Math 210B. Galois group of cyclotomic fields over $\mathbb{Q}$

1. Preparatory remarks

Fix $n \geq 1$ an integer. Let $K_n/\mathbb{Q}$ be a splitting field of $X^n - 1$, so the group of $n$th roots of unity in $K$ has order $n$ (as $\mathbb{Q}$ has characteristic not dividing $n$) and is cyclic (as is any finite subgroup of the multiplicative group of a field). By Exercise 3 in HW4, we have a natural injective homomorphism of groups

$$\text{Gal}(K_n/\mathbb{Q}) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times,$$

and it is an isomorphism when $n$ is a prime power due to an argument with Eisenstein’s criterion to prove that the polynomial $\Phi_p(X) = (X^p - 1)/(X^{p-1} - 1) = \Phi_p(X^{p-1})$ for $e \geq 1$ is irreducible over $\mathbb{Q}$. Concretely, the roots of $\Phi_p$ (in a splitting field over $\mathbb{Q}$) are clearly the full set of primitive $p^e$th roots of unity. Hence, the statement that the extension $K_{p^e}/\mathbb{Q}$ is “as big as is possible” really says that all primitive $p^e$th roots of unity are Galois conjugates of each other over $\mathbb{Q}$ (i.e., have the same minimal polynomial over $\mathbb{Q}$). This is a very special property of $\mathbb{Q}$.

For example, over $\mathbb{R}$ it is clear for odd $n > 1$ that the $\varphi(n)/2 \text{Gal}(\mathbb{C}/\mathbb{R})$-conjugate pairs. Likewise, over $\mathbb{F}_p$ (as well as many other interesting fields) one cannot say that “all primitive $n$th roots of unity are created equal”: they might have different minimal polynomials over the ground field. For example, if $n|(p-1)$ then $\mathbb{F}_p^\times$ contains a full set of $n$th roots of unity, so these are most definitely not “created equal”. As one instance, $\mathbb{F}_7$ contains 6 distinct 6th roots of unity; the primitive cube roots of unity in $\mathbb{F}_7$ are 2 and 4 (i.e., $X^2 + X + 1 = (X - 2)(X - 4)$ is a factorization of $\Phi_3$ in $\mathbb{F}_7[X]$).

The aim of this handout is to show that $\text{Gal}(K_n/\mathbb{Q}) \rightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ is an isomorphism even when $n$ is not a prime power. We cannot hope to use Eisenstein’s criterion, so we shall require another method (due to Gauss) which proceeds by a totally different approach and in particular proves the irreducibility of $\Phi_p$ in $\mathbb{Q}[X]$ by methods unrelated to Eisenstein’s criterion. The key to Gauss’ idea is to exploit the magical properties of the $p$th power map in $\mathbb{F}_p[X]$ for an auxiliary prime $p$. Since the number of primitive $n$th roots of unity in $K_n$ is exactly $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$ (as for the number of generators of any cyclic group of order $n$), and a Galois conjugate of a primitive $n$th root of unity is again a primitive $n$th root of unity (why?), to say they are Galois conjugates of each other over $\mathbb{Q}$ is to say that one of them (and hence all of them) has minimal polynomial over $\mathbb{Q}$ of degree $|(\mathbb{Z}/n\mathbb{Z})^\times|$. Any primitive $n$th root of unity $\zeta$ in $K_n$ actually generates $K_n$ over $\mathbb{Q}$, so $[K_n : \mathbb{Q}]$ is the degree of the minimal polynomial of $\zeta$ over $\mathbb{Q}$. Since $[K_n : \mathbb{Q}] = |\text{Gal}(K_n/\mathbb{Q})|$, we conclude that $\text{Gal}(K_n/\mathbb{Q}) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ is an isomorphism if and only if all primitive $n$th roots of unity in $K_n$ are Galois conjugate over $\mathbb{Q}$ (i.e., have the same minimal polynomial). This is what allows one to say that “all primitive $n$th roots of unity are created equal over $\mathbb{Q}$”; there is no algebraic way to distinguish them from each other once it is seen that $\text{Gal}(K_n/\mathbb{Q})$ acts transitively on this set (i.e., they’re all roots of the same minimal polynomial over $\mathbb{Q}$). The examples in the preceding paragraph show that this fails over other ground fields (such as $\mathbb{R}$ and finite fields).

