1 Endliche Körper

Sei k ein endlicher Körper. Dann ist der eindeutig bestimmte Ringhomomorphismus $\phi : \mathbb{Z} \to k$ nicht injektiv, weil $\mathbb{Z}$ unendlich viele Elemente besitzt. Weil k ein Körper ist, ist k nullteilerfrei, also $\{0\} \subset k$ ein Primideal und damit auch $\ker \phi = \phi^{-1}\{0\}$, also $\ker \phi = p\,\mathbb{Z}$ für eine Primzahl p. Das Bild von ϕ ist ein zu $\mathbb{Z}\,/p\,\mathbb{Z}$ isomorpher Unterkörper k' von k. Nun ist k ein Vektorraum über k' und da k endlich ist, ist die Dimension von k über k' endlich, sagen wir n.
Die additive Gruppe von k ist isomorph zu $(k')^n = k' \times \ldots \times k'$. Aber die multiplkativen Gruppen sind **nicht** isomorph, denn $(k')^n$ ist üblicherweise mit der komponentenweisen Multiplikation versehen.
Wären nun auch die multiplikativen Gruppen isomorph, so wäre k kein Körper, weil $(k')^n$ nicht-triviale Nullteiler besitzt (für $n > 1$).
Es sei noch einmal erwähnt (vgl. Anmerkungen zu Blatt 8), dass in einem Körper mit Charakteristik p nicht notwendig für alle $x \in k$ die Identität $x^p = x$ erfüllt ist.

2 Lösungen

2.1 Aufgabe 1

a) - Version 1:
Das Polynom $p := X^3 - 2X + X + 3 \in \mathbb{Z}\,[X]$ ist primitiv, Reduktion modulo zwei liefert das Polynom $\overline{p} := X^3 + X + 1 \in \mathbb{Z}_2\,[X]$. Wäre letzteres reduzibel, hätte es eine Nullstelle, aber $\{0,1\} = \mathbb{Z}_2$ enthält keine Nullstelle von $\overline{p}$. Also ist p irreduzibel.

Version 2:
Das Polynom $p = X^3 - 2X + X + 3 \in \mathbb{Q}\,[X]$ ist irreduzibel. Angenommen es wäre reduzibel, dann gäbe es o.B.d.A. normierte Polynome (weil p normiert ist) f, g mit positivem Grad und $p = fg$. Dann ist o.B.d.A. $\operatorname{grad} f = 1$ also $f = X + a$ für ein $a \in \mathbb{Q}$, d.h. p hätte eine rationale Nulstelle.
Da die Koeffizienten von p ganzzahlig sind, sind alle rationalen Nullstellen von f ganzzahlig. Somit hat auch f ganze Koeffizienten, also auch g (Satz über Division mit Rest angewand auf Polynome in $\mathbb{Z}\,[X]$). Insbesondere ist damit a ein Teiler von 3 (Produkt der Absolut-Terme von f und g). Nun sind aber die Teiler von 3 die Zahlen $-3, -1, 1, 3$, welche alle keine Nullstelle von p sind.

b) Das Polynom $X^5 + X^4 + X^3 + X^2 + X + 1$ hat -1 als Nullstelle, ist also durch $X + 1$ teilbar, also reduzibel.

2.2 Aufgabe 2

Sei $f = \sum_{i=0}^{p-1} X^i$ mit p prim. Es ist $f = \frac{X^p-1}{X-1}$. Durch $X \mapsto Y+1$ wird ein Ringisomorphismus $\phi : \mathbb{Z}[X] \to \mathbb{Z}[Y]$ definiert (das Inverse ist durch $Y \mapsto X-1$ definiert). Es gilt

$$g := \phi(f) = f(Y+1) = \frac{(Y+1)^p - 1}{Y+1-1} = \frac{\sum_{i=1}^{p} \binom{p}{i} Y^i}{Y} = \sum_{i=1}^{p} \binom{p}{i} Y^{i-1}$$

Da p prim ist, teilt p die Zahlen $\binom{p}{i}$ für $i = 1, 2, \ldots, p-1$. Nun teilt p^2 aber nicht das absolute Glied und p teilt nicht den Leitkoeffizienten, also ist g nach Eisenstein irreduzibel und somit auch f.

2.3 Aufgabe 3

Es ist $K(X) = \mathrm{Quot}(K[X])$. Wir Betrachten das Polynom $f = X^2 + Y^2 - 1$. Es ist aufgefasst als Polynom in $K[X][Y]$ primitiv. Das heißt, wenn wir zeigen, dass f irreduzibel in $K[X][Y]$ ist, dann auch ist es auch irreduzibel in $K(X)[Y]$.
Wir betrachten das Polynom $X+1$. Es ist ein Primelement in $K[X]$ (wegen Grad 1 irreduzibel und weil $K[X]$ faktoriell ist, ist es auch prim). Setzen wir $\mathrm{char}\, K \neq 2$ voraus, so sind $X-1$ und $X+1$ teilerfremd, also X^2-1 insbesondere nicht durch $(X+1)^2$ teilbar.
Das Polynom f erfüllt dann aber die Voraussetzungen des Eisensteinkriteriums ($R = K[X], p = X+1$) und somit ist f irreduzibel.

