Übungsaufgaben zur Vorlesung „Algebraische Zahlentheorie“

Lösungsskizze Blatt 2

Aufgabe 1:
Zeigen Sie, dass das Ideal $(2, X) \subset \mathbb{Z}[X]$ kein Hauptideal ist.

Angenommen, es gibt ein $f \in \mathbb{Z}[X]$ mit $(2, X) = (f)$. Dann gilt insbesondere $f \mid 2, X$. Insbesondere gibt es $g \in \mathbb{Z}[X]$ mit

$$2 = g \cdot f.$$

Wir erhalten

$$0 = \deg(2) = \deg(g_1) + \deg(f) \implies \deg(g_1) = \deg(f) = 0,$$

d.h. f ist konstant. Wir können $f > 0$ annehmen. Da $f \mid 2$, folgt $f \in \{1, 2\}$. Ist $f = 2$, so erhalten wir den Widerspruch $2 \mid X$ in $\mathbb{Z}[X]$. Wir müssen also noch $f = 1$ ausschließen. In diesem Fall gilt also $(2, X) = (1) = \mathbb{Z}[X]$ und es gibt $h_1, h_2 \in \mathbb{Z}[X]$ mit

$$2h_1 + Xh_2 = 1.$$

Einsetzen von 0 auf beiden Seiten liefert den Widerspruch

$$2 \underbrace{h_1(0)}_{\in \mathbb{Z}} = 1.$$

□

Aufgabe 2:

(1) Beweisen Sie den *Satz über rationale Nullstellen*:
Sei A ein faktorieller Ring mit Quotientenkörper K, sowie

$$f = a_n X^n + ... + a_1 X + a_0 \in A[X].$$

Ist $\alpha \in K$ eine Nullstelle von f, so gibt es $a, b \in A$, $b \neq 0$ mit $\alpha = \frac{a}{b}$ und $a \mid a_0$, $b \mid a_n$.

(2) Folgern Sie, dass faktorielle Ringe ganz abgeschlossen sind.

(1) Wie in der Aufgabenstellung betrachten wir eine Nullstelle $\alpha = \frac{a}{b} \in K$ von f. Da A faktoriell ist, können wir annehmen, dass der Bruch $\frac{a}{b}$ vollständig gekürzt ist (wir können nämlich a und b eindeutig als Produkt von irreduziblen Elementen schreiben und dann entsprechend kürzen). Multiplizieren der Gleichung $f(\alpha) = 0$ mit b^n liefert

$$a_n \cdot a^n + a_{n-1} \cdot a^{n-1} b + ... + a_0 b^n = 0. \qquad (*)$$

Wir stellen die Gleichung um und erhalten

$$a_n \cdot a^n + a_{n-1} \cdot a^{n-1} b + ... + a_1 \cdot a b^{n-1} = -a_0 b^n.$$

Die linke Seite wird von a geteilt, also auch die rechte Seite. Da kein irreduzibles Element a und b gleichzeitig teilt, folgt $a \mid a_0$, wie gewünscht. Die Aussage $b \mid a_n$ erhalten wir auf die gleiche Art, indem wir $(*)$ zu

$$-a_n \cdot a^n = a_{n-1} \cdot a^{n-1}b + ... + a_0 b^n$$

umstellen und bemerken, dass jetzt die rechte Seite von b geteilt wird. □

(In der Lösung haben wir das folgende Lemma verwendet: Seien x, y, z Elemente eines faktoriellen Rings. Die Elemente x und z seien teilerfremd, d.h. jedes irreduzible Element, das x teilt, teilt z nicht. Ferner gelte $x \mid yz$. Dann gilt $x \mid y$.)

(2) Nach der vorherigen Teilaufgabe gilt: Ist A faktoriell, $f \in A[X]$ normiert und $\alpha \in \mathrm{Frac}(A)$ eine Nullstelle von f, so gilt $\alpha \in A$. □

Aufgabe 3:
Sei $f\colon A \to B$ ein Ringhomomorphismus und $\mathfrak{p} \subset B$ ein Primideal. Verifizieren Sie, dass $f^{-1}(\mathfrak{p}) \subset A$ ein Primideal ist. Stimmt die Aussage auch, wenn man "Primideal" durch "maximales Ideal" ersetzt?

