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 $f(x) = x^2 + x + 1 = (x - \zeta)(x - \overline{\zeta})$, so the only non-trivial element in the Galois-group $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is given by the action defined via $\zeta \mapsto \overline{\zeta}$, which is the same as complex conjugation. We find
$$\mathrm{N}(x + \zeta y) = (x + \zeta y)(x + \overline{\zeta} y) = x^2 + (\zeta + \overline{\zeta})xy + \zeta\overline{\zeta} y^2.$$
The claim follows as $\zeta + \overline{\zeta} = -1$ and $\zeta\overline{\zeta} = 1$.

   It remains to show that the norm is always positive. The claim is trivial if x, y have different sign. If the sign is the same, we may wlog assume that both are positive. In that case, this is a special case of the AM-GM inequality. But for completeness, here is a calculation:
$$x^2 - xy + y^2 \geq x^2 - 2xy + y^2 = (x-y)^2 \geq 0$$

3. We want to show that there is an element $z = x + \zeta y \in \mathbb{Z}(\zeta)$ with $\mathrm{N}(z) = p$ if and only if $3 \mid p - 1$. We know from the lecture that $\mathbb{Z}[\zeta]$ is a principal ideal domain. First note that the "only if" part is trivial. Indeed, we have
$$x^2 - xy + y^2 \equiv \begin{cases} 1 \pmod 3, & \text{if } (x,y) = (1,1),(0,1),(1,0) \\ 0 \pmod 3, & \text{if } (x,y) = (0,0). \end{cases}$$
If $3 \mid x$ and $3 \mid y$ we find that $3 \mid \mathrm{N}(x + \zeta y)$, hence $\mathrm{N}(x + \zeta y)$ cannot be a prime. This shows that all primes of the form $x^2 - xy + y^2$ have residue 1 mod 3.

   To show the converse implication, let $p \in \mathbb{Z}$ be any prime. As $\mathbb{Z}[\zeta]$ is a PID, the prime elements $\pi \in \mathbb{Z}[\zeta]$ that divide p are in bijection with the maximal (equivalently, non-zero prime) ideals $\mathfrak{m} \subset \mathbb{Z}[\zeta]$ such that $\mathfrak{m} \cap \mathbb{Z} = (p)$. An easy computation shows (lecture 3) that these ideals are in bijection with the irreducible monic factors of $T^2 + T + 1$ in $\mathbb{F}_p[T]$. As $\mathbb{F}_p[T]$ has a non-trivial third root of unity if and only if $3 \mid p - 1$, we find that there are two prime ideals "above" (p) if $3 \mid p - 1$.

Hence, let π_1, π_2 be the two prime elements of $\mathbb{Z}[\zeta]$ that divide p and write $(p) = (\pi_1^{e_1})(\pi_2^{e_2})$. As in the lecture we find $\mathrm{N}(\pi_1) = \mathrm{N}(\pi_2) = p$, which implies $e_1 = e_2 = 1$. Now we have a primary decomposition $p = \pi_1\pi_2$, which implies that $\pi_1 = \overline{\pi}_2$, which gives the desired representation of p.

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)

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

   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 $\mathfrak{m}^n = (x^n, x^{n-1}y, \ldots, xy^{n-1}, y^n)$. 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 showd for principal ideal domains once $n \geq 1$.
3. We first show that there is a unique maximal ideal of A with $\mathbb{Z} \cap \mathfrak{m} = (2)$. Indeed, those maximal ideals are in bijection with the maximal ideals of $\mathbb{F}_2[T]/(T^2+3)$. As T^2+3 factors in $\mathbb{F}_2[T]$ as $(T+1)^2$, we find that $\mathfrak{m} = (2, \sqrt{-3}+1)$ is the unique maximal ideal of $\mathbb{Z}[\sqrt{-3}]$ above (2).

   Now $\mathfrak{m}^2 = (4, 2\sqrt{-3}+2, -2+2\sqrt{-3})$. Hence the elements 2 and $\sqrt{-3}+1$ do not lie in $\mathfrak{m}^2$ as they have norm 4 (after choosing an embedding into $\mathbb{C}$), while all elements generating $\mathfrak{m}^2$ have norm 16. Hence there are at least 3 elements in $\mathfrak{m}/\mathfrak{m}^2$, thereby $\dim_{\mathbb{F}_2} \mathfrak{m}/\mathfrak{m}^2 \neq 1$.

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 $\pi_1, \ldots, \pi_n$ 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. Write $\alpha = \pi_1^{e_1} \ldots \pi_n^{e_n}$. We claim that $I = (\alpha)$. The inclusion "$I \subset (\alpha)$" is trivial.

   To show the other direction, it suffices to show that $\alpha \in I$. Suppose that $I = (g_i \mid i \in I)$. Write $g_i = h_i\alpha$ and inspect the ideal $I' = (h_i \mid i \in I)$. By construction there is no prime $\pi \in A$ such that $I' \subset (\pi)$, otherwise the factors e_i would not have been chosen maximal. But this shows that $I' = (1)$, i.e., $\alpha \in I$.

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 $\mathfrak{p}_1 \supset \mathfrak{p}_2 \supset \ldots$ 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 $\mathfrak{p} = \bigcap_{i \in \mathbb{N}} \mathfrak{p}_i$, 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). Using that $\mathbb{Z}[x, y]$ is a UFD, we find that those prime ideals are given by (x) and (y).

Max von Consbruch, email: s6mavonc@uni-bonn.de. Date: April 24, 2023