Übung zu Algebraische und Geometrische Strukturen in der Mathematik, SoSe 2014

4. Übungsblatt – Lösungsskizze

Aufgabe P11

1. Dies ist irreduzibel, da es keine Nullstellen in $\mathbb{Z}_2$ gibt (Satz I.3.8).
2. Dies ist ebenfalls irreduzibel, das sieht man genauso wie in (1). Eine allgemeine Idee zur Bestimmung aller irreduziblen Polynome in $\mathbb{Z}_2$ ist das *Sieb des Eratosthenes*, siehe `http://de.wikipedia.org`. Dazu überlege man sich für einen Algorithmus, dass die Polynome mit einer geraden Anzahl von Summanden immer reduzibel sein müssen (warum?).

3. Dies ist reduzibel, da 1 eine Nullstelle ist. Über $\mathbb{Z}_2$ hat man

$$X^3 + X^2 + X + 1 = (X+1)^3$$

4. Dies ist reduzibel, da 1 eine Nullstelle ist. Über $\mathbb{Z}_3$ hat man

$$X^3 + X + 1 = (X-1)(X^2 + X - 1)$$

Aufgabe P12

Wir betrachten zunächst den Homomorphismus

$$\widetilde{\varphi}\colon k[X] \to E, \quad p \mapsto p(a).$$

Dass $\widetilde{\varphi}$ ein Homomorphismus von Ringen ist wurde in Aufgabe **H6** gezeigt, denn die Abbildung setzt für die Variable X gerade das Element a ein. Da $m_{a,k} \in \ker(\widetilde{\varphi})$ folgt $m_{a,k} \cdot k[X] \subseteq \ker(m_{a,k} \cdot k[X])$. Damit faktorisiert $\widetilde{\varphi}$ zu einem Homomorphismus

$$\varphi\colon k[X]/(m_{a,k} \cdot k[X]) \to E$$

von Ringen. Nach Aufgabe **P5** gilt außerdem $\mathrm{im}(\varphi) \subseteq k(a)$.
Da das Bild eines Körpers unter einem Ringhomomorphismus ein Körper ist (warum?) und da $k \subseteq \mathrm{im}(\varphi)$ und $a \in \mathrm{im}(\varphi)$ folgt auch $k(a) \supseteq \mathrm{im}(\varphi)$. Damit haben wir $k(a) = \mathrm{im}(\varphi)$ und φ surjektiv.
Um Injektivität zu zeigen, nehmen wir $p \in k[X]$, sodass $\varphi(p) = 0$. Dann ist a eine Nullstelle von p. Da aber $m_{a,k}$ das Minimalpolynom ist, gilt dann $p \in m_{a,k} \cdot k[X]$ (explizit kann man dies wieder durch Polynomdivision machen).

Aufgabe P13

1. Wir bemerken zunächst, dass $m_{\sqrt[3]{2},\mathbb{Q}} = X^3 - 2$ und $m_{\sqrt[7]{5},\mathbb{Q}} = X^7 - 5$ gilt (warum?). Darum auch $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ und $[\mathbb{Q}(\sqrt[7]{5}) : \mathbb{Q}] = 7$. Also $\mathbb{Q}(\sqrt[3]{2}) \neq \mathbb{Q}(\sqrt[7]{5})$. Angenommen $\sqrt[3]{2} \in \mathbb{Q}(\sqrt[7]{5})$. Dann gilt auch $\mathbb{Q}(\sqrt[3]{2}) \subsetneq \mathbb{Q}(\sqrt[7]{5})$ (warum?). Da 7 eine Primzahl ist, kann nach Aufgabe **P6** und der Gradformel aber kein Zwischenkörper
$$\mathbb{Q} \subsetneq E \subsetneq \mathbb{Q}(\sqrt[7]{5})$$
existieren, Widerspruch.

2. Angenommen, es gäbe ein solches E. Weil 3 eine Primzahl ist gilt nach Aufgabe **P6** dass $\mathbb{R}(a) = E$ für jedes $a \in E \setminus \mathbb{R}$ (nach dem gleichen Argument wir im vorigen Teil). Dies bedeutet aber, dass auch $(m_{a,\mathbb{R}}) = 3$ gilt. Dies ist ein Widerspruch zu Aufgabe **P9**, nach der ein Polynom vom Grad 3 über $\mathbb{R}$ nicht irreduzibel sein kann.

Aufgabe H9

1. Dies ist irreduzibel: Man benutzt die Variablensubstitution $X \mapsto 2Y$ und erhält damit das Polynom
$$14Y^4 + 8Y^3 + 20Y^2 + 12Y + 12$$
welches nach Teilen durch 2 und anwenden des Eisenstein-Kriteriums irreduzibel ist (man nehme $\alpha = 2$).

2. Dies ist irreduzibel: Man benutzt zunächst die Variablensubstitution $X \mapsto \frac{Y}{2}$ und erhält damit das Polynom $Y^3 - 3Y + 1$. Danach benutzt man den Reduktions-Satz (modulo 2). Das Polynom ist in $\mathbb{Z}_2[Y]$ äquivalent zu $Y^3 + Y + 1$, welches nach **P11** irreduzibel ist.

