Mathematisches Institut
der Universität München
Andreas Fackler



# Klausurenkurs Algebra

## Aufgabe 1 (Frühjahr 2003, Thema 3, Aufgabe 4)

Sei $I$ ein zweiseitiges Ideal. Angenommen, $I$ enthält ein Element $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ mit $a \neq 0 \neq c$ (dies ist bereits erfüllt, wenn es ein Element mit $a \neq 0$ und eines mit $b \neq 0$ gibt, da dann die Summe diese Eigenschaft hat). Dann ist auch für alle $a', b', c' \in K$:

$$\begin{pmatrix} \frac{a'}{a} & \frac{ab'-a'b}{ac} \\ 0 & \frac{c'}{c} \end{pmatrix} \cdot \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} \in I,$$

also ist $I$ dann ganz $R$.

Nehmen wir nun an, $I$ enthalte nur Elemente der Form $\begin{pmatrix} 0 & b \\ 0 & c \end{pmatrix}$, aber mindestens eines mit $c \neq 0$. Dann ist auch für alle $b', c' \in K$:

$$\begin{pmatrix} 0 & \frac{b'}{c} \\ 0 & \frac{c'}{c} \end{pmatrix} \cdot \begin{pmatrix} 0 & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} 0 & b' \\ 0 & c' \end{pmatrix} \in I,$$

und damit enthält $I$ alle Matrizen der Form $\begin{pmatrix} 0 & b \\ 0 & c \end{pmatrix}$.

Als nächstes nehmen wir an, $I$ enthalte nur Elemente der Form $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$, und mindestens eines mit $a \neq 0$. Dann ist für alle $a', b' \in K$:

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} \frac{a'}{a} & \frac{b'}{a} \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a' & b' \\ 0 & 0 \end{pmatrix} \in I,$$

und damit enthält $I$ alle Matrizen der Form $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$.

Nehmen wir schließlich noch an, $I$ enthalte nur Elemente der Form $\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}$, sei aber nicht das Nullideal. Dann gibt es ein Element, bei dem $b \neq 0$ ist. Für jedes $b' \in K$ ist dann:

$$\begin{pmatrix} \frac{b'}{b} & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & b' \\ 0 & 0 \end{pmatrix} \in I,$$

alse enthält $I$ alle Matrizen der Form $\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}$.

Man rechnet leicht nach, dass diese Mengen auch tatsächlich zweiseitige Ideale sind.

## Aufgabe 2 (Herbst 2003, Thema 3, Aufgabe 2)

**(a)** Zunächst beobachten wir, dass derr Ring $R$ kommutativ ist: Ein Primideal ist also einfach ein Ideal $I$, so dass für alle $a, b \in R$ gilt: Wenn $a \cdot b \in I$, so ist $a \in I$ oder $b \in I$.

Sei $I$ ein Primideal. Angenommen, $I$ enthält ein Element $\begin{pmatrix} z & a' \\ 0 & z \end{pmatrix}$ mit $z \neq 0$. Dann ist auch für jedes $a \in \mathbb{Q}$: $\begin{pmatrix} 0 & \frac{a}{z} \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} z & a' \\ 0 & z \end{pmatrix} = \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} \in I$. Enthalte also nun $I$ kein solches Element. Das Nullideal ist kein Primideal, da etwa $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ ist.

Also ist $I \neq 0$ und hat daher mindestens ein Element der Form $\begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix}$ mit $a \neq 0$. Sei $a = \frac{p}{q}$ und sei $\frac{r}{s}$ eine beliebige weitere rationale Zahl. Wir müssen zeigen, dass $I$ die Matrix $\begin{pmatrix} 0 & \frac{r}{s} \\ 0 & 0 \end{pmatrix}$ enthält. Betrachte hierzu:

$$\begin{pmatrix} ps & 0 \\ 0 & ps \end{pmatrix} \cdot \begin{pmatrix} 0 & \frac{1}{sq} \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & \frac{p}{q} \\ 0 & 0 \end{pmatrix} \in I$$

