Math 430 Tom Tucker
Notes From Class 10/30

Theorem 17.1. *Let m be any positive integer. Then $\mathbb{Z}[\xi_m]$ is Dedekind and the field $\mathbb{Q}(\xi_m)$ is Galois of degree of $\phi(m)$ over $\mathbb{Q}$. Thus, $\Phi_m(X)$ is irreducible over $\mathbb{Q}$ for all m.*

Proof. It is obvious that $\mathbb{Q}(\xi_m)$ is Galois. Indeed, $\xi_m^m = 1$ implies $\sigma(\xi_m)^m = 1$ for any conjugate $\sigma(\xi_m)$ of ξ_m. But every root of $x^m - 1 = 0$ is a power of ξ_m so is in $\mathbb{Q}(\xi_m)$. Hence, $\mathbb{Q}(\xi_m)$ is the splitting field for the minimal monic of ξ_m and is therefore Galois.

We will show that $\mathbb{Z}[\xi_m]$ is Dedekind and that $\mathbb{Q}(\xi_m)$ has degree$\phi(m)$ over $\mathbb{Q}$ by induction on the number r of distinct prime factors p of m. We have already treated the case $r = 1$. Then writing $m = m'q$ where m' has $r-1$ distinct prime factors and q is a prime power (which is prime to m'). The discriminant of $\mathbb{Z}[\xi'_m]$ divides $(m')^{m'}$ (the discriminant of $x^{m'} - 1$) so is prime to the discriminant of $\mathbb{Z}[\xi_q]$ (since $(m', q) = 1$). By this week's homework #5, it follows that $\mathbb{Z}[\xi_q, \xi_{m'}]$ is Dedekind, since $\mathbb{Z}[\xi_{m'}]$ and $\mathbb{Z}[\xi_q]$ are Dedekind by the inductive hypothesis and have coprime discriminants. Since ξ_m^q is a primitive m'-th root of unity and $\xi_m^{m'}$ is a primitive q-th root of unity, we have

$$\mathbb{Z}[\xi_m] = \mathbb{Z}[\xi_q, \xi_{m'}],$$

so $\mathbb{Z}[\xi_m]$ is Dedekind.

To calculate the degree of $\mathbb{Q}(\xi_m)$ it will suffice to show that $\mathbb{Q}(\xi_q)$ and $\mathbb{Q}(\xi_{m'})$ are disjoint over $\mathbb{Q}$, since that means that the degree of $\mathbb{Q}(\xi_m)$ is the product of the degrees of $\mathbb{Q}(\xi_q)$ and $\mathbb{Q}(\xi_{m'})$, and $\phi(m) = \phi(q)\phi(m')$ since m' and q are relatively prime. Now p ramifies completely in $\mathbb{Q}(\xi_q)$, and not at all in $\mathbb{Q}(\xi_m)$ so $\mathbb{Q}(\xi_q) \cap \mathbb{Q}(\xi_{m'}) = \mathbb{Q}$, as desired, by a previous homework problem.

To see that $\Phi_m(X)$ is irreducible over $\mathbb{Q}$ for all m we simply note that $\deg \Phi_m(X) = \phi(m) = [\mathbb{Q}(\xi_m) : \mathbb{Q}]$. □

We can use cyclotomic fields to prove the quadratic reciprocity theorem. Recall the definition the quadratic residue symbol for a prime p. It is defined for an integer a coprime to p as

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & : \ a \text{ is square} \pmod p \\ -1 & : \ a \text{ is not a square} \pmod p \end{cases}$$

From now on, p and q are distinct odd primes (there is also a form of quadratic reciprocity when one of them is 2, but we will not treat it). Quadratic reciprocity relates $\left(\frac{p}{q}\right)$ with $\left(\frac{q}{p}\right)$. It says that for p and

q odd we have

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(q-1)(p-1)}{4}}.$$

When p is odd and $(a,p) = 1$, we have

(1) $\left(\frac{a}{p}\right) = a^{(p-1)/2}$;
(2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;
(3) $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$;
(4) $\left(\frac{a}{p}\right) = (-1)^{\frac{p-1}{\mathrm{ord}(a)}}$, where $\mathrm{ord}_p(a)$ denotes the order of $a \pmod p$.

Properties 2, 3, and 4 follow immediately from 1. Property 1 follows from the fact that $(\mathbb{Z}/p\mathbb{Z})^*$ has a primitive root θ and a is square mod p if and only if $a = \theta^r$ for some even r. Now, $(\theta^r)^{(p-1)/2} = 1$ if r is even and -1 is r is odd, so we are done.

We will give a simple proof of quadratic reciprocity by factoring p in $\mathbb{Z}[\xi_q]$.

Lemma 17.2. *The field $\mathbb{Q}(\xi_q)$ contains exactly one quadratic field. It is $\mathbb{Q}(\sqrt{(-1)^{(q-1)/2}q})$.*

Proof. The field $\mathbb{Q}(\xi_q)$ is Galois since all the conjugates of ξ_q are powers of ξ_q and hence Φ_q splits completely in $\mathbb{Q}(\xi_q)$. It is clear that the Galois group is $(\mathbb{Z}/a\mathbb{Z})^*$ which is cyclic of even order, so there is exactly one subgroup of index 2, and one subfield of degree 2. Since $\mathbb{Q}(\xi_q)$ only ramifies at p, this quadratic field cannot ramify at 2, so it must have discriminant divisible only by q. There are only two possibilities $\mathbb{Q}(\sqrt{q})$ and $\mathbb{Q}(\sqrt{-q})$. By checking the ramification at 2, we see that if $q \equiv 1 \pmod 4$ it is $\mathbb{Q}(\sqrt{q})$, if $q \equiv 3 \pmod 4$, then $-q \equiv 1 \pmod 4$, so it must be $\mathbb{Q}(\sqrt{-q})$. □

What has this got to do with cyclotomic fields? The first fact is that $\left(\frac{q}{p}\right) = 1$ if and only if $x^2 - q$ factors mod p. This is the same thing as saying that

$$p\mathfrak{o}_E = \mathfrak{p}_1\mathfrak{p}_2$$

in a certain quadratic extension E. Why is this helpful? Because $\mathbb{Q}(\xi_q)$ contains a unique quadratic field.

Lemma 17.3. *The field $\mathbb{Q}(\xi_q)$ contains exactly one quadratic field. It is $\mathbb{Q}(\sqrt{(-1)^{(q-1)/2}q})$.*

Proof. The field $\mathbb{Q}(\xi_q)$ is Galois since all the conjugates of ξ_q are powers of ξ_q and hence Φ_q splits completely in $\mathbb{Q}(\xi_q)$. It is clear that the Galois group is $(\mathbb{Z}/a\mathbb{Z})^*$ which is cyclic of even order, so there is exactly one subgroup of index 2, and one subfield of degree 2. Since $\mathbb{Q}(\xi_q)$ only ramifies at p, this quadratic field cannot ramify at 2, so it must have discriminant divisible only by q. There are only two possibilities $\mathbb{Q}(\sqrt{q})$ and $\mathbb{Q}(\sqrt{-q})$. By checking the ramification at 2, we see that if $q \equiv 1 \pmod 4$ it is $\mathbb{Q}(\sqrt{q})$, if $q \equiv 3 \pmod 4$, then $-q \equiv 1 \pmod 4$, so it must be $\mathbb{Q}(\sqrt{-q})$. □