§2.6: Finite fields

Consider the field $\mathbb{F}_p$, and some fixed algebraic closure $\overline{\mathbb{F}}_p$. There are no nontrivial automorphisms of $\mathbb{F}_p$, since if $f$ is an automorphism of $\mathbb{F}_p$, and $i \in \mathbb{F}_p$ for $0 \leq i \leq p - 1$, then

$$f(i) = f \left( \underbrace{\overline{1} + \cdots + \overline{1}}_{\text{i times}} \right) = f(\overline{1}) + \cdots + f(\overline{1}) = \overline{1} + \cdots + \overline{1} = \overline{i}.$$ 

It follows that when computing the group of homomorphisms from one extension of $\mathbb{F}_p$ to another such extension, we do not need to worry about checking that these homomorphisms fix the base field.

We now consider a finite extension $L/\mathbb{F}_p$. Let $n$ be the dimension of this extension. Then we can choose a basis $\alpha_1, \ldots, \alpha_n$ of $L$ over $\mathbb{F}_p$. By the definition of a basis, every element in $L$ has a unique expression in the form $\sum_{i=1}^{n} x_i \alpha_i$, for $x_1, \ldots, x_n \in \mathbb{F}$; each such sum is an element of $L$, so $|L| = p^n$. Since $L \overset{\text{def}}{=} L \setminus \{0\}$ is a group under the multiplication operation of $L$, Lagrange’s theorem implies that for all $\alpha \in L^*$, $\alpha^{p^n - 1} = 1$, so $\alpha^{p^n} = \alpha$. By the obvious degree argument, the roots of $f(x) \overset{\text{def}}{=} x^{p^n} - x$ must be the exactly elements of $L$. (The distinctness of the roots of $f$ can also be seen by noting that $f' = -1$ is nonzero on $L$, but this seems unnecessary for our purposes.)

(Given a polynomial $f(x)$ in some polynomial ring $k[x]$, we say that $\alpha \in k$ is a multiple root of $f$ if, for some $g(x) \in k[x]$, $f(x) = (x - \alpha)^2g(x)$. It is a general fact that a nonzero polynomial $f(x)$ has multiple roots if and only if $(f, f') \neq 1$. To see this, say that $f(x) = (x - \alpha)^2g(x)$ for some element $\alpha \in k$ and polynomial $g(x) \in k[x]$. Then by the product rule, $f'(x) = (x - \alpha)(2g(x) + (x - \alpha)g'(x))$, so $(x - \alpha)$ divides $(f, f')$. We can say something more specific if $f$ is assumed to be irreducible. Say that $\alpha$ is a multiple root of $f$. Then $f$ is the irreducible polynomial of $\alpha$. As shown above, $\alpha$ is also a root of $f'$, so since the degree of $f'$ is strictly less than that of $f$, $f'$ must be zero; equivalently, the base field must be of characteristic $p > 0$, and $f(x)$ must be a polynomial in $x^{p^k}$.)

Since $L$ is exactly the set of roots of $x^{p^n} - x$, $L$ is the splitting field of $x^{p^n} - x$. Note that if $L$ exists, it is the unique splitting field of $x^{p^n} - x$, as long as we restrict ourselves to work within the fixed algebraic closure $\overline{\mathbb{F}}_p$.

**Theorem 1.** For some $p \in \mathbb{N}$, consider $\mathbb{F}_p$ and fix some algebraic closure $\overline{\mathbb{F}}_p$. For all $n \in \mathbb{N}$ there exists a unique subfield of $\overline{\mathbb{F}}_p$ containing $p^n$ elements. This field, $\mathbb{F}_{p^n}$, is the splitting field of $x^{p^n} - x$.

**Proof.** First, to prove existence. Let $\mathbb{F}_{p^n}$ be the set of roots of the polynomial $x^{p^n} - x$ in $\overline{\mathbb{F}}_p$. As discussed above, $\mathbb{F}_{p^n}$ is then of cardinality $p^n$. Consider a quick lemma.

**Lemma 1.** For all fields $F$ of characteristic $p \in \mathbb{N}$, $m \in \mathbb{N}$, $\alpha, \beta \in F$, $(\alpha + \beta)^{p^m} = \alpha^{p^m} + \beta^{p^m}$.

