Algebraische Zahlentheorie: [MTH-1483]

Ilia Pirashvili

Arbeitsblatt 11

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 (08/07). Viel Glück und viel Erfolg.

2 Aufgaben

Aufgabe 1 (1 Punkt). Sei $\mathcal{B} = \{b_1, \dots, b_d\}$ eine Ganzheitsbasis von $\mathfrak{o}_K$, $0 \neq a \in \mathfrak{o}_K$ und (a) das Hauptideal dazu. Beweise, dass $a\mathcal{B} = \{ab_1, \dots, ab_d\}$ eine Ganzheitsbasis von (a) ist.

Lösung. Wir müssen zeigen, dass 1. jedes $a\mathcal{B}$ eine $\mathbb{Q}$-Basis von K ist und 2. dass jedes Element $x \in (a)$ als eine $\mathbb{Z}$-lineare Kombination der Basiselemente ab_i dargestellt werden kann.

1. Wir brauchen nur zeigen, dass die ab_i's $\mathbb{Q}$-linear unabhängig sind. Aus Dimensionsgründen werden sie ein erzeugendes System sein. Da

$$\det(a\mathcal{B}) = a^d \det(\mathcal{B})$$

ist das eine genau dann Null, wenn das andere Null ist.

2. Sei $x \in (a)$ im Ideal. Dann gibt es ein $c \in \mathfrak{o}_K$, so dass $x = ac$. Da $\mathcal{B}$ eine Ganzheitsbasis von $\mathfrak{o}_K = (1)$ ist, gibt es $n_1, \cdots, n_d \in \mathbb{Z}$, so dass

$$c = n_1 b_1 + \cdots + n_d b_d.$$

Daher folgt

$$x = a(n_1 b_1 + \cdots + n_d b_d) = n_1 ab_1 + \cdots + n_d ab_d.$$

□

Aufgabe 2 (2 Punkte). Sei p eine Primzahl und $\mathfrak{p} \subseteq \mathfrak{o}_K$ ein Primideal. Beweise, dass folgende Aussagen äquivalent sind:

A. $\mathfrak{p} \mid p$, also $\mathfrak{p}$ liegt über p.

B. $p \in \mathfrak{p}$

C. $\mathsf{N}(\mathfrak{p})$ ist eine Potenz von p.

Lösung. A $\Rightarrow$ B. Folgt von Definition, da $\mathfrak{p} \mid p$ bedeutet $\mathbb{Z} \supseteq (p) = \mathfrak{p} \cap \mathbb{Z}$. Daher $p \in (p) \subseteq \mathfrak{p}$.

B $\Rightarrow$ C. Von der Vorlesung wissen wir, dass $\mathsf{N}(\mathfrak{p})$ eine Potenz einer Primzahl ist. Es gilt zu zeigen, dass es spezifisch von dem $p \in \mathfrak{p}$ ist. Da jedoch $p \in \mathfrak{p}$ impliziert, dass $(p) \subseteq \mathfrak{p}$, haben wir $\mathfrak{p} \mid (p)$. Daher, gibt es ein Ideal J, so dass $\mathfrak{p}J = (p)$. Wir wissen, dass $\mathsf{N}((p)) = |\mathsf{N}(p)| = p^d$, wobei $d = [K : \mathbb{Q}]$. Multiplikativität der Norm impliziert also, dass $\mathsf{N}(\mathfrak{p}) = p^k$, mit $1 \leq k \leq d$.

C $\Rightarrow$ A. Bei Annahme ist $\mathsf{N}(\mathfrak{p})$ eine Potenz von p, also es gibt ein $k \geq 1$, so dass $\mathsf{N}(\mathfrak{p}) = p^k$. Wir wissen, das für jedes Ideal I, $\mathsf{N}(I) \in I$. Daher, $p^k \in \mathfrak{p}$. Da $\mathfrak{p}$ Prim ist, muss $p \in \mathfrak{p}$ sein. Also folgt, dass $(p) \subseteq \mathbb{Z} \cap \mathfrak{p}$.

