Algebra II, SoSe 2012 – Lösung Blatt 4

4.1. Seien $\beta_1, \dots, \beta_n \in \mathbb{C}$ die Nullstellen von f. Dann:

$$E = \mathbb{Q}(\beta_1, \dots, \beta_n)$$

Wir betrachten irgendeine Nullstelle β_i von f. Zu zeigen:

$$E = \mathbb{Q}(\beta_i).$$

Als Zerfällungskörper von f ist $E/\mathbb{Q}$ eine endliche, normale Erweiterung. Da $\chi(\mathbb{Q}) = 0$ gilt, ist $E/\mathbb{Q}$ auch separabel und damit Galoiserweiterung. Wegen

$$\mathbb{Q} \subset \mathbb{Q}(\beta_i) \subset E$$

ist damit auch $E/\mathbb{Q}(\beta_i)$ eine Galoiserweiterung mit

$$Gal(E/\mathbb{Q}(\beta_i)) < Gal(E/\mathbb{Q}).$$

Da $Gal(E/\mathbb{Q})$ nach Voraussetzung abelsch ist, ist $Gal(E/\mathbb{Q}(\beta_i))$ sogar ein Normalteiler in $Gal(E/\mathbb{Q})$. Mit dem Hauptsatz der Galoistheorie folgt:

$$\mathbb{Q}(\beta_i)/\mathbb{Q} \text{ ist normale Erweiterung.}$$

$f(\beta_i)=0$, f irreduzibel $\Rightarrow$ f zerfällt in $\mathbb{Q}(\beta_i)$ vollständig in Linearfaktoren

$\Rightarrow$ Alle Nullstellen von f liegen in $\mathbb{Q}(\beta_i)$

$\Rightarrow$ $E = \mathbb{Q}(\beta_1, \dots, \beta_n) \subset \mathbb{Q}(\beta_i)$

$\Rightarrow$ $E = \mathbb{Q}(\beta_i)$.

∎

4.2. (i) • E ist als Zerfällungskörper der Familie

$$\{X^2-2,\ X^2-3,\ X^2-5\} \subset \mathbb{Q}[X]$$

normal über $\mathbb{Q}$. Da $\chi(\mathbb{Q}) = 0$ gilt, ist $E/\mathbb{Q}$ separabel.

$\Rightarrow$ $E/\mathbb{Q}$ Galoiserweiterung.

• Berechnen der Galoisgruppe: (Argument ist in dieser Ausführlichkeit nicht verlangt)

$$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = \deg(X^2-2) = 2.$$

Es ist $\sqrt{3} \notin \mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\}$, da sonst:

$$\sqrt{3} = a + b\sqrt{2} \quad \text{für gewisse } a,b \in \mathbb{Q}.$$

$\Rightarrow$ $b \neq 0$ (sonst: $\sqrt{3} \in \mathbb{Q}$ ↯) und

$a \neq 0$ (sonst: $\sqrt{\frac{3}{2}} = b \in \mathbb{Q}$ ↯)

$$\Rightarrow 3 = a^2 + 2ab\sqrt{2} + 2b^2$$

$$\Rightarrow \sqrt{2} = \frac{3-a^2-2b^2}{2ab} \in \mathbb{Q} \quad \text{↯}$$

Damit erhalten wir:

• $\mathbb{Q}(\sqrt{2}) \cap \mathbb{Q}(\sqrt{3}) = \mathbb{Q}$ und damit, da $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ Galoiserweiterungen sind (mit Vorlesung):

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}) \simeq \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\sqrt{3})/\mathbb{Q})$$

- $X^2 - 3 \in \mathbb{Q}(\sqrt{2})[X]$ ist Minimalpolynom von $\sqrt{3}$ über $\mathbb{Q}(\sqrt{2})$, d.h.

$$[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$$
$$= 2 \cdot 2 = 4$$

Nun ist $\sqrt{5} \notin \mathbb{Q}(\sqrt{2},\sqrt{3})$. Damit folgt analog wie eben:

- $[\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5}) : \mathbb{Q}] = 2 \cdot 4 = 8$
- $Gal(\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})/\mathbb{Q})$

$$\simeq Gal(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}) \times Gal(\mathbb{Q}(\sqrt{5})/\mathbb{Q})$$
$$\overset{s.o.}{\simeq} Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \times Gal(\mathbb{Q}(\sqrt{3}):\mathbb{Q}) \times Gal(\mathbb{Q}(\sqrt{5})/\mathbb{Q})$$
$$\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}. \qquad (*)$$

