Autumn Semester 2019

Introduction to Algebraic Number Theory

Lecturer: Prof. Dr. Özlem Imamoglu
Coordinator: Dr. Danylo Radchenko

Solutions to Exercise Sheet 12

Exercise 12.1. Show that the ring of integers of $K = \mathbb{Q}(\zeta_{23})$ is not a PID.

(a) Show that K contains a subfield F isomorphic to $\mathbb{Q}(\sqrt{-23})$;

(b) Show that 47 splits completely in $\mathcal{O}_K$;

(c) Assume that some prime ideal above 47 is of the form (x) for $x \in \mathcal{O}_K$. Show that $y = N_{K/F}(x) \in \mathcal{O}_F$ has norm 47, and obtain a contradiction.

(*Hint: in part (a) use Gauss sums.*)

Solution. (a) From Exercise 2.4 (b) we know that the Gauss sum $\tau(1) \in \mathbb{Z}[\zeta_{23}]$ satisfies $\tau(1)^2 = -23$. Therefore, $\mathbb{Q}(\tau(1))$ is the subfield $\mathbb{Q}(\sqrt{-23}) \subset \mathbb{Q}(\zeta_{23})$.

(b) We need to factorize $\Phi_{23}(x) = x^{22} + \cdots + x + 1 = \frac{x^{23}-1}{x-1}$ in $(\mathbb{Z}/47\mathbb{Z})[x]$. Since $47 \equiv 1 \pmod{23}$, and since the multiplicative group of the finite field $\mathbb{Z}/47\mathbb{Z}$ is cyclic, there exists $\lambda \in \mathbb{Z}/47\mathbb{Z}$ such that $\lambda^{23} \equiv 1 \pmod{47}$ but $\lambda \not\equiv 1 \pmod{47}$. But then

$$\Phi_{23}(x) \equiv (x-\lambda)\dots(x-\lambda^{22}) \pmod{47}\,.$$

This shows that 47 splits completely in $\mathbb{Z}[\zeta_{23}]$.

(c) Since $N_{F/\mathbb{Q}} \circ N_{K/F} = N_{K/\mathbb{Q}}$, we have $N_{F/\mathbb{Q}}(y) = N_{K/\mathbb{Q}}(x) = 47$ by part (b). Let $y = a + b\frac{1+\sqrt{-23}}{2}$, where $a, b \in \mathbb{Z}$. Then $N_{F/\mathbb{Q}}(y) = a^2 + ab + 6b^2$. From $\frac{23}{4}b^2 \le a^2 + ab + 6b^2 = 47$ we see that $|b| \le 2$.

Without loss of generality we may assume that $b \in \{0, 1, 2\}$. If $b = 2$, then $a^2 + 2a = 23$, so that $(a+1)^2 = 24$, if $b = 1$ then $(2a+1)^2 = 165$, and if $b = 0$, then $a^2 = 47$. Since none of 24, 47 or 165 is a square, there are no integral solutions to $a^2 + ab + 6b^2 = 47$. This contradiction shows that no prime ideal above 47 is principal, and hence $\mathbb{Z}[\zeta_{23}]$ is not a PID.

Exercise 12.2. Let p be an odd prime and let $K = \mathbb{Q}(\zeta_p) \subset \mathbb{C}$, where $\zeta_p = e^{2\pi i/p}$ is a primitive p-th root of unity. Show that any unit $u \in \mathcal{O}_K^\times$ can be written as $u = r\zeta_p^n$ for some $r \in \mathbb{R} \cap \mathcal{O}_K^\times$ and $n \in \{0, \dots, p-1\}$.

Solution. Denote by $\overline{}$ the complex conjugation. Note that for any automorphism $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ we have $\overline{u^\sigma} = \overline{u}^\sigma$. Therefore, the algebraic number $x = u/\overline{u}$ satisfies $|x^\sigma| = 1$ for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Since u and $\overline{u}$ are units, x is an algebraic integer, and by Kronecker's lemma, since all conjugates of x are on the unit circle, x has to be a root of unity. By Exercise 10.2(a) we know that the only roots of unity in K are $\pm\zeta_p^k$, $k = 0, \dots, p-1$.

Therefore, $u = \pm\zeta_p^k \overline{u}$. If we write $u = \sum_{j=0}^{p-1} a_i \zeta_p^j$, where $a_i \in \mathbb{Z}$, then $\overline{u} = \sum_{j=0}^{p-1} a_i \zeta_p^{-j}$. Since $(1-\zeta_p)$ divides $\zeta_p^a - \zeta_p^b$ for all a, b (see Exercise 10.2(b)), we have that $u - \overline{u}$ is divisible by $(1-\zeta_p)$. On the other hand,

$$u - \overline{u} = \overline{u}(1 \mp \zeta_p^k) \equiv \overline{u}(1 \mp 1) \pmod{1-\zeta_p},$$

and since the norm of $1-\zeta_p$ is $p > 2$, we see that the sign in $u = \pm\zeta_p^k \overline{u}$ has to be "+".

If k is odd, then we can write $\zeta_p^k = \zeta_p^{k+p}$. Thus, in all cases we can write $\zeta_p^k = \zeta_p^{2n}$ for some $n \in \mathbb{Z}$. But then $\overline{u/\zeta_p^n} = u/\zeta_p^n$, so that $u = r\zeta_p^n$, where $r \in \mathbb{R}$. Since u and ζ_p^n are units, so is r, so that $r \in \mathcal{O}_K^\times \cap \mathbb{R}$.

Exercise 12.3. We call a prime p regular if p does not divide the class number of $\mathbb{Q}(\zeta_p)$. Show that if $p \geq 5$ is regular and $x^p + y^p + z^p = 0$ for some $x, y, z \in \mathbb{Z}$, then $p|xyz$ as follows:

Assume that x, y, and z are relatively prime and $p \nmid xyz$.