As an important special case of the role of transitive Galois group actions to eliminate the possibility of algebraic distinguishability, when $n = 4$, one cannot say in any intrinsic sense that there is a “preferred” solution to $T^2 + 1 = 0$ in $\mathbb{C}$ (view $\mathbb{C}$ as simply an abstract choice of splitting field of $T^2 + 1$ over $\mathbb{R}$). It can be shown that there is always only one absolute value on $\mathbb{C}$ extending the usual one on $\mathbb{R}$, and this is how we give $\mathbb{C}$ a topological structure of normed field. Since the topology of $\mathbb{C}$ determines the subfield $\mathbb{R}$ as the closure of $\mathbb{Q}$, this subfield is intrinsic to $\mathbb{C}$ with its topology, and Galois($\mathbb{C}/\mathbb{R}$) permutes the two solutions to $T^2 + 1 = 0$. No canonical mathematical construction should depend on a choice of solution to this equation (though constructions may use such a choice if the end result is independent of the choice, such as in the statement of the residue formula in complex analysis).

2. Main result

With the motivation and background set up, it is time to prove the main result. We begin with some notation. Fix $n \geq 1$ and $K_n/\mathbb{Q}$ a splitting field of $X^n - 1$. Define

$$\Phi_n(X) = \prod_{\zeta \in K_n[X]}(X - \zeta),$$
where \( \zeta \) runs over all primitive \( n \)th roots of unity in \( K_n \), (i.e., all generators of the intrinsic order \( n \) cyclic group of solutions to \( T^n - 1 = 0 \) in \( K_n \)). It is clear from the intrinsic nature of primitive \( n \)th roots of unity that the action of \( \text{Gal}(K_n/\mathbb{Q}) \) permutes these around. Hence, even without knowing if \( \text{Gal}(K_n/\mathbb{Q}) \) is \enquote{\text{\big}\text{big}}, it is clear that the monic polynomial \( \Phi_n(X) \) is \enquote{\text{\textit{invariant}}} under the action of \( \text{Gal}(K_n/\mathbb{Q}) \) (which just shuffles its linear factors under the natural action on \( K_n[X] \)). Hence, by Galois theory (!) the coefficients of \( \Phi_n \) must lie in \( \mathbb{Q} \). Its degree is clearly \( \left( \left[ \mathbb{Z}/n\mathbb{Z} \right] \right)^* \). The main aim is therefore to prove:

**Theorem 2.1.** (Gauss) The polynomial \( \Phi_n \in \mathbb{Q}[X] \) is irreducible.

**Proof.** By construction, \( \Phi_n \in \mathbb{Q}[X] \) is monic, and over the extension field \( K_n \) we see that \( \Phi_n \) divides \( X^n - 1 \). Since formation of gcd commutes with extension of the ground field, the divisibility \( \Phi_n \vert (X^n - 1) \) in \( \mathbb{Q}[X] \) must hold because it is true in \( K_n[X] \) (i.e., \( \Phi_n \) serves as a gcd of \( \Phi_n \) and \( X^n - 1 \)). By Gauss’ Lemma, since \( X^n - 1 \in \mathbb{Q}[X] \) has integral coefficients, any \enquote{monic factorization} in \( \mathbb{Q}[X] \) is necessarily in \( \mathbb{Z}[X] \). That is, if we write \( X^n - 1 = \Phi_n h \) with \( h \in \mathbb{Q}[X] \), then since \( h \) is visibly monic (as \( X^n - 1 \) and \( \Phi_n \) are monic) it follows that both \( \Phi_n \) and \( h \) must lie in \( \mathbb{Z}[X] \).

Now suppose that \( \Phi_n \) is not irreducible in \( \mathbb{Q}[X] \), so there is a factorization \( \Phi_n = fg \) in \( \mathbb{Q}[X] \) with monic \( f \) and \( g \) of positive degree. We may also suppose \( f \) is irreducible. By Gauss’ Lemma applied to the monic factorization \( f g = \Phi_n \) with \( \Phi_n \in \mathbb{Z}[X] \), we must have \( f, g \in \mathbb{Z}[X] \). We seek to derive a contradiction. In \( K_n[X] \) we have the monic factorization \( \Phi_n = \prod(X - \zeta) \) where the product runs over all \textit{primitive} \( n \)th roots of unity in \( K_n \). Since \( f \) and \( g \) both have positive degree, there must exist \textit{distinct} primitive \( n \)th roots of unity \( \zeta \) and \( \zeta' \) in \( K_n \) such that \( X - \zeta \) is a factor of \( f \) and \( X - \zeta' \) is a factor of \( g \); that is, \( f(\zeta) = 0 \) and \( g(\zeta') = 0 \) in \( K_n \).

