MATH 6370, LECTURE 8
APRIL 03

GORDAN SAVIN

We shall now revisit cyclotomic fields and compute their Galois group in full generality. We start with the power of a prime case, so let p be a prime and $\omega \in \mathbb{C}^\times$ a primitive root root of order p^n. Thus ω is a root of $x^{p^n}-1$ but not a root of $x^{p^{n-1}}-1$, so it is a root of

$$\Phi_{p^n}(x) = \frac{x^{p^n}-1}{x^{p^{n-1}}-1} = (x^{p^{n-1}})^{p-1} + (x^{p^{n-1}})^{p-2} + \ldots + 1.$$

This polynomial is irreducible. This is proved using the Eisenstein criterion applied to $\Phi_{p^n}(x+1)$. Observe that $(x+1)^{p^{n-1}} \equiv x^{p^{n-1}}+1 \pmod p$ hence

$$\Phi_{p^n}(x+1) \equiv \frac{(x^{p^{n-1}}+1)^p-1}{x^{p^{n-1}}} = (x^{p^{n-1}})^{p-1} + p(x^{p^{n-1}})^{p-2} + \ldots + p.$$

Thus $\mathbb{Q}(\omega)$ is a Galois extension of degree $p^{n-1}(p-1)$. Let G be its Galois group. Let $\sigma \in G$. Then σ is determined by $\sigma(\omega)$, which has to be another primitive root. Hence $\sigma(\omega)=\omega^a$ for a unique $a \in (\mathbb{Z}/p^n\mathbb{Z})^\times$. Hence $G \cong (\mathbb{Z}/p^n\mathbb{Z})^\times$. The ring of integers is $A=\mathbb{Z}[\omega]$, this is similar to the case $n=1$ done in class, and we have the following equality of ideals

$$(1-\omega)^{p^{n-1}(p-1)} = Ap$$

which is checked by substituting 1 into the cyclotomic polynomial. Other primes $q \neq p$ are unramified since $x^{p^{n-1}}-1$ has no repeated roots modulo q, and $\mathrm{Fr}_q(\omega)=\omega^q$, hence it corresponds to $q \in (\mathbb{Z}/p^n\mathbb{Z})^\times \cong G$.

In order to deal with $\mathbb{Q}(\omega)$ where ω is a primitive m-th root of 1, and m is not a power of a prime, we need the following.

Lemma 0.1. *Let E and F be two Galois extension of $\mathbb{Q}$. Let G_E and G_F be the respective Galois groups. Let K be the smallest field containing E and F. Let G be its Galois group. If $E \cap F = \mathbb{Q}$ Then*

$$G \cong G_E \times G_F.$$

Proof. If E and F are splitting fields of polynomials $P(x)$ and $Q(x)$ then K is the splitting field of $P(x)Q(x)$ so it is Galois, and restricting $\sigma \in G$ to E and F gives a natural injection

$$G \to G_E \times G_F.$$

In particular,

$$|G| \leq |G_E| \cdot |G_F|.$$

In order to prove the lemma it suffices to show that we have equality here. Let N_E and N_F be the normal subgroups of G such corresponding to E and F via the Galois theory, that is, fixing the fields E and F. Moreover,

$$G_E \cong G/N_E \text{ and } G_F \cong G/N_F.$$

Hence $|G_E| = |G|/|N_E|$ and $|G_F| = |G|/|N_F|$, and the above inequality is equivalent to

$$|N_E| \cdot |N_F| \leq |G|.$$

Let N be the group generated by N_E and N_F. In view of normality of N_E and N_F, the group N, as a set is the product $N_E \cdot N_F$, hence $|N| \leq |N_F| \cdot |N_E|$. The group N is normal, and its fixed field is $E \cap F = \mathbb{Q}$, hence $G = N$, and all inequalities are equalities. $\square$

Now assume that ω is a primitive m-th root of 1, where $m = p^a q^b$ (for simplicity we assume that there are only 2 different primes appearing in the factorization of m). Then ω^{q^b} and ω^{p^a} are primitive roots of of order p^a and q^b, respectively. Let $E = \mathbb{Q}(\omega^{q^b})$, $F = \mathbb{Q}(\omega^{p^a})$ and $K = \mathbb{Q}(\omega)$. Clearly $E, F \subset K$. Moreover, since p^a and q^b are relatively prime, there exists integers u, v such that

$$up^a + vq^b = 1.$$

This implies that K is generated by E and F (why?). Next, consider $E \cap F$. Let r be a prime that ramifies in $E \cap F$. Then r ramifies in E, so $r = p$ and r ramifies in F, so $r = q$, a contradiction. Hence $E \cap F$ is everywhere unramified extension of $\mathbb{Q}$. But there are no such extensions, hence $E \cap F = \mathbb{Q}$. At this point the lemma applies, so the Galois group G of $\mathbb{Q}(\omega)$ is isomorphic to

$$(\mathbb{Z}/p^a\mathbb{Z})^\times \times (\mathbb{Z}/q^b\mathbb{Z})^\times$$

and hence

$$G \cong (\mathbb{Z}/m\mathbb{Z})^\times$$

by the Chinese reminder theorem. Of course, this isomorphism simple traces what an element $\sigma \in G$ does to ω. In particular, any prime r not dividing m is unramified and

$$\mathrm{Fr}_r = r \in (\mathbb{Z}/m\mathbb{Z})^\times$$

by the isomorphism.