Ein Automorphismus aus $Gal(E/\mathbb{Q})$ wird durch sein Verhalten auf $\sqrt{2}$, $\sqrt{3}$ und $\sqrt{5}$ eindeutig bestimmt.
Wir betrachten $\eta, \sigma, \tau \in Gal(E/\mathbb{Q})$, definiert durch

$$\eta: \sqrt{2} \mapsto -\sqrt{2},\ \sqrt{3} \mapsto \sqrt{3},\ \sqrt{5} \mapsto \sqrt{5}$$
$$\sigma: \sqrt{2} \mapsto \sqrt{2},\ \sqrt{3} \mapsto -\sqrt{3},\ \sqrt{5} \mapsto \sqrt{5}$$
$$\tau: \sqrt{2} \mapsto \sqrt{2},\ \sqrt{3} \mapsto \sqrt{3},\ \sqrt{5} \mapsto -\sqrt{5}$$

Dann (nach Einschränken):

$$Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{id, \eta\}$$

$Gal(\mathbb{Q}(\sqrt{3})/\mathbb{Q}) = \{id, \sigma\}$

$Gal(\mathbb{Q}(\sqrt{5})/\mathbb{Q}) = \{id, \tau\}$

Mit obigen Überlegungen folgt also:

$Gal(E/\mathbb{Q}) = \{id, \eta, \sigma, \tau, \eta\sigma, \eta\tau, \sigma\tau, \eta\sigma\tau\}$.

(beachte: $Gal(E/\mathbb{Q})$ abelsch wegen (*), d.h. $\eta\sigma = \sigma\eta$, etc.)

(ii) • Jedes von id verschiedene Element in $Gal(E/\mathbb{Q})$ hat die Ordnung 2 (wegen (*)).

$\Rightarrow$ Untergruppen der Ordnung 2:

$\{id, \eta\}$, $\{id, \sigma\}$, $\{id, \tau\}$, $\{id, \eta\sigma\}$, $\{id, \eta\tau\}$, $\{id, \sigma\tau\}$, $\{id, \eta\sigma\tau\}$

$\rightsquigarrow$ 7 solche Untergruppen.

• Untergruppen der Ordnung 4:

$\{id, \eta, \sigma, \eta\sigma\}$, $\{id, \eta, \tau, \eta\tau\}$, $\{id, \sigma, \tau, \sigma\tau\}$, $\{id, \eta\sigma, \eta\tau, \sigma\tau\}$

$\{id, \eta, \sigma\tau, \eta\sigma\tau\}$, $\{id, \sigma, \eta\tau, \eta\sigma\tau\}$, $\{id, \tau, \eta\sigma, \eta\sigma\tau\}$

$\rightsquigarrow$ 7 solche Untergruppen.

• Außerdem haben wir die trivialen Untergruppen

$\{id\}$ und $Gal(E/\mathbb{Q})$.

$\Rightarrow$ Haben 16 Untergruppen $\Rightarrow$ Es gibt 16 Zwischenkörper.

- Klar:

$$\{id\} \longleftrightarrow \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$$

$$Gal(E/\mathbb{Q}) \longleftrightarrow \mathbb{Q}.$$

Für die anderen Zwischenkörper bemerken wir:

Elemente in $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ haben eindeutige Darstellung

$$a_0 + a_1\sqrt{2} + a_2\sqrt{3} + a_3\sqrt{5} + a_4\sqrt{6} + a_5\sqrt{10} + a_6\sqrt{15} + a_7\sqrt{30}.$$

Beispiel: η lässt $\sqrt{3}$ und $\sqrt{5}$ fest.

$$\Rightarrow \{id, \eta\} \longleftrightarrow \mathbb{Q}(\sqrt{3}, \sqrt{5}).$$

Analog überlegt man sich (durch Untersuchen des Verhaltens der entsprechenden „verknüpften" Automorphismen):

$$\{id, \sigma\} \longleftrightarrow \mathbb{Q}(\sqrt{2}, \sqrt{5})$$

$$\{id, \tau\} \longleftrightarrow \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

$$\{id, \eta\sigma\} \longleftrightarrow \mathbb{Q}(\sqrt{5}, \sqrt{6})$$

$$\left(\eta\sigma(\sqrt{5}) = \sqrt{5},\ \eta\sigma(\sqrt{2}\sqrt{3}) = \eta\sigma(\sqrt{2})\,\eta\sigma(\sqrt{3}) = (-\sqrt{2})\cdot(-\sqrt{3}) = \sqrt{6},\ \ldots\right)$$

$$\{id, \eta\tau\} \longleftrightarrow \mathbb{Q}(\sqrt{3}, \sqrt{10})$$

$$\{id, \sigma\tau\} \longleftrightarrow \mathbb{Q}(\sqrt{2}, \sqrt{15})$$

$\{id, \eta\sigma\tau\} \longleftrightarrow \mathbb{Q}(\sqrt{6}, \sqrt{10}) = \mathbb{Q}(\sqrt{6}, \sqrt{15}) = \mathbb{Q}(\sqrt{10}, \sqrt{15})$

