Algebraic Number Theory — Exercise Sheet 1 (Solutions)

Manuel Luethi
Federico Viola

Spring 2024

1.
2. a) The fact that $\mathrm{N}(z)$ is multiplicative follows immediately from the fact that

$$\overline{z_1 z_2} = \overline{z_1} \cdot \overline{z_2} \quad \text{for all} \quad z_1, z_2 \in A.$$

b) We note that we have

$$\mathrm{N}(z) = a^2 - db^2 \in \mathbb{Z} \quad \text{for} \quad z = a + b\sqrt{d} \in A,$$

so what we want to prove is

$$A^\times = \{z \in A : \mathrm{N}(z) = \pm 1\}.$$

If $\mathrm{N}(z) = \pm 1$, we have $z\overline{z} = \pm 1$. Since $\overline{z} \in A$, we thus find that $z \in A^\times$. For the opposite inclusion, note first that we have seen above that $|\mathrm{N}(z)| \in \mathbb{N} \cup \{0\}$ for all $z \in A$. Hence it suffices to show that for all $z \in A^\times$ we have $|\mathrm{N}(z)| \neq 0$ and $|\mathrm{N}(z)| \leqslant 1$. If $\mathrm{N}(z) = 0$ then

$$\left(a + b\sqrt{d}\right)\left(a - b\sqrt{d}\right) = 0$$

and since d is squarefree, we have $\sqrt{d} \notin \mathbb{Q}$ and, thus, the only possibility is $a = b = 0$, which means that $z = 0 \notin A^\times$. If $|\,\mathrm{N}(z)| > 1$, we have $z \notin A^\times$ because otherwise there would exist some $z' \in A^\times$ with $zz' = 1$ but

$$|\,\mathrm{N}(zz')| = |\,\mathrm{N}(z)\,\mathrm{N}(z')| \geqslant |\,\mathrm{N}(z)| > 1.$$

In order to see that $A_1^\times$ forms a subgroup of $A^\times$, we see that $A_1^\times$ can be characterised as the set

$$A_1^\times = \{z \in A : \mathrm{N}(z) = 1\}.$$

By multiplicativity of $z \mapsto \mathrm{N}(z)$, we know that $\mathrm{N}|_{A^\times}$ is a homomorphism and $A_1^\times$ is its kernel. By the first isomorphsim theorem, the induced map

$$\begin{tikzcd}
A^\times \arrow[r, "\mathrm{N}"] \arrow[d, two heads] & \{\pm 1\} \\
A^\times / A_1^\times \arrow[ur, dashed, hook] &
\end{tikzcd}$$

is injective and, therefore, $[A^\times : A_1^\times] = |A^\times / A_1^\times| \leqslant |\{\pm 1\}| = 2$.

c) We skip the verification that ϕ is a group homomorphism; this is purely formal. If $z = a + b\sqrt{d} \in A$ is such that $\phi(z) = 0$, then $a + b\sqrt{d} = \pm 1$. Since $\sqrt{d}$ is irrational, this is only possible if $a \in \{\pm 1\}$ and $b = 0$, or in other words, if $z \in \{\pm 1\}$.

d) Our aim is to show that $\phi(A_1^\times)$ is a discrete subgroup of $\mathbb{R}$ (and thus cyclic). Let $B \subset (0, \infty)$ be compact. We will prove that the set of $z \in A_1^\times$ satisfying $z \in \phi^{-1}(B)$ is finite. Indeed, note that there exists $C > 1$ such that

$$C^{-1} < |z| < C \quad \text{for all} \quad z \in \phi^{-1}(B).$$

Thus, for $z = a + b\sqrt{d}$, we have

$$C^{-1} < |a + b\sqrt{d}| < C.$$

Furthermore, by multipliying both sides by the conjugate $\overline{z} = a - b\sqrt{d}$, we obtain

$$C^{-1}|a - b\sqrt{d}| < 1 < C|a - b\sqrt{d}| \qquad \iff \qquad C^{-1} < |a - b\sqrt{d}| < C.$$

