Autumn Semester 2019

Introduction to Algebraic Number Theory

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

Solutions to Ferienserie

Exercise 1. Let K be a quadratic extension of $\mathbb{Q}$ and let D be its discriminant. Show that $\mathcal{O}_K = \mathbb{Z}[\alpha_D]$, where $\alpha_D = \frac{D+\sqrt{D}}{2}$.

Solution. Since $\operatorname{Tr}(\alpha_D) = D$ and $N(\alpha_D) = \frac{D+\sqrt{D}}{2} \cdot \frac{D-\sqrt{D}}{2} = \frac{D(D-1)}{4}$, we see that

$$\alpha_D^2 - D\alpha_D + \frac{D(D-1)}{4} = 0\,.$$

Since D is the discriminant of a number field, we have $D \equiv 0, 1 \pmod 4$, so that α_D is an algebraic integer. Finally, the discriminant of $\{1, \alpha_D\}$ is equal to $D^2 - 4\frac{D(D-1)}{4} = D$. Since D is the discriminant of K, we conclude that $\mathcal{O}_K = \mathbb{Z}[\alpha_D]$.

Exercise 2. Show that $\mathbb{Z}[\sqrt{2}]$ is a principal ideal domain, and using this show that

$$\pm p = x^2 - 2y^2 \quad \Leftrightarrow \quad p \equiv 1, 7 \pmod 8$$

(here p is a prime and $\pm p = x^2 - 2y^2$ means that either p or $-p$ can be written as $x^2 - 2y^2$).

Solution. The Minkowski bound for $K = \mathbb{Q}(\sqrt{2})$ is $\sqrt{2} < 2$, so $\mathbb{Z}[\sqrt{2}] = \mathcal{O}_K$ is a PID.

First, if $\pm p = x^2 - 2y^2$, then reducing this identity modulo p we get that 2 is a quadratic residue modulo p (note that $x, y \not\equiv 0 \pmod p$), and by the supplementary quadratic reciprocity law we have $p \equiv 1, 7 \pmod 8$.

In the other direction, let $p \equiv 1, 7 \pmod 8$. Then 2 is a quadratic residue modulo p, so $x^2 - 2$ factors as $(x-a)(x+a)$ in $\mathbb{Z}/p\mathbb{Z}$. By Kummer's factorization theorem $(p) = \mathfrak{p}_1\mathfrak{p}_2$ and moreover $N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = p$ since the extension is quadratic. Since $\mathbb{Z}[\sqrt{2}]$ is a PID, we have $\mathfrak{p}_1 = (x + y\sqrt{2})$ and thus $N(x + y\sqrt{2}) = \pm p$, so that $\pm p = x^2 - 2y^2$, as claimed.

Exercise 3. Show that the class group of $K = \mathbb{Q}(\sqrt{-23})$ is isomorphic to $\mathbb{Z}/3\mathbb{Z}$ and find the representative ideals.

Solution. First, we compute the Minkowski bound $M_K = \frac{2\sqrt{23}}{\pi} < 4$. Therefore, each ideal class is represented by an integral ideal of norm ≤ 3.

Next, we compute the factorization of the ideals (2) and (3). Since $\mathcal{O}_K = \mathbb{Z}[\omega]$, where $\omega = \frac{1+\sqrt{-23}}{2}$ satisfies $\omega^2 - \omega + 6 = 0$. Both in $(\mathbb{Z}/2\mathbb{Z})[x]$ and in $(\mathbb{Z}/3\mathbb{Z})[x]$ we have $x^2 - x + 6 = x(x-1)$, so $(2) = \mathfrak{p}_1\mathfrak{p}_2$ and $(3) = \mathfrak{q}_1\mathfrak{q}_2$, where $\mathfrak{p}_1 \neq \mathfrak{p}_2$ and $\mathfrak{q}_1 \neq \mathfrak{q}_2$. Here $\mathfrak{p}_1 = (2, \omega)$, $\mathfrak{p}_2 = (2, \omega')$, $\mathfrak{q}_1 = (3, \omega)$, $\mathfrak{q}_2 = (3, \omega')$. Therefore, each ideal is equivalent to one of $\mathcal{O}, \mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{q}_1, \mathfrak{q}_2$.

