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
$$\prod_{a=1}^{q-1} (1 - \omega^a) = q.$$
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 $\boldsymbol{p}$.
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.)
4. Deduce that ω^a is a root of f for any a coprime to q, and conclude that $f = \Phi_q$.

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
$$\mathrm{Tr}(1) = q - 1, \qquad \mathrm{Tr}(\omega^a) = -1 \text{ for } 1 \leq a \leq q - 1.$$
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.)
3. Prove that $(1 - \omega)\mathbb{Z}_K \mid q\mathbb{Z}_K$ and that $(1 - \omega)\mathbb{Z}_K \cap \mathbb{Z} = q\mathbb{Z}$.

4. Deduce that for all $y \in \mathbb{Z}_K$, we have $\mathrm{Tr}((1-\omega)y) \in q\mathbb{Z}$.
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 $a_0 \in \mathbb{Z}$.
6. Similarly, find the element b_i such that, for any x as above, we have $\mathrm{Tr}(b_i x) = a_i$, and deduce that $a_i \in \mathbb{Z}$ for all i. (Hint: consider $\omega^j x$ for suitable j.)
7. Conclude that $\mathbb{Z}_K = \mathbb{Z}[\omega]$.

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.)
2. Deduce that $1 - \omega$ is a unit in $\mathbb{Z}_K$ (in contrast with Question 2 of Exercise 2).

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 $\omega_1 = 1$.
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 $\boldsymbol{p}$).
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 $|A/\boldsymbol{p}^2| \neq |A/\boldsymbol{p}|^2$.

4. Show that $\boldsymbol{p}$ is a prime ideal in A. Show that if $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_k$ 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.)
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 $\mathbb{Z}_K$).
6. Show that $\boldsymbol{q}\boldsymbol{p} = \boldsymbol{p}^2$.
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.)

Due date: 28.10.2024