We skip the explicit proof that the resulting inequality

$$C^{-2} < |a^2 - db^2| < C^2$$

can only have a finite number of solutions (with $a, b \in \mathbb{Z}$).

e) The existence of a non-trivial solution means simply that the group $\phi(A_1^\times)$ is non-trivial. Since it is cyclic, is is generated by an element $\phi(z_0)$ for some $z_0 \in A_1^\times$. Recalling that $\ker\phi = \{\pm 1\}$, we thus get

$$A_1^\times = \{\pm {z_0}^n : n \in \mathbb{Z}\}.$$

f) Given a number $x \in \mathbb{R}$, let

$$[x] = \sup\{n \in \mathbb{Z} \colon n \leqslant x\}$$

denote the integral part of x and define the fractional part of x by

$$\{x\} = x - [x] \in [0, 1).$$

Consider the $n + 2$ real numbers β_ℓ given by

$$\beta_\ell := \{\ell\alpha\} \quad \text{for} \quad \ell = 0, \ldots, n, \qquad \text{and} \qquad \beta_{n+1} := 1.$$

We set

$$m_0 := \min_{\ell_1, \ell_2 \in \{0, \ldots, n+1\}} |\beta_{\ell_1} - \beta_{\ell_2}|.$$

By the pigeonhole principle, we have that

$$m_0 \leqslant \frac{1}{n+1}.$$

Note that the case

$$m_0 = \frac{1}{n+1}$$

can only happen if

$$\{\beta_0, \ldots, \beta_{n+1}\} = \left\{0, \frac{1}{n+1}, \frac{2}{n+1}, \ldots, 1\right\}.$$

Let $0 \leqslant \ell \leqslant n$ such that $\beta_\ell = \frac{1}{n+1}$ and note that $\ell \neq 0$. Then

$$\alpha = \frac{[\ell\alpha]}{\ell} + \frac{1}{\ell(n+1)} \in \mathbb{Q},$$

which is absurd. Hence we even have the strict inequality

$$m_0 < \frac{1}{n+1}.$$

Choose $\ell_1 > \ell_2$ such that $m_0 = |\beta_{\ell_1} - \beta_{\ell_2}|$, and set

$$a := [\ell_1\alpha] - [\ell_2\alpha] \quad \text{and} \quad b := \ell_1 - \ell_2.$$

Then

$$\left|\alpha - \frac{a}{b}\right| = \frac{|\alpha(\ell_1 - \ell_2) - ([\ell_1\alpha] - [\ell_2\alpha])|}{b} = \frac{|\{\ell_1\alpha\} - \{\ell_2\alpha\}|}{b} = \frac{m_0}{b} < \frac{1}{b(n+1)},$$

which is what we wanted to show.

g) By setting $a_0 = [\alpha]$ and $b_0 = 1$, we get the first requested pair (a_0, b_0). Now, given a coprime pair (a_ℓ, b_ℓ), we will construct a new coprime pair $(a_{\ell+1}, b_{\ell+1})$ satisfying

$$\left|\alpha - \frac{a_{\ell+1}}{b_{\ell+1}}\right| < \left|\alpha - \frac{a_\ell}{b_\ell}\right|.$$

We start by choosing an integer N such that

$$\frac{1}{N+1} < \left|\alpha - \frac{a_\ell}{b_\ell}\right|,$$

which is always possible as α is irrational. Then we choose integers $a'_{\ell+1}, b'_{\ell+1} \in \{1, \ldots, N\}$ such that

$$\left|\alpha - \frac{a'_{\ell+1}}{b'_{\ell+1}}\right| < \frac{1}{(N+1)b'_{\ell+1}},$$

and set

$$a_{\ell+1} := \frac{a'_{\ell+1}}{(a'_{\ell+1}, b'_{\ell+1})} \quad \text{and} \quad b_{\ell+1} := \frac{b'_{\ell+1}}{(a'_{\ell+1}, b'_{\ell+1})}.$$

