Galois Theory

David Corwin

August 19, 2009

0 Preliminaries

Remark 0.1 (Notation)**.** $|G|$ denotes the order of a finite group G. $[E : F]$ denotes the degree of a field extension E/F. We write $H \leq G$ to mean that H is a subgroup of G, and $N \trianglelefteq G$ to mean that N is a normal subgroup of G. If E/F and K/F are two field extensions, then when we say that K/F is contained in E/F, we mean via a homomorphism that fixes F.

We assume the following basic facts in this set of notes, in addition to elementary number theory, group and ring theory, and linear algebra:

Fact 0.2. If F is a field, then $F[x]$ is a PID, so all nonzero prime ideals are maximal and are generated by a single irreducible polynomial. This irreducible polynomial is the polynomial of lowest positive degree in the ideal and is unique modulo units.

Fact 0.3. If α is an algebraic element in an extension E/F, then the set of polynomials in $F[x]$ which vanish at α is a prime ideal generated by an irreducible polynomial $f(x)$ (we can make this canonical by requiring $f(x)$ to be monic), and $F(\alpha) \cong F[x]/(f(x))$. This polynomial is called the *minimal polynomial* of α, as it has minimal positive degree in the ideal of polynomials vanishing at α.

Fact 0.4. If F and F' are isomorphic, and α and α' are algebraic elements in an extension which have the same minimal polynomial under the isomorphism, then we can extend the isomorphism of F and F' to an isomorphism from $F(\alpha)$ to $F'(\alpha')$.

Fact 0.5 (Tower Law)**.** If E/K and K/F are two field extensions, then $[E : K][K : F] = [E : F]$.

Fact 0.6. A set of k linear homogenous equations over a field in n unknowns for $n > k$ always has a nontrivial solution.

1 Splitting Fields

Definition 1.1. Let F be a field and suppose $f(x) \in F[x]$. A field extension E/F is said to be a *splitting field* for $f(x)$ over F if: (a) We can write $f(x) =$

$(x-a_1)...(x-a_n)$ in $E[x]$. That is to say, $f(x)$ *splits* over E. (b) The elements $a_1, ..., a_n$ generate the extension E/F. Equivalently, $f(x)$ splits in no subfield of E.

Theorem 1.2 (Uniqueness of Splitting Fields)**.** *Let F and F' be fields isomorphic by σ. Then if E and E' are splitting fields for $p(x)$ and $p'(x)$ respectively, where $p(x)$ is sent to $p'(x)$ under σ, then there exists an isomorphism $\phi : E \to E'$ which equals σ when restricted to F.*

Proof. We use induction on the number n of roots n of $p(x)$ not in F. We can factor $p(x)$ as $f_1(x) \cdots f_r(x)$ and similarly $p'(x) = f_1'(x) \cdots f_r'(x)$ where the f_i and f_i' are irreducible, and f_i is sent to f_i' under the isomorphism of F and F'. If $n = 0$, then $E = F$, $E' = F'$, so σ gives our desired automorphism.

Assume the theorem for $n \leq k$ where $k \geq 0$. Suppose now that $p(x)$ has $k+1$ roots outside of f.

Since $k \geq 0$, there exists $\alpha \in E - F$ which is a root of $p(x)$, say WLOG it is a root of $f_1(x)$. Then $p(x) \in F(\alpha)[x]$, so since $p(x)$ splits in E, and its roots generate E over F and therefore $F(\alpha)$, it follows that E is a splitting field for $p(x)$ over $F(\alpha)$. Similarly, if α' is a root of $f_1'(x)$, then E' is a splitting field for $p'(x)$ over $F'(\alpha')$. We can extend σ to an isomorphism of $F(\alpha)$ and $F'(\alpha')$. Then since α lies in $F(\alpha)$ but not in F, the polynomial $p(x)$ has at most k roots outside of $F(\alpha)$, and similarly for $p'(x)$, so we get an extension of the isomorphism of $F(\alpha)$ and $F'(\alpha')$ to an isomorphism of E and E', concluding the proof. □

Remark 1.3. If E/F is an extension in which $p(x) \in F[x]$ splits, then the subfield of E/F generated by all the roots of $p(x)$ is a splitting field for $p(x)$ over F, and is hence isomorphic to any other splitting field for $p(x)$.

2 Group Characters

Definition 2.1. If G is a group and F a field, then a homomorphism from G into $F^\times$ is called a *character* of G in F.

Definition 2.2. A finite set of characters $\{\sigma_i : G \to F\}_{1 \leq i \leq n}$ is said to be *dependent* if there exist $\{x_i\}_{1 \leq i \leq n}$ not all zero such that

$$\sum_{i=1}^{n} x_i \sigma_i(g) = 0$$

for all $g \in G$. A set of characters is said to be *independent* if they are not dependent.

Theorem 2.3. *Any finite set of characters $\{\sigma_i : G \to F\}_{1 \leq i \leq n}$ from a group G into a field F is independent.*

Proof. Suppose they are dependent. We choose $\{x_i\}$ so that a minimal number of the x_i are nonzero, say WLOG the first k of them, so that we have $\sum_{i=1}^{k} x_k\sigma_k = 0$ where $k \leq n$. Note that $k \geq 2$, or else $\sigma_1(g) = 0$ for all g.