**Proof of lemma.** By induction on $m$. For $m = 1$, this follows from the fact that $p$ divides $\binom{p}{i}$ for all $1 \leq i \leq p - 1$. Next, say that the claim holds up to, but not including, some $m \geq 2$. Then

$$(\alpha + \beta)^{p^m} = \left( \alpha^{p^{m-1}} + \beta^{p^{m-1}} \right)^p = \alpha^{p^m} + \beta^{p^m},$$

again using the binomial formula.

\[ \text{Date: January 20, 2010.} \]
It follows that for $\alpha, \beta \in \mathbb{F}_{p^n}$,

$$(\alpha + \beta)^{p^n} - (\alpha + \beta) = \left(\alpha^{p^n} + \beta^{p^n}\right) - (\alpha + \beta) = 0,$$

so $\mathbb{F}_{p^n}$ is closed under addition. It is closed under multiplication as well, since

$$(\alpha\beta)^{p^n} - \alpha\beta = \alpha^{p^n}\beta^{p^n} - \alpha\beta = 0.$$

Since 0 and 1 are clearly in $\mathbb{F}_{p^n}$, this shows that $\mathbb{F}_{p^n}$ is a subfield of $\mathbb{F}_p$. (Incidentally, this argument also proves that $p$ divides $\binom{p^n}{i}$ for all $n \in \mathbb{N}$ and $1 \leq i \leq p^n - 1$.)

The uniqueness of such a field is obvious: each of its elements must be a root of $x^{p^n} - x$, so it must be a subfield of $\mathbb{F}_{p^n}$; by the obvious cardinality argument, uniqueness follows.

**Corollary 1.** The field $\mathbb{F}_{p^n}$ is Galois over $\mathbb{F}_p$.

**Proof.** The claim is well-formulated, since $\mathbb{F}_{p^n}$ is well-defined after fixing an algebraic closure of $\mathbb{F}_p$. Furthermore, the claim is immediate, since $\mathbb{F}_{p^n}$ is the splitting field of a polynomial which has no multiple roots.

An obvious task, then, is to determine $\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. The proof is by construction. Let $\varphi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ send $x$ to $x^p$ ("the Frobenius automorphism")

**Claim 1.** $\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \simeq \langle \varphi \rangle$; that is, $\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \simeq \mathbb{Z}/n\mathbb{Z}$.

**Proof.** Since $\mathbb{F}_{p^n}$ is a Galois extension of degree $n$ over $\mathbb{F}_p$, $|\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)| = n$. Since $\varphi^n = \text{Id}_{\mathbb{F}_{p^n}}$, it only remains to show that for $1 \leq d \leq n - 1$, $\varphi^d \neq \text{Id}_{\mathbb{F}_{p^n}}$. We prove this by contradiction: say that for some $1 \leq d \leq n - 1$, $\varphi^d = \text{Id}_{\mathbb{F}_{p^n}}$. Then for all $\alpha \in \mathbb{F}_{p^n}$, $\alpha$ is a root of $x^{p^d} - x$, contradicting the fact that $x^{p^d} - x$ has exactly $p^d$ distinct roots.

**Corollary 2.** Fix $\overline{\mathbb{F}_p}$. For all $m \in \mathbb{N}$, there exists a unique extension $L$ of $\mathbb{F}_{p^n}$ of degree $m$.

**Proof.** Such an extension would have $p^{mn}$ elements, so if there exists such an $L$, it is unique, by Theorem 1. Such an $L$ certainly does exist: consider the splitting field of $x^{p^m} - x$ in $\overline{\mathbb{F}_p}$. An obvious inductive argument shows that $L$ contains $\mathbb{F}_{p^n}$.

**Corollary 3.** If $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$, then $n | m$.

**Proof.** This follows from the previous corollary.

---

**§2.7: Examples**

Fix a base field $k$, with $\text{char} \ k \neq 2, 3$, and consider a cubic $f(x) = ax^3 + bx^2 + cx + d$. By considering $\frac{1}{3} f \left( x - \frac{b}{3} \right)$, well-defined since $\text{char} \ k \neq 3$, we may assume without loss of generality that $f$ is monic and has no quadratic term. (An easy check shows that such a normalization leaves the splitting field of this polynomial unchanged.) If $f$ has any roots in $k$, then it is reducible, so say that $f$ has no roots in $k$. Every nontrivial factorization of $f$ has a term of degree 1, so it follows that $f$ must be irreducible over $k$. Furthermore, $f$ has no multiple roots in the algebraic closure of $k$, since the leading coefficient of $f'(x)$ is 3, which is nonzero under the assumption that $\text{char} \ k \neq 3$.

