Übungsblatt 7

Aufgabe 1. Zeigen Sie, dass für jedes $n \in \mathbb{N} \setminus \{0\}$ die reelle Zahle $\cos\left(\frac{\pi}{n}\right)$ algebraisch über $\mathbb{Q}$ ist.

Beweis. Wir betrachten zunächst $\mathbb{Q}\left(e^{i\frac{\pi}{n}}\right)$ und stellen fest, dass wegen $\left(e^{i\frac{\pi}{n}}\right)^{2n} - 1 = 0$ der Grad $\left[\mathbb{Q}\left(e^{i\frac{\pi}{n}}\right) : \mathbb{Q}\right]$ endlich ist. Somit sind alle Körperelemente von $\mathbb{Q}\left(e^{i\frac{\pi}{n}}\right)$ algebraisch über $\mathbb{Q}$, insbesondere auch $\cos\left(\frac{\pi}{n}\right) = \frac{1}{2}\left(e^{i\frac{\pi}{n}} + \left(e^{i\frac{\pi}{n}}\right)^{-1}\right)$. □

Aufgabe 2. Sei p eine Primzahl und $w \in \mathbb{C}$ eine primitive p–te Einheitswurzel, etwa $w = e^{\frac{2\pi i}{p}}$. Bestimmen Sie das Minimalpolynom von w über $\mathbb{Q}$ und den Grad $[\mathbb{Q}(w) : \mathbb{Q}]$.

Beweis. Nach Vorlesung erhalten wir die Zerlegung

$$X^p - 1 = (X-1)(X^{p-1} + X^{p-2} + \ldots + X + 1),$$

wobei wir $\Phi_p(X) := X^{p-1} + X^{p-2} + \ldots + X + 1$ setzen. Da offensichtlich $w^p - 1 = 0 \neq w - 1$ gilt und $\mathbb{C}$ ein Integritätsbereich ist, folgt $\Phi_p(w) = 0$. Nach der Vorlesung wissen wir, dass Φ_p irreduzibel über $\mathbb{Z}$ ist, somit, wegen der Primitivität von Φ_p, auch über $\mathbb{Q}$. Also ist Φ_p das Minimalpolynom von w über $\mathbb{Q}$. Nach dem Homomorphiesatz gilt

$$\mathbb{Q}[X]/(\Phi_p) \cong \mathbb{Q}(w)$$

und damit $p - 1 = \deg(\Phi_p) = [\mathbb{Q}[X]/(\Phi_p) : \mathbb{Q}] = [\mathbb{Q}(w) : \mathbb{Q}]$. □

Aufgabe 3. Fertigen Sie eine vollständige und irredudante List der irreduziblen Polynome Über $\mathbb{F}_2$, dem Körper mit zwei Elementen, vom Grad kleiner als 5 an. Schließen Sie, dass

$$L := \mathbb{F}_2[X]/(X^4 + X + 1)$$

ein Erweiterungskörper von $\mathbb{F}_2$ ist. Was ist der Grad $[L : \mathbb{F}_2]$? Listen Sie alle Elemente von L auf, und bestimmen Sie alle Unterkörper von L.

In Blatt 6 Aufgabe 3 haben wir bewiesen, dass ein Polynom aus $\mathbb{K}[X]$ vom Grad ≤ 3 genau dann invertierbar ist, wenn es keine Nullstelle besitzt. Dies machen wir uns im Folgenden zu Nutze.
Offensichtlich lauten die irreduziblen Polynome vom Grad 1

$$X,\ X + 1.$$

Das einzige irreduzible Polynome vom Grad 2 lautet

$$X^2 + X + 1.$$

Letzteres können wir wie folgt einsehen. Sei $f(X) = X^2 + aX + c \in \mathbb{F}_2[X]$ irreduzibel, d.h. es besitzt keine Nullstelle in $\mathbb{F}_2$, so impliziert letzteres, dass $f(0) = c = 1$ und $f(1) = 1 + a + c = 1 + a + 1 = a = 1$ gilt. Die irreduziblen Polynome vom Grad 3 lauten

$$X^3 + X + 1,\ X^3 + X^2 + 1.$$

Hier argumentieren wir analog. Sei $f(X) = X^3 + aX^2 + bX + c$ irreduzibel, so gilt $f(0) = c = 1$ und $f(1) = 1 + a + b + 1 = a + b = 1$, d.h. $a \in \mathbb{F}_2$ und $b \in \mathbb{F}_2 \setminus \{a\}$. Wir erhalten also die folgenden Möglichkeiten $a = 0, b = 1$ und $a = 1, b = 0$. Die irreduziblen Polynome vom Grad 4 lauten

