

Solutions to Sheet 1

Exercise 1

Let $n \in \mathbb{N}$ and $\zeta_n = e^{2\pi i/n} \in \mathbb{C}$. Recall that $\mathbb{Z}[\zeta_n]$ denotes the smallest subring of the field of complex numbers that contains \mathbb{Z} and ζ_n . Show that $1/3 \notin \mathbb{Z}[\zeta_n]$.

Solution. There are multiple ways to show this. Note that if $1/3 \in \mathbb{Z}[\zeta_n]$, we'd have $\mathbb{Z}[1/3] \subset \mathbb{Z}[\zeta_n]$ as well. But there is a fundamental difference between $\mathbb{Z}[\zeta_n]$ and $\mathbb{Z}[1/3]$. The latter is a finite free \mathbb{Z} -module while the former is neither finite nor free. As \mathbb{Z} is a PID and submodules of finite free modules over a PID are finite and free, we have a contradiction. This implies other differences between the two rings. For example, $1/3 \in \mathbb{Z}[1/3]$ is not integral over \mathbb{Z} , while every element of $\mathbb{Z}[\zeta_n]$ is.

Exercise 2

Here, ζ_3 is as in Exercise 1. For $f \in \mathbb{N}$ we define

$$A_f = \left\{ a + fb \frac{\sqrt{-3}+1}{2} \mid a, b \in \mathbb{Z} \right\}.$$

1. Show that $A_f \subset A_1 = \mathbb{Z}[\zeta_3]$ is a subring of \mathbb{C} for all $f \in \mathbb{N}$.
2. Let $|\cdot|$ denote the absolute value on \mathbb{C} . Show that $|\omega|^2 \in \mathbb{Z}$ for all $\omega \in \mathbb{Z}[\zeta_3]$.
3. Show that the unit group $\mathbb{Z}[\zeta_3]^\times$ is equal to $\{\omega \in \mathbb{Z}[\zeta_3] \mid |\omega| = 1\}$.

Solution.

1. Note that $\zeta_3 = \frac{\sqrt{-3}+1}{2}$, and that $1 + \zeta_3 + \zeta_3^2 = 0$. We have

$$(a + fb\zeta_3)(c + fd\zeta_3) = ac + f(ad + cb)\zeta_3 - f^2bd(1 + \zeta_3) \in A_f,$$

so A_f is closed under multiplication. We have $A_f \subset A_{f'}$ whenever $f' \mid f$, and $A_1 = \mathbb{Z}[\zeta_3]$ is a subring of \mathbb{C} .

2. Remember that for the absolute value on \mathbb{C} we have

$$|x + iy|^2 = (x + iy)(x - iy) = x^2 + y^2.$$

for $f \in \mathbb{N}$ and $a, b \in \mathbb{Z}$ this gives

$$\left| a + fb \frac{\sqrt{-3}+1}{2} \right|^2 = \left(a + \frac{bf}{2} \right)^2 + 3 \left(\frac{fb}{2} \right)^2 = a^2 + abf + (fb)^2 \in \mathbb{Z}.$$

3. All units have invertible absolute value, hence we can conclude that if ω is a unit, it has absolute value 1. This shows one implication. But $|\omega|^2 = 1$ implies that $\omega\bar{\omega} = 1$, hence $\omega^{-1} = \bar{\omega} \in \mathbb{Z}[\zeta_3]$, which shows the reverse implication.

Exercise 3

An integral domain A is called Euclidean if there exists a function $n : A \setminus \{0\} \rightarrow \mathbb{Z}_{\geq 0}$ such that for all $a \in A$ and $b \in A \setminus \{0\}$ there exist $q, r \in A$ such that $a = bq + r$ and either $r = 0$ or $n(r) < n(b)$.

1. Show that Euclidean domains are principal ideal domains.
2. Show that the ring $\mathbb{Z}[\zeta_3]$ is euclidean.
3. Show that $\mathbb{Z}[\sqrt{2}]$ is euclidean.

Solution.

1. Let R be a euclidean ring with norm function δ . Let $\mathfrak{a} \subset R$ be an ideal, and let $a \in \mathfrak{a}$ be an element such that $\delta(a)$ is minimal among all elements of \mathfrak{a} . Now we have $\mathfrak{a} = (a)$. Indeed, if $f \in \mathfrak{a}$ is another element, we have $f = qa + r$ with $q \in A$ and either $\delta(r) < \delta(a)$ or $r = 0$. As $r = f - qa \in \mathfrak{a}$ and $\delta(a)$ is already minimal among elements in \mathfrak{a} , $\delta(r) < \delta(a)$ is not possible. Therefore we find $r = 0$, hence $f = qa \in (a)$.
- 2.& 3. We show that $\nu : z \mapsto |N(z)|$ is a euclidean norm function in both cases (where N denotes the respective norm function). Write \mathcal{O}_K for the respective rings. Let $a, b \in \mathcal{O}_K$, $b \neq 0$. We want to show that there are $r \in \mathcal{O}_K$ and $q \in \mathcal{O}_K$ with $\nu(r) < \nu(b)$ and $a = qb + r$. The idea is simple. We try to approximate $\frac{a}{b} \in K = \text{Frac}(\mathcal{O}_K)$ by some algebraic integer $q = x + y\sqrt{d} \in \mathcal{O}_K$ such that $|N(\frac{a}{b} - q)| < 1$. Once we found such a q , we set $r = a - qb \in \mathcal{O}_K$ and find

$$\nu(r) = |N(r)| = \left| N(b)N\left(\frac{a}{b} - q\right) \right| < |N(b)| = \nu(b),$$

which finishes the proof.

So we really only need to show that for $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ and $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$, there are such elements q . In our cases, this is relatively simple. In the case of $\mathbb{Z}[\sqrt{2}]$ we write $\frac{a}{b} = u + v\sqrt{2}$ and choose $x, y \in \mathbb{Z}$ such that $|x - u| \leq 1/2$ and $|y - v| \leq 1/2$. Now

$$|N(\frac{a}{b} - q)| \leq |(x - u)^2 - 2(y - v)^2| \leq \frac{3}{4} < 1,$$

and we are done. The case $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ works the same way. Here we find

$$|N(\frac{a}{b} - q)| = |(x - u)^2 + (x - u)(y - v) + (y - v)^2| \leq \frac{3}{4} < 1.$$

Exercise 4

Let $x, y \in \mathbb{Z}$ such that $y^2 - y = x^3$. Show that $(x, y) = (0, 0)$ or $(x, y) = (0, 1)$.

Solution. As y and $y - 1$ share no prime factors, the equation $y^2 - y = y(y - 1) = x^3$ implies that both y and $y - 1$ are cubes. But this implies $y \in \{0, 1\}$, and it's easy to see that all solutions are of the given form.