Abgabe Algebra I, Blatt 09

Studierende(r): Weerts, Steffen, steffen.weerts@uni-oldenburg.de

Aufgabe 9.1

(a) Sei p eine Primzahl, $F_p := \sum_{i=0}^{p-1} t^i \in \mathbb{Q}[t]$ und $\zeta_p := e^{\frac{2\pi i}{p}}$.
Zu zeigen: F_p ist Minimalpolynom von ζ_p über $\mathbb{Q}$.
Es gilt:

$$\left(e^{\frac{2\pi i}{p}}\right)^p = e^{2\pi i} = 1.$$

$$\implies \text{ für } h := t^p - 1 \text{ gilt } h(\zeta_p) = 0.$$

Da jedoch h nicht irreduzibel ist, ist h nicht das Minimalpolynom von ζ_p über $\mathbb{Q}$. Es gilt:

$$\begin{aligned} t^p - 1 &= (t-1)(t^{p-1} + t^{p-2} + \cdots + t^2 + t + 1) \\ &= \sum_{i=0}^{p-1} t^i = (t-1) \cdot F_p. \end{aligned}$$

$$\implies e^{\frac{2\pi i}{p}} - 1 = 0 \text{ oder } F_p/e^{\frac{2\pi i}{p}} = 0.$$

Da $e^{\frac{2\pi i}{p}} - 1 = 0 \iff p = 1$, kann $e^{\frac{2\pi i}{p}} - 1 \neq 0$, denn p ist Primzahl und damit nicht 1. Folglich muss $F_p(\zeta_p) = 0$ gelten.
Zu zeigen: F_p ist irreduzibel.
Es gilt:

$$F_p = \sum_{i=0}^{p-1} t^i$$

$$\implies F_p \text{ konstant } \iff p = 1$$

$$\overset{p \text{ Primzahl}}{\implies} F_p \text{ nicht konstant.}$$

Sei $a := 1 \in \mathbb{Q}$. Es gilt:

$$\begin{aligned} F_p(t+1) &= \sum_{i=0}^{p-1} (t+1)^i \\ &= (t+1)^{p-1} + (t+1)^{p-2} + \cdots + (t+1)^2 + (t+1)^1 + (t+1)^0 \\ &= \sum_{i=0}^{p-1} \binom{p-1}{i} \cdot t^{p-1-i} \cdot 1^i + \sum_{i=0}^{p-2} \binom{p-2}{i} \cdot t^{p-2-i} \cdot 1^i + \cdots \\ &\quad + \sum_{i=0}^{2} \binom{2}{i} \cdot t^{2-i} \cdot 1^i + \sum_{i=0}^{1} \binom{1}{i} \cdot t^{1-i} \cdot 1^i + \sum_{i=0}^{01} \binom{0}{i} \cdot t^{0-i} \cdot 1^i \end{aligned}$$

$$= \sum_{i=0}^{p-1} \left(\sum_{j=0}^{i} \binom{i}{j} \cdot t^{i-j} \right)$$

Die Koeffizienten der einzelnen Summen (für $n \in \{0, \cdots, p-1\}$)) finden sich als Zeilen im Pascalschen Dreieck, wobei die Koeffizienten mit gleicher Potenz von t auf einer Spalte (von rechts oben nach links unten) liegen. Diese Summe kann man also als Summe der Spalten bis zur Zeile $p-1$ auffassen. Diese ist:

$$\sum_{i=0}^{p-1} \left(t^i \cdot \sum_{j=0}^{p-1} \binom{j}{i} \right) = \sum_{i=0}^{p-1} \left(t^i \cdot \sum_{j=i}^{p-1} \binom{j}{i} \right).$$

Nach (A1) (siehe Anhang) gilt:

$$\sum_{i=0}^{p-1} \left(t^i \cdot \sum_{j=i}^{p-1} \binom{j}{i} \right) \overset{\text{A1}}{=} \sum_{i=0}^{p-1} \binom{p}{i+1} \cdot t^i =: f$$

