Algebraische Zahlentheorie: [MTH-1483]

Ilia Pirashvili

Arbeitsblatt 9

1 Allgemeine Hinweise

Maximale Punktzahl die man in diesem Arbeitsblatt erwerben kann sind 10 Punkte. Aufgaben können frei gewählt werden.

Lösungen werden nächste Woche (Donnerstag) sowohl elektronisch (als PDF) bereitgestellt, wie auch in der Vorlesungszeit (12:15 – 13:45) live/online von mir via Zoom erklärt.

Bei Unverständnissen, Fragen oder wenn Ihr Fehler findet, bitte an
ilia.pirashvili@math.uni-augsburg.de
wenden.

Die Punkte der Arbeitsblätter werden in die Endnote eingehen! Abgabefirst ist bis einschließlich Mittwoch (24/06). Viel Glück und viel Erfolg.

2 Aufgaben

Aufgabe 1 (5 Punkte). Sei $K = \mathbb{Q}(\sqrt{-6})$ und betrachte $\mathfrak{o}_K$. Es gilt

$$10 = 2 \cdot 5 = (2 + \sqrt{-6})(2 - \sqrt{-6}).$$

i) (2 Teilpunkte) Zeige, dass es in $\mathfrak{o}_K$ keinen Elementen der Norm 2 oder 5 gibt und schlussfolgere, dass es zwei echt verschiedene Faktorisierung von $10 \in \mathfrak{o}_K$ in irreduziblen Elementen gibt.

ii) (2 Teilpunkte) Beweise, dass $\mathfrak{a} = (2, \sqrt{-6})$ ein Maximalideal von $\mathfrak{o}_K$ ist. Ferner, zeige, dass $\mathfrak{a}$ kein Hauptideal ist.

iii) (1 Teilpunkt) Zeige, dass $\mathfrak{a}^2 = 2R$.

Lösung. i) Die Norm eines beliebigen Elements $x = a + b\sqrt{-6}$ ist $N(x) = a^2 + 6b^2$. Sei $x \in \mathfrak{o}_K$ mit $N(x) = 2$ or $N(x) = 5$. Dann ist $a^2 + 6b^2 = 2$ or $a^2 + 6b^2 = 5$. Da a und B ganze Zahlen sind, haben wir $b = 0$, da sonst $a^2 + 6b^2 \geq 6$. Daher ist $a^2 = 2$ or $a^2 = 5$, was nicht möglich ist.

Es bleibt zu zeigen, dass $2, 5, 2 + \sqrt{-6}$ und $2 - \sqrt{-6}$ irreduzibel sind. Sei $2 = xy$, wobei $x, y \in \mathfrak{o}_K$. Daher

$$\mathsf{N}(2) = \mathsf{N}(xy)$$

als

$$4 = \mathsf{N}(x)\mathsf{N}(y).$$

Da $\mathsf{N}(2)$ nicht erlaubt ist (sieh oben), muss $\mathsf{N}(x) = 1$ oder $\mathsf{N}(y) = 1$ gelten. Daher, x ist eine Einheit oder y ist eine Einheit, was irreduzibilität impliziert. Das gleiche Argument wirkt in jedem Fall identisch.

Da gleiche Elemente die gleiche Norm haben (wohldefiniert), brauchen wir jetzt nur die Normen vergleichen, um zu sehen, dass es echt verschieden Darstellungen gibt.

ii) Betrachte die Abbildung

$$\phi : \mathfrak{o}_K \to \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$$

gegen durch

$$(a + b\sqrt{-6}) \mapsto a \mod 2.$$

Es ist klar, dass es surjektiv ist ($0 \mapsto 0$, $1 \mapsto 1$ und $0 \neq 1 \in \mathbb{Z} \subseteq \mathfrak{o}_K$). Wir haben

$$\phi(2) = 0 = \phi(\sqrt{-6}),$$

woraus wir schlussfolgern können, dass $\mathfrak{a} \subset \mathsf{Ker}(\phi)$. Wir behaupten, dass $\mathfrak{a} = \mathsf{Ker}(\phi)$. Sei dazu $x = a + b\sqrt{-6} \in \mathsf{Ker}(\phi)$, also $\phi(a + b\sqrt{-6}) = 0$. Dann ist $a = 2c$, $c \in \mathbb{Z}$ und daher $x \in (2, \sqrt{-6})$. Der erste Isomorphiesatz besagt nun, dass

$$\mathfrak{o}_K/\mathfrak{a} \simeq \mathbb{F}_2,$$

woraus wir schließen, dass $\mathfrak{a}$ ein Maximalideal ist. Sei $\mathfrak{a}$ ein Hauptideal erzeugt mit y. Da $2 \in (y)$ sehen, dass $N(y)|N(2) = 4$. Gleichwie $N(y)|N(\sqrt{-6}) = 6$. Es folgt, dass $N(y)|2$. Da $\mathfrak{a} \neq \mathfrak{o}_K$, haben wir $N(y) = 2$. So ein y existiert jedoch nicht, was uns zu einem Widerspruch führt.