Let $\alpha$ be a root of $f$. Then $[k(\alpha) : k] = 3$. Let $K$ be the splitting field of $f$. Then by the previous paragraph, $K$ is separable over $k$. Normality is immediate, so $K$ is a Galois extension of $k$. By the multiplicativity of degree, 3 divides the order of $\text{Gal}(K/k)$. Since $\text{Gal}(K/k)$ is a subgroup of $S_3$, it follows that $\text{Gal}(K/k)$ is either $A_3 \simeq \mathbb{Z}/3\mathbb{Z}$ or $S_3$.

Denote the roots of $f$ by $\alpha_1, \alpha_2, \alpha_3$, define $\delta = (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_1 - \alpha_3)$, and define $\Delta = \delta^2$ ("the discriminant of $f$'s"). For $\sigma \in \text{Gal}(K/k)$, $\sigma(\delta)$ is either $\delta$ or $-\delta$, so $\Delta$ is fixed under the action of $\text{Gal}(K/k)$. It follows that $\Delta$ is an element of the base field $k$. Since $\text{char} \ k \neq 2$, and since the roots of $f$ are distinct, $\delta \neq -\delta$, so an element $\sigma$ of $\text{Gal}(K/k)$ fixes $\delta$ if and only $\sigma$ is even when regarded as an element of $S_3$. It follows that $\text{Gal}(K/k)$ is the symmetric group if and only if $\Delta$ does not have a square root in $k$. 
In fact, both possibilities for the Galois group do occur. Recall the following degree diagram:

\[
\begin{array}{ccc}
\mathbb{Q} \left( e^{\frac{2\pi i}{3}}, \sqrt[3]{2} \right) & \mathbb{Q} \left( e^{\frac{2\pi i}{3}} \right) & \mathbb{Q} \left( \sqrt[3]{2} \right) \\
\mathbb{Q} & \mathbb{Q} & \mathbb{Q}
\end{array}
\]

Consider the left-hand legs. Every extension is separable, since every field in question is of characteristic zero. The full extension \( \mathbb{Q} \left( e^{\frac{2\pi i}{3}}, \sqrt[3]{2} \right) / \mathbb{Q} \) is normal, since it is the splitting field of \( x^3 - 2 \in \mathbb{Q}[x] \); since normality is preserved under lifting, the extension \( \mathbb{Q} \left( e^{\frac{2\pi i}{3}}, \sqrt[3]{2} \right) / \mathbb{Q} \left( e^{\frac{2\pi i}{3}} \right) \) is also normal. It follows that both \( \mathbb{Q} \left( e^{\frac{2\pi i}{3}}, \sqrt[3]{2} \right) / \mathbb{Q} \) and \( \mathbb{Q} \left( e^{\frac{2\pi i}{3}}, \sqrt[3]{2} \right) / \mathbb{Q} \left( e^{\frac{2\pi i}{3}} \right) \) are Galois. We can now conclude that the Galois group of the splitting field of \( x^3 - 2 \) over \( \mathbb{Q} \left( e^{\frac{2\pi i}{3}} \right) \) is of cardinality 3, thus isomorphic to \( \mathbb{Z}/3\mathbb{Z} \), while the Galois group of the splitting field of \( x^3 - 2 \) over \( \mathbb{Q} \) is of cardinality 6, thus isomorphic to \( S_3 \).

The bottom extension \( \mathbb{Q} \left( e^{\frac{2\pi i}{3}} \right) / \mathbb{Q} \) is normal, since it is of degree 2. An analogous characterization for the quartic case exists, but it is more complicated, since there are 5 subgroups of \( S_4 \) of order divisible by 4. No such characterization exists for polynomials of degree 5 and higher, so we restrict ourselves to the question of when the Galois group of a splitting field of a polynomial \( f \) of prime degree \( p \) is all of \( S_p \). When working over \( \mathbb{Q} \), there is a straightforward sufficient condition:

**Proposition 1.** If \( f(x) \in \mathbb{Q}[x] \) is of prime degree \( p \), is irreducible, and has exactly two nonreal roots, then the Galois group \( G \) of the splitting field \( L \) of \( f \) is \( S_p \).