It remains to figure out the equivalences between the above five ideals. First, $\mathfrak{p}_2 \sim \mathfrak{p}_1^{-1}$ and $\mathfrak{q}_2 \sim \mathfrak{q}_1^{-1}$. Next, we compute $\mathfrak{p}_1\mathfrak{q}_1 = (6, 2\omega, 3\omega, \omega - 6) = (6, \omega) = (\omega)$ since ω divides its norm 6. Similarly, $\mathfrak{p}_2\mathfrak{q}_2 = (\omega')$. Thus $\mathfrak{q}_1 \sim \mathfrak{p}_2$ and $\mathfrak{q}_2 \sim \mathfrak{p}_1$. Therefore, to finish the proof it is enough to check that $\mathfrak{p}_1 \not\sim \mathfrak{p}_2$ (this automatically implies $\mathfrak{p}_i \not\sim \mathcal{O}$ because of $\mathfrak{p}_2 \sim \mathfrak{p}_1^{-1}$).

If we had $\mathfrak{p}_1 \sim \mathfrak{p}_2$, then $\mathfrak{p}_1^2$ would be principal. However, if $(a+b\omega)$ is a principal ideal of norm 4, then $a^2+ab+6b^2=4$, and this easily implies $(a,b)=(\pm 2,0)$. Therefore, if $\mathfrak{p}_1^2$ where principal, we would have $\mathfrak{p}_1^2=(2)$, which contradicts the fact that $\mathfrak{p}_1 \neq \mathfrak{p}_2$.

Therefore, there are three classes of ideals in $\mathcal{O}_K$: $\mathcal{O}$, $\mathfrak{p}_1$, and $\mathfrak{p}_2$, and since there is only one group of order 3, the class group is isomorphic to $\mathbb{Z}/3\mathbb{Z}$.

Exercise 4. Let $K=\mathbb{Q}(\sqrt[3]{7})$.

(a) Show that $\mathcal{O}_K=\mathbb{Z}[\sqrt[3]{7}]$;

(b) Show that the class number of K is equal to 3.

Solution. The discriminant of x^3-7 is $-3^3\cdot 7^2$. Therefore, the index $[\mathcal{O}_K\colon \mathbb{Z}[\sqrt[3]{7}]]$ divides 21.

If $7|[\mathcal{O}_K\colon \mathbb{Z}[\sqrt[3]{7}]]$, then there is an element $\alpha=\frac{a+b\sqrt[3]{7}+c\sqrt[3]{7}^2}{7}\in \mathcal{O}_K\smallsetminus \mathbb{Z}[\sqrt[3]{7}]$. Since $\mathrm{Tr}(\alpha)=\frac{3a}{7}\in\mathbb{Z}$, we have $7|a$, and thus without loss of generality we may assume that $a=0$. Then we compute the norm $N(\alpha\sqrt[3]{7})=\frac{b^3}{7}+c^3$. Since this also has to be an integer, we must have $7|b$, so again we may assume $b=0$. But then $N(\alpha)=c^3/7$, so that $7|c$, and we conclude that $\alpha\in\mathbb{Z}[\sqrt[3]{7}]$, a contradiction.

Next, assume that $3|[\mathcal{O}_K\colon \mathbb{Z}[\sqrt[3]{7}]]$. Then there exists $\alpha=\frac{a+b\sqrt[3]{7}+c\sqrt[3]{7}^2}{3}\in \mathcal{O}_K\smallsetminus \mathbb{Z}[\sqrt[3]{7}]$. We have

$$N(\alpha) \;=\; \frac{a^3+7b^3+49c^3-21abc}{27}\,.$$

From this we see that $3|a^3+b^3+c^3$, or equivalently, since $t^3\equiv t \pmod 3$, we see that $3|a+b+c$. Thus we may assume $c=-a-b$. Then

$$N(\alpha) \;=\; -\frac{2a^3+14(a+b)^3}{9}\,.$$

Since $t^3\equiv 0,\pm 1 \pmod 9$, and $2\not\equiv 0,\pm 14 \pmod 9$, we must have $a^3\equiv (a+b)^3\equiv 0 \pmod 9$. But then $3|a,b,c$, and we get a contradiction to $\alpha\notin\mathbb{Z}[\sqrt[3]{7}]$. Therefore, $\mathcal{O}_K=\mathbb{Z}[\sqrt[3]{7}]$.