iii) Es gilt

$$\mathfrak{a}^2 = (2, \sqrt{-6})(2, \sqrt{-6}) = (4, 2\sqrt{-6}, -6) = (4, 2\sqrt{-6}, -6, -2) = (2).$$

□

Aufgabe 2 (6 Punkte). Sei $K = \mathbb{Q}(\sqrt{-5})$ und $\mathfrak{o}_K$ dessen assoziiertes Zahlenring.

i) (1 Teilpunkt) Zeige, dass $2\mathfrak{o}_K = \mathfrak{p}_2^2$, wobei

$$\mathfrak{p}_2 = (2, 1 + \sqrt{-5}).$$

Bestimme die Norm von $\mathfrak{p}_2$.

ii) (1 Teilpunk) Zeige, dass $3\mathfrak{o}_K = \mathfrak{p}_3\mathfrak{q}_3$, wobei

$$\mathfrak{p}_3 = (3, 1 + \sqrt{-5})$$

und

$$\mathfrak{q}_3 = (3, 1 - \sqrt{-5}).$$

iii) (1 Teilpunkt) Zeige, dass $5\mathfrak{o}_K = \mathfrak{p}_5^2$, wobei

$$\mathfrak{p}_5 = (\sqrt{-5}).$$

iv) (1 Teilpunkt) Zeige, dass $7\mathfrak{o}_K = \mathfrak{p}_7\mathfrak{q}_7$, wobei

$$\mathfrak{p}_7 = (7, 3 + \sqrt{-5})$$

und

$$\mathfrak{q}_7 = (7, 3 - \sqrt{-5}).$$

v) (2 Teilpunkte) Betrachte die Ideale $\mathfrak{p}_3$ und $\mathfrak{q}_3$.

v a) Zeige, dass jedes Element $a + b\sqrt{-5} \in \mathfrak{q}_3$ die Eigenschaft hat, dass $a + b$ durch 3 teilbar ist, also $3 \mid a + b$ gilt.
Gleichwie, dass jedes Element $c + d\sqrt{-5} \in \mathfrak{p}_3$ die Eigenschaft hat, dass $c - d$ ein Vielfaches von 3 ist.

v b) Basierend auf diese Beobachtung, zeige, dass $\mathfrak{p}_3$ und $\mathfrak{q}_3$ keine Hauptideale sind.

Lösung. i) Wir haben

$$\begin{aligned}(2,1+\sqrt{-5})^2 = (2,1+\sqrt{-5})(2,1+\sqrt{-5}) &= (4,2+2\sqrt{-5},-4+2\sqrt{-5}) \\ &= (4,2+2\sqrt{-5},-4+2\sqrt{-5},-6) = (2).\end{aligned}$$

Definiere $\psi : R \to \mathbb{F}_2$, durch

$$\psi(a+b\sqrt{-5}) = a+b \mod 2.$$

Dann ist ψ eine surjektives Ringhomomorphismus. Es folgt, dass $\mathsf{Ker}\psi = (2,1+\sqrt{-5})$ maximal ist.

ii) Es gilt

$$(3,1+\sqrt{-5})(3,1-\sqrt{-5}) = (9,3+3\sqrt{-5},3-3\sqrt{-5},6) = (3).$$

iii) Wir haben

$$(\sqrt{-5})^2 = (5).$$

iv) Wir haben

$$(7,3+\sqrt{-5})(7,3-\sqrt{-5}) = (49,21+7\sqrt{-5},21-7\sqrt{-5},14) = (7).$$

v) Da $-5 \equiv 3 \mod 4$ haben wir

$$\mathfrak{o}_K = \{a+b\sqrt{-5} | a,b \in \mathbb{Z}\}.$$

Daher ist ein allgemeines Element des Ideals $(3,1-\sqrt{-5})$ von der Form

$$(a+b\sqrt{-5})\cdot 3 + (m+n\sqrt{-5})(1-\sqrt{-5}),$$

wobei $a,b,m,n \in \mathbb{Z}$. Wir können dies umschreiben als

$$(3a+m-5n)+(3b-m+n)\sqrt{-5}.$$

Da $(3a+m+5n)+(3b-m+n) = 3a+3b+6n$, folgt die Aussage für $\mathfrak{q}_3$. Gleichwie können wir es auch für $\mathfrak{p}_3$ beweisen.