**Proof.** Let \( \alpha \) be some root of \( f \). Since \( f \) is the irreducible polynomial of \( \alpha \), \( |\mathbb{Q}(\alpha) : \mathbb{Q}| = p \), so \( p \) divides \( |L : \mathbb{Q}| \). By Sylow theory, \( G \) has an element of order \( p \). The order of an element of \( S_p \) is the least common multiple of the lengths of its component cycles, so since \( p \) is prime, \( (123 \cdots p) \in G \) after a possible relabeling of letters.

One algebraic closure of \( \mathbb{R} \) is \( \mathbb{C} \), so we can choose \( L \) to be a subfield of \( \mathbb{C} \). Conjugation is clearly a field automorphism of \( \mathbb{C} \), so it is also a field automorphism of \( L \). Furthermore, conjugation fixes \( \mathbb{Q} \), so the map \( z \mapsto \overline{z} \) is an element of \( G \). Since \( f \) has exactly two nonreal roots, it follows that \( G \) contains some transposition \( (rs) \).

By the fourth part of Exercise 38 from the first chapter of Lang, \( G \simeq S_p \), since \( p \) is prime.

Incidentally, both invocations of the primality of \( p \) were necessary. This is obvious in the first case, but perhaps not so in the second. Here is a counterexample to Lang’s Exercise 38 when \( p \) is not assumed to be prime: if \( x \overset{\text{def}}{=} (1234) \) and \( y \overset{\text{def}}{=} (13) \), then \( xy = yx^{-1} \) by computation, so every element of \( \langle x, y \rangle < S_4 \) can be written in the form \( x^a y^b \); it follows that \( \langle x, y \rangle \leq S_4 \).

**A reduction technique.** As Lang notes, reducing polynomials modulo prime numbers is a time-honored technique for obtaining elements in their Galois groups. This relies on the following theorem, which will not be proven until later in the course:

**Theorem 2.** Let \( f(x) \in \mathbb{Z}[x] \) be monic. Let \( p \) be a prime number, and \( \overline{f}(x) \in (\mathbb{Z}/p\mathbb{Z})[x] \) be the polynomial obtained by reducing the coefficients of \( f \) modulo \( p \). Assume that \( \overline{f} \) has no multiple roots in the algebraic closure of \( \mathbb{F}_p \). Then there exists a bijection

\[
(\alpha_1, \ldots, \alpha_n) \rightarrow (\overline{\alpha_1}, \ldots, \overline{\alpha_n})
\]
of the roots of $f$ onto those of $\overline{f}$, and an embedding
\[ \text{Gal} \left( (F_p \overline{f}) / F_p \right) \hookrightarrow \text{Gal} \left( \mathbb{Q}_f / \mathbb{Q} \right). \]

(It should be noted that if $\overline{f}$ has no multiple roots in the algebraic closure of $F_p$, then $f$ has no multiple roots in the algebraic closure of $\mathbb{Q}$.)

For example, consider $f(x) \equiv x^5 - x - 1$. Let $\overline{f}_5(x) \in \mathbb{F}_5[x]$ be $f$ reduced modulo 5. Then $\overline{f}_5(x) = -1$, so $\overline{f}_5$ has no multiple roots over $\mathbb{F}_5$. Furthermore, $\overline{f}_5(x)$ is irreducible. It seems that there is no slick way to show this, so we proceed with a mechanical argument by contradiction. Say that $\overline{f}_5(x) = gh$, for some nonunits $g, h \in \mathbb{F}_5[x]$. Neither can be of degree 1, since $\overline{f}_5(x)$ is nonzero on $\mathbb{F}_5[x]$ by computation. Thus $\deg g = 2$ and $\deg h = 3$, relabeling $g$ and $h$ if necessary. Normalizing $g$ and $h$ to be monic, we can write
\[ g(x) = x^3 + ax^2 + bx + c, \quad h(x) = x^2 + dx + e. \]

Expanding their product out, we have
\[ g(x)h(x) = x^5 + (a + d)x^4 + (b + ad + e)x^3 + (c + bd + ae)x^2 + (cd + be)x + ce. \]
This forces $d = -a$, which yields
\[ g(x)h(x) = x^5 + (b - a^2 + e)x^3 + (c + a(e - b))x^2 + (be - ac)x + ce. \]
This forces $b = a^2 - e$, which yields
\[ g(x)h(x) = x^5 + (c - a(2e - a^2))x^2 + (a(e - c) - e^2) + ce. \]
This forces $c = a(2b - a^2)$, which yields
\[ g(x)h(x) = x^5 + (3a^2e - a^4 - e^2)x + ae(a^2 - 2e). \]

Considering the linear term yields
\[ e = 3a^2, \]
where we have invoked Fermat’s little theorem to obtain $a^4 = 1$. The constant term of $gh$ is then zero, a contradiction. This shows that $\overline{f}_5$ is indeed irreducible, so the Galois group $G$ of $f$ over $\mathbb{Q}$ contains a 5-cycle.

