Mathematisches Institut der Universität München | Stefan Gille
Wintersemester 2009/10 | Lukas-Fabian Moser

Algebra – Lösungsideen zum 6. Übungsblatt

Aufgabe 1. Es ist $P = Rx$, wobei nach Vorlesung $x \in R$ ein Primelement ist. Angenommen, P wäre kein maximales Ideal; dann gäbe es ein $y \in R$ mit $Rx \subsetneq Ry \subsetneq R$. Dann hätten wir aber $y \mid x$, also (da x irreduzibel ist) $Ry = Rx$ oder $Ry = R$, Widerspruch. Also ist P doch maximal, und nach Vorlesung folgt daraus, daß R/P ein Körper ist.

Aufgabe 2. In einem Integritätsring addieren sich Grade von Polynomen beim Multiplizieren: es ist $\deg(fg) = \deg(f) + \deg(g)$ für alle $F, G \in R[X]$, wobei wir zur Sicherheit $\deg 0 := -\infty$ vereinbaren. Das überlegt man sich durch Ausmultiplizieren: das Produkt von $\sum_{i=0}^{n} a_i X^i$ und $\sum_{j=0}^{m} b_j X^j$ beginnt mit $a_n b_m X^{n+m}$, und aus $a_n \neq 0 \neq b_m$ folgt $a_n b_m \neq 0$, da R ein Integritätsring ist.
Jedenfalls folgt damit aus einer Gleichung $F \cdot G = 1$, daß $\deg(F) + \deg(G) = 0$ sein muß, also $\deg(F) = \deg(G) = 0$. Also ist $F \in R$ eine Zahl (will heißen, ein Element des Grundrings), und durch Einsetzen von $X = 0$ sieht man, daß F in R invertierbar sein muß. Das zeigt die Inklusion $R[X]^\times \subset R^\times$, und die umgekehrte Inklusion ist klar.
Also: Die Einheiten in $R[X]$ sind genau die des Grundrings.

Aufgabe 3. Zunächst ist ein Polynom vom Grad 1 über einem Körper *immer* irreduzibel: denn aus $F = GH$ mit $\deg(F) = 1$ folgt $1 = \deg(G) + \deg(H)$, und damit muß (notfalls nach Vertauschen von G und H) $\deg(G) = 0$ sein. Also ist $G \in K$ und sicherlich $G \neq 0$ (sonst hätte F kaum Grad 1), d.h. $G \in K^\times$ ist invertierbar. Ein Polynom vom Grad 0 über einem Körper ist dagegen niemals irreduzibel, denn es ist entweder Null oder eine Einheit.

i) Jedes nichtkonstante Polynom F über $\mathbb{C}$ hat eine Nullstelle $a \in \mathbb{C}$ („Fundamentalsatz der Algebra") und damit einen Faktor vom Grad 1, nämlich $X - a$. Ist insbesondere $\deg F \geqslant 2$, so ist F damit reduzibel. Also bleiben nur die Polynome vom Grad 1 übrig, die, wie gesagt, alle irreduzibel sind.
ii) Ist $n \geqslant 1$ beliebig, so ist beispielsweise das Polynom $X^n - 2 \in \mathbb{Q}[X]$ irreduzibel nach dem Kriterium von Eisenstein.

Aufgabe 4. Schön der Reihe nach.

i) Betrachten wir zunächst (nicht ganz so ehrgeizig) Faktorisierungen von F nicht in $\mathbb{Q}[X]$, sondern nur in $\mathbb{Z}[X]$ – davon gibt's ja sicher weniger. Aus $F = GH$ mit $G, H \in \mathbb{Z}[X]$ folgt $\overline{F} = \overline{GH}$ in $\mathbb{Z}/p\mathbb{Z}[X]$, also (notfalls nach Vertauschen von G und H) $\deg \overline{G} = 0$. Nun gilt aber $\deg \overline{G} = \deg G$, wie man beispielsweise an den Beziehungen

$$\deg \overline{G} + \deg \overline{H} = \deg \overline{F} = \deg F = \deg G + \deg H$$
$$\deg \overline{G} \leqslant \deg G$$
$$\deg \overline{H} \leqslant \deg H$$

ablesen kann. Das heißt also: Faktorisiert man F in $\mathbb{Z}[X]$, so hat einer der Faktoren Grad 0.