Since σ_1 and σ_k are distinct, we can find $a \in G$ such that $\sigma_1(a) \neq \sigma_k(a)$. Note that for any $g \in G$, we have

$$\sum_{i=1}^{n} x_i\sigma_i(ag) = \sum_{i=1}^{n} x_i\sigma_i(a)\sigma_i(g) = 0.$$

We also have

$$\sum_{i=1}^{k} x_i\sigma_k(a)\sigma_i(g) = 0.$$

Subtracting these equations, we get

$$\sum_{i=1}^{k} x_i(\sigma_i(a) - \sigma_k(a))\sigma_i(g) = 0.$$

This gives us a dependence relation on our characters since $\sigma_1(a) - \sigma_k(a) \neq 0$, but the coefficients of σ_k becomes 0, meaning this dependence relation has fewer nonzero coefficients, a contradiction. It follows that our characters are independent. □

Note that an automorphism of of a field E is a character from $E^\times$ into E. It follows from this theorem that a finite set of automorphisms of a field is independent.

This theorem will be very useful in establishing further facts.

3 Automorphisms and Degrees of Extensions

Definition 3.1. If $\sigma_1, \cdots, \sigma_n$ is a set of automorphisms of a field E, then the *fixed field* of these automorphisms is the set of $x \in E$ such that $\sigma_i(x) = \sigma_j(x)$ for all $1 \leq i, j \leq n$. Note that if one of the automorphisms is the identity, then F is the set of $x \in E$ such that $\sigma_i(x) = x$ for all $1 \leq i \leq n$. It's not too hard to show that F is a subfield of E.

Proposition 3.2. *If E is a field, $\sigma_1, \cdots, \sigma_n$ is a finite set of automorphisms of E, and F is the fixed field of the automorphisms $\sigma_1, \cdots, \sigma_n$, then $[E : F] \geq n$.*

Proof. Assume that there exists a spanning set $\omega_1, \cdots, \omega_r \in E$ for E over F with $r < n$. The r linear equations in n unknowns

$$\begin{aligned} x_1\sigma_1(\omega_1) + \cdots + x_n\sigma_n(\omega_1) &= 0 \\ &\cdots \\ x_1\sigma_1(\omega_r) + \cdots + x_n\sigma_n(\omega r) &= 0 \end{aligned}$$

has a nontrivial solution in E. If $\alpha = \sum_{i=1}^{r} a_i\omega_i$ with $a_i \in F$ is an arbitrary element of E, then

$$\begin{aligned}
\sum_{j=1}^{n} x_j\sigma_j(\alpha) &= \sum_{j=1}^{n} x_j\sigma_j\left(\sum_{i=1}^{r} a_i\omega_i\right) \\
&= \sum_{j=1}^{n}\sum_{i=1}^{r} x_j\sigma_1(a_i)\sigma_j(\omega_i) \\
&= \sum_{i=1}^{r}\sigma_1(a_i)\sum_{j=1}^{n} x_j\sigma_j(\omega_i) \\
&= \sum_{i=1}^{r}\sigma_1(a_i)\times 0 \\
&= 0
\end{aligned}$$

But this means that these automorphisms are dependent over E, which is a contradiction. □

The theorem also holds for an infinite set of automorphisms, since we can then show that $[E : F]$ is larger than any positive integer.

Corollary 3.3. *If F is fixed by a set of n automorphisms, then $[E : F] \geq n$.*

Proof. If F' is the fixed field of those automorphisms, then $[E : F] = [E : F'][F' : F] \geq n$. □

Corollary 3.4. *If $Aut(E/F)$ is the group of all automorphisms of E which fix F, then $|Aut(E/F)| \leq [E : F]$.*

.

From the theorem above, the best lower bound we can get is the order of the group of all automorphisms of E which fix F. It turns out that this bound becomes an equality. We prove the following:

Proposition 3.5. *If G is a finite group of automorphisms of E, and F is the fixed field of G, then $|G| = [E : F]$.*

Proof. Suppose $G = \{\sigma_1, \cdots, \sigma_n\}$. We know that $[E : F] \geq n$. Now suppose that $[E : F] > n$, so there is set $\omega_1, \cdots, \omega_r \in E$ independent over F with $r > n$. Then the set of n linear equations in r variables

$$\begin{aligned}
x_1\sigma_1(\omega_1) + \cdots + x_r\sigma_1(\omega_r) &= 0 \\
&\cdots \\
x_1\sigma_n(\omega_1) + \cdots + x_r\sigma_n(\omega r) &= 0
\end{aligned}$$

has a nontrivial solution. We can assume WLOG that $x_1 \neq 0$, and furthermore we choose x_1 to be any $a \in E$, since otherwise we could multiply everything by $\frac{a}{x_1}$.