On the other hand, let $\overline{f}_2(x) \in (\mathbb{F}_2)[x]$ be $f$ reduced modulo 2. Then $\overline{f}_2(x) = x^4 - 1$. At any root $x_0$ of $\overline{f}_2$, we have $x_0^4 = 1$, so
\[ \overline{f}_2(x_0) = x_0^5 - x_0 - 1 = -1 \neq 0; \]
that is, $\overline{f}_2$ has no multiple roots over $\mathbb{F}_2$. A computation shows that
\[ \overline{f}_2(x) = (x^3 + x^2 + 1)(x^2 + x + 1), \]
and since another check shows that $\overline{f}_2$ is nonzero on $\mathbb{F}_2$, each of the terms in this factorization must be irreducible, since any nontrivial factorization of either a quadratic or a cubic necessarily involves a linear term.

Recall a theorem from Lang:

**Theorem 3.** Let $K_1$ and $K_2$ be Galois extensions of a field $k$, with Galois groups $G_1$ and $G_2$, respectively. Assume $K_1, K_2$ are subfields of some field. Then $K_1K_2$ is Galois over $k$. Let $G$ be its Galois group. Map $G \to G_1 \times G_2$ by restriction, namely
\[ \sigma \mapsto (\sigma|_{K_1}, \sigma|_{K_2}). \]
This map is injective. If $K_1 \cap K_2 = k$ then this map is an isomorphism.

Let $K, K_1,$ and $K_2$ be the splitting fields of $f(x) = (x^3 + x^2 + 1)(x^2 + x + 1), x^3 + x^2 + 1, \text{ and } x^2 + x + 1,$ respectively, over $\mathbb{Q}$. Let $G, G_1,$ and $G_2$ be the Galois groups of $K = K_1K_2, K_1,$ and $K_2$, respectively, over $k$. It follows from the theorem that to show that $G$ contains a transposition, it suffices to show that $K_1 \cap K_2 = k$. (This argument will be completed in the next iteration of these notes.)

Since 5 is prime, it follows that the Galois group of $x^5 - x - 1$ over $\mathbb{Q}$ is $S_5$. 


Let \( k \) be a field of characteristic \( p \geq 0 \) and let \( \mu_n \subset \overline{k} \) be the roots of the polynomial \( f(x) \overset{\text{def}}{=} x^n - 1 \). This set is obviously a group under the multiplication operation inherited from \( \overline{k} \). We define an element \( \xi \in \mu_n \) to be primitive if it generates \( \mu_n \) as a group; equivalently, \( \xi \in \mu_n \) is primitive if, for all \( d \mid n \), \( \xi^d \neq 1 \).

Note that for a given field and integer \( n \), there need not be any primitive elements of \( \mu_n \). For instance, \( x^p - 1 = (x - 1)^p \) over \( \mathbb{F}_p \).

**Proposition 2.** If \( \xi \) is a primitive \( n \)-th root of unity with \( (p, n) = 1 \), then:

1. \( k(\xi)/k \) is Galois;
2. \( |k(\xi) : k| = \varphi(n) \);
3. \( \text{Gal}(k(\xi)/k) < (\mathbb{Z}/n\mathbb{Z})^* \);
4. \( |\mathbb{Q}(\xi) : \mathbb{Q}| = \varphi(n) \); and
5. \( \text{Gal}(\mathbb{Q}(\xi)/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^* \).

