{\frac{6}{5}}$ ist $f'(x) > 0$.

$\Rightarrow$ f ist für $x < -\sqrt[4]{\frac{6}{5}}$ streng monoton steigend,

für $-\sqrt[4]{\frac{6}{5}} < x < \sqrt[4]{\frac{6}{5}}$ streng monoton fallend,

für $\sqrt[4]{\frac{6}{5}} < x$ streng monoton steigend.

Wir berechnen:

$f(-2) = -17 < 0$

$f\left(-\sqrt[4]{\frac{6}{5}}\right) = \frac{24}{5} \cdot \sqrt[4]{\frac{6}{5}} + 3 > 0$

$f\left(\sqrt[4]{\frac{6}{5}}\right) = -\frac{24}{5} \cdot \sqrt[4]{\frac{6}{5}} + 3 < 0$

$f(2) = 23 > 0$

Mit dem Zwischenwertsatz folgt: f besitzt 3 reelle Nullstellen und wegen des oben ermittelten „Wachstumsverhaltens" sind dies alle reellen Nullstellen.

$\Rightarrow$ f besitzt genau 2 nicht reelle Nullstellen.

(ii)

$\Rightarrow$ $Gal(E/\mathbb{Q}) \simeq \mathcal{S}_5$ (Galoisgruppe von f).

11.2. $p \geq 5$, $f_p(X) = X^3(X-2)(X-4)\cdot\ldots\cdot(X-2(p-3)) - 2$.

- f_p ist irreduzibel nach Eisenstein mit $p=2$, denn:
  - f_p ist normiert, d.h. Bedingung an höchsten Koeffizienten ok.
  - Konstanter Term: -2, ok.
  - Jeder Term dazwischen enthält mindestens einen der Faktoren $-2, -4, \ldots, -2(p-3)$. ok.

- Schreibe $p = 2m+1$, dann: $2(p-3) = 2(2m-2)$

$$\Rightarrow f_p(X) = X^3 \prod_{j=1}^{2(m-1)} (X-2\cdot j) - 2 .$$

Für $K \in \{0, \ldots, m-1\}$ ist $2K \in \{0, 2, \ldots, 2m-2\}$ und daher für $x = 4K$ einer der Faktoren X^3 bzw. $(X-2j)$ gleich 0.

$$\Rightarrow f_p(4K) = -2 < 0 \quad \text{für } K \in \{0, \ldots, m-1\}$$

(d.h. an m verschiedenen Punkten).

Nun betrachten wir für $K \in \{0, \ldots, m-1\}$ die Zahl

$$x = 4K+1. \quad (\in \mathbb{Z}).$$

Es ist $X^3 \prod_{j=1}^{2(m-1)} (X-2j)$ für solches x eine Zahl aus $\mathbb{Z}$, für $K=0$ liefern die ersten (nach Voraussetzung $p \geq 5$, d.h. vorhandenen) Faktoren $(-2)\cdot(-4) = 8 > 2$, d.h.

die Zahl ist betraglich > 2. Für $K > 0$ liefert bereits X^3 einen Beitrag, der betraglich größer als 2 ist.

$\Rightarrow$ Für solche x ist in jedem Fall

$$\left| X^3 \prod_{j=1}^{2(m-1)} (X - 2j) \right| > 2.$$

Wir untersuchen das Vorzeichen der Zahl. Ist $K = 0$, d.h. $x = 1$, so ist das Vorzeichen von X^3 positiv und die Vorzeichen aller Faktoren $(X - 2j)$ sind negativ. Da wir insgesamt $2(m-1)$ also eine gerade Zahl solcher Vorzeichen haben, erhalten wir insgesamt eine positive Zahl > 2.

$\Rightarrow f(1) > 0$.

Gehen wir von K „einen Schritt weiter" zu $K+1$, so wird die Zahl x um 4 größer, d.h. zwischen

$$4K+1 \quad \text{und} \quad 4(K+1)+1$$

liegen zwei „zusätzliche" gerade Zahlen.