2.4 Aufgabe 4

Sei $I = (x^3 + 2x - 2)$ das von $x^3 + 2x - 2$ erzeugte Ideal in $\mathbb{Q}[x]$. Wir suchen ein Inverses von $x^2 + x + 1 + I$ in dem Ring $\mathbb{Q}[X]/I$. Wir suchen also ein Polynom p, so dass $(x^2 + x + 1) \cdot p - 1$ ein Vielfaches von $x^3 + 2x - 2$ ist. Also insgesamt suchen wir Polynome p, q mit

$$(x^2 + x + 1) \cdot p - 1 = (x^3 + 2x - 2) \cdot q$$
$$(x^2 + x + 1) \cdot p - (x^3 + 2x - 2) \cdot q = 1$$

Hat man das Problem erst einmal so umformuliert, ist offensichtlich, dass man den erweiterten euklidischen Algorithmus zur Lösung des Problems benutzen kann. Das werden wir nun machen:
Wir dividieren mit Rest:

$$(x^3 + 2x - 2) = (x^2 + x + 1)(x - 1) + (2x - 1)$$
$$(x^2 + x + 1) = (2x - 1)(\frac{x}{2} + \frac{3}{4}) + \frac{7}{4}$$

Multiplizieren wir die zweite Gleichung mit $\frac{4}{7}$ so erhalten wir

$$1 = \frac{4}{7}(x^2 + x + 1) - (2x - 1)(\frac{2x}{7} + \frac{12}{7})$$

Ersetzten wir hier nun $(2x - 1)$ durch $(x^3 + 2x - 2) - (x^2 + x + 1)(x - 1)$ (mit Hilfe der ersten Gleichung) so erhalten wir

$$1 = \frac{4}{7}(x^2 + x + 1) - ((x^3 + 2x - 2) - (x^2 + x + 1)(x - 1))(\frac{2x}{7} + \frac{12}{7})$$

Damit finden wir $p = \frac{4}{7} + (x - 1)(\frac{2x}{7} + \frac{12}{7}) = \frac{2}{7}x^2 + \frac{10}{7}x - \frac{8}{7}$.

2.5 Aufgabe 5

Sei k ein unendlicher Körper und seien $f, g \in k\,[X]$. Ist $f = g$ so ist trivialerweise $f(x) = g(x)$ für alle $x \in k$.
Sei nun $f(x) = g(x)$ für alle $x \in k$. Angenommen das Polynom $h = f - g$ ist nicht das Nullpolynom. Dann hat h positiven Grad n. Ein Polynom vom Grad n hat höchstens n Nullstellen, h hat aber unendlich viele Nullstellen, ein Widerspruch.
Wer die Aussage mit den n Nullstellen nicht glaubt, der vollziehe den folgenden Beweis durch vollständige Induktion nach:
Ist h von Grad 1, so ist $f = aX + b$ mit $a \neq 0$ hat also genau eine Nullstelle nämlich $-\frac{b}{a}$.
Sei nun h vom Grad $n > 1$. Wenn h keine Nullstelle hat, sind wir fertig (denn $0 < n$). Wenn nun aber h eine Nullstelle c besitzt, so teilen wir h mit rest durch $X - c$ und sehen dann mit dem üblichen Grad-Argument, dass der Rest das Nullpolynom sein muss.
Also ist h durch $X - c$ teilbar und der Quotient $h' := \frac{h}{X-c}$ ist ein Polynom vom Grad $n - 1$.
Dieser hat nach Induktionsannahme höchstens $n - 1$ Nullstellen. Ist nun $d \in k$ eine Nullstelle, die von c verschieden ist, so ist $0 = h(d) = h'(d) \cdot (d - c)$, also d eine Nullstelle von h'. Damit ist jede Nullstelle von h entweder c oder eine Nullstelle von h', also hat h höchstens n Nullstellen.

Sei k nun ein endlicher Körper. dann gibt es natürliche Zahlen n, p (p sogar prim) mit $|k| = p^n$. Nun ist $k^\times$ eine Gruppe von Ordnung $p^n - 1$, also gilt für $x \neq 0$

$$x^{p^n - 1} = 1 \qquad \Longrightarrow \qquad x^{p^n} = x$$

folglich ist $f = X^{p^n} - X$ ein Polynom, dass nicht das Nullpolynom ist, aber $f(x) = 0$ für alle $x \in k$ erfüllt.

Man kann, ohne sich vorher diese Überlegungen zu machen, aber auch sofort sehen, dass das Polynom $g = \prod_{s \in k}(X - s)$ auch nicht das Nullpolynom ist, aber $g(x) = 0$ für alle $x \in k$ erfüllt.

Als letztes sei noch angemerkt, dass für endliches k jede Abbildung $\psi : k \to k$ ein Polynom ist. Das soll heißen, dass es für jedes ψ ein Polynom $f_\psi \in k\,[x]$ gibt mit $\psi(x) = f_\psi(x)$.
Dies zu sehen ist einfach. Setze

$$f_\psi = \sum_{s \in k} \ell_s(X) \cdot \psi(s)$$

dabei ist $\ell_s := \prod_{t \neq s} \frac{X-t}{s-t}$. Es ist nun $\ell_s(s) = 1$ und $\ell_s(t) = 0$ für $t \neq s$. Damit gilt dann offensichtlich $f_\psi(x) = \psi(x)$ für alle $x \in k$.
Als Korollar hier raus hat man: Es gibt Polynome mit $f \neq g$ und $f(x) = g(x)$ für alle $x \in k$, denn es gibt unendlich viele Polynome über k aber nur endlich viele Abbildungen von k nach k.