Da $I$ Primideal ist, aber nur Matrizen dieser Form enthält, muss also der zweite Faktor in $I$ sein. Damit ist aber auch:

$$\begin{pmatrix} rq & 0 \\ 0 & rq \end{pmatrix} \cdot \begin{pmatrix} 0 & \frac{1}{sq} \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & \frac{r}{s} \\ 0 & 0 \end{pmatrix} \in I$$

Um die zweite Behauptung zu zeigen, definieren wir: $\varphi : R \to \mathbb{Z}, \qquad \varphi \begin{pmatrix} z & a \\ 0 & z \end{pmatrix} = z$. Man rechnet leicht nach, dass $\varphi$ ein Ringhomomorphismus ist. Offenbar ist $\varphi$ surjektiv und hat als Kern genau die Elemente $\begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix}$, also bilden diese ein Ideal $N$ mit $R/N \cong \mathbb{Z}$. Da $\mathbb{Z}$ ein Integritätsring ist, ist $N$ sogar prim.

**(b)** Da jedes Primideal Obermenge von $N$ ist, sind die Primideale von $R$ genau die Urbilder der Primideale von $R/N \cong \mathbb{Z}$, also außer $N$ die Ideale

$$\left\{ \begin{pmatrix} pz & a \\ 0 & pz \end{pmatrix} \mid z \in \mathbb{Z}, a \in \mathbb{Q} \right\}$$

für Primzahlen $p$.

## Aufgabe 3 (Frühjahr 2004, Thema 1, Aufgabe 2)

Wir wenden das Reduktionskriterium mit dem kanonischen Homomorphismus $\varphi : \mathbb{Z} \to \mathbb{Z}_2$ und zeigen, dass $f^\varphi(X) = X^4 + X^3 + 1$ irreduzibel in $\mathbb{Z}_2[X]$ ist. Wegen $f^\varphi(0) = 1 = f^\varphi(1)$ hat $f^\varphi$ keine Nullstelle, also keinen Faktor vom Grad 1. Nehmen wir nun an, $f^\varphi$ hätte eine Darstellung der Form $f^\varphi(X) = (X^2 + mX + 1)(X^2 + nX + 1)$. (Die konstanten und die höchsten Koeffizienten müssen offenbar 1 sein.) Da der Koeffizient von $X$ in $f^\varphi$ verschwindet, muss $n+m=0$ sein. Da der Koeffizient von $X^3$ in $f^\varphi$ eins ist, muss aber $n+m=1$ sein, ein Widerspruch.

## Aufgabe 4 **(Frühjahr 2004, Thema 3, Aufgabe 1)**

**(a)** Es ist

$$\begin{aligned} x^4+x^3+x^2+1 &\equiv x^4+x^2 \equiv x^2+x \mod (x^3+1) \text{ und} \\ x^2+1 &\equiv x^3+x^2 \mod (x^3+1), \end{aligned}$$

also können wir $f=x^2$ setzen.

**(b)** $x^2+1$ hat keine Nullstelle in $\mathbb{F}_3$, ist also irreduzibel. $x^3+1 \equiv (x+1)^3 \mod 3$. Also sind $x^2+1$ und $x^3+1$ in $K[x]$ teilerfremd, so dass man 1 als Linearkombination hiervon darstellen kann, so dass es also ein $a \in K[x]$ gibt mit $(x^2+1)\cdot a \equiv 1 \mod (x^3+1)$. $f=a\cdot g$ löst dann die gefragte Kongruenz.

**(c)** Wir wenden den erweiterten euklidischen Algorithmus im euklidischen Ring $K[X]$ an, um die 1 darzustellen:

$$\begin{aligned} x^3+1 &= x\cdot(x^2+1)+(-x+1) \\ x^2+1 &= (-x-1)\cdot(-x+1)-1 \end{aligned}$$

Also ist

$$\begin{aligned} (-x+1) &= (x^3+1)-x\cdot(x^2+1) \text{ und damit} \\ 1 &= (-x-1)\cdot(-x+1)-(x^2+1) \\ &= (-x-1)\cdot((x^3+1)-x\cdot(x^2+1))-(x^2+1) \\ &= (-x-1)\cdot(x^3+1)+(x^2+x-1)\cdot(x^2+1) \end{aligned}$$

in $K[x]$. Somit ist $f(x)=x^2+x-1$ eine Lösung der Kongruenz.