$\Rightarrow$ genau zwei der Faktoren $(X - 2j)$ ändern ihr Vorzeichen von negativ zu positiv

$\Rightarrow$ Insgesamt haben immernoch eine gerade Anzahl an Faktoren negatives Vorzeichen.

$\Rightarrow f_p(4(k+1)+1) > 0$.

Wir haben also induktiv gezeigt:

$f_p(4k+1) > 0$ für $k \in \{0, \dots, m-1\}$

(d.h. an m verschiedenen Punkten, die mit den vorherigen Punkten „verschränkt" sind).

- Wir haben nun insgesamt $2m$ Punkte gefunden, an denen f_p jeweils abwechselndes Vorzeichen besitzt.

Mit dem Zwischenwertsatz folgt daher: Es gibt $2m-1$ reelle Nullstellen

$$\alpha_1 < \dots < \alpha_{2m-1}.$$

Dies sind also

$$2m-1 = 2m+1-2 = p-2$$

reelle Nullstellen.

- Da $f_p(0) = f_p(2) = \dots = f_p(2(p-3)) = -2$ gilt, folgt mit dem Satz von Rolle:

f_p' hat in den offenen Intervallen

$$(0,2), (2,4), \dots, (2(p-4), 2(p-3))$$

jeweils eine Nullstelle, etwa

$$\beta_1 < \beta_2 < \dots < \beta_{p-3}.$$

Da f_p' wegen des Faktors X^3 in f im Nullpunkt weiter eine doppelte Nullstelle besitzt, haben wir wegen

$$\text{Grad } f_p' = p-1$$

alle Nullstellen von f_p' gefunden.

$\Rightarrow$ f_p' ändert in den Intervallen

$$(0,\beta_1),\ (\beta_1,\beta_2),\ \ldots,\ (\beta_{p-3},\infty)$$

sein Vorzeichen nicht und $\beta_1,\ldots,\beta_{p-3}$ sind Punkte, in denen f_p ein lokales Extremum annimmt

$\Rightarrow$ f_p ist in den Intervallen

$$(0,\beta_1),\ (\beta_1,\beta_2),\ \ldots,\ (\beta_{p-3},\infty)$$

streng monoton.

$\Rightarrow$ f_p kann im Intervall $(0,\infty)$ höchstens $p-2$ Nullstellen haben (gerade die, die wir gefunden haben.

Für $x<0$ ist aber

$$\underbrace{X^3}_{<0} \prod_{j=1}^{2(m-1)} \underbrace{(X-2j)}_{<0} \underbrace{-2}_{<0} \quad <0\ ,$$

d.h. $f_p(x)<0$ und offenbar $f_p(0)=-2<0$.

$\Rightarrow$ f_p besitzt genau $p-2$ reelle Nullstellen.

Wegen Grad $f_p = p$ besitzt f_p also genau 2 nicht reelle Nullstellen. Da wir zu Beginn die Irreduzibilität von f_p gezeigt hatten, ist Aufgabe 1 (i) anwendbar

$$\Rightarrow \quad \mathrm{Gal}(E/\mathbb{Q}) \simeq \gamma_p .$$

11.3. • Vorab: Ist K Körper mit $\chi(K) = 0$ und F/K Erweiterung vom Grad 2, so ist F/K Radikalerweiterung.

Dazu:

Es muss F/K einfach sein, also $F = K(\alpha)$ für $\alpha \in \overline{K}$ vom Grad 2.

$\Rightarrow \exists$ irreduzibles Polynom $f(X) = X^2 + aX + b \in K[X]$ mit $f(\alpha) = 0$.

Aber: Es ist

$$f(X) = \left(X + \frac{a}{2} + \frac{\sqrt{a^2-4b}}{2}\right)\left(X + \frac{a}{2} - \frac{\sqrt{a^2-4b}}{2}\right)$$

Für eine Nullstelle $\sqrt{a^2-4b}$ des Polynoms

$$X^2 - a^2 + 4b$$

ist also $\alpha = -\frac{a}{2} + \frac{\sqrt{a^2-4b}}{2}$ und daher

$$F = K(\alpha) = K\left(\sqrt{a^2-4b}\right),$$

d.h. F ist Radikalerweiterung.

