Mathematisches Institut
der Universität München
Andreas Fackler

Sommersemester 2009
Lösungsvorschlag zu Übungsblatt 10

Klausurenkurs Algebra

Aufgabe 1 (Frühjahr 2009, Thema 1, Aufgabe 3)

(a) Sei $r(t) = \alpha_n t^n + \ldots + \alpha_0 x^0 \in A[t] \setminus \{0\}$ mit $\alpha_n \neq 0$. Dann ist $p(t)r(t) = (1 + 5t)(\alpha_n t^n + \ldots + \alpha_0 x^0)$ die Summe von $5\alpha_n t^{n+1}$ und niedrigeren Potenzen von t. Aber da 5 eine Einheit ist, ist $5\alpha_n \neq 0$, also hat $p(t)r(t)$ mindestens Grad 1 und ist daher verschieden von 1. Folglich ist kein $r(t)$ ein Inverses von $p(t)$ und damit $p(t)$ keine Einheit.

(b) Setze $m = 6t$. Dann ist $m^4 = 8{\cdot}2{\cdot}3^4 t = 0$, also $q(t)(1-m)(1+m^2) = (1-m^2)(1+m^2) = 1 - m^4 = 1$. Das heißt aber, dass $(1-m)(1+m^2)$ ein Inverses von $q(t)$ ist.

Aufgabe 2 (Frühjahr 2009, Thema 1, Aufgabe 4)

$f(x) = x^2 + 4$ ist irreduzibel, da es keine Nullstelle in $\mathbb{Z}$ hat. Wir zeigen, dass $f(x+d) = x^2 + 2dx + d^2 + 4$ für kein $d \in \mathbb{Z}$ ein Eisensteinpolynom ist. Sei hierzu p ein Primteiler von $2d$. Falls $p \neq 2$ ist, so muss $p \mid d$ gelten. Dann ist aber $p \nmid (d^2+4)$ und wir sind fertig. Sei also nun $p = 2$. Falls d ungerade ist, gilt dann $p \nmid (d^2+4)$. Falls d gerade ist, gilt $p^2 \mid (d^2+4)$. In beiden Fällen ist das Eisensteinkriterium also nicht erfüllt.

Aufgabe 3 (Frühjahr 2009, Thema 2, Aufgabe 3)

Sei $\pi(x)$ Einheit in R/I. Dann gibt es ein $y \in R$, so dass xy in der Restklasse von 1 liegt, so dass also $xy - 1 \in I$. Folglich ist $xy - 1$ nilpotent, das heißt, es gibt ein $n \in \mathbb{N}$ mit $(xy-1)^n = 0$. Nun ist aber $(xy-1)^n - (-1)^n$ nach der binomischen Formel ein Vielfaches von x. Sei also $mx = (xy-1)^n - (-1)^n$. Dann ist $mx + (-1)^n = (xy-1)^n = 0$, also ist $mx = -(-1)^n$ und damit ist entweder m oder $-m$ ein Inverses von x.

Aufgabe 4 (Frühjahr 2009, Thema 2, Aufgabe 4)

(a) Offenbar $\alpha \in K$. Umgekehrt ist $\sqrt{7} = \frac{\alpha^5}{3 \cdot 7^2} \in \mathbb{Q}(\alpha)$ und damit auch $\sqrt[5]{3} = \frac{\alpha}{\sqrt{7}} \in \mathbb{Q}(\alpha)$.

(b) $\mathbb{Q}(\sqrt{7})$ hat über $\mathbb{Q}$ Grad 2, da $\sqrt{7}$ Nullstelle des nach Eisenstein irreduziblen Polynoms $X^2 - 7$ ist. $\mathbb{Q}(\sqrt[5]{3})$ hat über $\mathbb{Q}$ Grad 5, da auch $X^5 - 3$ nach Eisenstein irreduzibel ist. K hat also Unterkörper vom Grad 2 und 5, das heißt, $10 \mid [K : \mathbb{Q}]$. Andererseits ist $[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt{7})] \cdot [\mathbb{Q}(\sqrt{7}) : \mathbb{Q}] \leq 5 \cdot 2 = 10$. Also hat die Körpererweiterung Grad 10.

(c) Es ist $\alpha^{10} = 3^2 \cdot 7^5$, also ist α Nullstelle des Polynoms $X^{10} - 3^2 \cdot 7^5$. Da nach den ersten beiden Teilaufgaben α über $\mathbb{Q}$ Grad 10 haben muss, ist dies das Minimalpolynom.

Aufgabe 5 (Frühjahr 2009, Thema 3, Aufgabe 1)

(a) Ein Gruppenhomomorphismus $f : \mathbb{Z}/3\mathbb{Z} \to S_5$ ist durch $f(1)$ eindeutig bestimmt und $f(1)$ ist dann ein Element der Ordnung 1 oder 3. Die Elemente von S_5 der Ordnung 3 sind genau die 3-Zykel. Zu jeder Auswahl von drei Elementen aus S_5 gibt es genau zwei 3-Zykel, insgesamt also $\binom{5}{3} \cdot 2 = \frac{5!}{3!} = 20$. Da es genau ein Element der Ordnung 1 gibt, erhalten wir 21 Homomorphismen.