Die Untergruppen der Ordnung 4 liefern:

$\{id, \eta, \sigma, \eta\sigma\} \longleftrightarrow \mathbb{Q}(\sqrt{5})$

$\{id, \eta, \tau, \eta\tau\} \longleftrightarrow \mathbb{Q}(\sqrt{3})$

$\{id, \sigma, \tau, \sigma\tau\} \longleftrightarrow \mathbb{Q}(\sqrt{2})$

$\{id, \eta, \sigma\tau, \eta\sigma\tau\} \longleftrightarrow \mathbb{Q}(\sqrt{15})$

$\{id, \sigma, \eta\tau, \eta\sigma\tau\} \longleftrightarrow \mathbb{Q}(\sqrt{10})$

$\{id, \tau, \eta\sigma, \eta\sigma\tau\} \longleftrightarrow \mathbb{Q}(\sqrt{6})$.

$\{id, \eta\sigma, \eta\tau, \sigma\tau\} \longleftrightarrow \mathbb{Q}(\sqrt{30})$.

4.3. $a \in \mathbb{Z}$, $f_a(X) = X^3 + aX^2 + (a-3)X - 1 \in \mathbb{Q}[X]$.

(i) Es ist sogar $f_a(X) \in \mathbb{Z}[X]$ ein normiertes Polynom.

↗ $q \in \mathbb{Q}$ ist Nullstelle von f_a. Dann:

$$f_a(X) = (X-q) \cdot g \quad \text{für ein } g \in \mathbb{Q}[X] \text{ normiert.}$$

Gauß'sches Lemma $\Rightarrow$ $(X-q)$ und g liegen in $\mathbb{Z}[X]$.

$\Rightarrow$ $q \in \mathbb{Z}$

Nach Vieta gilt dann $q \mid -1$ und damit $q \in \{-1, 1\}$.

Aber:
$$f_a(1) = 1 + a + a - 3 - 1 = 2a - 3 \neq 0 \text{ da } a \in \mathbb{Z}.$$
$$f_a(-1) = -1 + a - a + 3 - 1 = 1 \neq 0. \quad \lightning$$

Also besitzt f_a keine rationalen Nullstellen.

(ii) Sei α eine Nullstelle von f_a, also $f_a(\alpha) = 0$.

Nach (i) ist $\alpha \neq -1$, d.h. $(1+\alpha) \neq 0$. Um Brüche zu vermeiden, berechnen wir:

$$(1+\alpha)^3 \cdot f_a\left(-\frac{1}{1+\alpha}\right) = (1+\alpha)^3 \left(-\frac{1}{(1+\alpha)^3} + a \cdot \frac{1}{(1+\alpha)^2} - (a-3)\frac{1}{1+\alpha} - 1\right)$$

$$= -1 + a(1+\alpha) - (a-3)(1+\alpha)^2 - (1+\alpha)^3$$

ausrechnen...

$$= -1 + a + a\alpha - a - 2a\alpha - a\alpha^2 + 3 + 6\alpha + 3\alpha^2 - 1 - 3\alpha^2 - 3\alpha - \alpha^3$$

$$= 1 - a\alpha - a\alpha^2 + 3\alpha - \alpha^3$$

$$= -\left(\alpha^3 + a\alpha^2 + (a-3)\alpha - 1\right)$$

$$= -f_a(\alpha)$$

$$= 0$$

$$\Rightarrow f_a\left(-\frac{1}{1+\alpha}\right) = 0 \qquad \text{ok.}$$

(iii) Zunächst ist $-\frac{1}{1+x} \neq 0 \quad \forall\, x \in \mathbb{R}\setminus\{0,-1\}$.

$$-\frac{1}{1+x} = -1 \iff 1+x = 1 \iff x = 0.$$

$$\Rightarrow \varphi : \mathbb{R}\setminus\{0,-1\} \to \mathbb{R}\setminus\{0,-1\},\ x \mapsto -\frac{1}{1+x}$$

ist wohldefiniert.

