6370-001 - FALL 2021 - WEEK 5 (9/21, 9/23)

Exercise 1.

(1) Compute the class groups of $\mathbb{Q}(\sqrt{-5})$, $\mathbb{Q}(\sqrt{-10})$, $\mathbb{Q}(\sqrt{-23})$, and $\mathbb{Q}(\sqrt{-47})$.
(2) It is a deep fact, due to Heegner, that $\mathbb{Q}(\sqrt{-n})$ has class number 1 if and only if $n = 1, 2, 3, 7, 11, 19, 43, 67$ or 163. Verify that the class number is 1 in each of these cases.

Exercise 2.

(1) Compute the Minkowski bound for $\mathbb{Q}(\zeta_p)$ for p prime (you may assume that the ring of integers is $\mathbb{Z}[\zeta_p]$. However, note that in terms of just getting a bound it is not really necessary to assume this – why?).
(2) Compute the class group of $\mathbb{Q}(\zeta_5)$.
(3) Calculate explicitly the Minkowski bound for $\mathbb{Q}(\zeta_{23})$. Use GP/Pari (or google) to find its class number.

Exercise 3. Find a real quadratic field (i.e. one of the form $\mathbb{Q}(\sqrt{m})$ with m positive squarefree) with class number not equal to 1.

Exercise 4.

(1) Show that $x^3 + ax + b$ has discriminant $-4a^3 - 27b^2$.
(2) Show that $x^3 + x + 1$ is irreducible over $\mathbb{Q}$
(3) Show that the ring of integers in $\mathbb{Q}[x]/x^3 + x + 1$ is $\mathbb{Z}[x]/x^3 + x + 1$.
(4) Compute the class group of $\mathbb{Q}[x]/x^3 + x + 1$.

Exercise 5 (Milne 4-7) For $K = \mathbb{Q}(\sqrt{-1}, \sqrt{-5})$, show $\mathcal{O}_K = \mathbb{Z}[\sqrt{-1}, \frac{1+\sqrt{5}}{2}]$. Show that the only primes that ramify in K are 2 and 5, each with ramification degree 2. Deduce $K/\mathbb{Q}(\sqrt{-5})$ is unramified.

Exercise 6 (*Not about class groups.*) Suppose K is a number field (a finite extension of $\mathbb{Q}$) and $\alpha \in \mathcal{O}_K$ is such that, for every embedding $\iota : K \hookrightarrow \mathbb{C}$, $|\iota(\alpha)| \leq 1$. Show that α is a root of unity.

Exercise 7. Let p be an odd prime. On last week's worksheet, we gave a short proof using ramification that the unique quadratic subfield of $\mathbb{Q}(\zeta_p)$ is $\mathbb{Q}(\sqrt{p^*})$. This exercise gives a different method to find an explicit formula for a square root of p^* using primitive pth roots of unity.

(1) Let $m(x) = \frac{x^p-1}{x-1} = x^{p-1} + \ldots + 1$. Show that $m(x) \in \mathbb{Q}[x]$ is irreducible. (Hint: use the Eisenstein criterion for irreducibility and the change of coordinates $x = t + 1$).

    Let $L = \mathbb{Q}[x]/(m(x))$. Part (1) implies that $(m(x))$ is a maximal ideal in the principal ideal domain $\mathbb{Q}[x]$, thus L is a field. We write $\zeta \in L$ for the image of x under the quotient map.

(2) Show that $\zeta, \zeta^2, \ldots, \zeta^{p-1}$ are a basis for L as a $\mathbb{Q}$-vector space.
(3) Show that there is a unique ring homomorphism $L \to \mathbb{C}$ sending ζ to $e^{2\pi i/p}$ and that the image is the smallest subfield of $\mathbb{C}$ containing $e^{2\pi i/p}$.
(4) For each $k \in (\mathbb{Z}/p\mathbb{Z})^\times$, show that there is a unique field automorphism

$$\sigma_k : L \xrightarrow{\sim} L$$

such that $\sigma_k(\zeta) = \zeta^k$.

(5) Use the uniqueness statement in (4) to show the map

$$(\mathbb{Z}/p\mathbb{Z})^\times \to \mathrm{Aut}(K),\ k \mapsto \sigma_k$$

is a group homomorphism.

