Prof. Dr. Oleg Bogopolski

Zahlentheorie

Lösungen zur Klausur (WS 2012/13)

Alle Antworten müssen begründet werden.

Aufgabe 1.

1) Was ist ein noetherscher Ring? Geben Sie ein Beispiel. [3 Punkte]

2) Was ist ein Primideal in einem Ring? [2 Punkte]

3) Wie viele Primideale hat $\mathbb{R}$? [2 Punkte]

Antworte.

1) Sei R ein kommutativer Ring mit 1. Der Ring heißt *noethersch*, falls eine der folgenden äquivalenten Bedingungen erfüllt ist:

a) jede unendliche aufsteigende Kette $A_1 \subseteq A_2 \subseteq A_3 \subset \dots$ von Idealen in R stabilisiert sich, d.h. es existiert ein $n \in \mathbb{N}$ mit $A_n = A_{n+1} = A_{n+2} \dots$.

b) jedes Ideal A in R ist endlich erzeugt, d.h. es existieren endlich viel $a_1, \dots, a_k \in A$ mit $A = a_1R + a_2R + \dots + a_kR$.

Beispiele. Der Ring $\mathbb{Z}$ und jeder Körper K sind noethersch. Jeder Ganzheitsring $\mathcal{O}_K$ ist noethersch. Wenn R noethersch ist, dann ist $R[x]$ es auch.

2) Sei R ein kommutativer Ring. Ein Ideal A in R heißt *prim*, falls das Folgende gilt:

a) A ist echt, d.h. $A \neq R$,

b) für je zwei Ideale B und C in R gilt:

$$\text{aus } BC \subseteq A \text{ folgt } B \subseteq A \text{ oder } C \subseteq A.$$

3) Wie jeder Körper hat $\mathbb{R}$ nur zwei Ideale: sich selbst und $\{0\}$. Davon ist nur $\{0\}$ ein Primideal.

Aufgabe 2.

Sei $K = \mathbb{Q}(\sqrt[5]{3}, e^{\frac{2\pi i}{3}})$. Berechnen Sie den Grad von K über $\mathbb{Q}$. [6 Punkte]

Lösung. Wir haben

$$[K : \mathbb{Q}] = [\mathbb{Q}((\sqrt[5]{3})(e^{\frac{2\pi i}{3}}) : \mathbb{Q}(\sqrt[5]{3})] \cdot [\mathbb{Q}(\sqrt[5]{3}) : \mathbb{Q}] = 2 \cdot 5 = 10,$$

weil:

a) das Minimalpolynom für $\sqrt[5]{3}$ über $\mathbb{Q}$ ist $x^5 - 3$;

b) das Minimalpolynom für $e^{\frac{2\pi i}{3}}$ über $\mathbb{Q}(\sqrt[5]{3})$ (sowie über $\mathbb{Q}$) ist $\frac{x^3-1}{x-1} = x^2 + x + 1$.

Achtung: Man muss verstehen, dass diese Polynome irreduzibel über entsprechenden Körpern sind.

Aufgabe 3.

1) Sei $K = \mathbb{Q}(\sqrt{-7})$.

   a) Ist das Element $2 + \sqrt{-7}$ irreduzibel im Ganzheitsring $\mathcal{O}_K$? [6 Punkte]

   b) Ist das Element $2 + 3\frac{1+\sqrt{-7}}{2}$ irreduzibel im Ganzheitsring $\mathcal{O}_K$? [6 Punkte]

Lösung. Wir haben $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\frac{1+\sqrt{-7}}{2}$, da $-7 \equiv 1 \,(\mathrm{mod}\ 4)$ ist.

a) Sei $\alpha = 2+\sqrt{-7}$. Nehmen wir an, dass $\alpha = xy$ für irgendwelche $x, y \in \mathcal{O}_K$ ist. Dann gilt $N(\alpha) = N(x)N(y)$. Da $N(\alpha) = 2^2 + 1^2 \cdot 7 = 11$ eine Primzahl ist und die Normen von Zahlen aus $\mathcal{O}_K$ in $\mathbb{Z}$ liegen, haben wir $N(x) = \pm 1$ oder $N(y) = \pm 1$. Dann ist x oder y eine Einheit in $\mathcal{O}_K$. Somit ist α irreduzibel.

