Exercise Sheet 3

1. The goal of of this exercise is to prove the irreducibility of cyclotomic polynomials in $\mathbb{Q}[X]$ (or in $\mathbb{Z}[X]$, which amounts to the same thing). For $q \geq 1$, we denote

$$\Phi_q = \prod_{\substack{1 \leq a \leq q-1 \\ (a,q)=1}} (X - e^{2i\pi a/q})$$

the q-th cyclotomic polynomial. We denote $\omega = e^{2i\pi/q}$ and let K be the cyclotomic field $\mathbb{Q}(e^{2i\pi/q}) = \mathbb{Q}(\omega)$.

Let $f \in \mathbb{Q}[X]$ be the monic minimal polynomial of ω; it has coefficients in $\mathbb{Z}$ and divides Φ_q and also $X^q - 1$. Let $g \in \mathbb{Z}[X]$ be the polynomial such that $X^q - 1 = fg$.

1. Show that

$$\prod_{a=1}^{q-1}(1 - \omega^a) = q.$$

Solution: Consider the polynomial $X^q - 1$, whose roots are 1 and w^a for $a = 1, \ldots, q-1$. Dividing $X^q - 1$ by $X - 1$ we get the polynomial

$$\frac{X^q - 1}{X - 1} = X^{q-1} + X^{q-2} + \cdots + X + 1, \tag{1}$$

but by factoring $X^q - 1$ as a product linear factors over $\mathbb{C}$ we get

$$\frac{X^q - 1}{X - 1} = \prod_{a=1}^{q-1}(X - w^a). \tag{2}$$

When $X = 1$, the right-hand side of (1) is q, whereas when $X = 1$ the right-hand side of (2) is precisely $\prod_{a=1}^{q-1}(1 - w^a)$, so we conclude the desired equality.

2. Let p be a prime number which does not divide q, and let $\boldsymbol{p}$ be a prime ideal in $\mathbb{Z}_K$ dividing $p\mathbb{Z}_K$. Show that the elements $(1, \omega, \ldots, \omega^{q-1})$ are distinct modulo $\boldsymbol{p}$.

Solution: Assume by contradiction that for some $0 \leq b < c \leq q-1$, $w^b \equiv w^c$ modulo $\boldsymbol{p}$. Then $1 \equiv w^{c-b} \mod \boldsymbol{p}$, so that

$$\begin{aligned} 1 - w^{c-b} &\in \boldsymbol{p} \\ \Rightarrow \prod_{a=1}^{q-1}(1 - w^a) &\in \boldsymbol{p} \\ \Rightarrow q &\in \boldsymbol{p}. \end{aligned}$$

But then we have $p, q \in \boldsymbol{p}$ with p and q relatively prime, so this implies that $1 \in \boldsymbol{p}$, which contradicts the assumption that $\boldsymbol{p}$ is a prime ideal. Thus $(1, w, \ldots, w^{q-1})$ are distinct modulo $\boldsymbol{p}$.

3. Show that ω^p is also a root of f. (Hint: argue by contradiction that otherwise $g(\omega^p) = 0$ and use reduction modulo $\boldsymbol{p}$ and the previous question; recall that if $x \in \mathbb{Z}_K/\boldsymbol{p}$ is a root of the reduction of a polynomial in $\mathbb{Z}[X]$, then x^p is also a root of the same polynomial.)

   Solution: Consider the reductions $\bar{f}$ and $\bar{g}$ of f and g, respectively, modulo $\boldsymbol{p}$. By the previous question, $\bar{f}$ and $\bar{g}$ must have distinct roots.

   Assume that $f(w^p) \neq 0$. Since w^p is a root of $X^q - 1$, it must therefore be a root of g. Since $g(w^p) = 0$, $\bar{g}(w^p) = 0 \in \mathbb{Z}_K/\boldsymbol{p}$. But since $f(w) = 0$ by assumption we also have $\bar{f}(w) = 0 \in \mathbb{Z}_K/\boldsymbol{p}$ and thus $\bar{f}(w^p) = 0 \in \mathbb{Z}_K/\boldsymbol{p}$, which contradicts the fact that $\bar{f}$ and $\bar{g}$ must have distinct roots.

   Thus $f(w^p) = 0$.