**Proof.**
1. Since \( (p, n) = 1 \), \((x^n - 1)^p = nx^{n-1} \) is zero only at zero, which is not an \( n \)-th root of unity, so \( k(\mu_n)/k = k(\xi)/k \) is separable. Furthermore, \( k(\xi)/k \) is normal, as it equals the splitting field \( k(\mu_n)/k \) of \( x^n - 1 \).
2. An element \( \sigma \in \text{Gal}(k(\xi)/k) \) is uniquely determined by its action on \( \mu_n \cong \mathbb{Z}/n\mathbb{Z} \), and, furthermore, it is clear that \( \text{Gal}(k(\xi)/k) \) determines a left action on \( \mathbb{Z}/n\mathbb{Z} \). Thus \( \text{Gal}(k(\xi)/k) \) is a subgroup of \( \text{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^* \). Finally, \( (\mathbb{Z}/n\mathbb{Z})^* = \varphi(n) \).
4. Let \( \Phi_n(x) = \text{Irr}(\xi, \mathbb{Q}) \). By the previous paragraph, it suffices to prove that \( \text{deg} \Phi_n = \varphi(n) \). Consider the following lemma.

**Lemma 2.** Let \( q \) be a prime that does not divide \( n \). Then \( \xi^q \) is a root of \( \Phi_n \).

**Proof of lemma.** Choose \( g \in \mathbb{Q}[x] \) so that \( x^n - 1 = \Phi_n(x)g(x) \). Say that \( \Phi_n(\xi^q) \neq 0 \). Then \( g(\xi^q) = 0 \), so \( \xi \) is a root of \( G(x) \overset{\text{def}}{=} g(x^q) \). We now reduce modulo \( q \). Let \( \overline{\Phi}_n, \overline{\xi}, \overline{G} \in \mathbb{F}_q[x] \) be the results of reducing \( \Phi_n, \xi, G \), respectively. Then \( \overline{G}(x) = \overline{G}(x^q) = (\overline{G}(x))^q \). It follows that \( \overline{\Phi}_n \) and \( \overline{G} \) share a common root, so \( x^n - 1 \in \mathbb{F}_q[x] \) has a multiple root. But since \( (q, n) = 1 \), \((x^n - 1)^q = nx^{n-1} \) is nonzero on \( \mathbb{F}_q \). Zero is certainly not a root of \( x^n - 1 \), so \( x^n - 1 \) has no multiple roots over \( \mathbb{F}_q[x] \), a contradiction.

If \( 1 \leq r \leq n - 1 \) is coprime to \( n \), then it can be written as a product of primes that do not divide \( n \). That is, each primitive \( n \)-th root of unity can be obtained by raising \( \xi \) to a succession of powers, each of which is a prime number not dividing \( n \). By the lemma and the fact that \( \text{char} \mathbb{Q} = 0 \), it follows that \( \text{deg} \Phi_n \geq \varphi(n) \). It now follows from the second part of this proposition that \( \text{deg} \Phi_n = \varphi(n) \).

We now note a more explicit expression for \( \Phi_n \). Again using the fact that \( \mathbb{Q} \) is of characteristic zero,

\[
x^n - 1 = \prod_{\xi \in \mathbb{Q}, \xi^n = 1} (x - \xi).
\]

Given \( \xi \in \mathbb{C} \), let \( \text{ord} \xi \) be the minimal natural number \( d \) such that \( \xi^d = 1 \). By convention, if there is no such natural number for a given complex number \( \xi \), we say that \( \text{ord} \xi = 0 \). Clearly an \( n \)-th root of unity is primitive if and only if it is of order \( n \), so by Lemma 2,

\[
\Phi_d(x) = \prod_{\text{ord} \xi = d} (x - \xi).
\]

Since every \( n \)-th root of unity is of some unique order between 1 and \( n \) dividing \( n \),

\[
x^n - 1 = \prod_{d \mid n} \Phi_d(x).
\]

Rearranging,

\[
\Phi_n(x) = \frac{x^n - 1}{\prod_{d \mid n, d \nmid n} \Phi_d(x)}.
\]
It can be shown from (1) by induction on \( n \) that \( \Phi_n(x) \) is a polynomial over \( \mathbb{Z} \). To see this, note first that the \( n = 1 \) case is trivial. Now, assume that the claim has been proven up to, but not including, some \( n \geq 2 \). By the inductive hypothesis, \( \prod_{d | n, d < n} \Phi_d(x) \) is a polynomial over \( \mathbb{Z} \). Since \( \prod_{d | n, d < n} \Phi_d(x) \) is monic, it follows from Lang’s Theorem 1.1 from §4, which shows that \( \mathbb{Z}[x] \) is nearly a Euclidean domain, that there exist polynomials \( f(x), g(x) \in \mathbb{Z}[x] \) such that

\[
x^n - 1 = \left( \prod_{d | n, d < n} \Phi_d(x) \right) f(x) + g(x),
\]

with \( \deg g < n - \varphi(n) \). The polynomials \( x^n - 1 \) and \( \prod_{d | n, d < n} \Phi_d(x) \) share \( n - \varphi(n) \) distinct roots, so \( g \) must also share these roots. It follows that \( g \) must be identically zero, and \( f \) must be equal to \( \Phi_n \).