Seien $a_1, a_2 \in A$ mit $a_1 a_2 \in f^{-1}(\mathfrak{p})$. Dann gilt $f(a_1 a_2) = f(a_1) f(a_2) \in \mathfrak{p}$. Da $\mathfrak{p}$ prim ist, folgt $f(a_1) \in \mathfrak{p}$ oder $f(a_2) \in \mathfrak{p}$, also $a_1 \in f^{-1}(\mathfrak{p})$ oder $a_2 \in f^{-1}(\mathfrak{p})$. Des Weiteren ist $f^{-1}(\mathfrak{p}) \neq A$, da $1 \notin \mathfrak{p}$ gilt. Also ist $f^{-1}(\mathfrak{p}) \subset A$ prim.
Die Aussage ist falsch für maximale Ideale, man betrachte z.B. die Inklusion $\mathbb{Z} \hookrightarrow \mathbb{Q}$. □

Aufgabe 4:
Sei B/A eine ganze Ringerweiterung von Integritätsringen.

(1) Zeigen Sie:

$$B \text{ ist ein Körper} \iff A \text{ ist ein Körper.}$$

(2) Sei $\mathfrak{p} \subset B$ ein Primideal und $\mathfrak{p}' = \mathfrak{p} \cap A$. Zeigen Sie, dass $\mathfrak{p}'$ genau dann ein maximales Ideal von A ist, wenn $\mathfrak{p}$ ein maximales Ideal von B ist.

Sei K nun ein Zahlkörper.

(3) Folgern Sie, dass jedes Primideal $\neq (0)$ in $\mathcal{O}_K$ maximal ist.

(1) Wir nehmen zunächst an, dass B ein Körper ist. Sei $a \in A \setminus \{0\}$. Da $A \subset B$ und B ein Körper ist, existiert ein $b \in B$ mit $ab = 1$ – wir müssen $b \in A$ zeigen. Nun ist b ganz über A, d.h. es existieren $a_0, ..., a_{n-1} \in A$ mit

$$b^n + a_{n-1}b^{n-1} + ... + a_0 = 0.$$

Wir multiplizieren diese Gleichung mit a^{n-1} durch. Unter Verwendung von $ab = 1$ erhalten wir dann

$$b = -(a_{n-1} + a a_{n-2} + ... + a^{n-1} a_0) \in A.$$

Ist umgekehrt A ein Körper und $b \in B \setminus \{0\}$, so erfüllt b wieder eine Ganzheitsgleichung der Form

$$b^n + a_{n-1}b^{n-1} + ... + a_0 = 0.$$

mit $a_0, ..., a_{n-1} \in A$. Da A und B Integritätsringe sind, können wir ohne Beschränkung der Allgemeinheit $a_0 \neq 0$ annehmen (denn sonst können wir die Gleichung mit einer geeigneten Potenz von b kürzen, um eine Gleichung mit konstantem Term $\neq 0$ zu erhalten). Dann folgt

$$a_0 = -b \cdot (b^{n-1} + a_{n-1}b^{n-2} + ... + a_1).$$

Multiplizieren mit $a_0^{-1} \in A$ auf beiden Seiten liefert dann ein multiplikatives Inverses von b, nämlich

$$-a_0^{-1} \cdot (b^{n-1} + a_{n-1}b^{n-2} + ... + a_1) \in B.$$

Das beweist die Aussage. Der Vollständigkeit halber stellen wir noch fest, dass die Aussage falsch ist, wenn B kein Integritätsring ist: Für jeden Körper K ist die Erweiterung $K \subset K[X]/(X^2)$ ganz, aber $K[X]/(X^2)$ ist kein Körper. □
(2) Da B/A ganz ist, ist $B/\mathfrak{p}$ ganz über $A/\mathfrak{p}'$. Ist nämlich $b + \mathfrak{p} \in B/\mathfrak{p}$, so erfüllt $b \in B$ eine Ganzheitsgleichung

$$b^n + a_{n-1}b^{n-1} + ... + a_0 = 0$$

über A. Reduzieren liefert dann

$$(b + \mathfrak{p})^n + (a_{n-1} + \mathfrak{p}')(b + \mathfrak{p})^{n-1} + ... + (a_0 + \mathfrak{p}') = 0 + \mathfrak{p}'.$$