(a) Show that the ideals $(x + \zeta_p^j y)$ are relatively prime for $j = 0, \ldots, p-1$;

(b) Show that $x + \zeta_p y = r\zeta_p^n \alpha^p$ for some $\alpha \in \mathbb{Z}[\zeta_p]$, $r \in \mathbb{Z}[\zeta_p]^\times \cap \mathbb{R}$ and $n \in \{0, \ldots, p-1\}$;

(c) Show that $\alpha^p \equiv a \pmod{p}$ for some integer a;

(d) Using parts (b) and (c) show that

$$\gamma = \zeta_p^n x + \zeta_p^{n-1} y - \zeta_p^{-n} x - \zeta_p^{-n+1} y \equiv 0 \pmod{p}$$

(e) Obtain contradiction using part (d).

Solution.

We write ζ instead of ζ_p.

(a) Assume that some prime ideal $\mathfrak{p}$ divides both $(x + \zeta^i y)$ and $(x + \zeta^j y)$ for some $0 \leq i < j \leq p-1$. Then $\mathfrak{p}$ must contain

$$\zeta^{-j}((x + \zeta^j y) - (x + \zeta^i y)) = (1 - \zeta^{i-j})y$$

and

$$(x + \zeta^i y) - \zeta^{i-j}(x + \zeta^j y) = (1 - \zeta^{i-j})x\,.$$

Since x and y are coprime integers, there exist $a, b \in \mathbb{Z}$ such that $ax + by = 1$. Therefore, $\mathfrak{p}$ contains $1 - \zeta^{i-j}$. Since $(1 - \zeta^{i-j})$ is a prime ideal (it has norm p), we must have $\mathfrak{p} = (1 - \zeta^{i-j}) = (1 - \zeta)$ (recall Exercise 10.2(b)). From this we conclude that $(1-\zeta)$ divides z^p. But the norm of $(1-\zeta)$ is p, thus taking the norms we get $p|z^{p^2}$, so that $p|z$, a contradiction.

(b) Using the factorization of $x^p + y^p$ in $\mathbb{Q}(\zeta)$ we obtain a factorization of ideals

$$(z)^p = \prod_{j=0}^{p-1} (x + \zeta^j y)\,.$$

By part (a) ideals $(x + \zeta^j y)$ are pairwise coprime, and hence from unique factorization into prime ideals we see that $(x + \zeta y) = \mathfrak{a}^p$ for some ideal $\mathfrak{a}$. If $\mathfrak{a}$ where not principal, then, since $\mathfrak{a}^p$ is principal, its order in the ideal class group would divide p. However, by our assumption p does not divide the order of the class group, thus $\mathfrak{a}$ is principal.

Thus $x + \zeta y = u\alpha^p$ for some $\alpha \in \mathbb{Z}[\zeta]$ and a unit u. Combined with Exercise 12.2 this gives us $x + \zeta y = r\zeta^n \alpha^p$ as needed.

(c) Since $(\sum_i x_i)^p \equiv \sum_i x_i^p \pmod{p}$ we have $\alpha^p = (\sum_i a_i \zeta^i)^p \equiv \sum_i a_i^p \pmod{p}$. Thus we can take $a = \sum_i a_i^p \in \mathbb{Z}$.

(d) From (b) and (c) we have

$$\zeta^{-n}(x + \zeta y) \equiv ra \pmod{p}\,.$$

Since r and a are real, by taking conjugates we also have

$$\zeta^{n}(x + \zeta^{-1} y) \equiv ra \pmod{p}\,.$$

Taking the difference of these two congruences we get

$$\gamma = \zeta^n x + \zeta^{n-1} y - \zeta^{-n} x - \zeta^{-n+1} y \equiv 0 \pmod{p}\,.$$

(e) Assume that $p \nmid xyz$. By part (d) we have $\gamma = \beta p$ for some $\beta \in \mathbb{Z}[\zeta]$. Note that if $I \subset \{0, \ldots, p-1\}$ is any subset of size $p-1$, then ζ^i, $i \in I$ form a $\mathbb{Z}$-basis for $\mathbb{Z}[\zeta]$. Since $p \geq 5$ we can pick such a set I that contains the residues $J = \{\overline{n}, \overline{n-1}, \overline{-n}, \overline{-n+1}\}$ modulo p. From this we conclude that if we write γ with respect to exponents in J, all coefficients should be divisible by p.

Note that $n, n-1, -n, -n+1$ are all distinct modulo p unless $n \equiv 0$, 1, or $\frac{p+1}{2} \bmod p$. In this case we must have $p|x, y$, contradicting our assumption $p \nmid xyz$.

Assume that $n \equiv 0 \pmod{p}$. Then $\gamma = y\zeta^{p-1} - y\zeta$ and hence $p|y$, a contradiction.

Similarly, if $n \equiv 1 \pmod{p}$, then $\gamma = x\zeta - x\zeta^{p-1}$ and hence $p|x$, a contradiction.

Finally, if $2n \equiv 1 \pmod{p}$, then $\gamma = \zeta^n(x - y) + \zeta^{n-1}(y - x)$, from which we see that $x \equiv y \pmod{p}$. Since the original equation $x^p + y^p + z^p$ is symmetric in x, y, z, repeating this argument we get $y \equiv z \pmod{p}$, and thus $3x^p \equiv 0 \pmod{p}$. But since $p \geq 5$, this can only happen if $p|x$, again contradicting our assumption.

Thus in each case we obtained a contradiction, and hence we must have $p|xyz$.