4. Deduce that ω^a is a root of f for any a coprime to q, and conclude that $f = \Phi_q$.

   Solution: Note that for any prime p, since f is the monic minimal polynomial of w and has w^p as a root, f must also be the monic minimal polynomial of w^p. Thus we can repeat the above argument for different primes p, to get that for any primes $p_1, \ldots, p_k$, all relatively prime to q, and any positive integers $e_1, \ldots, e_k$, $w^{p_1^{e_1} \cdots p_k^{e_k}}$ is a root of f. Any a coprime to q admits a factorization of this form, so w^a is a root of f.

   Thus every root of Φ_q is a root of f, so $\Phi_q | f$. We already have that $f | \Phi_q$, and both are monic, so equality must hold.

2. Let q be a prime number. The goal of this exercise is to show that the ring of integers of the cyclotomic field $\mathbb{Q}(e^{2i\pi/q})$ is $\mathbb{Z}[e^{2i\pi/q}]$. Let $\omega = e^{2i\pi/q}$.

1. Prove that
$$\mathrm{Tr}(1) = q - 1, \qquad \mathrm{Tr}(\omega^a) = -1 \text{ for } 1 \leq a \leq q - 1.$$

   Solution: Consider the basis $\{1, \ldots, w^{q-2}\}$ of $\mathbb{Q}(w)$ as a $\mathbb{Q}$-vector space. Note that $\mathbb{Q}(w)$ is a $(q-1)$-dimensional $\mathbb{Q}$-vector space, since Φ_q (using the notation from Problem 1) is irreducible of degree $q - 1$.

   Multiplication by 1 is described by the identity matrix, which has trace $q - 1$, so $\mathrm{Tr}(1) = q - 1$.

   Consider the matrix $M_a \in \mathrm{GL}(\mathbb{Q}(w))$ given by multiplication by w^a for $1 \leq a \leq q - 1$. Each basis element in $\{1, \ldots, w^{q-2}\}$ is taken to a different basis element when multiplied by w^a *except* for the element w^{q-1-a}, for which we have
$$w^a \cdot w^{q-1-a} = w^{q-1} = -\sum_{b=0}^{q-2} w^b.$$

   Thus the only nonzero element on the diagonal of M_a is the -1 in the $(q-1-a, q-1-a)$th position, so that $\mathrm{Tr}(w^a) = -1$.

2. Prove that for all a coprime to q, the element
$$\frac{\omega^a - 1}{\omega - 1}$$

is a unit in $\mathbb{Z}_K$, and that $1-\omega$ is not a unit in $\mathbb{Z}_K$. (Hint: use the formula from question 1 of Exercise 1.)

Solution: Note that

$$\frac{w^a-1}{w-1} = w^{a-1} + w^{a-2} + \cdots + 1.$$

All powers of w are in $\mathbb{Z}_K$, so $\frac{w^a-1}{w-1} \in \mathbb{Z}_K$. Let b be a positive integer such that $ab \equiv 1 \mod q$. Then similarly

$$\frac{w^{ab}-1}{w^a-1} = w^{a(b-1)} + w^{a(b-2)} + \cdots + w^a + 1 \in \mathbb{Z}_K,$$

but

$$\frac{w^a-1}{w-1} \cdot \frac{w^{ab}-1}{w^a-1} = \frac{w^{ab}-1}{w-1} = \frac{w-1}{w-1} = 1,$$

so $\frac{w^a-1}{w-1}$ has an inverse in $\mathbb{Z}_K$ and is thus a unit.

Now assume by contradiction that $1-w$ is a unit in $\mathbb{Z}_K$. Since $\frac{1-w^a}{1-w}$ is a unit in $\mathbb{Z}_K$, we also know that $1-w^a$ is a unit in $\mathbb{Z}_K$ for all a relatively prime to q, so $\prod_{a=1}^{q-1}(1-w^a)$ must be a unit as well. But by problem (1.1), we have just shown that q is a unit in $\mathbb{Z}_K$, or equivalently that $\frac{1}{q} \in \mathbb{Z}_K$. But $\frac{1}{q}$ is not an algebraic integer, so we have reached a contradiction. Thus $1-w$ is not a unit in $\mathbb{Z}_K$.

3. Prove that $(1-\omega)\mathbb{Z}_K \mid q\mathbb{Z}_K$ and that $(1-\omega)\mathbb{Z}_K \cap \mathbb{Z} = q\mathbb{Z}$.