If $1 \leq i, j \leq n$, we have

$$\sum_{k=1}^{r} x_k \sigma_i(\omega_k) = 0.$$

If we fix j, then applying σ_j to both sides of this equations gives

$$\sum_{k=1}^{r} \sigma_j(x_k)\sigma_j(\sigma_i(\omega_k)) = 0.$$

As σ_i runs over all elements of G, the expression $\sigma_j \circ \sigma_i$ also runs over all elements of G. It follows that $\{\sigma_j(x_k)\}_{1 \leq k \leq r}$ gives another solution to our system of linear equations. We can then set

$$y_k = \sum_{\sigma \in G} \sigma(x_k),$$

which will also be a solution to our equations. Furthermore, for $1 \leq k \leq r$, if $\sigma \in G$, then $\sigma(y_k) = y_k$, so $y_k \in F$. Since G is a group, one of its automorphisms, say WLOG σ_1 is the identity on E. Therefore,

$$\sum_{k=1}^{r} y_k \sigma_1(\omega_k) = \sum_{k=1}^{r} y_k \omega_k = 0.$$

But there exists $a \in E$ such that $\sum_{\sigma \in G} \sigma(a) \neq 0$ by the independence of automorphisms, so we could have chosen x_1 to be this a. Then $y_1 \neq 0$, and we have a dependence among the ω_k, contradicting the assumption that they were independent. □

Corollary 3.6. *If E/F is finite, and F is the fixed field of a group G of automorphisms of E, then G is the set of all automorphisms of E which fix F.*

Proof. We have $|G| = [E : F]$, and by Corollary 3.3, there are no more automorphisms of E fixing F. □

4 Applications to Symmetric Polynomials

Let K be a field, and let $k(x_1, \cdots, x_n)$ be the field of rational functions in n variables over K. For each permutation σ of $\{1, \cdots, n\}$, we get an automorphism of $K(x_1, \cdots, x_n)$ which sends x_i to $x_{\sigma(i)}$ for $i \in \{1, \cdots, n\}$. The fixed field S of this group of automorphisms (isomorphic to S_n) is called the *field of symmetric rational functions in n variables over k.*

Define t_k to be the sum of all products of k-tuples of the n variables for $1 \leq k \leq n$. These are known as the *elementary symmetric polynomials*. Then $k(t_1, \cdots, t_n) \subseteq S \subseteq K(x_1, \cdots, x_n)$, so $[K(x_1, \cdots, x_n) : K(t_1, \cdots, t_n)] \geq |S_n| = n!$.

But $K(x_1, \cdots, x_n)$ is the splitting field of the polynomial $x^n - t_1 x^{n-1} + \cdots + (-1)^n t_n$ over $K(t_1, \cdots, t_n)$, which means that $[K(x_1, \cdots, x_n) : S] \leq [K(x_1, \cdots, x_n) : K(t_1, \cdots, t_n)] \leq n!$, so $S = K(t_1, \cdots, t_n)$, and $[K(x_1, \cdots, x_n) : S] = n!$.

Now let $S^n = S$, and define $S^i = S^{i+1}(x_{i+1})$ for $1 \leq i \leq n$. It follows that $S^1 = K(x_1, \cdots, x_n)$. We have the sequence of fields $S = S^n \subseteq S^{n-1} \subseteq \cdots \subseteq S^1 = K(x_1, \cdots, x_n)$.

Let $t_{k,i}$ denote the sum of all products of k-tuples of the first i variables, $x_1, \cdots, x_i$ (so $t_k = t_{k,n}$).

Now suppose that a field F contains x_{i+1} and $t_{k,i+1}$ for all $k \leq i+1$. Then $t_{1,i} = t_{1,i+1} - x_{i+1}$, and in general, $t_{k+1,i} = t_{k+1,i+1} - x_{i+1} t_{k,i}$ for $1 \leq k \leq i-1$, so F contains $t_{k,i}$ for all $1 \leq k \leq i$. More strongly, $t_{k,i}$ can be expressed as a polynomial over K in x_{i+1} and all the $t_{k,i+1}$.

If we then induct downward on i, starting with $i = n$, we see that $t_{k,i}$ can be expressed as a polynomial over K in $x_{i+1}, \cdots, x_n$ and $t_1, \cdots, t_n$.

Since $x_i^i - t_{1,i} x_i^{i-1} + \cdots + t_{i,i} = 0$, and S^i is fixed by the $i!$ automorphisms of $K(x_1, \cdots, x_n)$ which permute the first i variables, the degree $[K(x_1, \cdots, x_n) : S^i] = i!$, and $[S^i : S^{i+1}] = i+1$.

As well, since $x_i^i - t_{1,i} x_i^{i-1} + \cdots + t_{i,i} = 0$, we can express any power of x_i with exponent at least i as a polynomial in x_i, $t_1, \cdots, t_n$, and $x_{i+1}, \cdots, x_n$ where the exponents of x_i are at most $i-1$. If we have a general polynomial $f \in K[x_1, \cdots, x_n]$, we can first get rid of all powers of x_1 with exponent at least 1, then all powers of x_2 with exponent at least 2, etc, until we get rid of all powers of x_n with exponent at least n. If $\{\nu_i\}_{1 \leq i \leq n}$ satisfy $0 \leq \nu_i \leq i-1$ for $1 \leq i \leq n$, define $x_{\{\nu_i\}} = \prod_{i=1}^{n} x_i^{\nu_i}$. Then we can write

$$p(x) = \sum_{\{\nu_i\}} s_{\{\nu_i\}} x_{\{\nu_i\}}$$

where $s_{\{\nu_i\}} \in K[t_1, \cdots, t_n]$.

