Universität Konstanz
Fachbereich Mathematik und Statistik
Jun.-Prof. Dr. Arno Fehm
Aaron Kunert
SS 2012

Übungen zur Vorlesung Zahlentheorie

Blatt 12

Aufgabe 48

Wir schreiben zunächst $R := \mathbb{Z}[\sqrt{-2}]$ und verwenden, dass R ein Hauptidealring, also insbesondere faktoriell ist.

a) Sei d ein gemeinsamer Teiler von $(y+\sqrt{-2})$ und $(y-\sqrt{-2})$ in R. Inbesondere teilt d dann auch $2y = (y+\sqrt{-2}) + (y-\sqrt{-2})$ und $2\sqrt{-2} = (y+\sqrt{-2}) - (y-\sqrt{-2})$. Es ist $N(\sqrt{-2}) = 2$, daher ist $\sqrt{-2}^3$ die Primfaktorzerlegung von $2\sqrt{-2}$. Dies zeigt, dass d eine Potenz von $\sqrt{-2}$ ist. Angenommen $d \neq 1$, so ist $\sqrt{-2}$ ein Teiler von $(y+\sqrt{-2})$ und damit ist 2 ein Teiler von y in $\mathbb{Z}$. Dies ist jedoch nicht möglich, denn dann ist $y^2 + 2 \equiv 2 \bmod 4$, also x gerade, aber dann ist $x^3 \equiv 0 \bmod 4$. Dies ist unmöglich und daher ist $d = 1$.

b) Sei $x = p_1^{e_1} \cdots p_r^{e_r}$ die Primfaktorzerlegung von x in R. Seien diese so angeordnet, dass $p_1, \ldots, p_l$ genau die Primteiler von x sind, die auch $(y+\sqrt{2})$ teilen. Dann folgt aus Teil a), dass $(p_1^{e_1} \cdots p_l^{e_l})^3 = (y+\sqrt{-2})$.

c) Sei $X^3 = Y^2 + 2$, dann gibt es wegen Teil b) ein $\alpha = (a + b\sqrt{-2})$ mit $a, b \in \mathbb{Z}$ und $\alpha^3 = (Y + \sqrt{-2})$. Man erhält

$$a^3 + 3\sqrt{-2}a^2b - 6ab^2 - 2\sqrt{-2}b^3 = Y + \sqrt{-2}.$$

Vergleich von Koeffizienten liefert

$$a^3 - 6a^2b = Y$$
$$3a^2b - 2b^3 = 1.$$

Da die zweite Gleichung durch b teilbar ist, folgt $b \in \mathbb{Z}^\times$, also $b = \pm 1$. Ist $b = 1$, so muss $3a^2 - 2 = 1$ gelten, also ist $a = \pm 1$. Ist $b = -1$, so müsste $3a^2 + 2 = 1$ gelten, was unmöglich ist. Also lässt sich obiges System nur lösen für $a = \pm 1$, $b = 1$. Dies führt dann zu den Lösungen $Y = \mp 5$ und damit zu $X = 3$.

Für den restlichen Teil der Aufgabe schreiben wir $R := \mathbb{Z}[\sqrt{-5}]$. Wir verwenden, dass die Klassengruppe von R Ordnung 2 hat.