vi) Sei $(3,1+\sqrt{-5}) = (x)$. Dann ist $x \mid 3$ und $x \mid 1+\sqrt{-5}$. Es folgt, dass $N(x) \mid N(3) = 9$ und $N(x)|6$. Daher haben wir $N(x)|3$. Jedoch hat die Gleichung $a^2+5b^2 = 3$ keine Lösung über die ganzen Zahlen. Also ist $N(x) \neq 3$, was $N(x) = 1$ impliziert. Wir haben gezeigt, dass x invertierbar ist und $(x) = (1) = \mathfrak{o}_K \neq (3)$. Daher ist $(3,1+\sqrt{-5})$ kein Hauptideal. Das Gleiche gilt für $(3,1-\sqrt{-5})$. □

Aufgabe 3 (6 Punkte). Sei $K = \mathbb{Q}(\sqrt{d})$.

i) (1 Teilpunkt) Sei $d \equiv 2 \mod 4$. Zeige, dass

$$2\mathfrak{o}_K = (2,\sqrt{d})^2$$

und das $\mathfrak{p} = (2,\sqrt{d})$ ein Maximalideal ist.

ii) (1 Teilpunkt) Sei $d \equiv 3 \mod 4$. Zeige, dass

$$2\mathfrak{o}_K = (2,1+\sqrt{d})^2$$

und das $\mathfrak{p} = (2,1+\sqrt{d})$ ein Maximalideal ist.

iii) (2 Teilpunkte) Sei $d \equiv 1 \mod 8$. Zeige, dass

$$2\mathfrak{o}_K = \mathfrak{p}\mathfrak{q},$$

wobei $\mathfrak{p} = (2,\frac{1+\sqrt{d}}{2})$ und $\mathfrak{q} = (2,\frac{1-\sqrt{d}}{2})$. Des weiteren, zeige, dass $\mathfrak{p},\mathfrak{q}$ unterschiedliche Maximalideale sind.

iv) (2 Teilpunkte) Sei $d \equiv 5 \mod 8$. Zeige, dass $2\mathfrak{o}_K$ ein Maximalideal ist.

Lösung. i) Wir setzen $d = 2 + 4k$. Dann ist

$$(2, \sqrt{d})^2 = (2, \sqrt{d})(2, \sqrt{d}) = (4, 2\sqrt{d}, d) = (4, 4k, 2\sqrt{d}, d) = (4, 2\sqrt{d}, d - 4k) = (4, 2\sqrt{d}, 2) = (2).$$

Die Abbildung

$$\psi : \mathfrak{o}_K \to \mathbb{F}_2,$$

gegeben durch

$$\phi(a + b\sqrt{d}) = a \mod 2$$

ist ein Ringhomomorphismus. Wenn $x = a + b\sqrt{d}$ und $x' = a' + b'\sqrt{d}$, dann ist

$$xx' = aa' + b^2 d + \sqrt{d}(ab' + a'b).$$

Da d gerade ist, haben wir

$$\psi(xx') = (aa' + b^2 d) \mod 2 = aa' \mod 2 = \psi(a)\psi(a').$$

Es gilt $\mathsf{Ker}(\psi) = \mathfrak{p}$. Da ψ surjektiv ist, muss $\mathfrak{p}$ maximal sein.

ii) Definiere $d = 3 + 4k$. Dann ist

$$\begin{aligned}(2, 1 + \sqrt{d})^2 &= (2, 1 + \sqrt{d})(2, 1 + \sqrt{d}) = (4, 2 + 2\sqrt{d}, 1 + d + 2\sqrt{d}) \\ &= (4, 2 + 2\sqrt{d}, 4 + 4k + 2\sqrt{d}) \\ &= (4, 2 + 2\sqrt{d}, 2\sqrt{d}) \\ &= (4, 2 + 2\sqrt{d}, 2\sqrt{d}, 2) \\ &= (2).\end{aligned}$$

Betrachte die Abbildung

$$\psi : \mathfrak{o}_K \to \mathbb{F}_2,$$

gegeben durch

$$\psi(a + b\sqrt{d}) = a + b \mod 2.$$

Da d ungerade ist, ist diese Abbildung ein Ringhomomorphismus mit $\mathsf{Ker}(\psi) = (2, 1 + \sqrt{d})$. Es ist auch surjektiv, woraus folgt, dass $(2, 1 + \sqrt{d})$ ein Maximalideal ist.