If $\dfrac{p(x)}{q(x)} \in K(x_1, \cdots, x_n)$, then

$$\frac{p(x)}{q(x)} = \frac{p(x) \prod_{\sigma \in S_n, \sigma \neq 1} \sigma(q(x))}{\prod_{\sigma \in S_n} \sigma(q(x))},$$

where 1 denotes the identity of S_n. The bottom is in S. If we write

$$p(x) \prod_{\sigma \in S_n, \sigma \neq e} \sigma(q(x)) = \sum_{\{\nu_i\}} s_{\{\nu_i\}} x_{\{\nu_i\}}$$

as above, we can then write

$$\begin{aligned}\frac{p(x)}{q(x)} &= \frac{p(x)\prod_{\sigma\in S_n,\sigma\neq 1}\sigma(q(x))}{\prod_{\sigma\in S_n}\sigma(q(x))} \\ &= \frac{\sum_{\{\nu_i\}} s_{\{\nu_i\}}x_{\{\nu_i\}}}{\prod_{\sigma\in S_n}\sigma(q(x))} \\ &= \sum_{\{\nu_i\}}\frac{s_{\{\nu_i\}}}{\prod_{\sigma\in S_n}\sigma(q(x))}x_{\{\nu_i\}}.\end{aligned}$$

This means that the $x_{\{\nu_i\}}$ span $K(x_1,\cdots,x_n)$ as a vector space over S, and since there are $n!$ such $x_{\{\nu_i\}}$ and the degree is $n!$, the $x_{\{\nu_i\}}$ must form a basis. If $f(x)\in K[x_1,\cdots,x_n]\cap S$, then we can express $f(x)$ both as $f(x)x_{\{0,\cdots,0\}}$ and as $\sum_{\{\nu_i\}} s_{\{\nu_i\}}x_{\{\nu_i\}}$. But the expression in terms of a basis is unique, so $f(x) = s_{\{0,\cdots,0\}} \in K[t_1,\cdots,t_n]$. Therefore, we have proved the celebrated theorem every symmetric polynomial in n variables over K can be expressed as a polynomial in the elementary symmetry polynomials.

5 Galois and Normal Extensions

Definition 5.1. An extension E/F is said to be *Galois* extension if it is finite and if F is the fixed field of some group of automorphisms of E.

It follows that F is the fixed field of the group of all automorphisms of E. By a corollary to an earlier theorem, there are at most $[E:F]$ of them. For an arbitrary extension E/F, we denote this group by $\mathrm{Gal}(E/F)$, and it is called the *Galois group* of E over F. We also sometimes refer to the Galois group over a polynomial over a field F, which is the Galois group of its splitting field over F.

Proposition 5.2. *An extension E/F is Galois iff $|\mathrm{Gal}(E/F)| = [E:F]$.*

Proof. If E/F is Galois, then F is the fixed field of $\mathrm{Gal}(E/F)$, so by an earlier theorem, $|\mathrm{Gal}(E/F)| = [E:F]$.

Conversely, if $|\mathrm{Gal}(E/F)| = [E:F]$, and F' is the fixed field of $\mathrm{Gal}(E/F)$, then $|\mathrm{Gal}(E/F)| = [E:F']$, so $[F':F] = 1$, and $F = F'$. □

We have so far talked mainly about linear algebra and automorphisms and little about polynomials and algebraic elements. We now establish a relation between polynomials and automorphisms.

Proposition 5.3. *If α is an algebraic element of an extension E/F, and $\sigma\in\mathrm{Gal}(E/F)$, then $\sigma(\alpha)$ has the same minimal polynomial over F as α.*

Proof. Let $f(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_0$ be the minimal polynomial of α over F. Then

$$\begin{aligned} f(\sigma(\alpha)) &= (\sigma(\alpha))^n + \cdots + b_1\sigma(\alpha) + b_0 \\ &= \sigma(\sigma^{-1}\alpha^n + \cdots + \sigma^{-1}(b_1)a + \sigma^{-1}(b_0)) \\ &= \sigma(\alpha^n + \cdots + b_1\alpha + b_0) \\ &= \sigma(0) \\ &= 0 \end{aligned}$$

Since $f(\sigma(\alpha)) = 0$, and $f(x)$ is irreducible, it follows that $\sigma(\alpha)$ has $f(x)$ as its minimal polynomial. □

Consider the extension $E = \mathbb{Q}(\sqrt[3]{2})$ of $\mathbb{Q}$. Then $\sqrt[3]{2}$ has minimal polynomial $x^3 - 2$ over $\mathbb{Q}$, but this polynomial has no other roots in E. Therefore, any element of $\mathrm{Gal}(E/\mathbb{Q})$ fixes $\sqrt[3]{2}$ and therefore fixes all of E. But this means that the only element of $\mathrm{Gal}(E/\mathbb{Q})$ is the identity, so its fixed field is all of E, and the extension $E/\mathbb{Q}$ is not Galois. The reason for this is that there aren't enough roots of $x^3 - 2$, and therefore there aren't enough automorphisms for $\mathbb{Q}$ to be all of the fixed field. The other roots of $x^3 - 2$ lie in other extensions. It turns out that if we take E to be the splitting field of $x^3 - 2$, then $E/\mathbb{Q}$ is Galois.