Wir in der Vorlesung (also wir $\mathfrak{p} \mid p$ eingeführt haben) diskutiert, ist $\mathbb{Z} \cap \mathfrak{p}$ eine andere Art und Weise, "Uhrbild" zu sagen, da es genau eine Abbildung $\mathbb{Z} \to R$ gibt, für jeden Ring und in dem Fall wenn $R = \mathfrak{o}_K$ ein Zahlenring ist, ist diese Abbildung injektiv. Wir haben bewiesen (1.1.38), dass das Uhrbild eines Primideals ein Primideal ist. Also muss $\mathbb{Z} \cap \mathfrak{p}$ ein Primideal von $\mathbb{Z}$ sein. In anderen Worten, $\mathbb{Z} \cap \mathfrak{p} = (q)$ für irgend eine Primzahl $q \in \mathbb{Z}$. Da $(p) \subseteq (q)$ aber $q \mid p$ impliziert, muss $p = q$ sein und als solches haben wir $(p) = \mathbb{Z} \cap \mathfrak{p}$, also $\mathfrak{p} \mid p$. □

Aufgabe 3 (2 Punkte). Sei $K = \mathbb{Q}(\sqrt{-7})$. Berechne folgende Normen:

i) $\mathsf{N}((11, 2 + \sqrt{-7})^2)$

ii) $\mathsf{N}((8, 1 + \sqrt{-7})^2)$

Lösung. Wir benutzen die Tatsache, dass $\mathsf{N}(I) = \mathsf{N}(\sigma(I))$, wobei $\sigma(I)$ das Konjugierte des Ideals bezeichnet.

i)

$$\begin{aligned}
\mathsf{N}((11, 2 + \sqrt{-7})^2) &= \mathsf{N}(11, 2 + \sqrt{-7})\mathsf{N}(11, 2 + \sqrt{-7}) \\
&= \mathsf{N}(11, 2 + \sqrt{-7})\mathsf{N}(11, 2 - \sqrt{-7}) \\
&= \mathsf{N}((11, 2 + \sqrt{-7})(11, 2 - \sqrt{-7})) \\
&= \mathsf{N}(11^2, 11(2 - \sqrt{-7}), 11(2 + \sqrt{-7}), (2 + \sqrt{-7})(2 - \sqrt{-7})) \\
&= \mathsf{N}((11^2, 11(2 - \sqrt{-7}), 11(2 + \sqrt{-7}), 11)) \\
&= \mathsf{N}((11)) \\
&= \mathsf{N}(11) \\
&= 11^{[K:\mathbb{Q}]} = 11^2.
\end{aligned}$$

ii)

$$\begin{aligned}
\mathsf{N}((8, 1 + \sqrt{-7})^2) &= \mathsf{N}(8, 1 + \sqrt{-7})\mathsf{N}(8, 1 + \sqrt{-7}) \\
&= \mathsf{N}(8, 1 + \sqrt{-7})\mathsf{N}(8, 1 - \sqrt{-7}) \\
&= \mathsf{N}((8, 1 + \sqrt{-7})(8, 1 - \sqrt{-7})) \\
&= \mathsf{N}(8^2, 8(1 - \sqrt{-7}), 8(1 + \sqrt{-7}), (1 + \sqrt{-7})(1 - \sqrt{-7})) \\
&= \mathsf{N}((8^2, 8(2 - \sqrt{-7}), 8(2 + \sqrt{-7}), 8)) \\
&= \mathsf{N}((8)) \\
&= \mathsf{N}(8) \\
&= 8^{[K:\mathbb{Q}]} = 2^6.
\end{aligned}$$