   Solution: Since, by Exercise (1.1), we have $(1-w)|q$, we must also have $(1-w)\mathbb{Z}_K|q\mathbb{Z}_K$. That is, if $qz \in q\mathbb{Z}_K$, then $qz = (1-w)\left(\prod_{a=2}^{q-1}(1-w^a)\right) z \in (1-w)\mathbb{Z}_K$.

   We have just shown that $q\mathbb{Z} \subseteq (1-w)\mathbb{Z}_K$ and we know that $q\mathbb{Z} \subseteq \mathbb{Z}$, so $q\mathbb{Z} \subseteq (1-w)\mathbb{Z}_K \cap \mathbb{Z}$. Moreover, $(1-w)\mathbb{Z}_K \cap \mathbb{Z}$ is an ideal in $\mathbb{Z}$, so since q is prime, $(1-w)\mathbb{Z}_K \cap \mathbb{Z}$ is either $q\mathbb{Z}$ or $\mathbb{Z}$ itself. Assume by contradiction that $(1-w)\mathbb{Z}_K \cap \mathbb{Z} = \mathbb{Z}$. Then $1 \in (1-w)\mathbb{Z}_K$, so for some $z \in \mathbb{Z}_K$ we have $1 = (1-w)z$. But then $(1-w)$ is a unit in $\mathbb{Z}_K$, which contradicts the previous part.

4. Deduce that for all $y \in \mathbb{Z}_K$, we have $\mathrm{Tr}((1-\omega)y) \in q\mathbb{Z}$.

   Solution: Recall that $\mathrm{Tr}(x) \in \mathbb{Z}$ for $x \in \mathbb{Z}_K$, so for all $y \in \mathbb{Z}_K$, we have $\mathrm{Tr}((1-w)y) \in \mathbb{Z}$. By the previous part, it remains to show only that $\mathrm{Tr}((1-w)y) \in (1-w)\mathbb{Z}_K$.

   But $\mathrm{Tr}((1-w)y) = \sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(w)/\mathbb{Q})} \sigma((1-w)y) = \sum_\sigma (1-\sigma(w))\sigma(y)$. Note that for all σ, there exists an a relatively prime to q such that $\sigma(w) = w^a$, which in turn implies that $(1-\sigma(w))\sigma(y) = (1-w)\frac{(1-w^a)}{(1-w)}\sigma(y) \in (1-w)\mathbb{Z}_K$. Thus $\mathrm{Tr}((1-w)y) \in \mathbb{Z}_K$, as desired.

5. Find an element b_0 of K such that for any

$$x = \sum_{i=0}^{q-2} a_i \omega^i$$

   in K, we have $\mathrm{Tr}(b_0 x) = a_0$. Deduce that if $x \in \mathbb{Z}_K$ then $a_0 \in \mathbb{Z}$.

Solution: Write $b_0 = \frac{1-w}{q}$, and assume that $a_i \in \mathbb{Q}$. Then we can compute explicitly

$$\begin{aligned}\operatorname{Tr}(b_0 x) &= \operatorname{Tr}\left(\sum_{i=0}^{q-2} a_i \frac{1-w}{q} w^i\right) \\ &= \sum_{i=0}^{q-2} \frac{a_i}{q}(\operatorname{Tr}(w^i) - \operatorname{Tr}(w^{i+1}).\end{aligned}$$

If $1 \leq i \leq q-2$, then $\operatorname{Tr}(w^i) = \operatorname{Tr}(w^{i+1}) = -1$, so that $\operatorname{Tr}(w^i) - \operatorname{Tr}(w^{i+1}) = 0$. If $i = 0$, then $\operatorname{Tr}(w^i) = q-1$ and $\operatorname{Tr}(w^{i+1}) = -1$, so that we have

$$\begin{aligned}\operatorname{Tr}(b_0 x) &= \frac{a_0}{q}(\operatorname{Tr}(1) - \operatorname{Tr}(w)) \\ &= \frac{a_0}{q} q = a_0.\end{aligned}$$

If $x \in \mathbb{Z}_K$, then we have $a_0 = \operatorname{Tr}\left(\frac{1-w}{q}x\right) = \frac{1}{q}\operatorname{Tr}((1-w)x)$. By the previous portion, $\operatorname{Tr}((1-w)x) \in q\mathbb{Z}$, so $\frac{1}{q}\operatorname{Tr}((1-w)x) \in \mathbb{Z}$. Thus $a_0 \in \mathbb{Z}$.

