Math 254A, UC Berkeley, Fall 2001 (Kedlaya)
Lecture 25: Cyclotomic Fields (Part 1)
October 31, 2001

Reference. Neukirch, Section 1.10. But we will supplant some of the proofs with the local arguments in Section 2.7, which we partially covered in class already.

Outline of lecture.

Throughout, let ζ_n denote a primitive n-th root of unity.

1. Prove that $\mathbb{Z}[\zeta_n]$ is the ring of integers of $\mathbb{Q}(\zeta_n)$ by showing that $\mathbb{Z}_p[\zeta_n]$ is the valuation ring of $\mathbb{Q}_p(\zeta_n)$ for each p, using Proposition II.7.13 in the case $n = p^l$ is a prime power. One can also give a global proof (which is pretty similar); see Section 1.10.

2. Calculate the discriminant of $\mathbb{Q}(\zeta_n)$, up to sign, in case $n = p^l$, by explicitly calculating the discriminant of the n-th cyclotomic polynomial. See the homework for the general case.

3. Prove the explicit formula for the splitting of a rational prime p in $\mathbb{Q}(\zeta_n)$: if $v_p(n) = m$ and f is the smallest positive integer such that $p^f \equiv 1 \pmod{n/p^m}$, then p splits into prime ideals with ramification index $\phi(p^m)$ and inertia degree f.

4. For $n = p$ an odd prime, Galois theory tells us that $\mathbb{Q}(\zeta_p)$ contains a unique quadratic subfield. Identify this subfield explicitly: the Gauss sum $\tau = \sum_{a \in \mathbb{F}_p^*} \left(\frac{a}{p}\right) \zeta_p^a$ satisfies $\tau^2 = (-1)^{(p-1)/2} p$.

5. Now suppose q is another odd prime. Show that q splits in $\mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p})$ if and only if q splits into an even number of prime ideals in $\mathbb{Q}(\zeta_p)$. Reobtain from this the law of quadratic reciprocity.