ii) Daraus kann man nun ganz allgemein die Irreduzibilität in $\mathbb{Q}[X]$ folgern: Sei nämlich $F = GH$ mit $G, H \in \mathbb{Q}[X]$. Wir können (da Konstanten in $\mathbb{Q}[X]$ nichts ausmachen) annehmen, daß G in $\mathbb{Z}[X]$ liegt und primitiv ist (d.h. Einheitsform hat). Ich behaupte, daß dann H ebenfalls automatisch in $\mathbb{Z}[X]$ liegt: Schreiben wir nämlich

$$F = a\widetilde{F} \quad \text{und} \quad H = \frac{b}{c}\widetilde{H}$$

mit primitiven Polynomen $\widetilde{F}, \widetilde{H} \in \mathbb{Z}[X]$ und $a, b, c \in \mathbb{Z}$, so folgt aus $F = GH$ die Beziehung

$$ac\widetilde{F} = bG\widetilde{H}$$

in $\mathbb{Z}[X]$. Nach dem Gaußschen Lemma ist aber $G\widetilde{H}$ wieder primitiv; der ggT der Koeffizienten der Seite der Gleichung ist also b, derjenige der linken Seite ac, und daraus folgt $b = \pm ac$. Daraus folgt aber $H = \pm a\widetilde{H} \in \mathbb{Z}[X]$, und damit ist $F = GH$ eine Faktorisierung in $\mathbb{Z}[X]$. Nach Teil i) hat damit aber G oder H den Grad 0 und ist damit (in $\mathbb{Q}[X]$) invertierbar. Also ist F in $\mathbb{Q}[X]$ irreduzibel.

Zusatzaufgabe. Die Polynome vom Grad 1 sind allesamt irreduzibel. Ein Polynom vom Grad 2 ist genau dann irreduzibel, wenn es keine reelle Nullstelle besitzt, wenn es also die Form $aX^2 + bX + c$ hat mit $b^2 - 4ac < 0$.
Sei nun $F \in \mathbb{R}[X]$ irreduzibel vom Grad > 2. F hat sicher eine komplexe Nullstelle a; da F aber keine reellen Nullstellen haben kann, folgt $a \in \mathbb{C} - \mathbb{R}$. Nun folgt aber aus $F(a) = 0$ auch $F(a^*) = 0$, wobei a^* die komplex Konjugierte von a bezeichnet. (Um das einzusehen, schreibe man die Gleichung $F(a) = 0$ aus und komplexkonjugiere beide Seiten). Da a aber nicht reell ist, folgt $a \neq a^*$, also ist F in $\mathbb{C}[X]$ sogar durch $G = (X - a)(X - a^*)$ teilbar – aber dies ist ein *reelles* Polynom, denn es ist $G = X^2 - 2\,\mathrm{Re}(a) + |a|^2$.
Aus $F, G \in \mathbb{R}[X]$ und $G \mid F$ in $\mathbb{C}[X]$ folgt aber $G \mid F$ in $\mathbb{R}[X]$; am einfachsten sieht man das wohl daran, daß beim Ausführen der Polynomdivision nur Körperoperationen verwendet werden, die also niemals aus $\mathbb{R}$ hinausführen können. Da aber F irreduzibel ist, folgt damit $\deg F = \deg G = 2$, Widerspruch.
Die irreduziblen Polynome über $\mathbb{R}$ sind also genau die linearen Polynome $aX + b$ mit $a \neq 0$ und die quadratischen Polynome $aX^2 + bX + c$ mit $b^2 < 4ac$.