Nun gilt:

(i) $p \nmid \binom{p}{(p-1)+1} = 1 = \mathrm{LC}(F_p)$,

(ii) $p \overset{(A2)}{\mid} \binom{p}{i+1} = a_i \qquad \forall i = 0, \cdots, p-2$,

(iii) $p^2 \nmid \binom{p}{1} = p = a_0$.

$$\overset{\text{Eisenstein}}{\Longrightarrow} F_p \text{ Minimalpolynom von } \zeta_p \text{ über } \mathbb{Q}.$$

Zu zeigen: $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$ und $(1, \zeta_p, \zeta_p^2, \cdots, \zeta_p^{p-2})$ ist Basis von $\mathbb{Q}(\zeta_p)$.
Es gilt:

$$\begin{aligned} & \zeta_p \text{ ist algebraisch über } \mathbb{Q} \\ \overset{6.2.9}{\Longrightarrow} \; & [\mathbb{Q}(\zeta_p) : \mathbb{Q}] = \deg(F_p) = p - 1 \text{ und } (1, \zeta_p, \zeta_p^2, \cdots, \zeta_p^{p-2}) \text{ ist Basis von } \mathbb{Q}(\zeta_p). \end{aligned}$$

Zu zeigen: Alle Nullstellen von F_p liegen in $\mathbb{Q}(\zeta_p)$.
Fehlt.

"$\square$"

(b) (i) Sei $f_1 = t^4 - 5 \in \mathbb{Q}[t]$.
Es gilt:

$$\begin{aligned} f_1 &= t^4 - 5 \\ &= (t^2 + \sqrt{5})(t^2 - \sqrt{5}) \\ &= (t + \sqrt[4]{5}i)(t - \sqrt[4]{5}i)(t + \sqrt[4]{5})(t - \sqrt[4]{5}) \end{aligned}$$

Da $\pm\sqrt[4]{5}, \pm\sqrt[4]{5}i \in \mathbb{Q}(\sqrt[4]{5}, i)$, zerfällt f_q über $\mathbb{Q}(\sqrt[4]{5}, i)$.

Zu zeigen: $[\mathbb{Q}(\sqrt[4]{5}, i) : \mathbb{Q}(\sqrt[4]{5})] = 2$.
Da $f_{i,\mathbb{Q}(\sqrt[4]{5})} = t^2 + 1$, ist $[\mathbb{Q}(\sqrt[4]{5}, i) : \mathbb{Q}(\sqrt[4]{5})] = \deg(f_{i,\mathbb{Q}(\sqrt[4]{5})}) = 2$.

Zu zeigen: $[\mathbb{Q}(\sqrt[4]{5}) : \mathbb{Q}] = 4$.
Angenommen, $\deg(f_{\sqrt[4]{5},\mathbb{Q}}) = 1$.
Es gilt:

$$\begin{aligned} f_{\sqrt[4]{5},\mathbb{Q}}(\sqrt[4]{5}) &= \sqrt[4]{5} + a_0 \overset{!}{=} 0 \\ \implies &\ a_0 = -\sqrt[4]{5} \notin \mathbb{Q} \\ \implies &\ \deg(f_{\sqrt[4]{5},\mathbb{Q}}) \neq 1. \end{aligned}$$

Angenommen, $\deg(f_{\sqrt[4]{5},\mathbb{Q}}) = 2$.
Es gilt:

$$\begin{aligned} f_{\sqrt[4]{5},\mathbb{Q}}(\sqrt[4]{5}) &= \sqrt[4]{5}^2 + a_1\sqrt[4]{5} + a_0 \overset{!}{=} 0 \\ \implies &\ a_0 = -\sqrt{5} - a_1\sqrt[4]{5} \notin \mathbb{Q} \quad \forall a_1 \in \mathbb{Q} \\ \implies &\ \deg(f_{\sqrt[4]{5},\mathbb{Q}}) \neq 2. \end{aligned}$$