6. Similarly, find the element b_i such that, for any x as above, we have $\operatorname{Tr}(b_i x) = a_i$, and deduce that $a_i \in \mathbb{Z}$ for all i. (Hint: consider $\omega^j x$ for suitable j.)
   Solution: Consider $b_0 w^{q-i}$ for $1 \leq i \leq q-2$. Then for any x as above,

$$\begin{aligned}\operatorname{Tr}(b_0 w^{q-i} x) &= \operatorname{Tr}\left(\sum_{j=0}^{q-2} a_j \frac{1-w}{q} w^{q-i} w^j\right) \\ &= \sum_{j=0}^{q-2} \frac{a_j}{q}(\operatorname{Tr}(w^{q-i+j}) - \operatorname{Tr}(w^{q-i+j+1})).\end{aligned}$$

   When $j = i$, we have $w^{q-i+j} = w^q = 1$, which has trace $q-1$, and when $j = i-1$, we have $w^{q-i+j+1} = w^q = 1$; all other traces in the above expression are -1, so

$$\begin{aligned}\operatorname{Tr}(b_0 w^{q-i} x) &= \frac{a_i}{q}(q-1+1) + \frac{a_{i-1}}{q}(-q) \\ &= a_i - a_{i-1}.\end{aligned}$$

   Thus choosing $b_i = b_0 \sum_{j=0}^{i} w^{q-j}$ is the desired element. By repeating the arguments from the previous two parts, this shows that $a_i \in \mathbb{Z}$ whenever $x \in \mathbb{Z}_K$.

7. Conclude that $\mathbb{Z}_K = \mathbb{Z}[\omega]$.
   Solution: Since $w \in \mathbb{Z}_K$, we certainly have $\mathbb{Z}[w] \subseteq \mathbb{Z}_K$. Now assume that $x = \sum_{i=0}^{q-2} a_i w^i \in \mathbb{Z}_K$. By the previous two parts, $a_i \in \mathbb{Z}$ for all i, so $x \in \mathbb{Z}[w]$. Thus $\mathbb{Z}_K \subseteq \mathbb{Z}[w]$, so equality holds.

3. In this exercise, we show that a naive adaptation of the previous argument can not work when q has more than one prime factor. Let $q \geq 1$ be an integer which is not a prime power (so it has at least two different prime factors), let $\omega = e^{2i\pi/q}$ and $K = \mathbb{Q}(\omega)$.

1. Let X_q be the set of integers a with $1 \leq a \leq q-1$ such that the order of ω^a in $\mathbb{C}^\times$ is not a prime power. Show that

$$\prod_{a \in X_q} (1 - \omega^a) = 1.$$

(Hint: use the formula from Question 1 of Exercise 1 for q and for p^v-th roots of unity, where v is the p-adic valuation of q.) Solution: Let v_p be the p-adic valuation of q. The elements w^a such that the order of w^a in $\mathbb{C}^\times$ is a power of p are precisely the p^{v_p}-th roots of unity. By Exercise 1.1, these satisfy

$$\prod_{b=1}^{p^{v_p}-1} (1 - e^{2\pi i b/p^{v_p}}) = p^{v_p}.$$

Then once more by Exercise 1.1, we have

$$\begin{aligned} q &= \prod_{a=1}^{q} (1 - w^a) \\ &= \prod_{\substack{p \mid q \\ \text{prime}}} \left(\prod_{\substack{a=1 \\ \text{ord}(w^a) \mid p^{v_p}}}^{q} (1 - w^a) \right) \times \prod_{a \in X_q} (1 - w^a) \\ &= \prod_{\substack{p \mid q \\ \text{prime}}} p^{v_p} \times \prod_{a \in X_q} (1 - w^a) \\ &= q \prod_{a \in X_q} (1 - w^a). \end{aligned}$$

By cancelling the qs on both sides of this identity we get the desired result.

2. Deduce that $1 - \omega$ is a unit in $\mathbb{Z}_K$ (in contrast with Question 2 of Exercise 2).
Solution: The element w itself has order q, which by assumption is not a prime power. Thus $(1 - w) | \prod_{a \in X_q} (1 - w^a) = 1$, so $1 - w$ is a unit in $\mathbb{Z}_K$ with inverse $\prod_{\substack{a \in X_q \\ a \neq 1}} (1 - w^a)$.