Denote $\theta=\sqrt[3]{7}$.

Next, we compute the Minkowski bound: $M_K=\frac{56}{3\sqrt{3}\pi}<11$. Therefore, each ideal is equivalent to an integral ideal of norm ≤ 10. Since $(7)=(\theta)^3$, the generators of the ideal class group are among the prime ideals dividing (2), (3), and (5).

We have the following factorizations of x^3-7: $x^3-7=(x+1)(x^2+x+1)$ modulo 2, $x^3-7=(x+2)^3$ modulo 3, and $x^3-7=(x+2)(x^2+3x-1)$ modulo 5. Therefore, the class group is generated by $\mathfrak{p},\mathfrak{q},\mathfrak{r}$, where $\mathfrak{p}=(2,\theta-1)$, $\mathfrak{q}=(3,\theta+2)=(3,\theta-1)$, and $\mathfrak{r}=(5,\theta+2)$, of norms 2, 3, and 5 respectively, and moreover $\mathfrak{q}^3=(3)$ is principal.

We calculate

$$\mathfrak{pq}=(2,\theta-1)(3,\theta-1)=(6,2(\theta-1),3(\theta-1),(\theta-1)^2)=(6,\theta-1)=(\theta-1)\,,$$

where $(\theta-1)|6$ since $N(\theta-1)=6$. Similarly,

$$\mathfrak{qr}=(3,\theta+2)(5,\theta+2)=(15,5(\theta+2),3(\theta+2),(\theta+2)^2)=(15,\theta+2)=(\theta+2)\,,$$

where $(\theta+2)|15$ since $N(\theta+2)=15$.

Therefore, the ideal class group is generated by $\mathfrak{q}$, which is of order dividing 3. To see that $\mathfrak{q}$ is not principal, note that its norm is 3, and if $\mathfrak{q} = (a + b\theta + c\theta^2)$, then we would have

$$a^3 + 7b^3 + 49c^3 - 21abc \;=\; 3$$

which implies $a^3 \equiv 3 \pmod 7$, but 3 is not a cube modulo 7. Therefore, $\mathfrak{q}$ is not principal, and thus the class number is equal to 3.

Exercise 5. Let $K = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3})$. Show that $\alpha = (1 + \sqrt[3]{2})/\sqrt[3]{3}$ is a unit in $\mathcal{O}_K$.

Solution. First, we calculate

$$\alpha^3 \;=\; \frac{(1+\sqrt[3]{2})^3}{3} \;=\; \frac{3 + 3\sqrt[3]{2} + 3\sqrt[3]{2}^2}{3} \;=\; 1 + \sqrt[3]{2} + \sqrt[3]{2}^2 = \beta\,.$$

We have $(\beta - 1)^3 = 2(1 + \sqrt[3]{2})^3 = 6\beta$, therefore $\beta^3 - 3\beta^2 - 3\beta - 1 = 0$. From this we conclude that

$$\alpha^9 - 3\alpha^6 - 3\alpha^3 - 1 \;=\; 0\,.$$

But this implies that $\alpha \in \mathcal{O}_K$ and that $N_{K/\mathbb{Q}}(\alpha) = 1$, hence α is a unit.

Exercise 6. Let $p \equiv 1 \pmod 4$ be a prime number, and consider the element $\varepsilon \in \mathbb{Q}(\zeta_p)$ defined by

$$\varepsilon \;=\; \prod_{a=1}^{p-1} (1 - \zeta_p^a)^{\left(\frac{a}{p}\right)},$$

where $\left(\frac{\cdot}{p}\right)$ denotes the Legendre symbol.