Consider the field $\mathbb{F}_2(x)$ of rational functions, and let $E = \mathbb{F}_2(x)(\alpha)$ where α is a root of the polynomial $t^2 - x \in \mathbb{F}_2(x)[t]$. Then in E, the polynomial $t^2 - x$ splits as $(x-\alpha)^2$, and therefore it only has one root. It follows that $\mathrm{Gal}(E/\mathbb{F}_2(x))$ has only the identity element, and again, our extension is not Galois. In this case, our extension has all of the roots of $t^2 - x$, but this polynomial has a repeated root, and so there still aren't enough automorphisms in this extension for it to be Galois.

We have motivated some of the material to come.

Definition 5.4. A polynomial is said to be *separable* if its irreducible factors have no repeated roots. An algebraic element in an extension is said to be *separable* if its minimal polynomial is separable. An algebraic field extension is said to be *separable* if all its elements are separable.

We now prove the following theorem:

Theorem 5.5. *A finite extension E/F is Galois iff it is the splitting field of a separable polynomial $p(x)$ over F.*

Proof. Suppose E/F is Galois. Let $\omega_1, \cdots, \omega_n$ be a basis for E over F. For $1 \leq i \leq n$, let $\{\sigma_1(\omega_i), \cdots, \sigma_r(\omega_i)\}$ be the orbit of ω_i under $\mathrm{Gal}(E/F)$, where $r < |\mathrm{Gal}(E/F)|$. If $\sigma \in \mathrm{Gal}(E/F)$, then $\{\sigma(\sigma_1(\omega_i)), \cdots, \sigma(\sigma_r(\omega_i))\}$ is a set of r distinct elements in the orbit of ω_i and is therefore equal to the orbit of ω_i.

Now define $f_i(x) = \prod_{j=1}^{r}(x - \sigma_j(\omega_i))$. The coefficients are symmetric in the elements of the orbit of ω_i and are therefore invariant under $\mathrm{Gal}(E/F)$. It follows that they lie in F because E/F is Galois. Thus $f_i(x)$ is a separable polynomial with $f_i(\omega_i) = 0$. It is even irreducible since every element of the orbit of ω_i has the same irreducible polynomial.

Now let $p(x) = \prod_{i=1}^{n} f_i(x)$. Since each f_i splits in E, $p(x)$ splits in E. As well, ω_i is a root of $p(x)$ for $1 \leq i \leq n$, so E is a splitting field for $p(x)$ over F. Finally, the irreducible factors f_i of $p(x)$ have no multiple roots, so $p(x)$ is separable.

To prove the converse, we use induction on the number of roots n of $p(x)$ which lie outside F. If $n = 0$, then $E = F$, and E/F is trivially Galois since F is fixed under the identity automorphism. Now suppose the theorem is true for $n \leq k \geq 0$, and suppose that $p(x)$ has $k+1$ roots outside of F. Let α be one of these roots, and suppose its minimal polynomial $f(x)$ has degree r. Then E is a splitting field for $p(x)$ over $F(\alpha)$, and $p(x)$ has at most k roots outside of $F(\alpha)$, and $E/F(\alpha)$ is Galois by hypothesis. Therefore, if θ is fixed under every element of $\mathrm{Gal}(E/F)$, then it is fixed under every element of $\mathrm{Gal}(E/F(\alpha))$, so $\theta \in F(\alpha)$.

If β is another root of $f(x)$, then there is an isomorphism from $F(\alpha)$ to $F(\beta)$ sending α to β. Since E is a splitting field for $p(x)$, this can be extended to an automorphism of E sending α to β.

We can therefore write $\theta = c_0 + c_1\alpha + \cdots + c_{r-1}\alpha^{r-1}$ for $c_0, \cdots, c_{r-1} \in F$. If β is any other root of $f(x)$, we can apply the automorphism of E sending α to β to both sides to find that $\theta = c_0 + c_1\beta + \cdots + c_{r-1}\beta^{r-1}$. If we let $g(x) = c_0 - \theta + c_1 x + \cdots c_{r-1}x^{r-1} \in E[x]$, then $g(x)$ has a root at every root of $f(x)$. But $f(x)$ has r distinct roots since $p(x)$ is separable, and the degree of $f(x)$ at most $r-1$, so it follows that $f(x)$ is identically 0, and $\theta = c_0 \in F$. Hence the fixed field of $\mathrm{Gal}(E/F)$ is F, and E/F is Galois. □

We can even sharpen our characterization of Galois extensions further:

Definition 5.6. An extension E/F is *normal* if whenever an irreducible polynomial $f(x) \in F[x]$ has a root in E, then it splits in E.

Proposition 5.7. *A finite extension E/F is Galois iff it is normal and separable.*

Proof. If $\omega_1, \cdots, \omega_n$ is a basis for E over F, let $f_i(x)$ be the minimal polynomial of ω_i. Then E/F is a splitting field for the product of the f_i, and each f_i is separable because E/F is.

