Universität Konstanz
Fachbereich Mathematik und Statistik
Prof. Dr. Markus Schweighofer
Dr. Sven Wagner

Sommersemester 2010
Übungsblatt 24
21.06.2010

Lineare Algebra II

Aufgabe 24.1:

(a) Bestimmen Sie eine Primfaktorzerlegung von

(i) 15246 in $\mathbb{Z}$,
(Lösung: $15246 = 2 \cdot 7623$, $7 + 6 + 2 + 3 = 18 \equiv 0 mod 9$, $7623 = 847 \cdot 3 \cdot 3$, $847 = 7 \cdot 121$, $121 = 11 \cdot 11$, also $15246 = 2 \cdot 3 \cdot 3 \cdot 7 \cdot 11 \cdot 11$.)

(ii) $X^3 - 2X^2 + X - 2$ in $\mathbb{Q}[X]$ und
(Lösung: 2 ist offensichtlich Nullstelle, $X^3 - 2X^2 + X - 2 = (X-2)(X^2+1)$, X^2+1 irreduzibel (also prim), da nur Primfaktoren vom Grad ≤ 2 in Frage kommen, es aber keine Nullstelle in $\mathbb{Q}$ hat.)

(iii) $X^5 + X^4 + X^3 + X^2 + 1$ in $\mathbb{F}_3[X]$.
(Lösung: Keine Nullstellen in $\mathbb{F}_3$, ausprobieren aller normierten Polynome vom Grad 2 mit von 0 verschiedenem konst. Term (6 solche gibt es) ergibt: $X^5 + X^4 + X^3 + X^2 + 1 = (X^2 + X - 1)(X^3 - X - 1)$.)

(b) Bestimmen Sie einen ggT und ein kgV von $X^8 - X^6 + X^5 - X^4 - X^2 - X + 1$ und $X^5 + X^4 + X^3 + X^2 + 1$ in $\mathbb{F}_3[X]$.
(Lösung: Betrachten die Primfaktorzerlegung von $X^5 + X^4 + X^3 + X^2 + 1$: $X^2 + X - 1$ ist kein Teiler von $X^8 - X^6 + X^5 - X^4 - X^2 - X + 1$, aber $X^3 - X - 1$. Es gilt dann $X^8 - X^6 + X^5 - X^4 - X^2 - X + 1 = (X^3 - X - 1)^2(X^2 + 1)$. Aus den beiden Primfaktorenzerlegungen kann man direkt einen ggT und ein kgV ablesen.)

Aufgabe 24.2:

Wir betrachten den Integritätsbereich $\mathbb{Z}[\mathring{\imath}] = \{a + b\mathring{\imath} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$.

(a) Zeigen Sie, dass $\mathbb{Z}[\mathring{\imath}]^\times = \{x \in \mathbb{Z}[\mathring{\imath}] \mid |x| = 1\}$ gilt, und geben Sie alle Einheiten an.
(Lösung: $a^2 + b^2 = 1$ gdw. entweder $a = \pm 1$ und $b = 0$ oder umgekehrt.)

(b) Zeigen Sie, dass eine Primzahl $p \in \mathbb{P}$ genau dann reduzibel in $\mathbb{Z}[\mathring{\imath}]$ ist, wenn es $a, b \in \mathbb{Z}$ mit $p = a^2 + b^2$ gibt.
(Lösung: $\Leftarrow$: $p = a^2 + b^2 = (a + b\mathring{\imath})(a - b\mathring{\imath})$. $\Rightarrow$: $p = (a + b\mathring{\imath})(c + d\mathring{\imath})$, beide Faktoren keine Einheit. Das Quadrat des Betrages in $\mathbb{C}$ ergibt dann $p^2 = (a^2 + b^2)(c^2 + d^2)$. p ist prim in $\mathbb{Z}$, teilt also eine der Quadratsummen, etwa $a^2 + b^2$. Aber p^2 teilt nicht $a^2 + b^2$, da sonst $c^2 + d^2 = 1$ wäre und somit $c + d\mathring{\imath}$ eine Einheit, ein Widerspruch. Also $a^2 + b^2 = p = c^2 + d^2$.)

(c) Überprüfen Sie, ob die Elemente $1 + \mathring{\imath}$, 2, 3 irreduzibel oder gar prim in $\mathbb{Z}[\mathring{\imath}]$ sind.
(Lösung: In Wirklichkeit ist hier *irreduzibel* gleich *prim*, da $\mathbb{Z}[\mathring{\imath}]$ faktoriell ist, aber das wissen die Studenten nicht. $2 = 1 + 1$ ist nach (b) reduzibel, also auch nicht prim. (3 ist nach (b) irreduzibel.) $1 + \mathring{\imath}$ und 3 sind prim: Man sieht $1 + \mathring{\imath}$ teilt $a + b\mathring{\imath}$ genau dann, wenn $a + b$ gerade ist, also teilt $1 + \mathring{\imath}$ genau dann $(a + b\mathring{\imath})(c + d\mathring{\imath})$, wenn $ac - bd + ad + bc$ gerade ist. Das ist genau dann der Fall, wenn $ac - bd + ad + bc + 2bd = (a + b)(c + d)$ gerade ist. Somit muß dann $a + b$ oder $c + d$ gerade sein, und $1 + \mathring{\imath}$ teilt dementsprechend

$a+b\mathring{i}$ oder $c+d\mathring{i}$. 3 teilt $(a+b\mathring{i})(c+d\mathring{i})$ gdw. 3 teilt $ac-bd$ und $ad+bc$. Durch Rechnen modulo 3 (alle 9 Restklassenkombinationen von c und d durchprobieren), sieht man: Teilt 3 nicht c und d, so teilt 3 aber a und b. Mir fällt gerade keine elegantere Methode ein, aber vielleicht euch oder den Studenten.)

Aufgabe 24.3:

Nun betrachten wir den Integritätsbereich $\mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ und die Abbildung $N\colon \mathbb{Z}[\sqrt{5}] \to \mathbb{Z}$, $a + b\sqrt{5} \mapsto a^2 - 5b^2$.

(a) Zeigen Sie, dass $N(xy) = N(x)N(y)$ für alle $x, y \in \mathbb{Z}[\sqrt{5}]$ gilt.
(Lösung: $N(a + b\sqrt{5}) = (a + b\sqrt{5})(a - b\sqrt{5})$.)

(b) Zeigen Sie, dass $\mathbb{Z}[\sqrt{5}]^\times = \{x \in \mathbb{Z}[\sqrt{5}] \mid N(x) \in \mathbb{Z}^\times\}$ gilt, und geben Sie eine Einheit an, die nicht ± 1 ist.
(Lösung: klar mit (a), $2 + \sqrt{5}$.)

(c) Zeigen Sie, dass 2 ein irreduzibles Element von $\mathbb{Z}[\sqrt{5}]$ ist, das nicht prim ist.
(Lösung: $N(2) = 4$, wäre 2 reduzibel, so wäre $a^2 - 5b^2 = N(a + b\sqrt{5}) = 2$ für einen Nichteinheitsteiler $a + b\sqrt{5}$ von 2, aber 2 ist kein Quadrat modulo 5. 2 ist nicht prim, da $2 \cdot 2 = 4 = (1 + \sqrt{5})(-1 + \sqrt{5})$, aber 2 teilt nicht $1 + \sqrt{5}$ und nicht $-1 + \sqrt{5}$ in $\mathbb{Z}[\sqrt{5}]$.)

Abgabe bis Montag, den 28. Juni, 10 Uhr in die Briefkästen neben F411.