$$X^4 + X + 1,\ X^4 + X^3 + 1,\ X^4 + X^3 + X^2 + X + 1.$$

Für Polynome vom Grad 4 ist die Irreduzibilität nicht gleichbedeuten mit der Eigenschaft keine Nullstelle zu besitzen, trotzdem berechnen wir zunächst alle Polynome, die keine Nullstelle haben. Sei also $f(X) = X^4 + aX^3 + bX^2 + cX + d$. Es gilt $f(0) = d = 1$ und $f(1) = 1 + a + b + c + 1 = 1$, d.h. $a + b + c = 1$. Wir erhalten also die folgenden vier Polynome, die keine Nullstellen in $\mathbb{F}_2$ besitzen

$$X^4 + X + 1,\ X^4 + X^3 + 1,\ X^4 + X^3 + X^2 + X + 1, X^4 + X^2 + 1.$$

Allerdings gilt $X^4 + X^2 + 1 = (X^2 + X + 1)^2$, d.h. $X^4 + X^2 + 1$ ist reduzibel. Die Irreduzibilität der restlichen Polynome überprüft man mittels einer Polynomdivision durch das einzige irreduzible Polynom vom Grad 2.
Da $X^4 + X + 1$ irreduzibel in $\mathbb{F}_2[X]$ ist, ist $(X^4 + X + 1)$ ein maximales Ideal und dementsprechend ist L ein Erweiterungskörper von $\mathbb{F}_2$. Es gilt $[L : \mathbb{F}_2] = \deg(X^4 + X + 1) = 4$ und damit $|L| = 2^4 = 16$. Sei nun $\mathbb{F}_2 \subseteq F \subseteq L$ ein Unterkörper so gilt wegen

$$[L : \mathbb{F}_2] = [L : F] \cdot [F : \mathbb{F}_2]$$

$k := [F : \mathbb{F}_2] \in \{1, 2, 4\} = \{d \in \mathbb{N} \mid d|4\}$. Wenn $k = 1$ ist, so gilt $F = \mathbb{F}_2$. Wenn $k = 4$ ist, so ist $F = L$ und wenn $k = 2$ ist, so ist L ein Körper mit $2^{[F:\mathbb{F}_2]} = 2^2 = 4$ Elementen. Aus letzterem folgt weder die Existenz noch Eindeutigkeit eines Unterkörpers mit 4 Elementen.

Für Interessierte folgt nun ein Beweis, dass es neben L und $\mathbb{F}_2$ genau ein Unterkörper der Kardinalität 4 existiert. (Später wird diese Fragestellung in allgemeinerer Form in der Vorlesung beantwortet.)

Die multiplikative Gruppe L^* mit Ordnung $|L^*| = |L| - 1 = 15$ ist zyklisch, denn die Ordnung von $X + 1$ ist 15. Letzteres kann man einfach verfizieren, indem man nachrechnet, dass $(X + 1)^3 \neq 1 \neq (X + 1)^5$ in L^* gilt. Betrachte nun das folgende Lemma.

Lemma. *Ist G eine zyklische Gruppe der Ordnung $m < \infty$, so besitzt G zu jedem Teiler d von m genau eine Untergruppe der Ordnung d.*

Beweis. Seien $G = \langle g \rangle$ und $m = k \cdot d$ für $k \in \mathbb{N}_0$, so hat die Untergruppe $\langle g^k \rangle$ die Ordnung d. Sei U eine weitere Untergruppe der Ordnung d, so zeigen wir analog zum Beweis von Satz 1.27 aus der Vorlesung, dass $U = \langle g^k \rangle$ gilt. Betrachte hierfür den Homomorphismus

$$\Phi : \mathbb{Z} \to G;\ l \mapsto g^l$$

und es existiert ein $n \in \mathbb{N}_0$ mit $\Phi^{-1}(U) = n\mathbb{Z}$. D.h. $\Phi(n) = g^n$ ist ein Erzeuger von U und somit folgt $n = \frac{m}{d} = k$. □

Sei nun $\mathbb{F}_2 \subseteq F \subseteq L$ ein Zwischenkörper, so ist F^* zyklisch der Ordnung $d \in \{1, 3, 5, 15\}$ und für jeden weiteren Zwischenkörper K mit $|K^*| = |F^*|$ gilt nach obigem Lemma $F = K$.
Es gibt keinen Zwischenkörper F der Kardinalität 6, denn ansonsten gelte $6 = |F| = 2^{[F:\mathbb{F}_2]}$, ein Widerspruch. Also gilt $|F^*| \in \{1, 3, 15\}$, bzw. $|F^* \cup \{0\}| = |F| \in \{2, 4, 16\}$. Ist $|F| = 2$, so ist $F = \mathbb{F}_2$ und für $|F| = 16$ ist $F = L$. Betrachte nun $|F| = 4$, d.h.