The fact that the cyclotomic polynomials have integer coefficients can also be proven using Gauss’s lemma, though the notion of content must be expanded so as to be well-defined on fraction fields.

§2.9: KUMMER THEORY

**Definition 1.** Let \( K/k \) be Galois. Then \( K/k \) is cyclic (resp. Abelian) if \( \text{Gal}(K/k) \) is cyclic (resp. Abelian).

We will build up to the following theorem, which can be thought of as the Fundamental Theorem of Kummer Theory.

**Theorem 4.** Say that \( \text{char} \ k = p \geq 0 \) and \( (p,n) = 1 \); say also that \( k \) contains some primitive \( n \)-th root of unity \( \xi \). If \( K/k \) is a cyclic Galois extension of degree \( n \), then for some \( \alpha \in K \), \( K = k(\alpha) \), and \( \alpha^n \in k \). Conversely, if \( \alpha^n \in k \), then \( k(\alpha) \) is cyclic over \( k \) and of degree \( d \), where \( d \) is some divisor of \( n \).

First, we construct two useful tools.

**Definition 2.** Let \( L/k \) be a finite separable extension, fix an algebraic closure \( \overline{k} \) of \( k \), and let \( \sigma_1, \ldots, \sigma_n \) be the set of embeddings of \( L \) in \( \overline{k} \) that fix \( k \). (Since \( L/k \) is finite, there are only finitely many such embeddings.)

Given \( \alpha \in L \), define the norm \( N_{L/k}(\alpha) \) to be \( \prod_{i=1}^n \sigma_i(\alpha) \); define the trace \( \text{Tr}_{L/k}(\alpha) \) to be \( \sum_{i=1}^n \sigma_i(\alpha) \).

We make two observations. First, if \( L/k \) is, furthermore, normal, then the product and sum in the definition of the norm and trace are taken over \( \text{Gal}(L/k) \). Second, say that for some \( \alpha \in \overline{k} \), \( L = k(\alpha) \). Let \( p(x) = \text{Irr} (\alpha, k) \). If

\[
p(x) = x^n - a_1 x^{n-1} + \cdots + (-1)^n a_n,
\]

then by the separability of \( L/k \), \( a_1 = \text{Tr}_{L/k}(\alpha) \) and \( a_n = N_{L/k}(\alpha) \).

**Proposition 3.** If \( L/k \) is finite and separable, then \( N_{L/k} \) is a group homomorphism of \( L^* \) into \( k^* \). Furthermore, the norm and trace are transitive. That is, if \( k \subset E \subset L \) is a tower of separable extensions, then

\[
N_{L/k} = N_{E/k} \circ N_{L/E}, \quad T_{L/k} = T_{E/k} \circ T_{L/E}.
\]

**Proof.** Homework.

We now move on to a discussion of characters.

**Definition 3.** If \( G \) is a group and \( k \) is a field, then a group homomorphism \( \chi : G \rightarrow k^* \) is a character of \( G \) on \( k \). (Those who know some representation theory can see that \( \chi \) is a one-dimensional representation of \( G \) on \( k \).)

**Example 1.** Consider a homomorphism \( \chi : \mu_n \rightarrow k^* \). Let \( \sigma \in \overline{k} \) be a generator of the multiplicative group \( \mu_n \). Then \( (\chi(\sigma))^n = \chi(\sigma^n) = 1 \), so \( \chi \) must send \( \sigma \) to an \( n \)-th root of unity. Furthermore, since \( \sigma \) generates \( \mu_n \), \( \chi \) is uniquely determined by \( \chi(\sigma) \). Indeed, there is a bijective correspondence between \( \mu_n \) and the characters of \( \mu_n \) on \( k \).

**Example 2.** If \( K/k \) is Galois, then every element of \( \text{Gal}(K/k) \) is a character of \( K^* \) on \( K \).