iii) Sei $d = 8k + 1$. Dann ist

$$\begin{aligned}\left(2, \frac{1 + \sqrt{d}}{2}\right)\left(2, \frac{1 - \sqrt{d}}{2}\right) &= (4, 1 + \sqrt{d}, 1 - \sqrt{d}, 4k) \\ &= (4, 1 + \sqrt{d}, 1 - \sqrt{d}, 2, 4k) \\ &= (2).\end{aligned}$$

iv) Sei $d = 8k + 5$. Wir wissen, dass $\{1, \alpha = \frac{1+\sqrt{d}}{2}\}$ eine Ganzheitsbasis ist. Es gilt

$$\alpha^2 - \alpha - \frac{1 - d}{4} = 0.$$

Da $1 - d = -4 - 8k$ folt

$$\mathfrak{o}_K = \mathbb{Z}[x]/(x^2 - x + 1 + 2k).$$

Wir erhalten

$$\mathfrak{o}_K/2\mathfrak{o}_K = \mathbb{F}_2[x]/(x^2 - x + 1 + 2k) = F_2[x]/(x^2 - x + 1) = F_4,$$

wobei $\mathbb{F}_4$ das Körper mit 4 Elementen bezeichnet. (Zur Erinnerung, $\mathbb{F}_4 \neq \mathbb{Z}/4\mathbb{Z}$). Hier benutzen wir die Tatsache, dass $x^2 + x + 1$ über $\mathbb{F}_2$ irreduzibel ist. □

Aufgabe 4 (3 Punkte). Sei $\alpha = \sqrt[3]{2}$ und $K = \mathbb{Q}(\alpha)$. Dann ist $\mathfrak{o}_K = \mathbb{Z}[\alpha]$ mit Ganzheitsbasis $\{1, \alpha, \alpha^2\}$. Wir definieren $\mathfrak{p} = (5, \alpha + 2)$ und $\mathfrak{q} = (5, \alpha^2 + 3\alpha + 4)$.

i) (1 Teilpunkt) Beweise, dass das Polynom $f(x) = x^2 + 3x + 4$ irreduzibel ist über $\mathbb{F}_5$ und schlussfolgere, dass $\mathfrak{q}$ ein Maximalideal von $\mathfrak{o}_K$ ist.

ii) (1 Teilpunkt) Zeige, dass es ein wohldefinierten Ringhomomorphismus

$$f : \mathfrak{o}_K \to \mathbb{F}_5$$

gibt, mit $f(\alpha) = 3 \in \mathbb{F}_5$. Schlussfolgere, dass $\mathsf{Ker}(f) = \mathfrak{p}$ ein Maximalideal von $\mathfrak{o}_K$ ist.

iii) (1 Teilpunkt) Bestätige, dass

$$1 = 5 + 2(\alpha + 1)(\alpha + 2) - 2(\alpha^2 + 3\alpha + 4)$$

und basierend darauf, beweise, dass

$$5\mathfrak{o}_K = \mathfrak{p}\mathfrak{q}.$$

Lösung. i) Ein Polynom vom Grad 2 ist genau dann irreduzibel, wenn es keine Lösungen hat. Daher brauchen wir einfach die 5 Elemente von $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$ zu überprüfen. Um die Rechnung etwas einfacher zu machen nehmen wir $\{-2, -1, 0, 1, 2\}$ als unsere Repräsentanten. Da keines von diesen Elementen das Polynom $f(x) = x^2 + 3x + 4$ annihiliert, wissen wir, dass $f(x)$ irreduzibel ist. Daher ist das Hauptideal $(x^2+3x+4) \subseteq \mathbb{F}_5[X]$ ein Maximalideal, woraus folgt, dass $K = \mathbb{F}_5[X]/(x^2+3x+4)$ ein Körper ist.

Sei β das Bild von X unter der kanonischen Abbildung $\mathbb{F}_5[X] \to K$. Daher ist jedes Element von K von der Form $x + y\beta$, mit $x, y \in \mathbb{F}_5$ und

$$\beta^2 = -3\beta - 4 = 2\beta + 1 \mod 5.$$

Es folgt, dass

$$\beta^3 = 2\beta^2 + \beta = 4\beta + 2 + \beta = 2 \mod 5.$$

Also ist die Abbildung

$$h : \mathfrak{o}_K \to K, \quad \text{gegeben durch} \quad \alpha \to \beta,$$

wohldefiniert. Es ist eine surjektive (einfach) Abbildung in einem Körper und als solches ist $\mathsf{Ker}(h) \subseteq \mathfrak{o}_K$ ein Maximalideal. Wir behaupten, dass