This is the requested new pair: By definition it is coprime, and we have

$$\left|\alpha - \frac{a_{\ell+1}}{b_{\ell+1}}\right| = \left|\alpha - \frac{a'_{\ell+1}}{b'_{\ell+1}}\right| < \frac{1}{(N+1)b'_{\ell+1}} \leqslant \frac{1}{{b'_{\ell+1}}^2} \leqslant \frac{1}{{b_{\ell+1}}^2},$$

as well as

$$\left|\alpha - \frac{a_{\ell+1}}{b_{\ell+1}}\right| = \left|\alpha - \frac{a'_{\ell+1}}{b'_{\ell+1}}\right| < \frac{1}{(N+1)b'_{\ell+1}} \leqslant \frac{1}{N+1} \leqslant \left|\alpha - \frac{a_\ell}{b_\ell}\right|.$$

h) By the previous exercise, we know that there exist infinitely many coprime pairs (x, y) such that

$$\left|\sqrt{d} - \frac{x}{y}\right| < \frac{1}{y^2}.$$

Furthermore, for these pairs we have

$$\begin{aligned} 0 < \left|x^2 - dy^2\right| &= y^2 \left|\sqrt{d} - \frac{x}{y}\right| \left|\sqrt{d} + \frac{x}{y}\right| \\ &< \sqrt{d} + \frac{x}{y} \leqslant \sqrt{d} + \left(\sqrt{d} + \frac{1}{y^2}\right) \leqslant 2\sqrt{d} + 1. \end{aligned}$$

In other words, there are infinitely many pairs (x, y) such that

$$0 < \left|x^2 - dy^2\right| \leqslant 2\sqrt{d} + 1.$$

In particular, there must be an integer n with $|n| \leqslant 2\sqrt{d} + 1$ such that

$$x^2 - dy^2 = n$$

has infinitely many solutions. Finally, since there are only finitely many residue classes mod n, we can surely find (x_1, y_1) and (x_2, y_2) such that

$$x_1 \equiv x_2 \bmod n \quad \text{and} \quad y_1 \equiv y_2 \bmod n.$$

i) First note that $z_0 \in A$. Indeed, noting that

$$x_1x_2 - y_1y_2d \equiv {x_1}^2 - d{y_1}^2 \equiv 0 \bmod n$$

and

$$y_1x_2 - y_2x_1 \equiv y_1x_1 - y_1x_1 \equiv 0 \bmod n,$$

we have

$$z_0 = \frac{(x_1 + y_1\sqrt{d})(x_2 - y_2\sqrt{d})}{n} = \frac{x_1x_2 - dy_1y_2}{n} + \frac{y_1x_2 - x_1y_2}{n}\sqrt{d} \in A.$$

Furthermore, because of $\mathrm{N}(z_1) = \mathrm{N}(z_2) = n$, we have $\mathrm{N}(z_0) = 1$, which shows that z_0 is indeed a solution to Pell's equation.

3. Let $P = X^2 + bX + c \in \mathbb{Z}[X]$, assume that $b^2 - 4c < 0$. Let ζ be a root of P and consider the ring $\mathbb{Z}[\zeta] \subset \mathbb{C}$.

a) To show that

$$\mathbb{Z}[\zeta] = \mathbb{Z} + \mathbb{Z}\zeta.$$

one can use the fact that ζ satisfies a quadratic monic polynomial over $\mathbb{Z}$ and the Euclid's algorithm. In order to deduce that $\mathbb{Z}+\mathbb{Z}\zeta$ is a lattice, we note first that 1 and ζ are linearly independent over $\mathbb{R}$ as $\zeta \notin \mathbb{R}$, so $\mathbb{Z}+\mathbb{Z}\zeta$ contains an $\mathbb{R}$-basis of $\mathbb{C} \cong \mathbb{R}^2$. It remains to show that $\mathbb{Z}+\mathbb{Z}\zeta$ is discrete and, as $\mathbb{Z}+\mathbb{Z}\zeta$ is a group, it suffices to show that 0 is isolated. So let $(z_n)_{n\in\mathbb{N}}$ be a sequence in $\mathbb{Z}+\mathbb{Z}\zeta$ and assume that $z_n \to 0$ as $n \to \infty$. Write