Des Weiteren stellen wir fest, dass $\mathfrak{p}'$ nach Aufgabe **??** prim ist, d.h. die Ringe $A/\mathfrak{p}'$ und $B/\mathfrak{p}$ sind Integritätsringe.

Ist nun $\mathfrak{p}$ bzw. $\mathfrak{p}'$ maximal, so ist $B/\mathfrak{p}$ bzw. $A/\mathfrak{p}'$ ein Körper. Da $B/\mathfrak{p}$ und $A/\mathfrak{p}'$ Integritätsringe sind und die Erweiterung ganz ist, folgt die Behauptung aus der vorherigen Teilaufgabe.
(Für diesen Beweis benötigt man nicht, dass A, B selbst Integritätsringe sind, sondern nur, dass $A/\mathfrak{p}'$ und $B/\mathfrak{p}$ Integritätsringe sind.) □

(3) Sei $(0) \neq \mathfrak{p} \subset \mathcal{O}_K$ ein Primideal. Wir betrachten $\mathfrak{p}' = \mathfrak{p} \cap \mathbb{Z}$. Da $\mathbb{Z}$ ein Hauptidealring ist, ist in $\mathbb{Z}$ jedes Primideal $\neq (0)$ maximal. Nach der vorherigen Teilaufgabe folgt dann, dass $\mathfrak{p}$ maximal ist, wenn wir $\mathfrak{p}' \neq (0)$ gezeigt haben. Sei dazu $\beta \in \mathfrak{p} \setminus \{0\}$. Da $\mathcal{O}_K$ ganz über $\mathbb{Z}$ ist, existieren $a_0, ..., a_{n-1} \in \mathbb{Z}$ mit

$$\beta^n + a_{n-1}\beta^{n-1} + ... + a_0 = 0.$$

Wie in der ersten Teilaufgabe dürfen wir $a_0 \neq 0$ annehmen. Es folgt

$$\underbrace{a_0}_{\in \mathbb{Z}\setminus\{0\}} = \underbrace{-(\beta^n + a_{n-1}\beta^{n-1} + ... + a_1\beta)}_{\in \mathfrak{p}}.$$

Das beweist $0 \neq a_0 \in \mathfrak{p} \cap \mathbb{Z} = \mathfrak{p}'$. □

Bonusaufgabe 5:
Betrachten Sie den Ring $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$. In der Einleitung zum Skript wurde behauptet, dass dieser nicht faktoriell ist. Hier verifizieren Sie alle Details.

(1) Sei $N\colon \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}$ durch $N(a+b\sqrt{-5}) = a^2+5b^2$ definiert. Begründen Sie kurz, dass N multiplikativ ist, d.h. für alle $a, b, c, d \in \mathbb{Z}$ gilt

$$N((a + b\sqrt{-5})(c + d\sqrt{-5})) = N(a + b\sqrt{-5})N(c + d\sqrt{-5}).$$

(2) Zeigen Sie, dass ± 1 die einzigen Einheiten von $\mathbb{Z}[\sqrt{-5}]$ sind.

(3) Zeigen Sie, dass die Elemente $2, 3, 1+\sqrt{-5}$ und $1-\sqrt{-5}$ in $\mathbb{Z}[\sqrt{-5}]$ zwar irreduzibel, aber nicht prim sind.

(4) Folgern Sie, dass $\mathbb{Z}[\sqrt{-5}]$ nicht faktoriell ist.

