Math 80220 Algebraic Number Theory
Problem Set 4

Andrei Jorza

due Wednesday, March 19

Do 3 of 5 problems.

1. Let K be a number field.

   (a) Show that if I is an ideal there exists a number field L/K such that $I\mathcal{O}_L$ is principal. [Hint: some power of I must be principal.]

   (b) Show that there exists a number field L/K such that every ideal of $\mathcal{O}_K$ becomes principal in $\mathcal{O}_L$.

2. Let $f(X) = X^3 - 3X + 1$.

   (a) Show that $f(X)$ is irreducible over $\mathbb{Q}$ and has 3 real roots. Let $K = \mathbb{Q}(\alpha)$ where α is a root. Show that

   $$3^n\mathcal{O}_K \subset \mathbb{Z}[\alpha] \subset \mathcal{O}_K$$

   for some n. [Hint: show that the discriminant of $1, \alpha, \alpha^2$ is the same as the discriminant of f.]

   (b) Show that $\alpha, \alpha + 2$ are units and that $(\alpha + 1)^3 = 3\alpha(\alpha + 2)$. What is the factorization of $(3)\mathcal{O}_K$ in $\mathcal{O}_K$?

   (c) Show that $\mathcal{O}_K = \mathbb{Z}[\alpha] + (3)\mathcal{O}_K$. [Hint: what is $\mathcal{O}_K/(3)$?]

   (d) Deduce that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. [Hint: if e_1, e_2, e_3 is an integral basis for $\mathcal{O}_K$ what can you say about the highest power of 3 in the denominators of e_i?]

   (e) Show that K has class number 1.

   (f) What is the subgroup $\mu_K \subset \mathcal{O}_K^\times$ of roots of unity? [Hint: What is the degree of ζ_n over $\mathbb{Q}$?]

   (g) Show that α and $\alpha + 2$ are independent in $\mathcal{O}_K^\times$. Are they a basis for the free part of $\mathcal{O}_K^\times$? [Hint: For the first part, show that the three roots lie in $(-2, -1)$, $(0, 1)$ and $(1, 2)$ and if α and $\alpha + 2$ have a dependence then the same is true for the other two roots. For the second part compute $1/(\alpha + 2)$.]

3. Let $K = \mathbb{Q}(\sqrt[3]{7})$ with $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{7}]$.

   (a) Determine which integral primes p ramify in K and how.

   (b) Find examples of unramified primes p with decomposition $(p)\mathcal{O}_K = \mathfrak{q}_1 \dots \mathfrak{q}_r$ in the following cases:

      i. $r = 3$, $f_{\mathfrak{q}_i/p} = 1$;

      ii. $r = 2$, $f_{\mathfrak{q}_1/p} = 1$ and $f_{\mathfrak{q}_2/p} = 2$;

      iii. $r = 1$, $f_{\mathfrak{q}_1/p} = 3$.

   (c) Show that $\mathrm{Cl}(K) \cong \mathbb{Z}/3\mathbb{Z}$ generated by $(2, \sqrt[3]{7} + 1)$. [Feel free to use a computer for multiplying fractional ideals.]

   (d) Show that $2 - \sqrt[3]{7}$ is a unit.

(e) Show that in fact $2 - \sqrt[3]{7}$ generates the free part of $\mathcal{O}_K^\times$:

i. Suppose $u > 1$ is a generator for the rank 1 abelian group $\mathcal{O}_K^\times$. Let $\sigma(u) = re^{i\theta}$ and $\overline{\sigma}(u)$ be the two complex conjugates of u. Show that $u = r^{-2}$.

ii. Show that

$$\operatorname{disc}(1, u, u^2) = -4\sin^2(\theta)(r^3 + r^{-3} - 2\cos(\theta))^2$$

and deduce that

$$|\operatorname{disc}(u)| < 4(u^3 + u^{-3} + 6)$$

[Hint: For fixed $c = \cos(\theta)$ maximize $(1 - c^2)(x - 2c)^2 - x^2$ where $x = r^3 + r^{-3}$.]

iii. Show that $u^3 > |\operatorname{disc}(K)|/4 - 7$. Show that $\operatorname{disc}(K) = -1323$ and deduce that $u^3 > 323.75$. Show that $2 - \sqrt[3]{7} = u^{-k}$ for some $k > 0$ and deduce that $2 - \sqrt[3]{7}$ is a generator of the free part of $\mathcal{O}_K^\times$. [Feel free to use a calculator for the numerical estimates.]

4. Let $m < 0$ be square-free and consider $K = \mathbb{Q}(\sqrt{m})$. Recall from problem set 3 problem 2 how primes p in $\mathbb{Q}$ split in K.