(a) Show that ε is a unit;

(b) Show that ε belongs to the quadratic subfield $\mathbb{Q}(\sqrt{p})$ in $\mathbb{Q}(\zeta_p)$;

(c) Compute ε for $p = 5$.

Solution. Let us denote $\zeta = \zeta_p$.

(a) As we have already seen in Exercise 10.2(b), for any $1 \le a \le p-1$, the number $\varepsilon_a = \frac{1-\zeta^a}{1-\zeta}$ is a unit. Therefore,

$$\varepsilon \;=\; (1-\zeta)^{\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)} \prod_{a=1}^{p-1} \varepsilon_a^{\left(\frac{a}{p}\right)} \;=\; \prod_{a=1}^{p-1} \varepsilon_a^{\left(\frac{a}{p}\right)}\,,$$

since $\sum_{a=1}^{p-1}\left(\frac{a}{p}\right) = 0$ (as there are equal numbers of residues and non-residues modulo p). Therefore, ε is a unit.

(b) Let $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ be given by $\zeta \mapsto \zeta^b$. Then we compute

$$\varepsilon^\sigma \;=\; \prod_{a=1}^{p-1} (1 - \zeta_p^{ab})^{\left(\frac{a}{p}\right)} \;=\; \left(\prod_{a=1}^{p-1} (1 - \zeta_p^{ab})^{\left(\frac{ab}{p}\right)}\right)^{\left(\frac{b}{p}\right)} \;=\; \varepsilon^{\left(\frac{b}{p}\right)}\,.$$

Therefore, $\varepsilon + \varepsilon^{-1}$ is fixed by the Galois group of K, hence $\varepsilon + \varepsilon^{-1} \in \mathbb{Q}$ (and in fact in $\mathbb{Z}$). This means that ε lies in a quadratic subfield of K. However, since the Galois group is cyclic, there is only one quadratic subfield, and by Exercise 2.4 the Gauss sum $\tau(1) = \pm\sqrt{p}$ lies in $\mathbb{Q}(\zeta)$, so we must have $\varepsilon \in \mathbb{Q}(\sqrt{p})$.

(c) We compute

$$\varepsilon \;=\; \frac{(1-\zeta)(1-\zeta^4)}{(1-\zeta^2)(1-\zeta^3)} \;=\; \frac{(2-\zeta-\zeta^{-1})^2}{5} \;=\; \zeta^3+\zeta^2+2\,.$$

Then $\varepsilon^{-1} = \zeta + \zeta^4 + 2$, and we find $\varepsilon + \varepsilon^{-1} = 3$, or $\varepsilon^2 - 3\varepsilon + 1 \;=\; 0$. From this we find

$$\varepsilon \;=\; \frac{3 \pm \sqrt{5}}{2}\,.$$

Note that this is in fact a fundamental unit in $\mathbb{Q}(\sqrt{5})$.

Exercise 7. Let $K/\mathbb{Q}$ be a Galois extension such that a prime number p is inert in K (i.e. (p) is a prime ideal). Show that $\mathrm{Gal}(K/\mathbb{Q})$ is a cyclic group.

(*Hint: recall the decomposition and the inertia subgroups, and the fact that the Galois groups of any finite extensions of a finite field is cyclic.*)

Solution. Let us write p for the prime ideal in $\mathbb{Z}$, and $\mathfrak{p}$ for the prime ideal $p\mathcal{O}_L$ in $\mathcal{O}_L$, and let $k_p := \mathbb{Z}/p\mathbb{Z}$ and $k_{\mathfrak{p}} := \mathcal{O}_L/p\mathcal{O}_L$ denote the corresponding residue fields. Finally, let

$$D(\mathfrak{p}/p) = \{\sigma \in \mathrm{Gal}(K/\mathbb{Q})\colon \sigma(\mathfrak{p}) = \mathfrak{p}\}$$

and

$$I(\mathfrak{p}/p) = \{\sigma \in D(\mathfrak{p}/p)\colon \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{p}}\,,\ \text{for all } \alpha \in \mathcal{O}_L\}$$

be the decomposition and inertia subgroups. From Galois theory we know that $D(\mathfrak{p}/p)/I(\mathfrak{p}/p)$ is canonically isomorphic to $\mathrm{Gal}(k_{\mathfrak{p}}/k_p)$.