b) Sei $\alpha = 2 + 3\frac{1+\sqrt{-7}}{2}$. Nehmen wir an, dass $\alpha = xy$ für irgendwelche $x, y \in \mathcal{O}_K$ ist. Dann gilt $N(\alpha) = N(x)N(y)$. Da $N(\alpha) = (2 + \frac{3}{2})^2 + (\frac{3}{2})^2 \cdot 7 = 28$ ist, eine der möglichen Varianten ist $N(x) = 2$ und $N(y) = 14$. Wir werden zeigen, dass solche x, y in $\mathcal{O}_K$ tatsächlich existieren. Schreibe $x = a+b\frac{1+\sqrt{-7}}{2}$ mit $a, b \in \mathbb{Z}$. Dann gilt $(a+\frac{b}{2})^2+(\frac{b}{2})^2 \cdot 7 = 2$, was äquivalent der Gleichung $a^2 + ab + 2b^2 = 2$ ist. Wir können $a = 0$, $b = 1$ nehmen. Dann ist $x = \frac{1+\sqrt{-7}}{2}$ und $y = \frac{\alpha}{x} = (4 - \frac{1+\sqrt{-7}}{2})$. Diese x, y liegen in $\mathcal{O}_K$ und sind keine Einheiten. Also ist $\alpha = xy$ nicht irreduzibel.

Aufgabe 4. Sei $\alpha \in \mathbb{C}$ eine Nullstelle des Polynoms $f(x) = x^3 + 2x - 1$.

1) Beweisen Sie, dass das Polynom $f(x)$ irreduzibel über $\mathbb{Q}$ ist. [2 Punkte]
2) Nach a) ist $1, \alpha, \alpha^2$ eine Basis der Erweiterung $\mathbb{Q}(\alpha)$ über $\mathbb{Q}$.
   Berechnen Sie

   a) $\chi_\alpha(x)$, [2 Punkte]

   b) $N(\alpha)$, [2 Punkte]

   c) $\mathrm{Sp}(1), \mathrm{Sp}(\alpha), \mathrm{Sp}(\alpha^2)$. [3 Punkte]
3) Berechnen Sie die Diskriminante $\Delta(1, \alpha, \alpha^2)$. [5 Punkte]
4) Beweisen Sie, dass $1, \alpha, \alpha^2$ eine Ganzheitsbasis in $\mathcal{O}_{\mathbb{Q}(\alpha)}$ ist. [4 Punkte]
5) Beweisen Sie, dass jedes Ideal in $\mathcal{O}_{\mathbb{Q}(\alpha)}$
   einem Ideal mit der Norm $N \leqslant 5$ äquivalent ist. [5 Punkte]

Lösung.

1) *Der erste Lösungsweg*: Nach Gauß ist $f(x) \in \mathbb{Z}[x]$ irreduzibel über $\mathbb{Q}$ genau dann, wenn $f(x)$ irreduzibel über $\mathbb{Z}$ ist. Nemen wir an, dass $f(x)$ reduzibel über $\mathbb{Z}$ ist. Dann existiert eine Zerlegung $f(x) = (x+a)(x^2+bx+c)$ mit $a, b, c \in \mathbb{Z}$. Dann ist $ac = 1$. Daraus folgt $a = \pm 1$. Aber weder 1, noch -1 eine Nullstelle von $f(x)$ ist. Der Widerspruch zeigt uns, dass $f(x)$ irreduzibel über $\mathbb{Z}$ (und so über $\mathbb{Q}$) ist.

Der zweite Lösungsweg: Es gibt ein Kriterium: Ist $f(x) \in \mathbb{Z}[x]$ mit dem Hauptkoeffizient 1 über $\mathbb{Z}$ reduzibel, dann ist $f(x)$ über $\mathbb{Z}_p$ für jede Primzahl p reduzibel.