3. Dies ist irreduzibel: Man benutzt direkt den Reduktions-Satz (modulo 2).

4. Dies ist irreduzibel: Man benutzt das Eisenstein-Kriterium und $\alpha = 2$.

5. Dies ist reduzibel, man sieht das direkt mit der ("ersten") Binomischen Formel, da $X^4 + 2X^2 + 1 = (X^2 + 1)^2$.

6. Dies ist reduzibel: Es ist $X = -7$ eine Nullstelle und so erhält man mit dem Euklidischen Algorithmus (Polynomdivision)
$$3X^3 + 21X^2 - 2X - 14 = (X + 7)(3X^2 - 2)$$

Aufgabe H10

1. Das Polynom $X^3+X^2-2X-1 \in \mathbb{Q}[X]$ ist irreduzibel nach Satz I.3.10, da $X^3+X^2+1 \in \mathbb{Z}_2[X]$ irreduzibel ist. Somit bleibt zu zeigen, dass a eine Nullstelle von X^3+X^2-2X-1 ist. Sei $\theta := \frac{2\pi}{7}$. Dann rechnen wir mit den üblichen trigonometrischen Identitäten nach, dass folgendes gilt:

$$\begin{aligned} a^3+a^2-2a-1 &= 8\cos^3(\theta)+4\cos^2(\theta)-2\cos(\theta)-1 \\ &= 8\cdot\frac{3\cos(\theta)+\cos(3\theta)}{4}+4\cdot\frac{1+\cos(2\theta)}{2}-2\cos(\theta)-1 \\ &= 2\cdot\cos(3\theta)+2\cdot\cos(2\theta)+2\cdot\cos(\theta)+1. \end{aligned}$$

   Da $6\theta = 2\pi-\theta$, $5\theta = 2\pi-2\theta$ und $4\theta = 2\pi-3\theta$ gilt, folgen $\cos(4\theta)=\cos(3\theta)$, $\cos(5\theta)=\cos(2\theta)$ und $\cos(6\theta)=\cos(\theta)$. Somit folgt, dass

$$\begin{aligned} &a^3+a^2-2a-1 \\ =&\cos(6\theta)+\cos(6\theta)+\cos(5\theta)+\cos(4\theta)+\cos(3\theta)+\cos(2\theta)+\cos(\theta)+1=0. \end{aligned}$$

2. Angenommen, man könnte mit Zirkel und Lineal ein regelmäßiges 7-Eck in den Einheitskreis einbeschreiben. Sei r der Abstand zwischen zwei benachbarten Ecken des 7-Ecks. Dann ist $e^{i\frac{2\pi}{7}}$ ein Schnittpunkt des Kreises von Radius r und Mittelpunkt 1 mit dem Kreis von Radius 1 und Mittelpunkt (warum?). Somit ist $e^{i\frac{2\pi}{7}} = \cos(\frac{2\pi}{7})+i\sin(\frac{2\pi}{7})$ konstruierbar. Aber da die Menge der konstruierbaren Punkte abgeschlossen unter Realteilen und Multiplikation ist, folgt daraus, dass auch $2\cdot\cos(\frac{2\pi}{7})$ konstruierbar ist.

   Dies ist allerdings ein Widerspruch, da aus Aufgabenteil (1) folgt, dass $[\mathbb{Q}(2\cdot\cos(\frac{2\pi}{7})):\mathbb{Q}] = \deg(m_{2\cdot\cos(\frac{2\pi}{7}),\mathbb{Q}}) = 3$.

Aufgabe H11

1. Es ist $m_{\sqrt{7},\mathbb{Q}} = X^2-7$. Dass dieses Polynom irreduzibel ist, folgt aus dem Eisenstein-Kriterium mit $\alpha = 7$.

2. Es gilt, dass $\frac{\sqrt{5}+1}{2}$ eine Nullstelle des Polynoms $4X^2-4X-4$ ist. Damit sieht man, dass $m_{\frac{\sqrt{5}+1}{2},\mathbb{Q}} = X^2-X-1$. Dieses Polynom ist nach Satz I.3.10 irreduzibel, da $X^2+X+1 \in \mathbb{Z}_2[X]$ irreduzibel ist.

3. Man rechnet nach, dass $\frac{i\sqrt{3}-1}{2}$ eine Nullstelle des Polynoms $-4X^2-4X-4$ ist. Dann folgt ebenso wie in der vorherigen Teilaufgabe, dass $m_{\frac{i\sqrt{3}-1}{2},\mathbb{Q}} = X^2+X+1$.

4. Zunächst gilt $\sqrt{2}+\sqrt{3} = \sqrt{5+2\sqrt{6}}$. Durch Rückwärtsanwendung der pq-Formel sieht man, dass $5+2\sqrt{6}$ eine Nullstelle des Polynoms $X^2-10X+1$ ist. Damit folgt, dass $m_{\sqrt{2}+\sqrt{3},\mathbb{Q}} = X^4-10X^2+1$, da $\deg(m_{\sqrt{2}+\sqrt{3},\mathbb{Q}}) = [\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}] = 4$.