Angenommen, $\deg(f_{\sqrt[4]{5},\mathbb{Q}}) = 3$.
Es gilt:

$$\begin{aligned} f_{\sqrt[4]{5},\mathbb{Q}}(\sqrt[4]{5}) &= \sqrt[4]{5}^3 + a_2\sqrt[4]{5}^2 + a_1\sqrt[4]{5} + a_0 \\ &= \sqrt{5}\sqrt[4]{5} + a_2\sqrt{5} + a_1\sqrt[4]{5} + a_0 \overset{!}{=} 0 \\ \implies &\ a_0 = -\sqrt{5}\sqrt[4]{5} - a_2\sqrt{5} - a_1\sqrt[4]{5} \notin \mathbb{Q} \quad \forall a_1, a_2 \in \mathbb{Q} \\ \implies &\ \deg(f_{\sqrt[4]{5},\mathbb{Q}}) \neq 3. \end{aligned}$$

Angenommen, $\deg(f_{\sqrt[4]{5},\mathbb{Q}}) = 4$.

Es gilt:

$$
\begin{aligned}
f_{\sqrt[4]{5},\mathbb{Q}}(\sqrt[4]{5}) &= \sqrt[4]{5}^4 + a_3\sqrt[4]{5}^3 + a_2\sqrt[4]{5}^2 + a_1\sqrt[4]{5} + a_0 \\
&= 5 + a_3\sqrt{5}\sqrt[4]{5} + a_2\sqrt{5} + a_1\sqrt[4]{5} + a_0 \stackrel{!}{=} 0 \\
\implies a_0 &= -5 - a_3\sqrt{5}\sqrt[4]{5} - a_2\sqrt{5} - a_1\sqrt[4]{5} \in \mathbb{Q} \text{ für } a_1 = a_2 = a_3 = 0 \\
\implies f_{\sqrt[4]{5},\mathbb{Q}} &= t^4 - 5 \\
\implies [\mathbb{Q}(\sqrt[4]{5}) : \mathbb{Q}] &= \deg(f_{\sqrt[4]{5},\mathbb{Q}}) = 4.
\end{aligned}
$$

Insgesamt ergibt sich:

$$
[\mathbb{Q}(\sqrt[4]{5}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{5}, i) : \mathbb{Q}(\sqrt[4]{5})] \cdot [\mathbb{Q}(\sqrt[4]{5}) : \mathbb{Q}] = 2 \cdot 4 = 8.
$$

$\square$

(ii) Sei $f_2 = t^4 + 1$.
Es gilt:

$$
\begin{aligned}
f_2 &= t^4 + 1 \\
&= (t^2 + i)(t^2 - i) \\
&= (t + i\sqrt{i})(t - i\sqrt{i})(t + \sqrt{i})(t - \sqrt{i}).
\end{aligned}
$$

Da $\sqrt{i}, i\sqrt{i} \notin \mathbb{Q}$, zerfällt f_2 nicht über $\mathbb{Q}$, jedoch über $\mathbb{Q}(i, \sqrt{i})$, denn $\sqrt{i}, i\sqrt{i}$ sind die Nullstellen von f_2 in $\mathbb{Q}(i, \sqrt{i})$.

Zu zeigen: $[\mathbb{Q}(i) : \mathbb{Q}] = 2$.
Es gilt:

$$
\begin{aligned}
f_{i,\mathbb{Q}} &= t^2 + 1. \\
\implies [\mathbb{Q}(i) : \mathbb{Q}] &= \deg(f_{i,\mathbb{Q}}) = 2.
\end{aligned}
$$

Zu zeigen: $[\mathbb{Q}(i, \sqrt{i}) : \mathbb{Q}(i)] = 2$.
Angenommen, $\deg(f_{\sqrt{i},\mathbb{Q}(i)}) = 1$.
Es gilt:

$$
\begin{aligned}
f_{\sqrt{i},\mathbb{Q}(i)}(\sqrt{i}) &= \sqrt{i} + a_0 \stackrel{!}{=} 0 \\
\implies a_0 &= -\sqrt{i} \notin \mathbb{Q}(i) \\
\implies \deg(f_{\sqrt{i},\mathbb{Q}(i)}) &\neq 1.
\end{aligned}
$$

Angenommen, $\deg(f_{\sqrt{i},\mathbb{Q}(i)}) = 2$.