d) Zunächst überlegen wir uns, dass y gerade sein muss. Angenommen y wäre ungerade, dann ist $y \equiv 1 \bmod 8$ und daher wäre y^2+5 gerade. Dann wäre $2 \mid x$ und somit $8 \mid x^3$, aber $y^2 + 5 \equiv 6 \bmod 8$, ein Widerspruch. Wir betrachten das Ideal $I = (y+\sqrt{-5}) + (y-\sqrt{-5})$. Zu zeigen ist $I = R$. Angenommen, dies ist nicht der Fall. Dann gibt es ein Primideal $\mathfrak{p}$ mit $I \subseteq \mathfrak{p}$. Analog zu Teil a) zeigt man, dass $2y$ und $2\sqrt{-5}$ in $\mathfrak{p}$ liegen. Da $\mathfrak{p}$ ein Primideal ist, liegt 2 oder $\sqrt{-5}$ in $\mathfrak{p}$. Angenommen $2 \in \mathfrak{p}$. Die 2 ist verzweigt in R und es ist $(2) = (2, \sqrt{-5}+1)^2$, daher ist $\mathfrak{p} = (2, \sqrt{-5}+1)$. Wegen $I \subseteq \mathfrak{p}$ ist daher insbesondere $2y, y+1 \in \mathfrak{p}$. Da y gerade ist, sind $2y$ und $y+1$ teilerfremd in $\mathbb{Z}$, daher ist $R = (2y, y+1) = \mathfrak{p}$. Dies ist ein Widerspruch. Also ist $\sqrt{-5} \in \mathfrak{p}$. Die Primzahl 5 zerlegt sich (nach Satz 5.18) in R als $(5) = (\sqrt{-5})^2$. Daher ist $(\sqrt{-5})$ ein Primideal und somit $\mathfrak{p} = (\sqrt{-5})$. Also ist $y \in \mathfrak{p} = \sqrt{-5}$ und daher $y = \sqrt{-5}u$ für ein $u \in \mathbb{R}$. Dann

aber ist $5 \mid N(y) = y^2$, woraus folgt $5 \mid y$. Wegen $x^3 = y^2 + 5$ muss daher auch $5 \mid x$ sein und deswegen $125 \mid x^3$. Anderseits kann $y^2 + 5$ nicht durch 125 teilbar sein, ebenfalls ein Widerspruch. Dies zeigt, dass $(y+\sqrt{-5})+(y-\sqrt{-5})$ in keinem Primideal enthalten sein kann. Die Behauptung folgt.

e) Sei $(x) = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$ die Zerlegung in Primideale. Seien diese so nummeriert, dass $\mathfrak{p}_1, \dots, \mathfrak{p}_l$ genau die Primideale sind, die über $(y + \sqrt{-5})$ liegen. Schreibe $\mathfrak{a} := \mathfrak{p}_1^{e_1} \dots p_l^{e_l}$. Wegen $x^3 = y^2 + 5$ und der Teilerfremdheit von $(y+\sqrt{-5})$ und $(y - \sqrt{-5})$ gilt $\mathfrak{a}^3 = (y + \sqrt{-5})$. Gelesen in der Klassengruppe ist also $\overline{3\mathfrak{a}} = 0$. Da die Klassengruppe Ordnung 2 hat, muss schon $\overline{\mathfrak{a}} = 0$ sein. Daher ist $\mathfrak{a}$ ein Hauptideal.

f) Angenommen es gäbe $X, Y \in \mathbb{Z}^2$ mit $X^3 = Y^2 + 5$. Dann gibt es ein Hauptideal $\mathfrak{a}$ mit $\mathfrak{a}^3 = (Y + \sqrt{-5})$. Sei $\mathfrak{a}$ erzeugt von $(a + b\sqrt{-5})$ mit $a, b \in \mathbb{Z}$. Dann ist $(a+b\sqrt{-5})^3$ assoziert zu $Y+\sqrt{-5}$. Wegen $R^\times = \{-1, 1\}$, kann man annehmen, dass $(a + b\sqrt{-5})^3 = Y + \sqrt{-5}$ gilt. Dies führt zu

$$Y + \sqrt{-5} = a^3 + 3\sqrt{-5}a^2b - 15ab^2 - 5\sqrt{-5}b^3.$$

Durch Koeffizientenvergleich erhält man

$$a^3 - 15ab^2 = Y$$
$$3a^2b - 5b^3 = 1$$

Die zweite Gleichung faktorisiert zu $b(3a^2 - 5b^2) = 1$, woraus $b, (3a^2 - 5b^2) \in \{-1, 1\}$ folgt. Dann müsste insbesondere $3a^2 - 5 = \pm 1$ sein, dies ist jedoch nicht möglich. Dies zeigt, dass die Gleichung $X^3 = Y^2 + 5$ über $\mathbb{Z}$ unlösbar ist.