- φ ist injektiv, denn:

$$-\frac{1}{1+x} = -\frac{1}{1+y} \iff 1+x = 1+y \iff x = y.$$

- φ ist surjektiv, denn sei $y \in \mathbb{R}\setminus\{0,-1\}$. Definiere

$$x := -\frac{1+y}{y}$$

↗ $x = 0$, dann: $1+y = 0 \Rightarrow y = -1$ ↯

↗ $x = -1$, dann: $-1 = -\frac{1+y}{y} \Rightarrow y = 1+y$ ↯

$\Rightarrow x \in \mathbb{R}\setminus\{0,-1\}$ und

$$\varphi(x) = -\frac{1}{1-\frac{1+y}{y}} = -\frac{1}{\frac{y-1-y}{y}} = y.$$

- φ ist fixpunktfrei, denn:

$$\varphi(x) = x \iff x = -\frac{1}{1+x} \iff x(1+x) = -1$$

$$\iff x^2 + x + 1 = 0$$

$$\iff x^2 + 2\cdot\frac{1}{2}x + \left(\frac{1}{2}\right)^2 - \frac{1}{4} + 1 = 0$$

$$\iff \left(x + \frac{1}{2}\right)^2 + \frac{3}{4} = 0$$

$$\iff \left(x + \frac{1}{2}\right)^2 - \left(i\frac{\sqrt{3}}{2}\right)^2 = 0$$

$$\iff \left(x + \frac{1}{2} - i\frac{\sqrt{3}}{2}\right)\left(x + \frac{1}{2} + i\frac{\sqrt{3}}{2}\right) = 0 \quad \lightning_{x \in \mathbb{R}\setminus\{0,-1\}}.$$

- $\varphi(x) = -\frac{1}{1+x}$.

$$\Rightarrow \varphi^2(x) = -\frac{1}{1-\frac{1}{1+x}} = -\frac{1}{\frac{1+x-1}{1+x}} = -\frac{1+x}{x}$$

$$\Rightarrow \varphi^3(x) = -\frac{1}{1-\frac{1+x}{x}} = -\frac{1}{\frac{x-1-x}{x}} = x$$

$$\Rightarrow \varphi^3 = \mathrm{id}.$$

Damit sind alle Behauptungen nachgewiesen.

(iv) Es ist $\deg f_a = 3$

$\overset{\text{Analysis}}{\Rightarrow}$ f_a besitzt eine reelle Nullstelle $\alpha \in \mathbb{R}$.

(i) $\Rightarrow$ $\alpha \in \mathbb{R}\setminus\{0,-1\}$

$\overset{\text{(ii),(iii)}}{\Rightarrow}$ $-\frac{1}{1+\alpha} \in \mathbb{Q}(\alpha)$ ist eine weitere, von α verschiedene Nullstelle von f_a.

$\Rightarrow$ f_a zerfällt in $\mathbb{Q}(\alpha)$ in Linearfaktoren, d.h.

$$E = \mathbb{Q}(\alpha) \qquad (*)$$

und als endliche, normale und separable ($\chi(\mathbb{Q})=0$) Erweiterung, ist $\mathbb{Q}(\alpha)/\mathbb{Q}$ eine Galoiserweiterung.

Wegen (i) spaltet sich in $\mathbb{Q}[X]$ kein Linearfaktor von f_a ab. $\overset{\deg f_a = 3}{\Rightarrow}$ $f_a \in \mathbb{Q}[X]$ ist irreduzibel.

$\Rightarrow$ f_a ist das Minimalpolynom von α über $\mathbb{Q}$, d.h.

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3.$$

$\overset{\text{VL}}{\Rightarrow}$ $\#\,\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) \overset{\text{Galoiserweiterung!}}{=} [\mathbb{Q}(\alpha) : \mathbb{Q}] = 3.$

$\overset{\text{Algebra I}}{\Rightarrow}$ $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ ist zyklisch von der Ordnung 3. $(**)$

Insgesamt folgt aus $(*)$ und $(**)$:

$$\mathrm{Gal}(E/\mathbb{Q}) \simeq \left(\mathbb{Z}/3\mathbb{Z}, +\right)$$

$\square$

4.4. Es ist $\mathbb{F}_3 = \{0,1,2\}$ mit

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

und

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

(i) $f(X) = X^3 - X + 1 \in \mathbb{F}_3[X]$ reduzibel

$\overset{\deg f = 3}{\Rightarrow}$ Es spaltet sich ein Linearfaktor ab.

$\Rightarrow$ f besitzt in $\mathbb{F}_3$ eine Nullstelle.

Aber: $f(0) = 1 \neq 0$

$f(1) = 1^3 - 1 + 1 = 1 \neq 0$

$f(2) = \underbrace{2^3}_{=1\cdot 2} - 2 + 1 = 1 \neq 0$ ↯

$\Rightarrow f \in \mathbb{F}_3[X]$ ist irreduzibel.