Wir betrachten $f(x)$ über $\mathbb{Z}_3$. Dann ist $f(0) = f(1) = f(2) = 2 \neq 0$. Dann hat $f(x)$ keine Nullstelle in $\mathbb{Z}_3$ und somit ist $f(x)$ irreduzibel über $\mathbb{Z}_3$. Nach dem Kriterium ist $f(x)$ irreduzibel über $\mathbb{Z}$.

2)

a) $\{1, \alpha, \alpha^2\}$ ist eine Basis von K über $\mathbb{Q}$. Wir berechnen, wie α auf der Basis durch Multiplikation operiert:

$$\begin{aligned} 1 &\to \alpha \\ \alpha &\to \alpha^2 \\ \alpha^2 &\to \alpha^3 = 1 - 2\alpha. \end{aligned}$$

Daraus entsteht die Darstellungsmatrix für α:

$$A_\alpha = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & -2 & 0 \end{pmatrix}.$$

Dann ist $\chi_\alpha(x) = \det(xE_3 - A_\alpha) = x^3 + 2x - 1$.

b) $N(\alpha) = \det(A_\alpha) = 1$.

c) Da

$$A_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad A_\alpha = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & -2 & 0 \end{pmatrix}, \quad A_{\alpha^2} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & -2 & 0 \\ 0 & 1 & -2 \end{pmatrix}$$

ist, ist $\mathrm{Sp}(1) = 3$, $\mathrm{Sp}(\alpha) = 0$, $\mathrm{Sp}(\alpha^2) = -4$.

3) Wir haben noch

$$\mathrm{Sp}(\alpha^3) = \mathrm{Sp}(1 - 2\alpha) = \mathrm{Sp}(1) - 2\mathrm{Sp}(\alpha) = 3,$$

$$\mathrm{Sp}(\alpha^4) = \mathrm{Sp}(\alpha - 2\alpha^2) = \mathrm{Sp}(\alpha) - 2\mathrm{Sp}(\alpha^2) = 8.$$

Dann gilt:

$$\Delta(1, \alpha, \alpha^2) = \det \begin{pmatrix} \mathrm{Sp}(1) & \mathrm{Sp}(\alpha) & \mathrm{Sp}(\alpha^2) \\ \mathrm{Sp}(\alpha) & \mathrm{Sp}(\alpha^2) & \mathrm{Sp}(\alpha^3) \\ \mathrm{Sp}(\alpha^2) & \mathrm{Sp}(\alpha^3) & \mathrm{Sp}(\alpha^4) \end{pmatrix} = \det \begin{pmatrix} 3 & 0 & -4 \\ 0 & -4 & 3 \\ -4 & 3 & 8 \end{pmatrix} = -59.$$

4) Sei $\beta_1, \beta_2, \beta_3$ eine Ganzheitsbasis von $\mathcal{O}_K$:

$$\mathcal{O}_K = \mathbb{Z}\beta_1 \oplus \mathbb{Z}\beta_2 \oplus \mathbb{Z}\beta_3.$$

Wir drucken die Zahlen $1, \alpha, \alpha^2$ als ganzzahlige Kombinationen von $\beta_1, \beta_2, \beta_3$ aus:

$$\begin{aligned} 1 &= c_{11}\beta_1 + c_{12}\beta_2 + c_{13}\beta_3, \\ \alpha &= c_{21}\beta_1 + c_{22}\beta_2 + c_{23}\beta_3, \\ \alpha^2 &= c_{31}\beta_1 + c_{32}\beta_2 + c_{33}\beta_3. \end{aligned}$$

Nach Satz 2.7 des Kurzskripts gilt $\Delta(1, \alpha, \alpha^2) = (\det C)^2 \Delta(\beta_1, \beta_2, \beta_3)$.