□

Aufgabe 4 (3 Punkt). Sei $K = \mathbb{Q}(\sqrt[3]{2})$. Berechne die Norm der Ideale

i) (1 Teilpunkt) $(2, \sqrt[3]{2})$

ii) (1 Teilpunkt) $(3, 1 + \sqrt[3]{2})$

iii) (1 Teilpunkt) $(2, 1+\sqrt[3]{2})$

Lösung. Sei $1 \neq \zeta_3$ eine Wurzel von x^3-1. Daher sind $\zeta_3\sqrt[3]{2}$ und $\zeta_3^2\sqrt[3]{2}$ die Konjugierten von $\sqrt[3]{2}$. Wir benutzen den selben Trick wie in der vorigen Aufgabe, aber diesmal haben wir eine kubische Erweiterung.

i)

$$\begin{aligned}
\mathsf{N}((2,\sqrt[3]{2})^3) &= \mathsf{N}(((2,\sqrt[3]{2})(2,\zeta_3\sqrt[3]{2})(2,\zeta_3^2\sqrt[3]{2}))) \\
&= \mathsf{N}((2^3, 4\zeta_3^2\sqrt[3]{2}, 4\zeta_3\sqrt[3]{2}, 2\zeta_3\sqrt[3]{2}\zeta_3^2\sqrt[3]{2}, 4\sqrt[3]{2}, 2\sqrt[3]{2}\zeta_3^2\sqrt[3]{2}, 2\sqrt[3]{2}\zeta_3\sqrt[3]{2}, \sqrt[3]{2}\zeta_3\sqrt[3]{2}\zeta_3^2\sqrt[3]{2})) \\
&= \mathsf{N}((2^3, 4\zeta_3^2\sqrt[3]{2}, 4\zeta_3\sqrt[3]{2}, 2\sqrt[3]{4}, 4\sqrt[3]{2}, 2\zeta_3^2\sqrt[3]{4}, 2\zeta_3\sqrt[3]{4}, 2)) \\
&= \mathsf{N}((2)) = 2^3.
\end{aligned}$$

Daher ist $(2, \sqrt[3]{2}) = 2$.

ii)

$$\begin{aligned}
\mathsf{N}((3,1+\sqrt[3]{2})^3) &= \mathsf{N}((3,1+\sqrt[3]{2})(3,1+\zeta_3\sqrt[3]{2})(3,1+\zeta_3^2\sqrt[3]{2})) \\
&= \mathsf{N}((3^3, 9(1+\zeta_3^2\sqrt[3]{2}), 9(1+\zeta_3\sqrt[3]{2}), 3(1+\zeta_3\sqrt[3]{2})(1+\zeta_3^2\sqrt[3]{2}), 9(1+\sqrt[3]{2}), 3(1+\sqrt[3]{2}\zeta_3^2)(1+\sqrt[3]{2}) \\
&\quad , 3(1+\sqrt[3]{2})(1+\zeta_3\sqrt[3]{2}), (1+\sqrt[3]{2}\zeta_3)(1+\sqrt[3]{2}\zeta_3^2)(1+\sqrt[3]{2}))) \\
&= \mathsf{N}((3^3, 3(\cdots), \ldots, 3(\cdots), (1+\sqrt[3]{2}\zeta_3)(1+\sqrt[3]{2}\zeta_3^2)(1+\sqrt[3]{2}))) \\
&= \mathsf{N}((3^3, 3(\cdots), \ldots, 3(\cdots), \mathsf{N}(1+\sqrt[3]{2}))) \\
&= \mathsf{N}((3^3, 3(\cdots), \ldots, 3(\cdots), 3) \\
&= \mathsf{N}((3)) = \\
&= |\mathsf{N}(3)| = 3^3.
\end{aligned}$$

Daher ist $\mathsf{N}((3,1+\sqrt[3]{2})) = 3$.