$$z_n = a_n + b_n\zeta \quad (a_n, b_n \in \mathbb{Z}).$$

Then

$$0 = \lim_{n\to\infty} \operatorname{Im}(z_n) = \lim_{n\to\infty} b_n \operatorname{Im}(\zeta)$$

and therefore $b_n = 0$ for all but finitely many n. It follows that $\operatorname{Re}(z_n) = a_n + b_n \operatorname{Re}(\zeta) = a_n$ for all but finitely many n and thus also $a_n = 0$ for all but finitely many $n \in \mathbb{N}$.

b) Let $s = c + d\zeta$ with $c, d \in \mathbb{Z}$. If $x = a + b\zeta$, we have

$$xs = ac + (ad + bc)\zeta + bd\zeta^2 = ac - bdC + (ad + bc - bdB)\zeta.$$

Substituting in the equation, we get

$$(ac - bdC, ad + bc - bdB) = (a, b)\begin{pmatrix} \iota(s)_{11} & \iota(s)_{12} \\ \iota(s)_{21} & \iota(s)_{22} \end{pmatrix} \quad \forall a, b \in \mathbb{Z}^2.$$

Setting $a = 1, b = 0$ we get

$$(c, d) = (\iota(s)_{11}, \iota(s)_{12}).$$

Setting $a = 0, b = 1$ we get

$$(-dC, c - dB) = (\iota(s)_{21}, \iota(s)_{22}).$$

Therefore we have

$$\iota(c + d\zeta) = \begin{pmatrix} c & d \\ -dC & c - dB \end{pmatrix} \quad \forall c, d \in \mathbb{Z}^2.$$

It is clear that this defines an injective homomorphism of $\mathbb{Z}$-modules. Observe that

$$\iota(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \iota(\zeta) = \begin{pmatrix} 0 & 1 \\ -C & -B \end{pmatrix}.$$

In order to check multiplicativity and conclude that ι is a homomorphism of rings, it remains to check that $\iota(\zeta)^2 = \iota(\zeta^2)$. We have

$$\iota(\zeta)^2 = \begin{pmatrix} 0 & 1 \\ -C & -B \end{pmatrix}^2 = \begin{pmatrix} -C & -B \\ BC & -C+B^2 \end{pmatrix} = \iota(-C - B\zeta) = \iota(\zeta^2).$$

c) Consider the homomorphism of $\mathbb{Z}$-modules obtained with the composition

$$\mathbb{Z}[\zeta] \xrightarrow{\theta} \mathbb{Z}^2 \xrightarrow{\pi} \mathbb{Z}^2/M_s$$

where π is the natural projection of $\mathbb{Z}^2$ onto its quotient $\mathbb{Z}^2/M_s$.
This composition is clearly surjective, since θ is an isomorphism. Its kernel is the set of $x \in \mathbb{Z}[\zeta]$ such that $\theta(x) \in M_s$. We claim that it coincides with the ideal (s). Indeed, if $x = ys$ for some $y \in \mathbb{Z}[\zeta]$ then

$$\theta(x) = \theta(ys) = \theta(y)\iota(s) \in \mathbb{Z}^2\iota(s) = M_s.$$

Vice versa, if $\theta(x) = z\iota(s)$ for some $z \in \mathbb{Z}^2$ then setting $y = \theta^{-1}(z) \in \mathbb{Z}[\zeta]$ we get $\theta(x) = \theta(y)\iota(s) = \theta(ys)$ and hence $x = ys \in (s)$.
We can conclude that $\mathbb{Z}[\zeta]/(s) \cong \mathbb{Z}^2/M_s$.