6370-001 - FALL 2021 - WEEK 6 (9/28, 9/30)

Exercise 0. Compute the units in $\mathcal{O}_K$ for $K = \mathbb{Q}(\sqrt{m})$, $m < 0$ squarefree.

Exercise 1 (Marcus 5-33, 34). Let $m > 0$ be squarefree, and let $K = \mathbb{Q}(\sqrt{m})$.

1. Suppose $m \equiv 2$ or $3 \bmod 4$. Consider the numbers $mb^2 \pm 1$, $b \in \mathbb{Z}$, and take the smallest positive b such that one of these is a square a^2 for $a \in \mathbb{Z}$ (why does the unit theorem imply such a b exists?). Prove that $a + b\sqrt{m}$ is the fundamental unit in O_K.
2. Establish a similar criteria for $m \equiv 1 \mod 4$.
3. Compute the fundamental unit in $\mathcal{O}_K$ for all $2 \le m \le 30$ except 19 and 22.

Exercise 2 (Milne 5-2 plus some more). Read the very short section "Example: real quadratic fields," in Chapter 5 of Milne. Then,

1. Use this on a few examples from the previous exercise to convince yourself it's right.
2. Use this to find a fundamental unit when $m = 19, 22, 67$. Use Pari to check your answer.
3. Prove that the continued fraction expansion for an irrational number is periodic if and only if it generates a degree 2 extension of $\mathbb{Q}$.
4. Why does this algorithm work? (see Borevich and Shafarevich - Number Theory, Ch 2 §7.3).

Exercise 3.

1. Fix a positive integer m and a positive real number M. Show there are only finitely many elements $\alpha \in \mathbb{C}$ such that
   (a) α is integral over $\mathbb{Z}$ with minimal polynomial of degree $\le m$
   (b) all of conjugates of α have absolute value $\le M$ (here we mean all of the other roots of the minimal polynomial over $\mathbb{Q}$, not just the complex conjugate, which is the other root of the minimal polynomial over $\mathbb{R}$).
2. Show that if $\alpha \in \mathbb{C}$ is integral over $\mathbb{Z}$ and all conjugates of α have absolute value ≤ 1 then α is a root of unity (this was also on last week's exercises, stated in a slightly different way).
3. (Milne 5-1) Is the set of algebraic integers $\alpha \in \mathbb{C}$ with minimal polynomial of degree $\le m$ and $|\alpha| < M$ is finite?

Exercise 4. Let $A = \mathbb{F}_q[t]$ and consider the absolute valute $|f(t)| = 2^{\deg f}$ (where we say $\deg 0 = \infty$).

1. Explain how to extend this absolute value to $K = \mathrm{Frac}(A) = \mathbb{F}_q(t)$.
2. Show that the completion of K for the metric induced by this absolute value is $\mathbb{F}_q((s))$, where $s = 1/t$.
3. We first enumerate some facts which will be justified (to some extent) later in the course
   Fact 1: This absolute value extends uniquely to any algebraic closure $\overline{\mathbb{F}_q((s))}$.
   Fact 2: $\mathbb{C}_\infty := \widehat{\overline{\mathbb{F}_q((s))}}$, the completion for the metric induced by this extended absolute value, is algebraically closed (Krasner's lemma) and complete.

   $\mathbb{C}_\infty$ is a complete algebraically closed extension of $\mathbb{F}_q(t)$ that plays the same role as $\mathbb{C}$ in the theory of number fields if we think of $\mathbb{F}_q[t]$ as being analogous to $\mathbb{Z}$!

If m is a positive integer and M is a positive real number, show there are only finitely many elements of $\mathbb{C}_\infty$ that are integral over $\mathbb{F}_q[t]$ with minimal polynomial of degree $\le m$ and all of whose conjugates have absolute value $\le M$.

(4) Deduce that if $\alpha \in \mathbb{C}_\infty$ is integral over $\mathbb{F}_q[t]$ and all of its conjugates have absolute value ≤ 1, then α is a root of unity.

(5) What would happen in the previous question if we replaced $\mathbb{F}_q$ with $\mathbb{C}$ (i.e. started with $\mathbb{C}[t]$ instead of $\mathbb{F}_q[t]$)? If you know a little bit of the algebraic geometry of curves, then explain the answer geometrically.

Exercise 5. Suppose K is a totally real field (i.e. a number field such that every embedding $K \hookrightarrow \mathbb{C}$ factors through $\mathbb{R}$). Let α be an element of K such that $\iota(\alpha) < 0$ for every embedding $\iota : K \hookrightarrow \mathbb{R}$, and let $L = K(\sqrt{(\alpha)})$ [a number field of this form is called a *CM field*].

(1) Show $[L : K] = 2$ (i.e. show α is not a square in K).

(2) Show the ranks of $\mathcal{O}_L^\times$ and $\mathcal{O}_K^\times$ are the same.

(3) Show that $\mu(L)\mathcal{O}_K^\times$ is of index at most 2 in $\mathcal{O}_L^\times$. *Hint: consider the homomorphism from $\mathcal{O}_L^\times$ to $\mu(L)/\mu(L)^2$, $\eta \mapsto \overline{\eta}/\eta$.*

Exercise 6. For K a number field, the *narrow* class group $\mathrm{Cl}^+(\mathcal{O}_K)$ is the quotient of the group of fractional ideals by the group of principal fractional ideals (a) generated by elements $a \in K^\times$ such that $\iota(a) > 0$ for all $\iota : K \hookrightarrow \mathbb{R}$. We write $h_K^+ = |\mathrm{Cl}^+(\mathcal{O}_K)|$.

(1) Show that $h_K^+ \le 2^r h_K$, where r is the number of real embeddings.

(2) Deduce the narrow class number of an imaginary quadratic field is equal to its class number.

(3) Describe in terms of a fundamental unit when the narrow class number of a real quadratic field will be equal to the class number.

(4) The class numbers of $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{5})$ are 1. What are their narrow class numbers?

(5) The following is one of the main results of class field theory:

Fact. The narrow class number of K is equal to the degree of the largest abelian extension L/K such that every prime $\mathfrak{p}$ of $\mathcal{O}_K$ is unramified in L. Actually, the narrow class group is canonically isomorphic to the Galois group of this extension!

Assuming this fact, what is the maximal extension of $\mathbb{Q}(\sqrt{5})$ satisfying this property? How about $\mathbb{Q}(\sqrt{-5})$ (recall Week 5 - Exercise 5)? How about $\mathbb{Q}(\sqrt{3})$?

Exercise 7 (Milne 4-5). Here's another closely related fact from class field theory:
Fact. The class number of K is equal to the degree of the largest abelian extension L/K such that every prime $\mathfrak{p}$ of $\mathcal{O}_K$ is unramified in L *and* every real embedding of K extends to a real embedding of L. Actually, the class group is canonically isomorphic to the Galois group of this extension! This extension L is called the *Hilbert class field* of K.

(1) Assuming the first part of this fact, give another explanation of why the narrow class group of a imaginary quadratic field is the same as its class group.

(2) We also have the additional
Fact. Every ideal in $\mathcal{O}_K$ becomes a principal in $\mathcal{O}_L$ for L/K the Hilbert class field.

(3) *Without assuming this fact*, prove that there is *some* extension L of K such that every ideal in $\mathcal{O}_K$ becomes principal in $\mathcal{O}_L$ (Hint: use the finiteness of the class number).