Es gilt:

$$\begin{aligned}
f_{\sqrt{i},\mathbb{Q}(i)}(\sqrt{i}) &= \sqrt{i}^2 + a_1\sqrt{i} + a_0 \\
&= i + a_1\sqrt{i} + a_0 \overset{!}{=} 0 \\
\implies a_0 &= -i - a_1\sqrt{i} \\
\implies (a_0 &\in \mathbb{Q}(i) \iff a_1 = 0) \\
\implies f_{\sqrt{i},\mathbb{Q}(i)} &= t^2 - i \\
\implies [\mathbb{Q}(i,\sqrt{i}) &: \mathbb{Q}(i)] = \deg(f_{\sqrt{i},\mathbb{Q}(i)}) = 2.
\end{aligned}$$

Insgesamt ergibt sich:

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

$\square$

(c) (i) Sei $K := \mathbb{Q} \subseteq \mathbb{Q}(i) =: L$ Körpererweiterung, $f = t^2 + 1 \in K[t], n := \deg(f) = 2$.
Es gilt:

$$\begin{aligned}
f &= t^2 + 1 \\
&= t^2 - i^2 \\
&= (t+i)(t-i).
\end{aligned}$$

Außerdem gilt:

$t+i, t-i \in L[t] \implies f$ zerfällt über L, aber nicht über K, da $i \notin K$.

Zu zeigen: $[L : K] = 2$.
Da $i \notin \mathbb{Q}$ ist, muss der Grad des Minimalpolymoms von i größer als 1 sein. Da $i^2 + 1 = 0$, ist f das Minimalpolynom von i über $\mathbb{Q}$.
Es gilt:

$$[L : K] = \deg(f) = 2.$$

$\square$

(ii) Sei $K = \mathbb{R} \subseteq \mathbb{C} = \mathbb{R}(i) = L$ eine Körpererweiterung, $f = t^2 + 1 \in \mathbb{R}[t]$ Polynom.
Es gilt:

$$f = t^2 + 1 = (t+i)(t-i)$$

Außerdem gilt:

$$\begin{aligned}
&i \text{ algebraisch über } \mathbb{R} \\
\implies &[\mathbb{C} : \mathbb{Q}] = [\mathbb{Q}(i) : \mathbb{Q}] = \deg(f) = 2 = 2!.
\end{aligned}$$

$\square$

(iii) Seien $K = \mathbb{Q}, L = \mathbb{Q}(\sqrt{2}, i)$ Körper, $f := t^3 \in \mathbb{Q}[t]$ mit $n := \deg(f) = 3$.
Es gilt:

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

Außerdem gilt:

$$n = 3 < 4 = [L : K] = 4 < 6 = 3! = n!$$

Da f über $\mathbb{Q}$ zerfällt, zerfällt f auch über $\mathbb{Q}(\sqrt{2}, i)$.

$\square$

Aufgabe 9.2

(a) Sei $f := t^4 + t^3 + 2t^2 + 1 \in \mathbb{Z}_3[t]$.
Zu zeigen: $f = (t + 1) \cdot (t^3 + 2t + 1)$ ist eine Zerlegung von f in irreduzible Polynome über $\mathbb{Z}_3$.
Es gilt:

$$\begin{aligned} f &= t^4 + t^3 + 2t^2 + 1 \\ &= t^4 + t^3 + 2t^2 + 2t + t + 1 \\ &= (t + 1)(t^3 + 2t + 1). \end{aligned}$$