4. Let K be a number field with $[K : \mathbb{Q}] \geq 2$. Let p be a prime number. The goal of this exercise is to give many examples of rings related to $\mathbb{Z}_K$ but which are not Dedekind domains, and to show this failure explicitly.

Let p be a prime number, and define $A = \mathbb{Z} + p\mathbb{Z}_K \subset \mathbb{Z}_K$. Let

$$\boldsymbol{q} = pA \subset A, \qquad \boldsymbol{p} = p\mathbb{Z}_K.$$

1. Show that there is a $\mathbb{Z}$-basis $(\omega_i)_{1 \leq i \leq [K:\mathbb{Q}]}$ of $\mathbb{Z}_K$ such that $\omega_1 = 1$.
Solution: This can be done in several ways, but consider the $\mathbb{Z}$-module quotient $\mathbb{Z}_K/\mathbb{Z}$. Let $x \in \mathbb{Z}_K \setminus \mathbb{Z}$ have image $\bar{x} \neq 0 \in \mathbb{Z}_K/\mathbb{Z}$.

Assume by contradiction that $\bar{x}$ is a torsion element of minimal order m in $\mathbb{Z}_K/\mathbb{Z}$; that is, with $m\bar{x} = 0 \in \mathbb{Z}_K/\mathbb{Z}$. Then there exists $n \in \mathbb{Z}$ with $mx = n$. Note that m and n are relatively prime, since $\frac{m}{\gcd(m,n)}x \in \mathbb{Z}$ as well.

Thus there exist integers a and b with $am + bn = 1$, which implies that $bmx = bn = (1 - am)$, so that $m(bx + a) = 1$. Thus $bx + a = 1/m \in \mathbb{Z}_K$, so since $m \in \mathbb{Z}$ we must have $m = \pm 1$, and thus $\bar{x} = 0 \in \mathbb{Z}_K/\mathbb{Z}$, a contradiction.

We have shown in particular that $\mathbb{Z}_K/\mathbb{Z}$ has no torsion, so it must be a free $\mathbb{Z}$-module with $\mathbb{Z}$-basis $\{\omega_2, \dots, \omega_n\}$. Then $\{1, \omega_2, \dots, \omega_n\}$ is a $\mathbb{Z}$-basis of $\mathbb{Z}_K$, and $n = [K : \mathbb{Q}]$.

2. Show that A is a subring of $\mathbb{Z}_K$ and that $\boldsymbol{p}$ is an ideal in A and also in $\mathbb{Z}_K$ such that $\boldsymbol{q} \subset \boldsymbol{p} \subset A$. Show also that $\boldsymbol{p} = \boldsymbol{q}\mathbb{Z}_K$ (i.e., the $\mathbb{Z}_K$-ideal generated by $\boldsymbol{q}$ is equal to $\boldsymbol{p}$).

   Solution: The set A is certainly closed under addition and additive inverses; it suffices to show that it is closed under multiplication. Let $(n_1 + px_1), (n_2 + px_2)$ be two elements of A with $n_1, n_2 \in \mathbb{Z}$ and $x_1, x_2 \in \mathbb{Z}_K$. Then $(n_1 + px_1)(n_2 + px_2) = n_1n_2 + p(n_1x_2 + n_2x_1 + px_1x_2)$. Since $n_1n_2 \in \mathbb{Z}$ and $n_1x_2 + n_2x_1 + px_1x_2 \in \mathbb{Z}_K$, the product is also in A.

   It is immediate that $\boldsymbol{q} \subset \boldsymbol{p} \subset A$ and that $\boldsymbol{p}$ is an ideal in $\mathbb{Z}_K$. Since $A \subset \mathbb{Z}_K$, the product of any element of $\boldsymbol{p}$ and any element of A remains in $\boldsymbol{p}$. Thus $\boldsymbol{p} \subset A$ is also an ideal.

   We have that $\boldsymbol{q}\mathbb{Z}_K = pA\mathbb{Z}_K \subset p\mathbb{Z}_K = \boldsymbol{p}$; it remains to show the other inclusion. But $p \in \boldsymbol{q}$ since $1 \in A$, so $\boldsymbol{p} = p\mathbb{Z}_K \subset \boldsymbol{q}\mathbb{Z}_K$, as desired.