We can write \( \zeta' = \zeta^r \) for some unique \( r \in \left( \mathbb{Z}/n\mathbb{Z} \right)^* \) since \( \zeta \) and \( \zeta' \) are both primitive \( n \)th roots of unity. Since \( \zeta \neq \zeta' \), we must have \( r \neq 1 \). Choose a positive integer representing this residue class \( r \), and again denote it by \( r \), so \( r > 1 \) and \( \text{gcd}(r, n) = 1 \). Consider the prime factorization \( X = \prod p_j \) with primes \( p_j \) not necessarily pairwise distinct. To go from \( \zeta \) to \( \zeta' = \zeta^r \) we successively raise to exponents \( p_1 \), then \( p_2 \), etc. Since \( f(\zeta) = 0 \) and \( g(\zeta') = 0 \), so \( f(\zeta^r) \neq 0 \) and \( g(\zeta^r) \neq 0 \) (as the factorization \( \Phi_n = fg \) and separability of \( \Phi_n \) forces \( f \) and \( g \) to have no common roots), there must exist a least \( j \) for which \( \zeta^{p_1 \cdots p_j n} \) is a root of \( f \) and its \( p_j \)th power is a root of \( g \). In other words, we can find a primitive \( n \)th root of unity \( \zeta_0 \) and a prime \( p \) not dividing \( n \) such that \( f(\zeta_0) = 0 \) and \( g(\zeta_0^r) = 0 \). From this fact we shall deduce a contradiction.

Since \( f \) is irreducible over \( \mathbb{Q} \), it must be the minimal polynomial of \( \zeta_0 \). But \( g(\zeta_0^r) = 0 \), so \( g(X^p) \in \mathbb{Q}[X] \) has \( \zeta_0 \) as a root. Thus, \( f | g(X^p) \) is \( \mathbb{Q}[X] \). We can therefore write \( g(X^p) = f q \) in \( \mathbb{Q}[X] \), with \( q \) necessarily monic (as \( g(X^p) \) and \( f \) are monic). Since \( g(X^p) \) has coefficients in \( \mathbb{Z} \), Gauss’ Lemma once again ensures that \( q \in \mathbb{Z}[X] \). Thus, the identity \( g(X^p) = f q \) takes place in \( \mathbb{Z}[X] \). Now reduce mod \( p \) in \( \mathbb{F}_p[X] \); we get

\[
\overline{f} \overline{q} = \overline{g}(X^p) \Rightarrow \overline{g}(X^p) = \overline{g}(X^p),
\]

the final equality using the fact that \( a^p = a \) for all \( a \in \mathbb{F}_p \). The monicity of \( f \) and \( g \), coupled with the condition that both have positive degree, ensures that \( \overline{f}, \overline{g} \in \mathbb{F}_p[X] \) have \enquote{positive degree} (though may well be reducible). From the divisibility relation \( \overline{f} \overline{g} \) leads to the conclusion that \( \overline{f} \overline{g} \) must have a non-trivial reducible factor in common. Hence, the product \( \overline{f} \overline{g} \) has a non-trivial irreducible factor appearing with multiplicity more than \( 1 \). But in \( \mathbb{Z}[X] \) we have \( f q = \Phi_n((X^n - 1) \text{ mod } p) \), so by Gauss’ Lemma we even get \( f | g((X^n - 1) \text{ mod } p) \), so we may reduce mod \( p \) to get \( \overline{f} \overline{g}|(X^n - 1) \text{ mod } p \). It follows that \( X^n - 1 \in \mathbb{F}_p[X] \) has a non-trivial square factor and hence is not separable. But this is absurd, since \( p \) doesn’t divide \( n \) and hence the derivative test ensures that \( X^n - 1 \in \mathbb{F}_p[X] \) is separable! Contradiction.

Note that although the \( \Phi_n \)'s were constructed abstractly, they’re easy to compute explicitly in \( \mathbb{Z}[X] \). In fact, since each \( n \)th root of unity is a primitive \( d \)th root of unity for a unique \( d \), we obviously have \( X^n - 1 = \prod_{d|n} \Phi_d(X) \). This allows a computer to recursively compute \( \Phi_d(X) \) by long division using \( X^n - 1 \) and \( \Phi_d(X) \)'s for proper divisors \( d \) of \( n \); the abstract theory is needed to prove that when \( 2 \) is known for all \( d < n \), then \( \prod_{d|n, d < n} \Phi_d \) actually divides \( X^n - 1 \) in \( \mathbb{Q}[X] \); by thinking about the root structure in a splitting field, such a divisibility claim is obvious (without thinking about root structure in a big extension, such issues become quite tedious to handle).