Zu zeigen: $t + 1$ irreduzibel über $\mathbb{Z}_3$.
Es gilt:

$$\mathbb{Z}_3 \text{ Körper und } \deg(t + 1) = 1 \overset{5.1.2}{\Longrightarrow} t + 1 \text{ irreduzibel über } \mathbb{Z}_3.$$

Zu zeigen: $h := t^3 + 2t + 1$ irreduzibel über $\mathbb{Z}_3$.
Angenommen, h sei reduzibel über $\mathbb{Z}_3$. Da $\mathbb{Z}_3$ Körper ist und $\deg(h) = 3$ hat h nach Beobachtung 5.1.6 eine Nullstelle in $\mathbb{Z}_3$. Es gilt:

$$\begin{aligned} h(0) &= 0^3 + 2 \cdot 0 + 1 = 1 \neq 0, \\ h(1) &= 1^3 + 2 \cdot 1 + 1 = 1 \neq 0, \\ h(2) &= 2^3 + 2 \cdot 2 + 1 = 1 \neq 0. \end{aligned}$$

Dies steht im Widerspruch zu Beobachtung 5.1.6, weshalb h nicht reduzibel über $\mathbb{Z}_3$ sein kann.
Insgesamt ergibt sich, dass $f = (t + 1) \cdot (t^3 + 2t + 1)$ eine Zerlegung von f in irreduzible Polynome über $\mathbb{Z}_3$ ist.

$\square$

(b) Fehlt.

(c) Fehlt.

Aufgabe 9.3

Sei $R := \mathbb{Z}_6$ und $M := R \times R$.
Zu zeigen: $X := ((2,4))$ linear unabhängig.
Es gilt:

$$\begin{aligned} & 0 \neq 3 \in R \\ \Longrightarrow\ & 3 \cdot (2,4) = (3 \cdot 2, 3 \cdot 4) = (0,0) \\ \Longrightarrow\ & ((2,4)) \text{ ist eine linear abhängige Familie.} \end{aligned}$$

$\square$

Anhang

(A1) Sei $n \in \mathbb{N}_0$, $p \in \mathbb{N}$. Dann ist

$$\sum_{i=0}^{p-1} \binom{n+i}{n} = \binom{n+p}{n+1}.$$

Beweis:

(IA) Sei $\underline{p=1}$. Es gilt:

$$\sum_{i=0}^{1-1} \binom{n+i}{n} = \binom{n}{n} = \binom{n+1}{n+1} = \binom{n+p}{n+1}.$$

(IV) Gelte die Behauptung für ein beliebiges, aber festes $p \in \mathbb{N}$.

(IS) $\underline{p \rightsquigarrow p+1}$.
Es gilt:

$$\begin{aligned} \sum_{i=0}^{(p+1)-1} \binom{n+i}{n} &= \sum_{i=0}^{p-1} \binom{n+i}{n} + \binom{n+p}{n} \\ &= \binom{n+l}{n+1} + \binom{n+p}{n} = \binom{n+(p+1)}{n+1}. \end{aligned}$$

$\square$

(A2) Sei p Primzahl. Sei $n \in \{1, 2, \cdots, p-1\}$. Dann gilt:

$$p \mid \binom{p}{n}.$$

Beweis:
Sei p Primzahl, $n \in \{1, 2, \cdots, p-1\}$. Es gilt:

$$\begin{aligned}
\binom{p}{n} \cdot n! &= \frac{p!}{n! \cdot (p-n)!} \cdot n! \\
&= \frac{p!}{(p-n)!} \\
&= p(p-1)(p-2)\cdots(p-n+2)(p-n+1)
\end{aligned}$$

$$\Longrightarrow p \mid \frac{p!}{(p-n)!}$$

$$\Longrightarrow p \mid \binom{p}{n} \cdot n!$$

$$\overset{p \text{ Primzahl}}{\underset{p>n>0}{\Longrightarrow}} p \mid \binom{p}{n}.$$

$\square$

korrigiert von am