iii)

$$\begin{aligned}
\mathsf{N}((2,1+\sqrt[3]{2})^3) &= \mathsf{N}((2,1+\sqrt[3]{2})(2,1+\zeta_3\sqrt[3]{2})(2,1+\zeta_3^2\sqrt[3]{2})) \\
&= \mathsf{N}((2^3, 2(\cdots), \ldots, 2(\cdots), \mathsf{N}(1+\sqrt[3]{2}))) \\
&= \mathsf{N}((2^3, 2(\cdots), \ldots, 2(\cdots), 3) \\
&= \mathsf{N}((1)) = 1
\end{aligned}$$

Daher ist $\mathsf{N}((3,1+\sqrt[3]{2})) = 1$. □

Aufgabe 5 (3 Punkte). Sei $[K:\mathbb{Q}] = d$ und sei $\alpha \in \mathfrak{o}_K$ mit $\mathsf{N}(\alpha) = a$.

i) (2 Teilpunkte) Beweise, dass $\mathsf{N}((a,\alpha)^d) = a^d$.

ii) (1 Teilpunkt) Was ist $\mathsf{N}((a,\alpha))$?

Lösung. i) Wir haben

$$\begin{aligned}
\mathsf{N}((a,\alpha)^d) &= \mathsf{N}((a,\alpha)(a,\sigma_1(\alpha))\cdots(a,\sigma_d(\alpha))) \\
&= \mathsf{N}((a^d, a(\cdots), \ldots, a(\cdots), \mathsf{N}(\alpha))) \\
&= \mathsf{N}((a^d, a(\cdots), \ldots, a(\cdots), a)) \\
&= \mathsf{N}((a)) \\
&= |\mathsf{N}(a)| = a^d
\end{aligned}$$

wie gewollt.

ii) Da $\mathsf{N}((a,\alpha)^d) = a^d$ und die Norm immer in $\mathbb{Z}$ liegt, haben wir, dass $\mathsf{N}((a,\alpha))$ bis auf Vorzechen a sein muss. Da jedoch die Norm eines Ideals immer positiv ist (es ist die Anzahl der Elemente im Quotientenring $\mathfrak{o}_K/I$) gilt $\mathsf{N}((a,\alpha)) = a$. □

Bemerkung 2.0.1. Mit $(A, B) = 1$ meinen wir, dass das schnitt aller Ideale die sowohl A wie auch B enthalten, ganz $\mathfrak{o}_K$ ist. Anders gesagt: es gibt $a \in A, b \in B$, so dass $1 = a + b$.

Aufgabe 6 (2 Punkte). Sein $0 \neq \mathfrak{p}, \mathfrak{q} \subseteq \mathfrak{o}_K$ Primideale mit $\mathfrak{p} \neq \mathfrak{q}$.

i) (1 Teilpunkt) Beweise, dass $(\mathfrak{p}, \mathfrak{q}) = (1)$ und

ii) (1 Teilpunkt) dass $\mathfrak{p} \cap \mathfrak{q} = \mathfrak{pq}$.

Lösung. i) Bei Definition ist $\mathfrak{p} \subseteq (\mathfrak{p}, \mathfrak{q})$. Daher gibt es eine Abbildung

$$\lambda : \mathfrak{o}_K/\mathfrak{p} \to \mathfrak{o}_K/(\mathfrak{p}, \mathfrak{q}).$$

Wir wollen den Kern von λ berechnen. Da in $\mathfrak{o}_K$ jedes Primideal ungleich Null ein Maximalideal ist, muss$\mathfrak{o}_K/\mathfrak{p}$ ein Körper sein. Daher hat es nur zwei Ideale $\{(0), (1)\}$.

Da $\mathsf{Ker}(\lambda) \subseteq \mathfrak{o}_K/\mathfrak{p}$ ein Ideal ist, muss $\mathsf{Ker}(\lambda) = (0)$ oder $\mathsf{Ker}(\lambda) = (1)$ sein. Im ersten Fall bedeutet es, dass $\mathfrak{q} \subseteq \mathfrak{p}$ ist, mit $\mathfrak{q} \neq \mathfrak{p} \neq (1)$, was der Maximalität von $\mathfrak{q}$ widerspricht.

