Math 80220 Algebraic Number Theory
Problem Set 7

Andrei Jorza

due Friday, March 23

1. Let m be a square-free integer $\neq 1$. Let $K = \mathbb{Q}(\sqrt{m})$ and $\mathcal{O}_K$ be the ring of integers. Show that the following are prime factorizations of $(p)\mathcal{O}_K$ in $\mathcal{O}_K$:

   (a) if $p \mid m$ then $(p)\mathcal{O}_K = (p, \sqrt{m})^2$.

   (b) if m is odd then
   $$(2)\mathcal{O}_K = \begin{cases} (2, 1+\sqrt{m})^2 & m \equiv 3 \pmod 4 \\ (2, \frac{1+\sqrt{m}}{2})(2, \frac{1-\sqrt{m}}{2}) & m \equiv 1 \pmod 8 \\ (2) & m \equiv 5 \pmod 8 \end{cases}$$
   [Careful how you apply the decomposition theorem from class.]

   (c) if $p > 2$ and $p \nmid m$ then
   $$(p)\mathcal{O}_K = \begin{cases} (p, a+\sqrt{m})(p, a-\sqrt{m}) & m \equiv a^2 \pmod p \\ (p) & m \text{ not a square mod } p \end{cases}$$

2. Let $p > 2$ be a prime. You may suppose that the ring of integers of $K = \mathbb{Q}(\zeta_{p^n})$ is $\mathcal{O}_K = \mathbb{Z}[\zeta_{p^n}]$. Show that:

   (a) $(p)\mathcal{O}_K = (p, 1-\zeta_{p^n})^{p^{n-1}(p-1)}$ and

   (b) if $q \neq p$ is a prime and r is the smallest positive integer such that $q^r \equiv 1 \pmod{p^n}$ then $(q)\mathcal{O}_K = \mathfrak{q}_1 \cdots \mathfrak{q}_d$ where $d = p^{n-1}(p-1)/r$ is the prime factorization of the ideal $(p)\mathcal{O}_K$ and $K/\mathbb{Q}$ is unramified at $\mathfrak{q}_i/q$ with $f_{\mathfrak{q}_i/q} = r$.

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

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

   (b) Find examples of unramified primes p with decomposition $(p)\mathcal{O}_K = \mathfrak{q}_1 \ldots \mathfrak{q}_r$ 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. $r = 1$, $f_{\mathfrak{q}_1/p} = 3$.

4. Let $m < 0$ be square-free and consider $K = \mathbb{Q}(\sqrt{m})$.

   (a) Show that there is a multiplication map
   $$\Phi : \bigoplus_{e_{\mathfrak{p}/p} > 1} (\mathbb{Z}/2\mathbb{Z})[\mathfrak{p}] \to \mathrm{Cl}(K)[2]$$
   where $\mathrm{Cl}(K)[2] = \{I \in \mathrm{Cl}(K) | I^2 = 1\}$ 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) (Original version of this part was wrong, fixed now) Suppose $[I] \in \mathrm{Cl}(K)[2]$. Show that there exists a fractional ideal $J \in [I]$ such that $J = \overline{J}$. [Hint: Show that the principal ideal $I\overline{I}^{-1}$ is generated by some $\alpha\overline{\alpha}^{-1}$ using Hilbert 90.]

(d) Deduce that Φ is surjective and therefore

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

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