By our assumption $D(\mathfrak{p}/p)$ is the whole Galois group, and since p is unramified, the inertia group is trivial (since $e = 1$ and $f = n$ where n is the degree of the extension). Therefore, $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to $\mathrm{Gal}(k_{\mathfrak{p}}/k_p)$. Since the latter is a Galois group of a finite extension of a finite field, it is cyclic (generated by the Frobenius automorphism), and hence $\mathrm{Gal}(K/\mathbb{Q})$ is also cyclic.

Exercise 8. Prove that for any $n > 1$ there are infinitely many prime numbers congruent to 1 modulo n.

(*Hint: Assuming that there are only finitely many, let P denote their product. Obtain contradiction by considering a prime p dividing $\Phi_n(knP)$ for some $k \in \mathbb{Z}$, where Φ_n is the n-th cyclotomic polynomial.*)

Solution. As in the hint, let $\Phi_n(x)$ be the n-th cyclotomic polynomial, i.e., $\Phi_n(x) = \prod_{\zeta}(x-\zeta)$, where the product runs over all primitive n-th roots of unity. For $n > 2$ we have $\Phi_n(0) = 1$, and therefore for any $k \in \mathbb{Z}$ we have $\Phi_n(knP) \equiv 1 \pmod{nP}$. This is so because more generally $(a-b)|(Q(a) - Q(b))$ for any $Q \in \mathbb{Z}[x]$.

Since a non-constant polynomial has only finitely many roots, there exists $k \in \mathbb{Z}$ such that $\Phi_n(knP) \neq 1$. Let p be any prime that divides $\Phi_n(knP)$. By above, we have $p \nmid nP$.

The number $t = knP$ is an n-th root of unity in $\mathbb{Z}/p\mathbb{Z}$, since $\Phi_n(t) \equiv 0 \pmod{p}$ and $\Phi_n(x)|x^n - 1$. Assume that t is a primitive l-th root of unity in $\mathbb{Z}/p\mathbb{Z}$, where $n = lm$ and $m > 1$. Then $\Phi_n(t)|\frac{t^n-1}{t^l-1} = 1 + t^l + \cdots + t^{(m-1)l} \equiv m \pmod{p}$. However, by assumption $p|\Phi_n(t)$, a contradiction since $m \not\equiv 0 \pmod{p}$. Therefore, t is a primitive n-th root of unity in $\mathbb{Z}/p\mathbb{Z}$, and by Lagrange's theorem $n|(p-1)$ since $p-1$ is the order of $(\mathbb{Z}/p\mathbb{Z})^\times$. Since $p \nmid P$ this contradicts the assumption that P is the product of all primes congruent to 1 modulo n.

Alternatively, we can derive a contradiction as follows. Since $p| \prod_\zeta (t-\zeta)$, one of the ideals $(t-\zeta)$ is divisible by some prime $\mathfrak{p}$ above p. By Galois symmetry we get that *each* $(t-\zeta)$ is divisible by some prime $\mathfrak{p}$ above p. However, the ideals $(t-\zeta_1)$ and $(t-\zeta_2)$ are coprime, since they both have norm $\Phi_n(t) \equiv 1 \pmod{n}$ and their sum contains $\zeta_1 - \zeta_2$ which has norm dividing some power of n. This implies that p is divisible by $\varphi(n)$ distinct prime ideals (one for each factor $t-\zeta$). Since the cyclotomic field $\mathbb{Q}(\zeta_n)$ has degree $\varphi(n)$, this implies that p splits completely in $\mathbb{Q}(\zeta_n)$, and we know from lectures that p splits completely if and only if $p \equiv 1 \pmod{n}$.