(b) $f(X-1) = X^5 - 6X^3 + 2X + 6$ ist nach Eisenstein irreduzibel, also ist auch f irreduzibel und damit $\mathbb{Q}[X]/(f) \supset \mathbb{Q}$ eine Körpererweiterung vom Grad 5. Da $\mathbb{Q}$ vollkommen ist, ist auch der Separabilitätsgrad 5. $\mathbb{C}$ ist algebraisch abgeschlossen, also gibt es genau 5 Homomorphismen von $\mathbb{Q}[X]/(f)$ nach $\mathbb{C}$.

Aufgabe 6 (Frühjahr 2009, Thema 3, Aufgabe 4)

(a) $\zeta := \zeta_{15}$ ist eine primitive fünfzehnte Einheitswurzel. Da über $\mathbb{Q}$ alle Kreisteilungspolynome irreduzibel sind, ist das Minimalpolynom von ζ das fünfzehnte Kreisteilungspolynom Φ_{15}. Wegen $X^{15} - 1 = \Phi_{15} \cdot \Phi_5 \cdot \Phi_3 \cdot \Phi_1 = \Phi_{15} \cdot (X^2 + X + 1) \cdot (X^5 - 1)$ gilt:

$$\begin{aligned}
\Phi_{15} &= \frac{X^{15} - 1}{(X^2 + X + 1) \cdot (X^5 - 1)} = \frac{X^{10} + X^5 + 1}{X^2 + X + 1} = X^8 + \frac{-X^9 - X^8 + X^5 + 1}{X^2 + X + 1} \\
&= X^8 - X^7 + \frac{X^7 + X^5 + 1}{X^2 + X + 1} = X^8 - X^7 + X^5 + \frac{-X^6 + 1}{X^2 + X + 1} \\
&= X^8 - X^7 + X^5 - X^6 + \frac{X^5 + X^4 + 1}{X^2 + X + 1} \\
&= X^8 - X^7 + X^5 - X^4 + X^3 + \frac{-X^3 + 1}{X^2 + X + 1} = X^8 - X^7 + X^5 - X^4 + X^3 - X + 1
\end{aligned}$$

(b) Sei $\alpha^{15} - 10 = 0$. Nach Eisenstein ist $X^{15} - 10$ irreduzibel über $\mathbb{Q}$. Da $\mathbb{Q}$ vollkommen ist, ist es auch separabel, M also galoissch über $\mathbb{Q}$. Die Nullstellen von $X^{15} - 10$ sind genau die Zahlen $\zeta^n \alpha$ für $0 \leq n < 15$. Es ist also $\zeta = \frac{\zeta\alpha}{\alpha} \in M$, also auch $\alpha \in M$. Daraus folgt $M = \mathbb{Q}(\alpha, \zeta)$. Da $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 15$ und $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 8$ ist, muss $8 \cdot 15 \mid [M : \mathbb{Q}]$ sein. Andererseits ist $[M : \mathbb{Q}] = [M : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] = 8 \cdot 15$. Es folgt $[M : \mathbb{Q}] = 8 \cdot 15 = 5!$.

Jedes $\sigma \in G$ ist durch $\sigma(\alpha)$ und $\sigma(\zeta)$ eindeutig bestimmt. Da es für den ersteren Wert 15 und für den zweiteren 8 Möglichkeiten gibt und $|G| = 8 \cdot 15$ ist, entspricht jeder Wahl einer Nullstelle $\zeta^n \alpha = \sigma(\alpha)$ von $X^{15} - 10$ und einer primitiven fünfzehnten Einheitswurzel $\zeta^m = \sigma(\zeta)$ genau ein Element von G. Wir zeigen, dass

$$h : \mathbb{Z}/15\mathbb{Z} \rtimes_\tau (\mathbb{Z}/15\mathbb{Z})^\times \to G, \quad h(\bar{n}, \bar{m}) = \sigma \text{ mit } \sigma(\alpha) = \zeta^n \alpha, \sigma(\zeta) = \zeta^m,$$

wobei $\tau(\bar{m})(\bar{n}) = \bar{m}\bar{n}$, ein Isomorphismus ist. Da $\zeta^{15} = 1$ ist, ist h wohldefiniert. Da ζ^m genau dann primitve fünfzehnte Einheitswurzel ist, wenn $\bar{m} \in (\mathbb{Z}/15\mathbb{Z})^\times$, ist h bijektiv.

Schließlich gilt müssen wir für $\sigma_0 = h(\bar{n}_0, \bar{m}_0)$ und $\sigma_1 = h(\bar{n}_1, \bar{m}_1)$ zeigen, dass $\sigma_0 \circ \sigma_1$ gleich $\sigma_3 = h((\bar{n}_0, \bar{m}_0)(\bar{n}_1, \bar{m}_1)) = h(\bar{n}_0 + \bar{m}_0\bar{n}_1, \bar{m}_0 \cdot \bar{m}_1)$ ist:

$$\begin{aligned}
\sigma_0 \circ \sigma_1(\zeta) &= \sigma_0(\zeta^{m_1}) = \sigma_0(\zeta)^{m_1} = \zeta^{m_0 m_1} = \sigma_3(\zeta) \\
\sigma_0 \circ \sigma_1(\alpha) &= \sigma_0(\zeta^{n_1}\alpha) = \sigma_0(\zeta)^{n_1}\sigma_0(\alpha) = \zeta^{n_0 + m_0 n_1}\alpha = \sigma_3(\alpha)
\end{aligned}$$

Da G ein Element der Ordnung 15 hat, ist G nicht isomorph zu S_{15}.