• Damit zur Aufgabe. Nach 23.6. ist der Zerfällungskörper E von $X^{15} - 1$ Galoiserweiterung von $\mathbb{Q}$ vom Grad

$$\varphi(15) = \varphi(3)\varphi(5) = 2 \cdot 4 = 8$$

und mit

$\left(\mathbb{Z}/15\mathbb{Z}\right)^*$ als Galoisgruppe.

Ist nun K ein Zwischenkörper $\mathbb{Q} \subset K \subset E$, so ist nach dem Hauptsatz der Galoistheorie

$U := \mathrm{Gal}(E/K)$ Untergruppe von $\left(\mathbb{Z}/15\mathbb{Z}\right)^*$.

Wegen $\mathrm{ord}\left(\mathbb{Z}/15\mathbb{Z}\right)^* = 8$ haben wir 4 Fälle zu unterscheiden: $\mathrm{ord}\, U \in \{1, 2, 4, 8\}$.

- Ist $\mathrm{ord}\, U = 8 \overset{\text{HS}}{\Rightarrow} K = \mathbb{Q} = \mathbb{Q}(1)$
  und 1 ist Nullstelle von $X - 1$.
  $\Rightarrow$ K Radikalerweiterung.
- Ist $\mathrm{ord}\, U = 1 \overset{\text{HS}}{\Rightarrow} K = E = \mathbb{Q}(\zeta_{15})$ für primitive 15-te Einheitswurzel ζ_{15}, d.h. Nullstelle von $X^{15} - 1$.
  $\Rightarrow$ K Radikalerweiterung
- Ist $\mathrm{ord}\, U = 4 \Rightarrow [E : K] = 4 \Rightarrow [K : \mathbb{Q}] = 2$.
  $\Rightarrow$ K Radikalerweiterung nach Vorüberlegung.
- Ist $\mathrm{ord}\, U = 2 \Rightarrow [E : K] = 2 \Rightarrow [K : \mathbb{Q}] = 4$
  $\left(\mathbb{Z}/15\mathbb{Z}\right)^*$ abelsch $\Rightarrow$ $U \triangleleft \left(\mathbb{Z}/15\mathbb{Z}\right)^*$ und

damit: $K/\mathbb{Q}$ Galoiserweiterung mit

$$Gal(K/\mathbb{Q}) \simeq (\mathbb{Z}/15\mathbb{Z})^* / U \qquad \text{(Hauptsatz!)}$$

Es hat $Gal(K/\mathbb{Q})$ die Ordnung $4 = 2^2$, also gibt es gemäß der Sylowsätze eine Untergruppe $U_1 < Gal(K/\mathbb{Q})$ der Ordnung 2, welche (Hauptsatz) zu einem Zwischen-Körper $\mathbb{Q} \subset K_1 \subset K$ mit $[K_1 : \mathbb{Q}] = 2$ und damit auch

$$[K : K_1] = 2$$

Anlass gibt. Nach der Vorüberlegung sind dann

$$K/K_1 \text{ und } K_1/\mathbb{Q}$$

Radikalerweiterungen und damit (vgl. Definition!) auch

$$K/\mathbb{Q}.$$

∎

11.4. • Wie in Aufgab 3 gilt:

E hat als Zerfällungskörper von X^7-1 über $\mathbb{Q}$ den Grad $\varphi(7)=6$ und

$$Gal(E/\mathbb{Q}) \simeq \left(\frac{\mathbb{Z}}{7\mathbb{Z}}\right)^*.$$

7 ist Primzahl $\Rightarrow$ $\frac{\mathbb{Z}}{7\mathbb{Z}}$ ist ein Körper und $\left(\frac{\mathbb{Z}}{7\mathbb{Z}}\right)^*$ seine Einheitengruppe.

$\Rightarrow$ $ord\left(\frac{\mathbb{Z}}{7\mathbb{Z}}\right)^* = 6$, $\left(\frac{\mathbb{Z}}{7\mathbb{Z}}\right)^*$ ist zyklisch.

