WS 05/06
Priv.-Doz. Dr. S. Wewers
Andreas Martin

Algebra I

9. Übungsblatt

Lösungen.

Lemma *Ist $a \in \mathbb{Z}[i]$, und ist $|a|^2$ eine Primzahl, so ist a ein Primelement von $\mathbb{Z}[i]$.*
Beweis: Da $\mathbb{Z}[i]$ ein faktorieller Ring ist, genügt es zu zeigen, daß a irreduzibel ist. Wir nehmen also an, es gäbe eine Faktorisierung $a = b \cdot c$ mit $b, c \in \mathbb{Z}[i]$. Dann folgt

$$|a|^2 \;=\; |b|^2 \cdot |c|^2 \;,$$

und da $|a|^2$ eine Primzahl ist, gilt $|b|^2 = 1$ oder $|c|^2 = 1$, d.h. $|b| = 1$ oder $|c| = 1$. Im Ring $\mathbb{Z}[i]$ sind aber die Elemente mit komplexem Betrag 1 genau die Einheiten $\pm 1, \pm i$. Also ist b oder c eine Einheit in $\mathbb{Z}[i]$. Folglich ist a irreduzibel. □

Aufgabe 1:

(a) Wir betrachten die Primfaktorzerlegung in $\mathbb{Z}$ von $|a|^2$, d.h.

$$x^2 + y^2 \;=\; |a|^2 \;=\; p_1 \cdot \ldots \cdot p_r$$

mit (nicht notwendig verschiedenen) Primzahlen $p_1, \ldots, p_r$. Wegen $a \cdot \bar{a} = |a|^2$ gilt

$$a \mid p_1 \cdot \ldots \cdot p_r$$

in $\mathbb{Z}[i]$. Da a ein Primelement ist, folgt $a | p_\varrho$ für ein $\varrho \in \{1, \ldots, r\}$. Mit $p := p_\varrho$ gilt daher $a|p$ und $p|(x^2 + y^2)$.

Zusatz: Aus $a|p$ in $\mathbb{Z}[i]$ folgt auch noch $|a|^2 = (x^2 + y^2)|p^2$ in $\mathbb{Z}$. Also ist $|a|^2 = p$ oder $|a|^2 = p^2$.

(b) „$\Rightarrow$“: Ist $p = x^2 + y^2$ für gewisse $x, y \in \mathbb{Z}$, so folgt $x^2 \equiv 0$ oder $1 \mod 4$ und $y^2 \equiv 0$ oder $1 \mod 4$. Daher ist $p = x^2 + y^2 \equiv 0, 1$ oder $2 \mod 4$. Mit anderen Worten, es gilt $p \not\equiv 3 \mod 4$. Ferner gilt dann

$$p \;=\; (x + iy)(x - iy) \;,$$

und $x + iy$ bzw. $x - iy$ haben den komplexen Betrag $\sqrt{p}$. Nach obigem Lemma handelt es sich um Primelemente von $\mathbb{Z}[i]$.

„$\Leftarrow$“: Im Falle $p \neq 2$ ist die bereits in der Vorlesung bewiesen worden. Im Falle $p = 2$ gilt $p = 1^2 + 1^2$.

(c) Wir unterscheiden drei Fälle. (Bemerkung: Die Begriffe „irreduzibel“ und „Primelement“ sind im faktoriellen Ring $\mathbb{Z}[i]$ gleichbedeutend.)

- Fall $p = 2$. Dann ist $p = (1 + i)(1 - i)$, also nicht irreduzibel.
- Fall $p \equiv 1 \mod 4$. Dann zerfällt p in ein Produkt zweier Primelemente nach (b). Also ist p nicht irreduzibel.

- Fall $p \equiv 3 \mod 4$. Wir nehmen an, p wäre nicht irreduzibel in $\mathbb{Z}[i]$. Also gilt $p = \pi\sigma$ mit gewissen $\pi, \sigma \in \mathbb{Z}[i]$, welche keine Einheiten sind. Es folgt $|\pi| > 1$ und $|\sigma| > 1$. Es wird
$$p^2 \;=\; |\pi|^2 \cdot |\sigma|^2 \;,$$
und daher $|\pi|^2 = |\sigma|^2 = p$. Wir schreiben $\pi = x + iy$ für gewisse $x, y \in \mathbb{Z}$ und haben also
$$p \;=\; \pi \cdot \bar{\pi} \;=\; x^2 + y^2 \;,$$
im Widerspruch zur in der Vorlesung bewiesenen Tatsache, daß Primzahlen $\equiv 3 \mod 4$ nicht Summe zweier Quadrate sind.

(d) (i) Nach Teil (c) und dem obigen Lemma sind alle angegebenen Elemente der Menge P in der Tat Primelemente von $\mathbb{Z}[i]$.

(ii) Wegen $(\mathbb{Z}[i])^\times = \{\pm 1, \pm i\}$ sind sie auch paarweise nicht assoziiert.