Conversely, if E/F is Galois, and $f(x) \in F[x]$ is irreducible and has a root α in E, then let $\sigma_1(\alpha), \cdots, \sigma_r(\alpha)$ be the orbit of α under $\mathrm{Gal}(E/F)$. The polynomial $\prod_{i=1}^{r}(x - \sigma_i(\alpha))$ is separable and irreducible in $F[x]$, and it splits over E, so E/F is normal and separable. □

Remark 5.8. The proof of Proposition 5.7 is intentionally brief because most of its ideas were convered in earlier proofs.

6 The Fundamental Theorem of Galois Theory

Definition 6.1. An *intermediate field* of an extension E/F is a subfield of E containing F.

Definition 6.2. If E/F is Galois, then two intermediate fields B and B' are said to be *conjugate* in E/F if there is $\sigma \in \mathrm{Gal}(E/F)$ such that $\sigma(B) = B'$.

Note that if two intermediate fields B and B' are isomorphic, then they are automatically conjugate, since if E is a splitting field for $p(x)$ over F, then E is also a splitting field for $p(x)$ over each of B and B', so the isomorphism from B to B' can be extended to an automorphism of E. It is clear that if two intermediate fields are conjugate, then they are isomorphic.

Proposition 6.3. *An intermediate field B of a Galois extension E/F has a conjugate (other than itself) iff B/F is normal.*

Proof. If B/F is normal, then it is also separable because E/F is separable, so B/F is Galois. Hence it is the splitting field of a polynomial $p(x)$ over F, and it is the field generated by the roots of $p(x)$ in E. Any conjugate B' of B in E is also a splitting field for $p(x)$ over F and hence is the field generated by the roots of $p(x)$ in E. But that means $B = B'$.

Suppose that B/F is not normal. We use induction on $[B : F]$. If $[B : F] = 1$, then $B = F$, and B trivially has no other conjugates. Now suppose the theorem is true for $[B : F] \leq k \geq 1$, and suppose $[B : F] = k + 1$. Then there is $\alpha \in B$ such that the minimal polynomial $f(x)$ of α over F does not split in B. Therefore, it has an irreducible factor $g(x)$ in $B[x]$ of degree greater than 1. But $f(x)$ splits in E because E/F is Galois, so $g(x)$ has a root β in E but not in $F(\alpha)$. We have an isomorphism from $F(\alpha)$ to $F(\beta)$ which fixes F since α and β are both roots of $f(x)$, and we can extend this to an automorphism of E since E is a splitting field of the same polynomial over both $F(\alpha)$ and $F(\beta)$. This automorphism sends B to a field B' which is not equal to B because B' contains β, so B has a distinct conjugate in E. □

We can now prove:

Theorem 6.4 (Fundamental Theorem of Galois Theory)**.** *Let E/F be a Galois extension, and let $G = \mathrm{Gal}(E/F)$. If B is an intermediate field, then $\mathrm{Gal}(E/B)$ is a subgroup of $\mathrm{Gal}(E/F)$. If $H \leq \mathrm{Gal}(E/F)$, let E^H denote the fixed field of H. Then:*

1. *If $H \leq G$, then $\mathrm{Gal}(E/E^H) = H$.*
2. *If B is an intermediate field, then $E^{\mathrm{Gal}(E/B)} = B$.*
3. *If B is an intermediate field, then $|\mathrm{Gal}(E/B)| = [E : B]$ and $[G : \mathrm{Gal}(E/B)] = [B : F]$ where $[G : \mathrm{Gal}(E/B)]$ is the index of $\mathrm{Gal}(E/B)$ in G.*
4. *B and C are intermediate fields with $B \subseteq C$ iff $\mathrm{Gal}(E/C) \leq \mathrm{Gal}(E/B)$.*
5. *$\mathrm{Gal}(E/B)$ is normal in G iff B/F is normal. If these hold, then B is Galois.*
6. *If B/F is normal, then $\mathrm{Gal}(B/F) \cong G/\mathrm{Gal}(E/B)$.*

Proof. 1. This follows immediately from Corollary 3.6.

2. Since E is the splitting field of a separable polynomial $p(x)$ over F, it is also such over B and therefore Galois, so B is the fixed field of $\mathrm{Gal}(E/B)$.

3. By the above $E^{\mathrm{Gal}(E/B)} = B$, so by Proposition 3.5, $|\mathrm{Gal}(E/B)| = [E : B]$. Then $[G : \mathrm{Gal}(E/B)] = \dfrac{|G|}{|\mathrm{Gal}(E/B)|} = \dfrac{[E : F]}{[E : B]} = [B : F]$.

4. If $B \subseteq C$, then any automorphism which fixes all of C also fixes all of B, so $\mathrm{Gal}(E/C) \leq \mathrm{Gal}(E/B)$. If $\mathrm{Gal}(E/C) \leq \mathrm{Gal}(E/B)$, then anything fixed under all of $\mathrm{Gal}(E/B)$ is also fixed under all of $\mathrm{Gal}(E/C)$, so $E^{\mathrm{Gal}(E/B)} \subseteq E^{\mathrm{Gal}(E/C)}$ or $B \subseteq C$.