3. Prove that

$$|\boldsymbol{q}/\boldsymbol{p}^2| = p, \qquad |\boldsymbol{p}/\boldsymbol{q}| = p^{[K:\mathbb{Q}]-1}, \qquad |A/\boldsymbol{p}| = p, \qquad |\mathbb{Z}_K/A| = p^{n-1}.$$

   (Hint: find $\mathbb{Z}$-bases of these various abelian groups in terms of the basis of question 1.)

   In particular, note that $|A/\boldsymbol{p}^2| \neq |A/\boldsymbol{p}|^2$.

   Solution: Consider the $\mathbb{Z}$-basis $w_1, \dots, w_n$ of $\mathbb{Z}_K$ with $n = [K : \mathbb{Q}]$ and $w_1 = 1$. Then A has $\mathbb{Z}$-basis $\{w_1, pw_2, \dots, pw_n\}$, whereas $\boldsymbol{p}$ has $\mathbb{Z}$-basis $\{pw_1, \dots, pw_n\}$, $\boldsymbol{p}^2$ has $\mathbb{Z}$-basis $\{p^2w_1, \dots, p^2w_n\}$, and $\boldsymbol{q}$ has $\mathbb{Z}$-basis $\{pw_1, p^2w_2, \dots, p^2w_n\}$.

   The quotient $\boldsymbol{q}/\boldsymbol{p}^2$ is thus generated by pw_1, which is an element of order p, so that $|\boldsymbol{q}/\boldsymbol{p}^2| = p$. The quotient $\boldsymbol{p}/\boldsymbol{q}$ is generated by $\{pw_2, \dots, pw_n\}$, where every element has additive order p, and thus $|\boldsymbol{p}/\boldsymbol{q}| = p^{n-1}$. The quotient $A/\boldsymbol{p}$ is generated by $w_1 = 1$, which has order p, so $|A/\boldsymbol{p}| = p$. Finally the quotient $\mathbb{Z}_K/A$ is generated by $\{w_2, \dots, w_n\}$, each of order p, so that $|\mathbb{Z}_K/A| = p^{n-1}$.

   Notably,

$$|A/\boldsymbol{p}^2| = |A/\boldsymbol{p}| \cdot |\boldsymbol{p}/\boldsymbol{q}| \cdot |\boldsymbol{q}/\boldsymbol{p}^2| = p^{n+1},$$

   whereas $|A/\boldsymbol{p}|^2 = p^2$.

4. Show that $\boldsymbol{p}$ is a prime ideal in A. Show that if $\boldsymbol{p}_1, \dots, \boldsymbol{p}_k$ are prime ideals of A such that $\boldsymbol{p} \mid \boldsymbol{p}_1 \cdots \boldsymbol{p}_k$, then $\boldsymbol{p} = \boldsymbol{p}_j$ for some j. (Hint: the last property is a general fact about prime ideals in a commutative ring.)

Solution: Note that $|A/\boldsymbol{p}| = p$, so in fact we must have $|A/\boldsymbol{p}| \cong \mathbb{Z}/p\mathbb{Z}$. This is an integral domain, so $\boldsymbol{p}$ is prime.

Let $\boldsymbol{p}_1, \dots, \boldsymbol{p}_k$ be prime ideals of A and assume that $\boldsymbol{p}|\boldsymbol{p}_1 \cdots \boldsymbol{p}_k$, or equivalently that $\boldsymbol{p}_1 \cdots \boldsymbol{p}_k = \boldsymbol{p}\boldsymbol{r}$ for some ideal $\boldsymbol{r} \subset A$. Then $\boldsymbol{p}_1 \cdots \boldsymbol{p}_k \subset \boldsymbol{p}$. Assume by contradiction that for all j, $\boldsymbol{p} \not\supset \boldsymbol{p}_j$. Then for each j there exists $a_j \in \boldsymbol{p}_j$ with $a_j \notin \boldsymbol{p}$. However, by assumption $a = a_1 \cdots a_k \in \boldsymbol{p}$, which contradicts the primality of $\boldsymbol{p}$.