(iii) Es bleibt zu zeigen, daß jedes Primelement von $\mathbb{Z}[i]$ zu einem Element von P assoziiert ist. Es sei also $a = x + iy$ ein Primelement von $\mathbb{Z}[i]$. Nach (a) gibt es eine Primzahl $p \in \mathbb{Z}$ so, daß $a|p$ und $p|(x^2 + y^2)$ gilt. Nach dem Zusatz in (a) folgt außerdem $x^2 + y^2 = p$ oder $x^2 + y^2 = p^2$. Wir unterscheiden diese beiden Fälle.

- Fall $x^2 + y^2 = p$. Also gilt auch $x, y \neq 0$. Nach (b) folgt $p = 2$ oder $p \equiv 1 \mod 4$.
  Im Falle $p = 2$ ist $a \cdot \bar{a} = (1+i)(1-i)$, und diese sind nach dem Lemma allesamt Primelemente. Wegen $1 + i \sim 1 - i$ und der Eindeutigkeit der Primfaktorzerlegung folgt $a \sim 1 + i$.
  Im Falle $p \equiv 1 \mod$ kann man a mit einer Einheit $\pm$ oder $\pm i$ multiplizieren, so daß o.B.d.A. $x \geq |y| > 0$ gilt. Der Fall $x = |y|$ ist jedoch ausgeschlossen, da sonst $p = 2x^2$ gerade wäre. Also ist $x > |y| > 0$.
- Fall $x^2 + y^2 = p^2$. Mit a ist auch $\bar{a}$ ein Primelement, denn die komplexe Konjugation stellt einen Ringautomorphismus von $\mathbb{Z}[i]$ dar. Also folgt aus $a \cdot \bar{a} = p$ sogleich $a|p$ und $\bar{a}|p$. Daher gibt es $r, s \in \mathbb{Z}[i]$ so, daß $ar = p = \bar{a}s$. Es folgt
$$p^2 \;=\; ar\bar{a}s \;=\; p^2 rs \;,$$
und daher $rs = 1$, d.h. $r, s \in \mathbb{Z}[i]$. Folglich gilt $a \sim p$, und nach (c) folgt $p \equiv 3 \mod 4$.

(e) Indem wir zunächst die Primfaktorzerlegung in $\mathbb{Z}$ bestimmen und dann Teil (b) zur weiteren Faktorisierung verwenden, erhalten wir
$$\begin{aligned} 1258 &= 2 \cdot 17 \cdot 37 \;=\; (1^2 + 1^2)(4^2 + 1^2)(6^2 + 1^2) \\ &= (1 + i)(1 - i)(4 + i)(4 - i)(6 + i)(6 - i) \;. \end{aligned}$$
Nach (b) bzw. (d) sind dies jeweils Primelemente.

Im Falle von $5 + 7i$ bestimmen wir zunächst die Primfaktorzerlerung von $|5 + 7i|^2$ zu
$$\begin{aligned} (5 + 7i)(5 - 7i) &= 25 + 49 \;=\; 74 \;=\; 2 \cdot 37 \\ &= (1 + i)(1 - i)(6 + i)(6 - i) \;. \end{aligned}$$
Wegen $1 + i \sim 1 - i$ muß $1 + i$ ein Teiler von $5 + 7i$ sein (man kann alternativ auch einen der vier möglichen Faktoren erraten). Es wird
$$\frac{5 + 7i}{1 + i} \;=\; \frac{(5 + 7i)(1 - i)}{2} \;=\; 6 + i \;,$$

d.h. es gilt

$$5 + 7i = (1+i)(6+i) .$$

Aufgabe 3:

(a) Über einem Körper sind alle Polynome vom Grade 0 nicht irreduzibel (da sie 0 oder Einheiten sind), und alle Polynome vom Grade 1 sind irreduzibel. Ferner sind genau diejenigen Polynome vom Grade 2 oder 3 irreduzibel, welche keine Nullstelle in jenem Körper haben. (Vorsicht! Dieses Kriterium gilt **nur** für Polynome vom Grade 2 und 3.) Die Nullstellenfreiheit in $\mathbb{F}_3$ überprüft man durch Einsetzen von $0, 1$ und 2 (, wobei man anstelle von 2 auch -1 schreiben kann). Es genügt, zuerst die normierten Polynome anzugeben. Sämtliche irreduziblen Polynome erhält man dann, indem man diese mit 2 (der einzigen Einheit $\neq 1$) mutlipliziert. Damit ergibt sich folgende Liste der irreduziblen Polynome in $\mathbb{F}_3[X]$ vom Grade ≤ 3.

$$\begin{array}{l}
X, \quad X+1, \quad X+2, \\
2X, \quad 2X+2, \quad 2X+1, \\
X^2+1, \quad X^2+X+2, \quad X^2+2X+2, \\
2X^2+2, \quad 2X^2+2X+1, \quad 2X^2+X+1 \\
X^3+2X+1, \quad X^3+2X+2, \\
X^3+X^2+2, \quad X^3+X^2+X+2, \\
X^3+X^2+2X+1, \quad X^3+2X^2+1, \\
X^3+2X^2+X+1, \quad X^3+2X^2+2X+2, \\
2X^3+X+2, \quad 2X^3+X+1, \\
2X^3+2X^2+1, \quad 2X^3+2X^2+2X+1, \\
2X^3+2X^2+X+2, \quad 2X^3+X^2+2, \\
2X^3+X^2+2X+2, \quad 2X^3+X^2+X+1 \quad .
\end{array}$$

