Algebra 1 Probeklausur

February 25, 2026

Aufgabe 1b

Satz: Bis auf Isomorphie gibt es genau einen Körper mit 4 Elementen.

Beweis:

1. Charakteristik und Dimension.

Sei K ein Körper mit $|K| = 4$. Die Charakteristik eines endlichen Körpers ist eine Primzahl p, und es gilt

$$|K| = p^n$$

für ein $n \in \mathbb{N}$.

Da $4 = 2^2$, folgt $p = 2$ und $n = 2$. Somit ist der Primkörper von K gleich $\mathbb{F}_2 = \{0, 1\}$, und K ist ein zweidimensionaler Vektorraum über $\mathbb{F}_2$:

$$[K : \mathbb{F}_2] = 2.$$

2. Existenz eines Körpers mit 4 Elementen.

Betrachte das Polynom

$$f(x) = x^2 + x + 1 \in \mathbb{F}_2[x].$$

Es gilt

$$f(0) = 1, \qquad f(1) = 1,$$

also besitzt f keine Nullstelle in $\mathbb{F}_2$ und ist daher irreduzibel.

Somit ist der Faktorring

$$\mathbb{F}_2[x]/(x^2 + x + 1)$$

ein Körper. Da das Polynom Grad 2 hat, besitzt dieser Körper

$$2^2 = 4$$

Elemente.

Damit existiert ein Körper mit 4 Elementen.

3. Eindeutigkeit bis auf Isomorphie.

Sei nun K ein beliebiger Körper mit 4 Elementen. Dann ist K eine Erweiterung von $\mathbb{F}_2$ vom Grad 2.

Wähle ein $\alpha \in K \setminus \mathbb{F}_2$. Dann ist $\{1, \alpha\}$ eine Basis von K über $\mathbb{F}_2$. Das Minimalpolynom von α über $\mathbb{F}_2$ hat Grad 2 und ist daher ein irreduzibles quadratisches Polynom in $\mathbb{F}_2[x]$.

Das einzige monische irreduzible Polynom vom Grad 2 über $\mathbb{F}_2$ ist

$$x^2 + x + 1.$$

Folglich erfüllt α die Gleichung

$$\alpha^2 + \alpha + 1 = 0.$$

Damit erhält man einen surjektiven Ringhomomorphismus

$$\varphi : \mathbb{F}_2[x] \to K, \qquad x \mapsto \alpha.$$

Der Kern ist das Ideal $(x^2 + x + 1)$. Nach dem Homomorphiesatz folgt

$$K \cong \mathbb{F}_2[x]/(x^2 + x + 1).$$

Schlussfolgerung.

Es existiert ein Körper mit 4 Elementen, und jeder Körper mit 4 Elementen ist zu diesem isomorph. Also gibt es bis auf Isomorphie genau einen Körper mit 4 Elementen.

□

Aufgabe 1c

Aufgabe. Untersuchen Sie $f(X) = X^4 + X + 1 \in \mathbb{F}_4[X]$ auf Irreduzibilität.

Lösung. Sei $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$ mit $\alpha^2 + \alpha + 1 = 0$. Die Elemente von $\mathbb{F}_4$ sind $0, 1, \alpha, \alpha + 1$. Für alle $x \in \mathbb{F}_4$ gilt die Frobenius-Identität $x^4 = x$ (da $4 = \#\mathbb{F}_4$), also

$$f(x) = x^4 + x + 1 = x + x + 1 = 1 \neq 0.$$

Daraus folgt, dass f keine Nullstelle in $\mathbb{F}_4$ besitzt; insbesondere hat f keine Linearfaktoren über $\mathbb{F}_4$.

Es bleibt zu prüfen, ob f als Produkt zweier quadratischer Polynome in $\mathbb{F}_4[X]$ zerfällt. Betrachte die monischen quadratischen Polynome $X^2+X+\alpha$ und $X^2+X+(\alpha+1)$. Wir rechnen ihr Produkt (in Charakteristik 2):

$$\begin{aligned}\big(X^2+X+\alpha\big)\big(X^2+X+\alpha+1\big) &= X^4+X^3+(\alpha+1)X^2+X^3+X^2+(\alpha+1)X\\ &\quad+\alpha X^2+\alpha X+\alpha(\alpha+1)\\ &= X^4+\big((\alpha+1)+1+\alpha\big)X^2+\big((\alpha+1)+\alpha\big)X+\alpha(\alpha+1).\end{aligned}$$

Da in $\mathbb{F}_2$ die Summanden sich paarweise aufheben und $\alpha^2=\alpha+1$, vereinfacht sich dies zu

$$X^4+X+1.$$

(Man kann die mittleren Terme mit direkter Ausmultiplizierung in $\mathbb{F}_4$ auch elementweise überprüfen; die obige Vereinfachung nutzt die Rechenregeln in charakteristischer 2 und die Relation $\alpha^2+\alpha+1=0$.)

Damit gilt die Faktorisierung

$$X^4+X+1=(X^2+X+\alpha)(X^2+X+\alpha+1)\quad \text{in } \mathbb{F}_4[X].$$

Zuletzt prüfen wir die Irreduzibilität der quadratischen Faktoren: Ein Polynom vom Grad 2 ist genau dann reduzierbar über $\mathbb{F}_4$, wenn es eine Nullstelle in $\mathbb{F}_4$ hat. Für $X^2+X+\alpha$ erhält man durch Einsetzen $x\in\{0,1,\alpha,\alpha+1\}$ jeweils die Werte $\alpha,\alpha,\alpha+1,\alpha+1$, also niemals 0. Analog hat $X^2+X+\alpha+1$ keine Nullstelle in $\mathbb{F}_4$. Daher sind beide quadratischen Polynome irreduzibel über $\mathbb{F}_4$.

Schluss. Das Polynom X^4+X+1 ist *reduzierbar* in $\mathbb{F}_4[X]$ und zerfällt in zwei irreduzible quadratische Faktoren:

$$X^4+X+1=(X^2+X+\alpha)(X^2+X+\alpha+1).$$