It remains to show that $\boldsymbol{p}_j$ is maximal, which implies that $\boldsymbol{p}_j = \boldsymbol{p}$. Assume not. If $a \in \boldsymbol{p}_j \cap \mathbb{Z}$, then $aA \subset \boldsymbol{p}_j A \subset A$, and both aA and A have rank n as $\mathbb{Z}$-modules. Thus $A/\boldsymbol{p}_j$ is finite, and since it is a finite integral domain it must be a field, so $\boldsymbol{p}_j$ is maximal, and so $\boldsymbol{p}_j = \boldsymbol{p}$ as desired.

5. Show that

$$\{x \in K \mid x\boldsymbol{p} \subset \boldsymbol{p}\} = \mathbb{Z}_K,$$

and deduce that $\boldsymbol{p} \subset A$ is *not* principal as an ideal of A (although it is principal as an ideal of $\mathbb{Z}_K$).

Solution: Let $x \in K$ with $x\boldsymbol{p} \subset \boldsymbol{p}$. Write $x = \sum_{i=1}^n x_i w_i$ using the basis $(w_i)_i$ from part 1, and note that the elements of $\mathbb{Z}_K$ are precisely those with all $x_i \in \mathbb{Z}$, and the elements of $p\mathbb{Z}_K$ are precisely those with all $x_i \in p\mathbb{Z}$.

If $x \notin \mathbb{Z}_K$, then some $x_i \notin \mathbb{Z}$, so then $px_i \notin \mathbb{Z}$. Thus $px \notin \boldsymbol{p}$, so $x\boldsymbol{p} \not\subset \boldsymbol{p}$. On the other hand $p\mathbb{Z}_K \subset \mathbb{Z}_K$ is an ideal, so for all $x \in \mathbb{Z}_K$, $x\boldsymbol{p} \subset \boldsymbol{p}$.

Assume by contradiction that $\boldsymbol{p} \subset A$ is principal, and let $a \in A$ be such that $\boldsymbol{p} = aA$. Define $\tilde{\boldsymbol{p}} := a^{-1}A$, so that $\boldsymbol{p}\tilde{\boldsymbol{p}} = A$. But then

$$\begin{aligned} x\boldsymbol{p} \subset \boldsymbol{p} &\Leftrightarrow x\boldsymbol{p}\tilde{\boldsymbol{p}} \subset \boldsymbol{p}\tilde{\boldsymbol{p}} \\ &\Leftrightarrow xA \in A \\ &\Leftrightarrow x \in A. \end{aligned}$$

But then we have shown that $\mathbb{Z}_K \subset A$, a contradiction.

6. Show that $\boldsymbol{q}\boldsymbol{p} = \boldsymbol{p}^2$.

Solution: First note that $\boldsymbol{p}^2 = p^2\mathbb{Z}_K$. Since $p \in \boldsymbol{q}$, $\boldsymbol{q}\boldsymbol{p} \supset p^2\mathbb{Z}_K = \boldsymbol{p}^2$. Since $\boldsymbol{q} \subset \boldsymbol{p}$, we have $\boldsymbol{q}\boldsymbol{p} \subset \boldsymbol{p}^2$, so equality holds.

7. Show that $\boldsymbol{q}$ is an ideal of A which is *not* the product of prime ideals of A. (Hint: assuming that $\boldsymbol{q}$ is a product of primes, show that we would have necessarily $\boldsymbol{q} = \boldsymbol{p}^k$ for some integer $k \geq 1$; show using the previous results that this is not the case.)

Solution: Assume by contradiction that $\boldsymbol{q} = \boldsymbol{p}_1 \cdots \boldsymbol{p}_k$ for prime ideals $\boldsymbol{p}_1, \dots, \boldsymbol{p}_k$. Then $\boldsymbol{p}^2 = \boldsymbol{q}\boldsymbol{p} = \boldsymbol{p}_1 \cdots \boldsymbol{p}_k\boldsymbol{p}$. Thus for each j, $\boldsymbol{p}_j|\boldsymbol{p}^2$ by part (4), so for each j, $\boldsymbol{p}_j = \boldsymbol{p}$. Thus $\boldsymbol{q} = \boldsymbol{p}^k$ for some $k \geq 1$. Since $|\boldsymbol{q}/\boldsymbol{p}| \neq 1$, we cannot have $k = 1$. But if $k \geq 2$ then we must have $|\boldsymbol{q}/\boldsymbol{p}^2| = 1$, which is also false. Thus we have reached a contradiction, so $\boldsymbol{q}$ is not the product of prime ideals of A.

Due date: 28.10.2024