

Solutions to Sheet 2

Exercise 1

Define $\zeta = \frac{-1+\sqrt{-3}}{2} \in \mathbb{C}$.

1. Show that ζ is a primitive third root of unity.
2. Show that the norm (for the field extension $\mathbb{Q}(\zeta)/\mathbb{Q}$ of an element $x + y\zeta \in \mathbb{Q}(\zeta)$, where $x, y \in \mathbb{Q}$, is given by $x^2 - xy + y^2$, and that this is non-negative for all $x, y \in \mathbb{Q}$.
3. Following the discussion of $\mathbb{Z}[i]$ from the lecture, show that a prime $p \neq 3$ is of the form $p = x^2 - xy + y^2$ for some $x, y \in \mathbb{Z}$ if and only if $p \equiv 1 \pmod{3}$.

Solution.

1. We have

$$\zeta^3 = \left(\frac{1}{2}(-1 + \sqrt{-3})\right)^3 = 1/8(-1 + 3\sqrt{-3} - 9 + 3\sqrt{-3}) = 1.$$

As $\zeta \neq 1$ (and 3 has no non-trivial divisors), it is a primitive (third) root.

2. The norm is defined as the product of all galois-conjugates. The minimal polynomial of ζ is given by $f(x) = x^2 + x + 1 = (x - \zeta)(x - \bar{\zeta})$, so the only non-trivial element in the Galois-group $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is given by the action defined via $\zeta \mapsto \bar{\zeta}$, which is the same as complex conjugation. We find

$$N(x + \zeta y) = (x + \zeta y)(x + \bar{\zeta} y) = x^2 + (\zeta + \bar{\zeta})xy + \zeta\bar{\zeta}y^2.$$

The claim follows as $\zeta\bar{\zeta}$ and $\zeta + \bar{\zeta}$ are given by the constant and the negative of the second-to-highest coefficient of the minimal polynomial of ζ (which are both given by 1).

Exercise 2

1. Let A be a principal ideal domain that is not a field, and let $\mathfrak{m} \subset A$ be a maximal ideal. Prove that $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ is a one-dimensional vector space over A/\mathfrak{m} for any $n \geq 0$.
2. Let $A = \mathbb{C}[x, y]$ and $\mathfrak{m} = (x, y)$. Compute $\dim_{A/\mathfrak{m}}(\mathfrak{m}^n/\mathfrak{m}^{n+1})$ for $n \geq 0$. Deduce that A is not a principal ideal domain.
3. Let $A = \mathbb{Z}[\sqrt{-3}]$. Show that A has a unique maximal ideal \mathfrak{m} with $\mathfrak{m} \cap \mathbb{Z} = (2)$. Compute $\dim_{A/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2$. Deduce that A is not a principal ideal domain.

Solution.

1. Let $\pi \in A$ such that $(\pi) = \mathfrak{m}$. We have the map (of A -modules)

$$\varphi : A \rightarrow \mathfrak{m}^n/\mathfrak{m}^{n+1}, \quad a \mapsto a\pi^n$$

. It is obviously surjective, and one quickly verifies that the kernel is given by (π) . Hence we find $A/\mathfrak{m} \cong \mathfrak{m}^n/\mathfrak{m}^{n+1}$, and we are done.

2. We have $\mathfrak{m}^n = (x^n, x^{n-1}y, \dots, xy^{n-1}, y^n)$. These generators form a basis for $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ (they are generating and linearly independent over \mathbb{C}), hence the dimension is $n + 1$. This contradicts what we showed for principal ideal domains once $n \geq 1$.

Exercise 3

Let A be a unique factorization domain.

1. Show that for any prime element $\pi \in A$, the ideal $\mathfrak{p} = (\pi)$ is prime and only contains the prime ideals $\{0\}$ and \mathfrak{p} .
2. Conversely, let $0 \neq \mathfrak{p} \subset A$ be a prime ideal such that $\{0\}$ and \mathfrak{p} are the only prime ideals of A that are contained in \mathfrak{p} . Show that $\mathfrak{p} = (\pi)$ for some prime element $\pi \in A$.
3. Assume that each non-zero prime ideal $\mathfrak{p} \subset A$ satisfies the assumption in 2). Show that A is a principal ideal domain.

Solution.

1. Let $0 \neq \mathfrak{q}$ be a prime contained in \mathfrak{p} . Take some nonzero element $q \in \mathfrak{q}$. Write $q = a\pi^n$, where $a \in A$ is an element not divisible by π . Now, as \mathfrak{q} is prime, either $\pi^n \in \mathfrak{q}$ or $a \in \mathfrak{q}$. But we have $a \notin (\pi) \subset \mathfrak{q}$, hence $\pi^n \in \mathfrak{q}$. Induction shows that $\pi \in \mathfrak{q}$, which results in $\mathfrak{q} = \mathfrak{p}$.
2. Suppose $\pi \in \mathfrak{p}$ is a prime element contained in \mathfrak{p} . Then $(\pi) \subset \mathfrak{p}$, which by assumption shows $(\pi) = \mathfrak{p}$. We only need to show that there are prime ideals in any nonzero element \mathfrak{p} . For that sake, let $a \in \mathfrak{p}$. There is a finite decomposition $a = \prod_{i=1}^n p_i^{e_i}$, and we find that for some i , the prime element p_i lies in \mathfrak{p} .
3. Let $I \neq (0)$ be any ideal. Let π_1, \dots, π_n be the finite set of primes such that $I \subset (\pi_i)$ (this is a finite set because any $f \in I$ has only a finite number of divisors), and let e_i be the maximal integer such that $I \subset (\pi_i^{e_i})$ holds. We claim that $I = (\pi_1^{e_1} \cdots \pi_n^{e_n})$. We write (f) for the right hand side. The inclusion " $I \subset (f)$ " is trivial.
To show the other direction, it suffices to show that $f \in I$.

Exercise 4

1. Let A be any ring. Show that A contains minimal prime ideals.
2. Determine the minimal prime ideals of $\mathbb{Z}[x, y]/(xy)$.

Solution.

1. What does Zorn's Lemma say again? Ah. If in an ordered set we can show that any totally ordered chain has a minimal element, then there are minimal elements. As our ordered set we take the set of prime ideals, ordered by inclusion. To apply Zorn's lemma, let $\mathfrak{p}_1 \supset \mathfrak{p}_2 \supset \dots$ be a decreasing chain of prime ideals. We need to show that this chain has a minimal element, which is a prime ideal \mathfrak{p} such that $\mathfrak{p}_i \supset \mathfrak{p}$. We set $\mathfrak{p} = \bigcup_{i \in \mathbb{N}} \mathfrak{p}_i$, and we have to show that this is a prime ideal. This is straight-forward. Assume that $ab \in \mathfrak{p}$. Assume $b \notin \mathfrak{p}$. Then, there is some i such that $b \notin \mathfrak{p}_i$, and hence $b \notin \mathfrak{p}_j$ for all $j \geq i$. But now, as all of the \mathfrak{p}_i are prime, we find that $a \in \mathfrak{p}_i$ for all i . Hence $a \in \mathfrak{p}$, and we are done.
2. We use that minimal prime ideals of $\mathbb{Z}[x, y]/(xy)$ are exactly those prime ideals of $\mathbb{Z}[x, y]$ that are minimal among those containing (xy) . As $\mathbb{Z}[x, y]$ is a UFD, the only prime ideals containing (xy) are (x) and (y) .