**Theorem 5** (Artin’s theorem on the linear independence of characters). If \( \chi_1, \ldots, \chi_n \) are distinct homomorphisms from \( G \) to \( k^* \), then \( \{\chi_1, \ldots, \chi_n\} \) is linearly independent over \( k \).
Proof. By contradiction. Suppose that for some distinct \(\chi_1, \ldots, \chi_n : G \to k^*\) and \(a_1, \ldots, a_n \in k\), with not all of \(a_1, \ldots, a_n\) zero, \(\sum_{i=1}^n a_i \chi_i = 0\). By discarding those characters with zero coefficients, we can assume without loss of generality that each \(a_i\) is nonzero. Since these characters are distinct, there exists \(z \in G\) with \(\chi_1(z) \neq \chi_2(z)\). By assumption on this linear combination of characters, for all \(g \in G\),

\[
a_1 \chi_1(z)g + a_2 \chi_2(z)g + \cdots + a_n \chi_n(z)g = 0.
\]

It follows that

\[(2) \quad a_1 \chi_1(z) + a_2 \chi_2(z) + \cdots + a_n \chi_n(z) = 0.\]

Again by assumption,

\[
a_1 \chi_1(g) + a_2 \chi_2(g) + \cdots + a_n \chi_n(g) = 0,
\]

so

\[(3) \quad a_1 \chi_1(z) + a_2 \chi_2(z) + \cdots + a_n \chi_n(z) = 0.\]

Subtracting (3) from (2) yields

\[
a_2 (\chi_1(z) - \chi_2(z)) + a_n (\chi_1(z) - \chi_n(z)) = 0.
\]

That is,

\[
\sum_{i=2}^n a_i (\chi_1(z) - \chi_i(z)) \chi_i
\]

is identically zero. By our choice of \(z\), not all the coefficients in this linear combination are zero, so \(\{\chi_2, \ldots, \chi_n\}\) is linearly dependent. Repeating this argument, it follows that \(\{\chi_n\}\) is linearly dependent, so \(\chi_n\) is identically zero, a contradiction, since every homomorphism from \(G\) to \(k^*\) must send \(1_G\) to \(1_k\). \(\square\)

Inhale; exhale the delicate fragrance of mathematical grace.

**Theorem 6** (Hilbert’s Theorem 90). Say that \(L/k\) is finite and Galois, with \(\text{Gal}(L/k) = \langle \sigma \rangle \simeq \mathbb{Z}/n\mathbb{Z}\). Then \(N_{L/k}(\beta) = 1\) if and only if \(\beta = \alpha/\sigma(\alpha)\) for some \(\alpha \in L\).

**Remark 1.** For those who have seen some cohomology theory, Hilbert’s Theorem 90 can be reformulated as the statement that \(H^1(G, L^*) = 1\).

**Proof.** The reverse implication is obvious, since if \(\beta = \alpha/\sigma(\alpha)\), then

\[
N_{L/k}(\beta) = \frac{N_{L/k}(\alpha)}{N_{L/k}(\sigma(\alpha))} = \frac{\prod_{i=0}^{n-1} \sigma^i(\alpha)}{\prod_{i=0}^{n-1} \sigma^{i+1}(\alpha)} = 1.
\]

Conversely, fix \(\beta \in L\) of norm 1 and define a map \(f : L \to L\) by

\[
f(\theta) = \theta + \beta \sigma(\theta) + \beta \sigma(\beta) \sigma^2(\theta) + \cdots + \beta \sigma(\beta) \cdots \sigma^{n-2}(\beta) \sigma^{n-1}(\theta).
\]

Then

\[
\beta \sigma(f(\theta)) = \beta \sigma(\theta) + \beta \sigma(\beta) \sigma^2(\theta) + \cdots + \beta \sigma(\beta) \cdots \sigma^{n-2}(\beta) \sigma^{n-1}(\theta) + \beta \sigma(\beta) \cdots \sigma^{n-1}(\beta) \sigma^n(\theta)
\]

\[
= \theta + \beta \sigma(\theta) + \beta \sigma(\beta) \sigma^2(\theta) + \cdots + \beta \sigma(\beta) \cdots \sigma^{n-2}(\beta) \sigma^{n-1}(\theta)
\]

\[
= f(\theta).
\]

Here we have used the fact that \(N_{L/k}(\beta) = 1\) and that \(\sigma^n\) is the identity on \(L\). By Artin’s theorem, \(f\) is not identically zero, so for some \(\theta_0 \in L\), \(f(\theta_0) \neq 0\). It follows that \(\beta = f(\theta_0)/\sigma(f(\theta_0))\). \(\square\)

We are now ready to prove Theorem 4.