Math 254A, UC Berkeley, Fall 2001 (Kedlaya)
Lecture 23: Quadratic Fields and Quadratic Reciprocity
October 26, 2001

Reference. Neukirch, Section 1.8.

Jargon watch. Recall that a rational integer $D \neq 1$ is called a *fundamental discriminant* if one of the following holds:

(a) D is odd, squarefree, and congruent to 1 mod 4;

(b) D is divisible by 4, and $D/4$ is odd, squarefree, and congruent to 3 mod 4.

(c) D is divisible by 8, and $D/8$ is odd and squarefree.

The point: D is a fundamental discriminant if and only if the discriminant of the quadratic field $\mathbb{Q}(\sqrt{D})$ is equal to D.

Outline of lecture.

1. Let D be a fundamental discriminant. We may apply the criterion from last time to test whether primes split in $\mathbb{Q}(\sqrt{D})$, since the ring of integers is $\mathbb{Q}[\alpha]$ for $\alpha = \sqrt{D/4}$, if $D \equiv 0 \pmod 4$, or $\alpha = (1+\sqrt{D})/2$, if if $D \equiv 1 \pmod 4$.

2. We compute the splitting behavior of a prime p as follows:

   (a) If p divides D, then p is ramified. That is, there is one prime $\mathfrak{p}$ above (p) with $e(\mathfrak{p}/(p)) = 2$ and $f(\mathfrak{p}/(p)) = 1$.

   (b) If p is odd and does not divide D, then (p) is unramified, and splits into two primes if and only if the polynomial $x^2 - D$ factors modulo p.

   (c) If $p = 2$ and D is odd, then (p) is unramified, and splits into two primes if and only if the polynomial $x^2 - x + (D-1)/4$ factors modulo 2, that is, if and only if $D \equiv 1 \pmod 8$.

3. For quadratic fields, it turns out there is a beautiful condition that reduces the question of whether D has a square root modulo p to a question about p modulo the prime factors of D: the *law of quadratic reciprocity.* To state it, define the Legendre symbol $\left(\frac{a}{p}\right)$, for integers a, p with $p > 0$ an odd prime, as

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & a \equiv 0 \pmod p \\ 1 & a \not\equiv 0 \pmod p \text{and} a \equiv x^2 \pmod p \text{for some } x \in \mathbb{Z} \\ -1 & a \not\equiv 0 \pmod p \text{and} a \not\equiv x^2 \pmod p \text{for all } x \in \mathbb{Z}. \end{cases}$$

   In other words, $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod p$ (because $\mathbb{F}_p^*$ is cyclic).

4. State Gauss's law of quadratic reciprocity: for p, q odd primes,
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}, \qquad \left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}, \qquad \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$
Of these, the second is elementary, and the third follows from the splitting result above.

5. Sketch the proof from Neukirch Section 1.8, using the Gauss sum
$$\tau = \sum_{a \in \mathbb{F}_p^*} \left(\frac{a}{p}\right) \zeta_p^a,$$
where ζ_p is a primitive p-th root of unity. Namely, calculate explicitly that $\tau^2 = \left(\frac{-1}{p}\right) p$. We will revisit this proof when we study cyclotomic fields, several lectures from now, and give it a more conceptual interpretation.

6. Advertise *class field theory*, which can be viewed (among other things) as a generalization of quadratic reciprocity to a splitting criterion for any Galois extension of any number field with abelian Galois group. (I will be covering class field theory next semester.)

Addendum to previous lecture. A more conceptual way to see the relationship, in case $\mathfrak{o}_L = \mathfrak{o}_K[\alpha]$, between the factorization of $\mathfrak{p}\mathfrak{o}_L$ and the factorization of $P(x)$ modulo $\mathfrak{p}$ (for $\mathfrak{p}$ a prime of $\mathfrak{o}_K$ and $P(x)$ the minimal polynomial of α) is as follows. Put $\mathfrak{p} = \prod_i \mathfrak{b}_i^{e_i}$ and suppose $P(x) \equiv \prod_j P_j(x)^{c_j} \pmod{\mathfrak{p}}$, where each P_j is irreducible modulo $\mathfrak{p}$. Then on one hand, by the Chinese remainder theorem, $\mathfrak{o}_L/(\mathfrak{p}\mathfrak{o}_L) \cong \prod_i \mathfrak{o}_L/\mathfrak{b}_i^{e_i}$. On the other hand,
$$\mathfrak{o}_L/(\mathfrak{p}\mathfrak{o}_L) \cong \mathfrak{o}_K[x]/[(P(x)) + \mathfrak{p}] \cong (\mathfrak{o}_K/\mathfrak{p})[x]/(P(x)) \cong \prod_j (\mathfrak{o}_K/\mathfrak{p})[x]/(P_j(x)^{c_j}).$$
We have now written the ring $\mathfrak{o}_L/(\mathfrak{p}\mathfrak{o}_L)$ as a finite product of local rings in two ways. It's a standard fact from algebra that such a decomposition is unique if it exists, so we can pair off the β_i with the P_j.

In case you haven't seen that standard fact before, here's how it's proved: call an element e of a ring an *idempotent* if $e^2 = e$. In a local ring, this implies $e(e-1) = 0$, and e and $e-1$ cannot both be in the maximal ideal. Thus either e is a unit, so $e - 1 = 0$, or $e - 1$ is a unit, so $e = 0$. That is, the only idempotents in a local ring are 0 and 1.

Suppose the ring R is isomorphic both to $\prod_i S_i$ and $\prod_j T_j$, where the S_i and T_j are local. Let e_i be the element of R which has 1 in S_i and 0 in the other S's, and let f_j be the element of R which has 1 in T_j and 0 in the other T's. Now $e_i x \in S_i$ for all $x \in R$ (that is, $e_i x$ has 0 in the S's other than S_i), and likewise $f_j x \in T_j$ for all $x \in R$. Also, $e_i f_j$ is an idempotent for all i, j; since it's in S_i, it's either equal to e_i or 0. But the sum of the f_j is 1, so $\sum_j e_i f_j = e_i \cdot 1 = e_i$, so the $e_i f_j$ cannot all be 0. So there is some j such that $e_i f_j = e_i$; by a similar argument, $e_i f_j = f_j$. Thus the rings S_i and T_j are isomorphic (they're both the image of multiplication by $e_i = f_j$), so we can factor them off and keep going.