(1) Unter der Identifizierung des Rings $\mathbb{Z}[\sqrt{-5}]$ mit dem Ring $\mathbb{Z}[\sqrt{5}i] \subset \mathbb{C}$, entspricht die Abbildung N schlicht dem Betragsquadrat komplexer Zahlen. Dieses ist multiplikativ. □

(2) Ist $z = a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ eine Einheit, so existiert ein $w \in \mathbb{Z}[\sqrt{-5}]$ mit $zw = 1$. Unter der Verwendung der Multiplikativität von N folgt

$$1 = N(1) = N(zw) = N(z)N(w).$$

Da $N(z) \in \mathbb{Z}_{\geq 0}$ gilt, folgt $N(z) = a^2 + 5b^2 = 1$. Da $a, b \in \mathbb{Z}$, muss $b = 0$ und $a = \pm 1$ gelten. Da ± 1 auch tatsächlich Einheiten sind, sind wir fertig. □

(3) Wir zeigen zunächst, dass die angegebenen Elemente irreduzibel sind. Es seien $z, w \in \mathbb{Z}[\sqrt{-5}]$.

- Wenn $2 = zw$ gilt, dann folgt $4 = N(2) = N(zw) = N(z)N(w)$, d.h. $N(z)$ und $N(w)$ sind Teiler von 4. In der vorherigen Teilaufgabe haben wir gesehen, dass Elemente mit der Norm 1 Einheiten sind. Um die Irreduzibilität von $2 \in \mathbb{Z}[\sqrt{-5}]$ zu zeigen, müssen wir also nur den Fall $N(z) = N(w) = 2$ ausschließen. Dazu reicht es zu zeigen, dass es kein $a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ mit $N(a + b\sqrt{-5}) = a^2 + 5b^2 = 2$ gibt. Das ist leicht einzusehen: Sofort erhalten wir $b = 0$ und dann $a^2 = 2$, eine Gleichung, die in $\mathbb{Z}$ nicht lösbar ist. Die Diskussion zeigt die Irreduzibilität von 2.

- Da $N(3) = 9$, reicht es für die Irreduzibilität von 3 zu zeigen, dass $\mathbb{Z}[\sqrt{-5}]$ kein Element mit Norm 3 enthält. Das sieht man wie im vorherigen Stichpunkt sofort ein.

- Die Elemente $1 \pm \sqrt{-5}$ haben die Norm $6 = 2 \cdot 3$. Wenn diese Elemente also in einer nicht-trivialen Art als Produkt zweier Elemente geschrieben werden können, so haben die Faktoren die Norm 2 bzw. 3. Wir haben aber bereits gesehen, dass es keine Elemente mit Norm 2 und 3 gibt.

Nun zeigen wir, dass die vier Elemente nicht prim sind. In $\mathbb{Z}[\sqrt{-5}]$ gilt

$$2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Wäre 2 prim, so gälte $2 \mid 1 + \sqrt{-5}$ oder $2 \mid 1 - \sqrt{-5}$. Dass das nicht der Fall ist, rechnet man entweder direkt nach, oder man verwendet N: Da

$$4 = N(2) \nmid 6 = N(1 \pm \sqrt{-5}),$$

kann 2 kein Teiler von $1 \pm \sqrt{-5}$ sein (denn die Norm ist multiplikativ). Also ist 2 nicht prim. Analog zeigt man, dass die anderen drei Elemente nicht prim sind. □

(4) In faktoriellen Ringen sind irreduzible Elemente prim. Nach der vorherigen Teilaufgabe ist z.B. $2 \in \mathbb{Z}[\sqrt{-5}]$ irreduzibel, aber nicht prim. Also ist $\mathbb{Z}[\sqrt{-5}]$ nicht faktoriell. □

Alternative: Nach den vorherigen beiden Teilaufgaben sind die Elemente 2, 3, $1 + \sqrt{-5}$ und $1 - \sqrt{-5}$ irreduzibel und paarweise nicht assoziiert. Da außerdem $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ gilt, ist die Zerlegung in irreduzible Elemente in $\mathbb{Z}[\sqrt{-5}]$ nicht eindeutig. □