(b) Es genügt zu zeigen, daß f irreduzibel in $\mathbb{Z}[X]$ ist. Wir betrachten die Reduktion modulo 3, d.h. den Ringhomomorphismus

$$\mathbb{Z}[X] \to \mathbb{F}_3[X], \; f \mapsto \overline{f} ,$$

welcher die Koeffizienten von f auf die zugehörigen Restklassen modulo 3 abbildet. Es gilt also

$$\overline{f} = X^4 + 2X^2 + 2X = X(X^3 + 2X + 2)$$

in $\mathbb{F}_3[X]$. Nach (a) ist dies die Primfaktorzerlegung von $\overline{f}$. Wir nehmen nun an, f wäre nicht irreduzibel. Dann gäbe es eine Faktorisierung $f = gh$ mit normierten Polynonem $g, h \in \mathbb{Z}[X]$ vom Grade ≤ 3. Es folgt

$$\overline{f} = \overline{gh} = \overline{g}\,\overline{h} ,$$

und die Polynome $\overline{g}, \overline{h} \in \mathbb{F}_3[X]$ sind ebenfalls nomiert und vom selben Grade wie g bzw. h. Wegen der Eindeutigkeit der Primfaktorzerlegung im faktoriellen Ring $\mathbb{F}_3[X]$ und obiger Primfaktorzerlegung von $\overline{f}$ folgt also $\overline{g} = X$ oder $\overline{h} = X$, d.h. $\deg g = 1$ oder $\deg h = 1$. Dann hätte f eine Nullstelle α in $\mathbb{Z}$. Diese müßte dann ein Teiler von 3 sein wegen $\alpha^4 - \alpha^2 + 2\alpha + 3 = 0$. Es gilt jedoch $f(\alpha) \neq 0$ für $\alpha = \pm 1, \pm 3$. Dies ist ein Widerspruch, und die Annahme war falsch. Daher ist f irreduzibel in $\mathbb{Z}[X]$ und in $\mathbb{Q}[X]$.

(c) Der Ring $\mathbb{F}_3[X]$ ist euklidisch, d.h. ein Hauptidealring. Das Polynom g ist irreduzibel nach (a). Nach Vorlesung ist daher (g) ein maximales Ideal von $\mathbb{F}_3[X]$. Folglich ist

$$K \;:=\; \mathbb{F}_3[X]/(g)$$

ein Körper. Wir bezeichnen dan kanonische Bild eines Polynoms $f \in \mathbb{F}_3[X]$ in K mit $\overline{f}$. In K gilt

$$h(\overline{X}) \;=\; \overline{X}^3 - \overline{X} + \overline{1} \;=\; \overline{g} \;=\; \overline{0} \;=\; 0\;.$$

Also ist $\overline{X}$ eine Nullstelle von h. Polynomdivision ergibt

$$h \;=\; (Y - \overline{X})(Y^2 + \overline{X}Y + \overline{X}^2 - 1)\;.$$

Zur vollständigen Faktorisierung suchen wir also $a, b \in K$ so, daß

$$(Y - a)(Y - b) \;=\; (Y^2 + \overline{X}Y + \overline{X}^2 - 1)\;,$$

d.h. es soll $ab = \overline{X}^2 - 1 = (\overline{X} - 1)(\overline{X} + 1)$ und $a + b = -\overline{X}$ gelten. Durch Raten ergibt sich $a = \overline{X} - 1$ und $b = \overline{X} + 1$ und somit

$$h \;=\; (Y - \overline{X})(Y - \overline{X} + 1)(Y - \overline{X} - 1)\;.$$

Aufgabe 3:

(a) Das Polynom $X^4 + 6X + 10$ ist irreduzibel in $\mathbb{Z}[X]$ und $\mathbb{Q}[X]$ nach Eisenstein, denn $p := 2$ teilt 6 und 10 aber nicht 1, und p^2 teilt nicht 10.

(b) Das Polynom $X^3 + 1$ hat die Nullstelle -1 in $\mathbb{F}_5$. Also läßt sich ein linearer Faktor abspalten, und es ist es nicht irreduzibel in $\mathbb{F}_5[X]$.

(c) Das Polynom $X^3 - X + 1$ hat keine Nullstelle in $\mathbb{F}_2$. Da es vom Grade 2 oder 3 ist, ist es daher irreduzibel in $\mathbb{F}_2[X]$.

(d) Wir betrachten $X^3 - XY - Y \in \mathbb{C}[X, Y] = \mathbb{C}[Y][X]$ als Polynom in X über dem faktoriellen Ring $\mathbb{C}[Y]$. Das Element $Y \in \mathbb{C}[Y]$ ist ein Polynom vom Grade 1, also irreduzibel in $\mathbb{C}[Y]$. Dann folgt die Irreduzibilität nach Eisenstein, denn Y teilt alle Koeffizienten außer dem führenden, und Y^2 teilt nicht den niedrigsten Koeffizienten.