Daher ist $\mathsf{Ker}(\lambda) = 1$, also muss

$$\mathfrak{o}_K/(\mathfrak{p}, \mathfrak{q}) = (\mathfrak{o}_K/\mathfrak{p})\mathsf{Ker}(\lambda) = 1$$

das triviale Ring sein. (Hier haben wir den Hauptisomorphiesatz benutzt). Es folgt, dass $(\mathfrak{p}, \mathfrak{q}) = 1$, da $R/I = 1$ genau dann wenn $I = R$.

ii) In jeden Ring für jede Ideale gilt immer

$$IJ \subseteq I \cap J.$$

Daher ist $\mathfrak{pq} \subseteq \mathfrak{pq}$. Auf der andern Seite haben wir

$$\mathfrak{p} \cap \mathfrak{q} = (\mathfrak{p} \cap \mathfrak{q})(1) = (\mathfrak{p} \cap \mathfrak{q})(\mathfrak{p}, \mathfrak{q}) = ((\mathfrak{p} \cap \mathfrak{q})\mathfrak{p}, (\mathfrak{p} \cap \mathfrak{q})\mathfrak{q}).$$

Da jedoch

$$(I \cap J)I \subseteq IJ \supseteq (I \cap J)J$$

immer gilt, muss $\mathfrak{p} \cap \mathfrak{q} \subseteq \mathfrak{pq}$ gelten, was uns

$$\mathfrak{pq} = \mathfrak{p} \cap \mathfrak{q}$$

wie gewünscht. □

Aufgabe 7 (2 Punkte). Sein $A, B, C \subseteq \mathfrak{o}_K$ Ideale, so dass $(A, B) = 1$.

i) (1 Teilpunkt) Beweise, dass wenn $A \mid BC$, dann $A \mid C$.

ii) (1 Teilpunkt) Beweise, dass wenn $A \mid C$, $B \mid C$, dann $AB \mid C$.

Lösung. i) $A \mid BC$ bedeutet, dass es ein $I \subseteq \mathfrak{o}_K$ gibt, so dass $AI = BC$. Wir zeigen, dass es ein $J \subseteq \mathfrak{o}_K$ gibt, mit $AJ = C$.

Wir haben

$$\begin{aligned} AI &= BC \Rightarrow \\ (AI, AC) &= (BC, AC) \Rightarrow \\ A(I, C) &= (A, B)C \Rightarrow \\ A(I, C) &= C, \end{aligned}$$

da $(A, B) = 1$. Als solches gibt es ein $J = (I, C)$, so dass $AJ = C$.

ii) Bei Annahme gibt es $I, J \subseteq \mathfrak{o}_K$, so dass $AI = C = BJ$. Wir wollen zeigen, dass es ein $E \subseteq \mathfrak{o}_K$ gibt, $ABF = C$. Wir haben

$$C = C(1) = C(A, B) = (CA, CB) = ((BJ)A, (AI)B) = AB(I, J).$$

Daher erfüllt $E = (I, J)$ die gewünschte Rolle. □

Aufgabe 8 (3 Punkte). Die Ringe $\mathbb{Z}[\sqrt{6}]$ und $\mathbb{Z}[\sqrt{7}]$ sind Hauptidealringe. (Dies darf man annehmen). Stelle folgende Ideale als Hauptideale dar: (Hinweis: Berechne die Norm der Ideale und finde Elemente β mit der entsprechenden Norm.)

i) (1 Teilpunkt) $(3, \sqrt{6})$,

ii) (1 Teilpunkt) $(5, 4+\sqrt{6})$,

iii) (1 Teilpunkt) $(2, 1+\sqrt{7})$.