$$\mathsf{Ker}(h) = (5, \alpha^2 + 3\alpha + 4).$$

Die Einbettung $(5, \alpha^2 + 3\alpha + 4) \in \mathsf{Ker}(h)$ ist klar. Sei $a + b\alpha + c\alpha^2 \in \mathsf{Ker}(h)$, wobei $a, b, c \in \mathbb{Z}$. Da

$$h(a + b\alpha + c\alpha^2) = a + b\beta + c(2\beta + 1) = (a + c) + (b + 2c)\beta,$$

folgt, dass

$$5|a + c \quad \text{und} \quad 5|b + 2c.$$

Wir haben

$$a + b\alpha + c\alpha^2 = (a + c) + (b + 2c)\alpha + c(\alpha^2 - 2\alpha - 1) \in (5, \alpha^2 - 2\alpha - 1) = \mathfrak{q}$$

und somit $\mathsf{Ker}(h) = \mathfrak{q}$.

ii) Wir wissen, dass es von $\mathbb{Z}$ in jedem Ring genau einen Ringhomomorphismus gibt. Die Abbildung $\mathbb{Z} \to \mathbb{F}_5$ ist durch $a \mapsto \overline{a} = a \mod 5$ gegeben. Da ein beliebiges Element in $\mathfrak{o}_K$ von der Form $a + b\alpha + c\alpha^2$, $a, b, c \in \mathbb{Z}$, ist, muss es unter $f : \mathfrak{o}_K \to \mathbb{F}_5$, wenn es so eine Abbildung existiert, zu

$$f(a + b\alpha + c\alpha^2) = \overline{a} + \overline{b}f(\alpha) + \overline{c}f(\alpha)$$

gesendet werden. Wenn also $f(\alpha) = 3$ gelten soll, muss

$$f(a + b\alpha + c\alpha^2) = \overline{a} + 3\overline{b} + 9\overline{c} = \overline{a} + 3\overline{b} + 4\overline{c} \mod 5$$

gelten. Das diese Abbildung existiert und wohldefiniert ist, ist nun recht einfach zu überprüfen. Es ist nun auch klar, dass diese Abbildung eindeutig ist.

Da jedes Element von $\mathbb{F}_5$ ein Vielfaches von 1 ist, ist diese Abbildung klar surjektiv. Als solches impliziert nun das Hauptisomorphiesatz, dass $\mathsf{Ker}(f)$ ein Maximalideal ist.

Laut unsere Konstruktion ist $f(5) = \overline{5} = 0$ und daher $f(\alpha + 2) = \overline{3 + 2} = 0.$ Also ist $(5, \alpha + 2) \subset Ker(f)$. Für die andere Seite, sei $f(a + b\alpha + c\alpha^2) = 0$. Es folgt, dass $\overline{a + 3b + 4c} = \overline{a - 2b + 4c}$, daher

$$a + b\alpha + c\alpha^2 = (a - 2b + 4c) + b(\alpha + 2) + c(\alpha^2 - 4).$$

Es gilt

$$a - 2b + 4c \in (5), b(\alpha + 2) \in (\alpha + 2) \quad \text{und} \quad \alpha^2 - 4 = (\alpha + 2)(\alpha - 2) \in (\alpha + 2).$$

Daher ist $\mathsf{Ker}(f) = (5, \alpha + 2)$, was die Maximalität von $(5, \alpha + 2)$ impliziert.

iii) Es gilt

$$5 + 2(\alpha + 1)(\alpha + 2) - 2(\alpha^2 + 3\alpha + 4) = 5 + 2\alpha^2 + 6\alpha + 4 - 2\alpha^2 - 6\alpha - 8 = 1.$$

Daher haben wir

$$\begin{aligned}
\mathfrak{pq} &= (5, \alpha + 2)(5 + \alpha^2 + 3\alpha + 4) \\
&= (25, 5(\alpha + 2), 5(\alpha^2 + 3\alpha + 4), \alpha^3 + 5\alpha^2 + 10\alpha + 8) \\
&= (25, 5(\alpha + 2), 5(\alpha^2 + 3\alpha + 4), 5\alpha^2 + 10\alpha + 10) \\
&= (5)(5, \alpha + 2, \alpha^2 + 3\alpha + 4, \alpha^2 + 2\alpha + 2) \\
&= (5),
\end{aligned}$$

da $5 + 2(\alpha + 1)(\alpha + 2) - 2(\alpha^2 + 3\alpha + 4) = 1$. □