(6) Show that if $\ell \in L$ satisifies $\sigma_k(\ell) = \ell$ for all $k \in (\mathbb{Z}/p\mathbb{Z})^\times$ then $\ell \in \mathbb{Q} \subset L$. (Hint: use the basis in (2), and the fact that $m(\zeta) = 0$ implies $\zeta + \zeta^2 + \ldots + \zeta^{p-1} = -1$).

In the following, you may use without proof that $\mathbb{Z}/p\mathbb{Z}$ is cyclic of order $p-1$.

(7) Show that there is a unique non-trivial character $\chi : (\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\}$, and that the kernel of χ consists of the squares in $(\mathbb{Z}/p\mathbb{Z})^\times$.

Let

$$\tau = \sum_{k \in (\mathbb{Z}/p\mathbb{Z})^\times} \chi(k)\sigma_k(\zeta) = \sum_{k \in (\mathbb{Z}/p\mathbb{Z})^\times} \chi(k)\zeta^k \in L.$$

(8) Show that for any $k \in (\mathbb{Z}/p\mathbb{Z})^\times$, $\sigma_k(\tau) = \chi(k)\tau$. (Hint: $\chi(k) = \chi(k)^{-1}$.)

(9) Show that for any $k \in (\mathbb{Z}/p\mathbb{Z})^\times$, $\sigma_k(\tau^2) = \tau^2$, and deduce $\tau^2 \in \mathbb{Q}$.

(10) Using the the embedding $K \hookrightarrow \mathbb{C}$ from (3) and Euler's identity $e^{2\pi i t} = \cos(t) + i\sin(t)$, to compute directly τ^2 when $p = 3$ and $p = 5$ (assuming the standard identities $\cos(\pm\pi/3) = -1/2$, $\cos(\pm\pi/5) = \frac{\sqrt{5}+1}{4}$, $\cos(\pm 2\pi/5) = \frac{\sqrt{5}-1}{4}$, and their counterparts for sin.)

In the remaining steps we will show $\tau^2 = -p$ if $p \equiv 3 \mod 4$ and $\tau^2 = p$ if $p \equiv 1 \mod 4$.

(11) Write $\alpha = \sum_{k \in (\mathbb{Z}/p\mathbb{Z})^\times} \sigma_k(\tau^2)$. Use (9) to deduce that $\alpha = (p-1)\tau^2$.

(12) Fill in the details of the following computations:

$$\begin{aligned}
\alpha &= \sum_{k \in (\mathbb{Z}/p\mathbb{Z})^\times} \sigma_k\left(\left(\sum_{s \in (\mathbb{Z}/p\mathbb{Z})^\times} \chi(s)\zeta^s\right)^2\right) \\
&= (p-1)^2 \cdot \chi(-1) + \left(\sum_{a,b \in (\mathbb{Z}/p\mathbb{Z})^\times, a \neq -b} \chi(a)\chi(b)\right) \cdot (\zeta + \zeta^2 + \ldots + \zeta^{p-1}) \\
&= (p-1)^2 \cdot \chi(-1) + \left(\left(\sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \chi(a)\right)^2 - \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \chi(a)\chi(-a)\right) \cdot (-1) \\
&= (p-1)^2 \cdot \chi(-1) + (0 - (p-1)\chi(-1)) \cdot (-1) \\
&= (p-1) \cdot p \cdot \chi(-1).
\end{aligned}$$

(13) Conclude that $\tau^2 = -p$ if $p \equiv 3 \mod 4$ and $\tau^2 = p$ if $p \equiv 1 \mod 4$.

Exercise 8.
Let A be a Dedekind domain with fraction field F, let $L/K/F$ be a separable extensions, let B be the integral closure of A in K and let C be the integral closure of A in L. Then:

$$\mathcal{D}_{C/A} = N_{B/A}(\mathcal{D}_{C/B}) \cdot \mathcal{D}_{B/A}^{[L:K]}$$

where here $\mathcal{D}$ denotes the relative discriminant (see Exercise 9 from last week) and N the norm of an ideal. Work through the proof of this following Rabinoff's notes: `https://services.math.duke.edu/~jdr/1516f-4803/disctower.pdf`.