Lösung. Damit zwei Ideale übereinstimmen, müssen ihre Normen übereinstimmen. Da $\mathsf{N}((a)) = |\mathsf{N}(a)|$ für jeden $a \in \mathfrak{o}_K$, suchen wir nach einem Element $a \in \mathfrak{o}_K$, dass die selbe Norm wie unsere Ideale hat (bis auf Vorzeichen). Das reich a-priori nicht aus, aber ist eine Mindestvoraussetzung, was uns eine starke Einschränkung an den Elementen gibt.

i) Es gilt

$$\begin{aligned}
\mathsf{N}((3,\sqrt{6})^2) &= \mathsf{N}((3,\sqrt{6})(3,-\sqrt{6}) \\
&= \mathsf{N}(9, 3\sqrt{6}, -3\sqrt{6}, 6) \\
&= \mathsf{N}((\mathsf{ggt}(3,6), 3\sqrt{6})) \\
&= \mathsf{N}((3)) \\
&= |\mathsf{N}(3)| = 9
\end{aligned}$$

Daher ist $\mathsf{N}((3,\sqrt{6})) = 3$. Wir suchen nun nach Elementen mit Norm 3. Daher, nach $a + b\sqrt{6} \in \mathbb{Z}[\sqrt{6}]$, so dass

$$a^2 - 6b^2 = \pm 3.$$

Ein Kandidat ist direkt $a = 3, b = 1$, also $3 + \sqrt{6}$. Da

$$(3+\sqrt{6})(3-\sqrt{6}) = 3,$$

folgt, dass $3 \in (3+\sqrt{6})$ und daher auch $\sqrt{6} = 3 + \sqrt{6} - 3$. Dies zeigt, dass

$$(3, \sqrt{6}) = (3+\sqrt{6}).$$

ii) Wir haben

$$\begin{aligned}
\mathsf{N}((5,4+\sqrt{6})^2) &= \mathsf{N}((5,4+\sqrt{6})(5,4-\sqrt{6})) \\
&= \mathsf{N}((25, 20-5\sqrt{6}, 20+5\sqrt{6}, 10)) \\
&= \mathsf{N}((5)) = 25
\end{aligned}$$

was $\mathsf{N}((5,4+\sqrt{6})) = 5$ impliziert. Wir such nach $a, b \in \mathbb{Z}$ mit

$$a^2 - 6b^2 = \pm 5,$$

was uns $a = b = 1$, also $1 + \sqrt{6}$ als Kandidaten gibt. Es gilt

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

was zeigt, dass $5 \in (1+\sqrt{6})$. Jedoch ist $4 + \sqrt{6} \notin (1+\sqrt{6})$, da sonst 3 auch drin wäre. da 5 drin ist, wäre es die Einheit. Die Norm ist aber 5, nicht 1.

Wir sehen uns also $1 - \sqrt{6}$ (also $a = 1, b = -1$) an. Auch hier ist $5 \in (1-\sqrt{6})$, weil es die Norm ist und des weiteren ist $5 - 1 + \sqrt{6} = 4 + \sqrt{6} \in (1-\sqrt{6})$. Daher gilt

$$(5, 4+\sqrt{6}) = (1-\sqrt{6}).$$

iii) Wir berechnen die Norm

$$\begin{aligned}\mathsf{N}((2,1+\sqrt{7})^2) &= \mathsf{N}((2,1+\sqrt{7})(2,1-\sqrt{7})) \\ &= \mathsf{N}((4,2+2\sqrt{7},2-2\sqrt{7},-6)) \\ &= \mathsf{N}((2)) = 4,\end{aligned}$$

was uns $\mathsf{N}((2,1+\sqrt{7})) = 2$ gibt. Daher suchen wir $a,b \in \mathbb{Z}$ mit

$$a^2 - 7b^2 = \pm 2.$$

Ein Kandidat ist $a = 3, b = 1$, also $3+\sqrt{7}$. Da die Norm davon 2 ist (bei Konstruktion) muss $2 \in (3+\sqrt{7})$ gelten. Daher ist auch $3+\sqrt{7}-2 = 1+\sqrt{7} \in (3+\sqrt{7})$ was uns

$$(2,1+\sqrt{7}) = (3+\sqrt{7})$$

gibt. □