Übungen zur Elementaren Zahlentheorie
-letztes Lösungsblatt-

Prof. Dr. K. Wingberg
J. Bartels

SS 2007

http://www.mathi.uni-heidelberg.de/~bartels/Uebungen.htm

Lösung zum elften Zettel

1 . Aufgabe :
a) Folgere aus obiger Aufgabe, daß jede Idealklasse ein Ideal

$$J = a\mathbb{Z} + \frac{b+\sqrt{D}}{2}\mathbb{Z} \text{ mit } |b| \le a \le c := \frac{b^2 - D}{4a}$$

enthält und daß man $b \ge 0$ annehmen kann, für den Fall, daß eines der obigen„$\le$“ ein „$=$“ ist.
b) Zeige, daß $\mathfrak{N}(J) = a \le \sqrt{|D|/3}$ gilt und vergleiche diesen Wert mit der oberen Schranke für die Norm aus Theorem 6.6.11 aus dem Buch von Schmidt.

a) Es sei

$$I = (a, \frac{b+\sqrt{D}}{2})$$

so, daß $a \in \mathbb{N}_{>0}$ minimal gewählt ist ein Ideal aus einer vorgegebenen Idealklasse. Das geht nach der Aufgabe auf dem letzten Blatt. Es ist dann $c \ge a$, weil $(c, \frac{-b+\sqrt{D}}{2})$ nach Aufgabe 1 b) des vorangegangenen Blatts in derselben Klasse liegt.
b) Aus der 1. Aufgabe des letzten Blatts folgt: $\mathfrak{N}(J) = a, (\delta = 1)$.
Insbesondere hat man wegen $|b| \le a \le c$ die Ungleichung:

$$|D| = 4ac - b^2 \ge 4a^2 - a^2 = 3a^2,$$

was $a \le \sqrt{\frac{|D|}{3}}$ ergibt.
Der Satz von Minkowskis liefert die Schranke $\frac{2\sqrt{D}}{\pi}$ und der Quotient ist

$$\frac{\frac{2}{\pi}}{\frac{1}{\sqrt{3}}} \approx 1,10,$$

d.h. man hat eine etwas bessere Schranke als die von Minkowski.

2 . Aufgabe (Fortsetzung)**:**
a) Zeige für $x, y \in \mathbb{Q}$ die folgende Gleichung:

$$N(ax + \frac{b+\sqrt{D}}{2}y) = a(ax^2 + bxy + cy^2)$$

und folgere daraus: $a^2 = \min_{x\in J\setminus\{0\}} N(x)$.
b) Ein Ideal $J = a\mathbb{Z} + \frac{b+\sqrt{D}}{2}\mathbb{Z}$, daß obigen Punkt erfüllt (d.h. daß $a^2 = \min_{x\in J\setminus\{0\}} N(x)$), heißt „reduziert". Zeige, daß es in jeder Idealklasse genau ein reduziertes Ideal gibt, indem man zunächst zeigt, daß $ac = \min_{x\in J\setminus\{0\}} N(x)$ gilt.
c) Folgere aus obigem den

0.0.1 Satz: *Ist K ein quadratischer Zahlkörper der Diskriminante $D < 0$, dann sind die Idealklassen aus $\mathcal{O}_K$ in Bijektion mit den Tripeln (a, b, c), so daß $b^2 - 4ac = D, |b| \leq a \leq c$ und $b \geq 0$, wenn $|b| = a$ oder $a = c$.*

a) Die Norm rechnet man aus und bekommt damit diese Gleichung.

$$J = \{ax + \frac{b+\sqrt{D}}{2}y | x, y \in \mathbb{Z}\}$$

Für $x = 1, y = 0$ ist die Norm des Elements aus J gleich a^2, d.h. dieser Wert wird tatsächlich angenommen. Andererseits gilt

$$ax^2 + bxy + cy^2 \geq ax^2 - |b||xy| + cy^2 \geq a(x^2 - |xy| + y^2) \geq a.$$

Dabei benutzt man, daß $x^2 + x + 1 \geq \frac{3}{4}$ auf $\mathbb{R}$, also ≥ 1 auf $\mathbb{Z}$ gilt.
b) Die Norm ac wird für $(x, y) = (0, 1)$ angenommen.
Sind $I = (a, \frac{b+\sqrt{D}}{2})$ und $I' = (a', \frac{b'+\sqrt{D}}{2})$ reduzierte Ideale derselben Klasse: $I = \alpha I'$, dann hat man $= a = \mathfrak{N}(\alpha)' = \mathfrak{N}(\alpha)a'$ und weiter:

$$\{Nu | u \in I \setminus \{0\}\} = \{N(\alpha u') | u' \in I' \setminus \{0\}\} = N(\alpha)\{Nu' | u' \in I' \setminus \{0\}\}$$

und die Minima der Normen sind $a^2 = N(\alpha)a'^2$, also: $N(\alpha) = 1$ und deshalb ist a gleich a' und $I \cap \mathbb{Z} = I' \cap \mathbb{Z}$. Die Mengen

$$\{N(u) | u \in I \setminus \mathbb{Z}\} = \{N(u') | u' \in I' \setminus \mathbb{Z}\}$$

haben das gemeinsame Minimum $ac = a'c'$, also ist $c' = c$.
Weil $D = b^2 - 4ac = b'^2 - 4a'c'$ gilt, folgt $b = \pm b'$ und es bleibt nur noch zu zeigen: $b \neq -b'$.
Man hat $a \in I$, also gibt es ein $u' \in I'$, so daß $\alpha u' = a$ gilt.
$N(u') = a^2$ und $u' = \pm a \neq 0 \Rightarrow \alpha = \pm 1$ ist eine Einheit, also Sind die Ideale I und I' gleich. Demnach gibt es zwei ganze Zahlen x, y, so daß $\frac{b+\sqrt{D}}{2} = xa + y\frac{-b+\sqrt{D}}{2}$ gilt. Es folgen $y = 1$ und $b = xa$; weil $|b| \leq a$ gilt, hat man $x = b = 0$, was absurd ist, also: $b = b'$.
c) folgt aus b).

3 . Aufgabe :
Berechne die Anzahl der Idealklassen von

$$\mathbb{Q}(\sqrt{-d}) \text{ für } d = 7, 15 \text{ und } 19.$$

Für

$$a \leq \sqrt{\frac{|D|}{3}}, a \in \mathbb{Z}$$

probiert man alle $b \in \mathbb{Z}$ aus für die gilt: $|b| \leq a$ und $b \geq 0$, wenn $|b| = a$:
Ist $c := \frac{b^2-D}{4a}$ eine ganze Zahl? Wenn $a = c$ ist, dann dürfen wir ein solches Tripel $(a, \pm b, c)$ nicht doppelt zählen, ansonsten registrieren wir die Anzahl der Tripel:

d	$\sharp Cl_K$	Tupel (a, b, c)
7	1	$(1, 1, 2)$
15	2	$(1, 1, 4), (2, 1, 2)$
19	1	$(1, 1, 5)$

Die letzte Aufgabe kommt noch.