$$F = \left\{(1 + X)^{5 \cdot n} \mid 1 \leq n \leq \frac{15}{5}\right\} \cup \{0\}.$$

Wir zeigen im Folgenden, dass F ein Körper ist. Zunächst geben wir explizit alle Elemente von F an. Dazu führen wir die folgenden Berechnungen durch.

$$\begin{aligned}
(1 + X)^5 &= X^5 + 5X^4 + 10X^3 + 10X^2 + 5X + 1 = X^5 + X^4 + X + 1 = X^5 = X(X + 1) \\
(1 + X)^{10} &= (1 + X)^{5 \cdot 2} = X^2(X + 1)^2 = X^2 + X + 1 \\
(1 + X)^{15} &= 1
\end{aligned}$$

Es gilt also $F = \{0, 1, X(X+1), X^2+X+1\}$ und wir weisen nach, dass F abgeschlossen bezüglich der Addition ist.

$$[X(X+1)] + [X^2+X+1] = 1 \in F$$
$$[X(X+1)] + 1 = X^2+X+1 \in F$$
$$[X^2+X+1] + 1 = X(X+1) \in F$$

Die restlichen Körperaxiome sind offensichtlich erfüllt, d.h. F ist ein Unterkörper von L.
Zusammengefasst besitzt L genau $|\{d \in \mathbb{N} \mid d|4\}| = 3$ Unterkörper und sie lauten

$$L,$$
$$\{0, 1, X(X+1), X^2+X+1\} \cong \mathbb{F}_{2^2} \text{ und}$$
$$\mathbb{F}_2.$$

Aufgabe 4. Entscheiden Sie, ob das Polynom

$$f(X) = 3X^5 - 5X^3 + 1 \in \mathbb{Q}[X]$$

irreduzibel ist.

Zunächst beweisen wir die Proposition 2.44 aus der Vorlesung.

Proposition. *Sei R faktoriell, $p \in R$ prim, $f \in R[X] \setminus \{0\}$ ein Polynom, dessen Leitkoeffizient nicht durch p teilbar ist. Bezeichne mit*

$$\phi : R[X] \to R/(p)[X]$$

die natürliche (Koeffizienten-)Reduktion modulo p. Wenn $\phi(f)$ irreduzibel in $R/(p)[X]$ ist, so ist f irreduzibel in $Q(R)[X]$. Ist f zusätzlich primitiv, so ist f irreduzibel in $R[X]$.

Beweis. Sei zunächst $f \in R[X]$ als primitiv angenommen. Ist f reduzibel, so gibt es $g, h \in R[X]$ mit $\deg(h), \deg(g) > 0$ und $f = gh$. Das Element p teilt nicht die Leitkoeffizienten von g und h, also gilt

$$\phi(f) = \phi(g)\phi(h)$$

mit nicht konstanten Polynomen $\phi(g)$ und $\phi(h)$. Somit ist $\phi(f)$ reduzibel.
Ist f nicht primitiv, so existiert ein $c \in R$ mit $f = c \cdot \tilde{f}$, wobei $\tilde{f}$ ein primitives Polynom in $R[X]$ ist. Das Element p teilt weder c noch den Leitkoeffizienten von $\tilde{f}$. Also folgt aus der Irreduzibilität von $\phi(f)$ die Irreduzibilität von $\phi(\tilde{f})$ und nach vorheriger Argumentation gilt, dass $\tilde{f}$ irreduzibel in $R[X]$ ist. Also sind $\tilde{f}$ und damit f irreduzibel in $Q(R)[X]$.
Für primitive Polynome ist die Irreduzibilität in $R[X]$ gleichbedeutend mit der Irreduzibilität in $Q(R)[X]$, woraus die letzte Behauptung folgt. □

Wir behaupten, dass das Polynom f irreduzibel ist.

Beweis. Dazu betrachten wir $\bar{f}(X) = X^5 + X^3 + 1 \in \mathbb{F}_2[X]$ und überprüfen, ob $\bar{f}$ von eines der irreduziblen Polynome aus Augabe 3 geteilt wird. Da $\bar{f}$ keine Nullstellen in $\mathbb{F}_2$ besitzt, müssen wir lediglich nachrechnen, dass $\bar{f}$ nicht von X^2+X+1 in $\mathbb{F}_2[X]$ geteilt wird. Es gilt

$$\bar{f}(X) = X^5 - X^3 + 1 = (X^2+X+1)(X^3+X^2+X) + (X+1),$$

somit ist $\bar{f}$ nicht durch X^2+X+1 teilbar, d.h. $\bar{f}$ ist irreduzibel in $\mathbb{F}_2[X]$. Also ist auch f nach obiger Proposition irreduzibel in $\mathbb{Z}[X]$ und auch irreduzibel in $\mathbb{Q}[X]$. □