5. Suppose B is an intermediate field. If σ is an automorphism, then $\sigma\mathrm{Gal}(E/B)\sigma^{-1}$ fixes all of $\sigma(B)$, so it is contained in $\mathrm{Gal}(E/\sigma(B))$. But $[B : F] = [\sigma B : F]$, so
$$|\mathrm{Gal}(E/\sigma B)| = |\mathrm{Gal}(E/B)| = |\sigma\mathrm{Gal}(E/B)\sigma^{-1}|,$$
so
$$\mathrm{Gal}(E/\sigma(B)) = \sigma\mathrm{Gal}(E/B)\sigma^{-1}.$$
It follows that $\sigma\mathrm{Gal}(E/B)\sigma^{-1}$ and $\mathrm{Gal}(E/B)$ are distinct are distinct iff $\sigma(B)$ and B are distinct since the transformation sending B to $\mathrm{Gal}(E/B)$ from intermediate fields to subgroups of G has an inverse and is therefore injective. It follows that $\mathrm{Gal}(E/B)$ has no conjugates in G other than itself iff B has no conjugates in E other than itself. But the former is the definition of a normal subgroup, and the latter is equivalent to B/F being normal by Proposition 6.3, so B is normal iff $\mathrm{Gal}(E/B)$ is normal in G. Since B is contained in E, and every element of E is separable over F, we have that B is separable over F, so if B is normal, then B is Galois by Proposition 5.7.

6. If B/F is normal, then the image of B under any element of $\mathrm{Gal}(E/F)$ is B since B has no conjugates other than itself, so the restriction of elements of $\mathrm{Gal}(E/F)$ to B defines a homomorphism of $\mathrm{Gal}(E/F)$ to $\mathrm{Gal}(B/F)$. The kernel is precisely those elements of $\mathrm{Gal}(E/F)$ which fix B, and this homomorphism is onto since its image has order $\dfrac{|\mathrm{Gal}(E/F)|}{|\mathrm{Gal}(E/B)|} = \dfrac{[E : F]}{[E : B]} = [B : F] = |\mathrm{Gal}(B/F)|$.

□

7 Additional Facts

We continue with some useful facts that were not necessary for the proof of the Fundamental Theorem.

Definition 7.1. A field F is *perfect* if all of its finite extensions are separable. Equivalently, all the irreducible polynomials in $F[x]$ are separable.

Over a perfect field, the splitting field of any polynomial is a Galois extension.

Example 7.2. The field $\mathbb{F}_2(x)$ is not perfect, as was shown earlier.

Proposition 7.3. *Any field F of characteristic 0 is perfect.*

Proof. Suppose $f(x) \in F[x]$ is irreducible and inseparable. Then it has a multiple root, call it α. Therefore, $f'(\alpha) = 0$. But $f(x)$ is the minimal polynomial for α, so $f'(x)$ must be identically 0. But in a field of characteristic zero, this means that $f(x)$ is constant, so it certainly does not have multiple roots. □

Proposition 7.4. *If E/F and K/E are Galois, then so is K/F.*

Proof. We show that the fixed field of $\mathrm{Gal}(K/F)$ is F. Suppose θ is fixed by all of $\mathrm{Gal}(K/F)$. Then it is fixed by all of $\mathrm{Gal}(K/E)$, so $\theta \in E$. Then each element of $\mathrm{Gal}(E/F)$ can be extended to an element of $\mathrm{Gal}(K/F)$, since K is a splitting field over E, so θ is fixed under each element of $\mathrm{Gal}(E/F)$. It follows that $\theta \in F$ because E/F is Galois. □

Definition 7.5. The *compositum* $B \cup C$ of two intermediate fields B and C of an extension E/F is the intersection of all intermediate fields containing both of them. If H and K are two subgroups of a group G, the subgroup $H \cup K$ is defined to be the intersection of all subgroups of G containing both of them.

Proposition 7.6. *If E/F is Galois, and $B_1, \cdots, B_k$ are intermediate fields, then:*

1. $\mathrm{Gal}(E/B_1) \cap \cdots \cap \mathrm{Gal}(E/B_k) = \mathrm{Gal}(E/B_1 \cup \cdots \cup B_k)$.
2. $\mathrm{Gal}(E/B_1) \cup \cdots \cup \mathrm{Gal}(E/B_k) \subseteq \mathrm{Gal}(E/B_1 \cap \cdots \cap B_k)$.

Proof. 1. If $\sigma \in \mathrm{Gal}(E/F)$ fixes $B_1 \cup \cdots \cup B_k$, then it fixes B_i for $1 \leq i \leq k$, so it is contained in $\mathrm{Gal}(E/B_i)$ for $1 \leq i \leq k$, hence $\mathrm{Gal}(E/B_1 \cup \cdots \cup B_k) \subseteq \mathrm{Gal}(E/B_1) \cap \cdots \cap \mathrm{Gal}(E/B_k)$.

If $\sigma \in \mathrm{Gal}(E/F)$ fixes B_i for $1 \leq i \leq k$, then it fixes $B_1 \cup \cdots \cup B_k$, so $\mathrm{Gal}(E/B_1) \cap \cdots \cap \mathrm{Gal}(E/B_k) \subseteq \mathrm{Gal}(E/B_1 \cup \cdots \cup B_k)$, showing their equality.