(a) Show that there is a multiplication map

$$\Phi : \bigoplus_{e_{\mathfrak{p}/p} > 1} (\mathbb{Z}/2\mathbb{Z})\mathfrak{p} \to \operatorname{Cl}(K)[2]$$

where $\operatorname{Cl}(K)[2] = \{I \in \operatorname{Cl}(K) | I^2 = 1\}$ and the map is

$$\Phi : \oplus e_i \mathfrak{p}_i \mapsto \prod \mathfrak{p}_i^{e_i}$$

(b) Show that the kernel of the map Φ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ with generator $\oplus\mathfrak{p}$ where the sum is over $\mathfrak{p} \mid p \mid m$. [Hint: Use that $m < 0$ to show that $(n, \sqrt{m})$ is not principal for $n \mid m$ unless $n = m$. You will have to treat the cases $m \equiv 1, 2 \pmod 4$ and $m \equiv 3 \pmod 4$ separately.]

(c) Suppose $I \in \operatorname{Cl}(K)[2]$ has prime decomposition $\prod \mathfrak{q}_i^{a_i}$. Show that it cannot happen that every $\mathfrak{q}_i \mid p_i$ is unramified and each p_i is split in K. [Hint: Show that if $\prod \mathfrak{q}_i^{2a_i}$ is principal then it can be generated by $\prod p_i^{a_i}$ and deduce a contradiction from unique factorization using $p_i = \mathfrak{q}_i\overline{\mathfrak{q}}_i$.]

(d) Deduce that Φ is surjective and therefore

$$|\operatorname{Cl}(K)[2]| = 2^{M-1}$$

where M is the number of primes p which ramify in K.

5. In this problem you will construct number fields whose rings of integers cannot be generated by few elements. Let $n \geq 2$ be an integer and let $K = \mathbb{Q}(\sqrt[n]{2})$ with ring of integers $\mathcal{O}_K$.

(a) Suppose $p \nmid 2[\mathcal{O}_K : \mathbb{Z}[\sqrt[n]{2}]]$ be a prime which splits completely in K. Show that $n \mid p - 1$ and that $2^{(p-1)/n} \equiv 1 \pmod p$.

(b) Show that there exists a unique subfield $F \subset \mathbb{Q}(\zeta_p)$ with $[F : \mathbb{Q}] = n$.

(c) Let $\mathfrak{q} \mid 2$ be an ideal of $\mathbb{Z}[\zeta_p]$ and $\mathfrak{p} = \mathfrak{q} \cap F$. Show that the image of $\operatorname{Frob}_{\mathfrak{q}/2}$ in $G_{F/\mathbb{Q}}$ is $\operatorname{Frob}_{\mathfrak{p}/2}$ and deduce that $\operatorname{Frob}_{\mathfrak{p}/2} = 1$. [Hint: What is $\operatorname{Frob}_{\mathfrak{q}/2} \in G_{\mathbb{Q}(\zeta_p)/\mathbb{Q}} \cong (\mathbb{Z}/p\mathbb{Z})^\times$?]

(d) Deduce that 2 splits completely in F.

(e) Assume that $\mathcal{O}_F = \mathbb{Z}[\alpha_1, \ldots, \alpha_m]$. Show that we have induced ring homomorphisms

$$\mathbb{Z}[X_1, \ldots, X_m] \twoheadrightarrow \mathcal{O}_F \twoheadrightarrow \oplus_{\mathfrak{p}|2} k_{\mathfrak{p}/2}$$

where the n quotients $\mathbb{Z}[X_1, \ldots, X_m] \twoheadrightarrow k_{\mathfrak{p}/2} \cong \mathbb{F}_2$ are distinct.

(f) Show that there are at most 2^m distinct ring homomorphisms $\mathbb{Z}[X_1, \ldots, X_m] \twoheadrightarrow \mathbb{F}_2$ and deduce that $\mathcal{O}_F$ cannot be generated as an algebra over $\mathbb{Z}$ by fewer than $\lceil \log_2(n) \rceil$ elements. [Hint: where can X_i go under such a ring homomorphism?]

For example, $p = 151$ splits completely in $\mathbb{Q}(\sqrt[5]{2})$ and so 2 splits completely in $\mathbb{Q}(\zeta_{151})$. The subfield $F \subset \mathbb{Q}(\zeta_{151})$ of order 5 over $\mathbb{Q}$ is the splitting field of the polynomial $X^5+X^4-60X^3-12X^2+784X+128$ and has ring of integers that cannot be generated by two elements. Can it be generated by 3 elements?

Moreover, for any n there exist infinitely many p which split completely in $\mathbb{Q}(\sqrt[n]{2})$ and so we have an infinite family of examples. I got this example from `http://wstein.org/129-05/challenges.html`