(ii) Ist α eine Nullstelle von f in einem Erweiterungs-Körper von $\mathbb{F}_3$, dann:

$$f(\alpha+1) = (\alpha+1)^3 - (\alpha+1) + 1$$

$$\overset{\text{Frobenius}}{=} \alpha^3 + 1 - \alpha - 1 + 1$$

$$= \alpha^3 - \alpha + 1$$

$$= f(\alpha)$$

$$= 0 \qquad \Rightarrow \alpha+1 \text{ ist Nullstelle}$$

und:

$$f(\alpha+2) = (\alpha+2)^3 - (\alpha+2) + 1$$

$$= \alpha^3 + \underbrace{2^3}_{=2} - \alpha - 2 + 1$$

$$= \alpha^3 - \alpha + 1$$

$$= f(\alpha)$$

$$= 0 \qquad \Rightarrow \alpha+2 \text{ ist Nullstelle.}$$

f ist irreduzibel $\Rightarrow L = \mathbb{F}_3[X]/(f)$ ist ein Erweiterungs-Körper von $\mathbb{F}_3$ und (Verfahren von Kronecker!)

$\overline{X} \in L$ ist eine Nullstelle von f.

$\overset{\text{s.o.}}{\Rightarrow}$ $\overline{X}$, $\overline{X}+1$, $\overline{X}+2 \in L$ sind 3 verschiedene Nullstellen von f, d.h. f zerfällt in L in (irreduzible) Linear-faktoren:

$$f(Z) = (Z - \overline{X})(Z - (\overline{X}+1))(Z - (\overline{X}+2)).$$

(iii) Es ist $L = \mathbb{F}_3(\overline{X})$ und f ist das Minimalpolynom von $\overline{X}$ über $\mathbb{F}_3$.

$\Rightarrow [L : \mathbb{F}_3] = 3$. $\Rightarrow$ Als Vektorraum ist $L \simeq (\mathbb{F}_3)^3$

Wegen $\#\mathbb{F}_3 = 3$ folgt: $\#L = 3^3 = 27 \Rightarrow \#L^* = 26$.

Wir suchen also in L^* ein Element der Ordnung 26.

Beachte: Wegen $26 = 2 \cdot 13$ hat nach Lagrange jedes Element in L^* eine Ordnung aus $\{1, 2, 13, 26\}$.

Wir versuchen es mit $\overline{X} \in L^*$ und berechnen Potenzen:

$\overline{X}$, $\overline{X}^2$ nicht zu vereinfachen $\Rightarrow \operatorname{ord} \overline{X} \in \{13, 26\}$.

Da $f(\overline{X}) = 0$ gilt, ist $\overline{X}^3 - \overline{X} + 1 = 0$, d.h.

$$\overline{X}^3 = \overline{X} - 1 = \overline{X} + 2.$$

Damit:

$$\overline{X}^4 = \overline{X}^2 + 2\overline{X}$$

$$\overline{X}^5 = \overline{X}^3 + 2\overline{X}^2 = 2\overline{X}^2 + \overline{X} + 2$$

$$\overline{X}^{10} = \overline{X}^5 \cdot \overline{X}^5 = (2\overline{X}^2 + \overline{X} + 2)(2\overline{X}^2 + \overline{X} + 2)$$

$$= \underbrace{2 \cdot 2}_{=1} \overline{X}^4 + \underbrace{(2+2)}_{=1} \overline{X}^3 + \underbrace{(2 \cdot 2 + 2 \cdot 2 + 1)}_{=0} \overline{X}^2 + \underbrace{(2+2)}_{=1} \overline{X} + \underbrace{2 \cdot 2}_{=1}$$

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

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

$$= \overline{X}^2 + \overline{X}$$

$$\overline{X}^{13} = \overline{X}^{10} \cdot \overline{X}^3 = (\overline{X}^2 + \overline{X})(\overline{X} + 2) = \overline{X}^3 + (2+1)\overline{X}^2 + 2\overline{X}$$

$$= \overline{X}^3 + 2\overline{X} = \overline{X} + 2 + 2\overline{X}$$

$$= 2 \neq 1$$

$\Rightarrow \operatorname{ord} \overline{x} \neq 13$, d.h. $\operatorname{ord} \overline{x} = 26$ und damit:

$$L^* = \langle \overline{x} \rangle .$$

Tatsächlich berechnen wir:

$$\overline{x}^{26} = (\overline{x}^{13})^2 = 2 \cdot 2 = 1 .$$