Da $\Delta(1, \alpha, \alpha^2) = -59$ ist, ist $\det(C) = \pm 1$. Daraus folgt, dass man die Zahlen $\beta_1, \beta_2, \beta_3$ als ganzzahlige Kombinationen der Zahlen $1, \alpha, \alpha^2$ ausdrucken kann. Dann ist $1, \alpha, \alpha^2$ auch eine Ganzheitsbasis von $\mathcal{O}_K$.

5) Nach Minkowski ist jedes Ideal A in $\mathcal{O}_K$ einem Ideal I mit

$$N(I) \leqslant \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|\Delta_K|}$$

äquivalent. Hier ist:
n der Grad $[K : \mathbb{Q}]$,
s die Anzahl der Paare von zueinander konjugierten komplexen (nicht reellen) Einbettungen von K in $\mathbb{C}$,
Δ_K die Diskriminate des Körpers K.

In unserem Fall ist
$n = 3$,
$s \leqslant 1$ (die Anzahl von Nullstellen von $x^3 + 2x - 1$ ist 3, deswegen ist die Anzahl der möglichen Paare $\leqslant 1$),
$\Delta_K = -59$.
Deswegen gilt

$$N(I) \leqslant \frac{3!}{3^3} \left(\frac{4}{\pi}\right)^1 \sqrt{|-59|} \leqslant 5.$$

Aufgabe 5. Sei $K = \mathbb{Q}(\sqrt{-7})$.
1) Berechnen Sie die Norm $N(2\mathcal{O}_K)$. [6 Punkte]
2) Zerlegen Sie das Ideal $2\mathcal{O}_K$ in Primideale. [6 Punkte]

Lösung. 1) Da $-7 \equiv 1 \pmod 4$ ist, ist $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\alpha$, wobei $\alpha = \frac{1+\sqrt{-7}}{2}$ ist. Sei $\gamma \in \mathcal{O}_K$ eine beliebige Zahl. Modulo $2\mathcal{O}_K$ können wir γ zu einer Zahl $\bar{\gamma} = n_1 + n_2\alpha$ mit $n_1, n_2 \in \{0, 1\}$ reduzieren. So haben wir 4 Repräsentanten: $0, 1, \alpha, 1 + \alpha$. Sie sind alle verschieden modulo $2\mathcal{O}_K$. Um das zu verstehen, ist es genügend zu zeigen, dass $1, \alpha, 1 + \alpha$ nicht in $2\mathcal{O}_K$ liegen. Betrachten wir nur einen von drei Fällen (die anderen sind analog): Wenn $1 + \alpha \in 2\mathcal{O}_K$ ist, dann ist $1 + \alpha = 2n + m\alpha$ mit $n, m \in \mathbb{Z}$, was unmöglich ist.
Also haben wir $N(2\mathcal{O}_K) = 4$.

2) Wir benutzen die folgende Bezeichnung für Nebenklassen:

$$[x] := x + 2\mathcal{O}_K.$$

Um das Ideal $2\mathcal{O}_K$ in Primideale zu zerlegen, suchen wir Nullteiler in dem Faktorring $\mathcal{O}_K/2\mathcal{O}_K = \{[0], [1], [\alpha], [1 + \alpha]\}$.

$$[\alpha] \cdot [1 + \alpha] = [\alpha(1 + \alpha)] = [\Big(\frac{1 + \sqrt{-7}}{2}\Big)\Big(\frac{3 + \sqrt{-7}}{2}\Big)]$$

$$= [\frac{(3 - 7) + 4\sqrt{-7}}{4}] = [-1 + \sqrt{-7}] = [2(-1 + \frac{1 + \sqrt{-7}}{2})] = [0].$$

Deswegen gilt $(2, \alpha)(2, 1 + \alpha) = (4, 2\alpha, 2 + 2\alpha, \alpha(1 + \alpha)) = (2)$. Die Ideale $(2, \alpha)$ und $(2, 1 + \alpha)$ sind Prim, da $N((2, \alpha)) = N((2, 1 + \alpha)) = 2 \in \text{Prim}(\mathbb{Z})$ ist.