$\Rightarrow$ es gibt (genau) eine Untergruppe $U_2 < \left(\frac{\mathbb{Z}}{7\mathbb{Z}}\right)^*$ der Ordnung 2.

Bezeichne K den zugehörigen Fixkörper, also

$$\mathbb{Q} \subset K \subset E.$$

$\Rightarrow$ $[E:K]=2$, d.h. $[K:\mathbb{Q}]=3$.

• Wir zeigen, dass $K/\mathbb{Q}$ keine Radikalerweiterung ist.

↗ $K/\mathbb{Q}$ wäre Radikalerweiterung.

$\Rightarrow$ $K=\mathbb{Q}(\alpha)$ für eine Nullstelle α eines Polynoms

$$X^n - a \in \mathbb{Q}[X].$$

Sei ζ eine primitive n-te Einheitswurzel

$\Rightarrow$ Die Nullstellen von $X^n - a$ sind

$$\alpha \zeta^v \quad \text{für} \quad v \in \{0, \dots, n-1\} \qquad (*)$$

Wegen $K = \mathbb{Q}(\alpha)$ und $[K : \mathbb{Q}] = 3$, hat α den Grad 3 über $\mathbb{Q}$. Sei $f_\alpha(X) \in \mathbb{Q}[X]$ das Minimalpolynom von α über $\mathbb{Q}$. $\Rightarrow$ Grad $f_\alpha = 3$.
Nach Konstruktion haben wir

$$f_\alpha(X) \mid X^n - a$$

$\Rightarrow$ Als Nullstellen von f_α kommen außer α nur zwei der Zahlen aus $(*)$ in Frage, etwa

$$\alpha \zeta^{v_1}, \ \alpha \zeta^{v_2} \quad \text{für gewisse } v_1, v_2 \in \{1, \dots, n-1\}.$$

Da $(\mathbb{Z}/7\mathbb{Z})^* \cong \mathrm{Gal}(E/\mathbb{Q})$ zyklisch und damit abelsch ist, ist die Untergruppe U ein Normalteiler.

Hauptsatz $\Rightarrow$ Die Erweiterung $K/\mathbb{Q}$ ist normal.

$\Rightarrow$ Da f_α irreduzibel ist und eine Nullstelle $\alpha \in K$ besitzt, müssen bereits alle Nullstellen von f_α in K liegen.

$\Rightarrow$ $\alpha \zeta^{v_1}, \alpha \zeta^{v_2} \in K$ und $f_\alpha(X) = (X - \alpha)(X - \alpha\zeta^{v_1})(X - \alpha\zeta^{v_2})$.
Insbesondere folgt: $\zeta^{v_1}, \zeta^{v_2} \in K$.

Da $[K:\mathbb{Q}]=3$ gilt, haben ζ^{v_1} und ζ^{v_2} über $\mathbb{Q}$ den Grad 1 oder 3.

Einheitswurzeln vom Grad 1 sind aber genau ± 1.

Da $\alpha, \alpha\zeta^{v_1}, \alpha\zeta^{v_2}$ verschieden sind, folgt:

Mindestens eine der Zahlen ζ^{v_1}, ζ^{v_2} hat über $\mathbb{Q}$ den Grad 3, OE sei dies ζ^{v_1}.

Für $m \in \mathbb{N}$ gilt allgemein nach Vorlesung: Jede primitive m-te Einheitswurzel η hat über $\mathbb{Q}$ den Grad $\varphi(m)$.

Wir haben also: Für geeignetes $m \in \mathbb{N}$ ist ζ^{v_1} eine primitive m-te Einheitswurzel mit Grad

$$\varphi(m) = 3.$$

$\Rightarrow$ Insbesondere gilt $\varphi(m)=3$ für ein geeignetes m.

Schreiben wir $m = p_1^{b_1} \cdot \ldots \cdot p_r^{b_r}$ (Primfaktorzerlegung), dann:

$$3 = \varphi(m) = p_1^{b_1-1}(p_1-1) \cdot \ldots \cdot p_r^{b_r-1}(p_r-1) \neq 3 \quad \lightning$$

$\Rightarrow$ $K/\mathbb{Q}$ ist keine Radikalerweiterung.

∎