2. If $\sigma \in \mathrm{Gal}(E/F)$ is in $\mathrm{Gal}(E/B_1) \cup \cdots \cup \mathrm{Gal}(E/B_k)$, then it is in $\mathrm{Gal}(E/B_i)$ for some $1 \leq i \leq k$, so it fixes $B_1 \cap \cdots \cap B_k$ and hence is in $\mathrm{Gal}(E/B_1 \cup \cdots \cup B_k)$.

□

8 Finite Fields

Lemma 8.1. *If G is a finite group in which the equation $x^n = 1$ has at most n solutions for each n, then G is cyclic.*

Proof. Suppose that G is not cyclic. Let n_k denote the number of elements of G of order k. Then we have $\sum_{k||G|} n_k = |G|$. Suppose that $n_k \leq \phi(k)$ for all k. We have $n_{|G|} = 0$, so

$$|G| = \sum_{k||G|} n_k \leq \sum_{k||G|, k \neq |G|} \phi(k) < \sum_{k||G|} \phi(k) = |G|,$$

a contradiction. Therefore, there is k such that $n_k > \phi(k)$. Let $a \in G$ have order k. Then the k elements of the subgroup generated by a satisfy $x^k = 1$. But this subgroup has $\phi(k)$ elements of order k, so there is another element of G of order k not in this subgroup, which also satisfies $x^k = 1$, so there are more than k solutions to $x^k = 1$ in G, a contradiction. It follows that G is cyclic. □

Corollary 8.2. *Any finite subgroup of the multiplicative group of a field is cyclic*

Proof. The equation $x^n = 1$ has at most n solutions in any field. □

Lemma 8.3. *If F is a field of characteristic p, then $(a+b)^p = a^p + b^p$ for $a, b \in F$.*

Proof. The binomial coefficient $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ for $1 \leq k \leq p-1$ is divisible by p since there are no multiples of p in the denominator. Therefore, $(a+b)^p = \sum_{k=0}^{p} a^k b^{p-k} \binom{p}{k} = a^p + b^p$. □

It follows that the map sending x to x^p is an automorphism of the field F.

Definition 8.4. This automorphism is called the *Frobenius automorphism* of F.

If $|E| = p^k$, then there is an element a of order $p^k - 1$. If we apply the Frobenius automorphism fewer than k times to a, we get an element distinct from a, and if we apply it k times, we get a again. It follows that because a generates $E^\times$, the Frobenius automorphism has order k. Since E has degree k over $\mathbb{F}_p$, all elements of $\mathrm{Gal}(E/\mathbb{F}_p) \cong C_k$ are powers of the Frobenius automorphism, and $E/\mathbb{F}_p$ is Galois. It follows that all extensions of finite fields are Galois (as they are the splitting field of a separable polynomial).

For any positive integer k, we can construct the splitting field E of $f(x) = x^{p^k} - x$ over $\mathbb{F}_p$. The derivative of this polynomial is -1, so it has no repeated roots. Thus E has at least p^k elements. Furthermore, the p^k roots of this polynomial form a subfield of E, and since $f(x)$ splits in this subfield, it follows that this subfield must be equal to E, so E has p^k elements. Furthermore, if E and E' both have p^k elements, then each is a splitting field for $x^{p^k} - x$ over $\mathbb{F}_p$, so they are isomorphic. We have proved:

Theorem 8.5. *There is a unique finite field of each prime power order p^k, denoted $\mathbb{F}_{p^k}$. Its Galois group over $\mathbb{F}_p$ is the cyclic group of order k.*

In fact, any finite field must have prime power order, as it is a vector space over $\mathbb{F}_p$, where p is its characteristic.

Here is another proof of the uniqueness of finite fields of a given order, which, although unnecessary, is a nice application of the Fundamental Theorem of Galois Theory.

Proposition 8.6. *If E and F are two finite fields of the same order, then they are isomorphic.*

Proof. Let E and F be two fields of order p^k, and say they are formed by adjoining a root of the polynomials q and r with degree k respectively. If they are not isomorphic, then E does not contain a root of r, so we can form an extension L of E that contains a root of r. Then L contains both E and F. But the Galois group of L is cyclic, and cyclic groups have at most one subgroup of each order, so by the fundamental theorem of Galois theory, we have that there is at most one subfield of a given order. This means that $E = F$ as subfields of L, so they are isomorphic. □

9 Gauss's Lemma and Unique Factorization in U[x]

Definition 9.1. If U is a UFD, then the *content* of a polynomial $p(x) \in U[x]$ is the greatest common divisor of its coefficients. A polynomial is said to be *primitive* if it has content 1.

Any polynomial in $U[x]$ can be uniquely expressed as an element of U times a primitive polynomial, and this element of U is its content.

Lemma 9.2. *If $f(x), g(x) \in U[x]$ are primitive, then so is $f(x)g(x)$.*

Proof. Suppose $f(x)$ and $g(x)$ are primitive, and suppose $f(x)g(x)$ is primitive. Then there is a prime $p \in U[x]$ such that p divides all the coefficients of $f(x)g(x)$. Since $f(x)$ and $g(x)$ are primitive, p does not divide all the coefficients of either of $f(x)$ and $g(x)$. It follows that when reduced modulo p, $f(x)$ and $g(x)$ are nonzero, while $f(x)g(x)$ is zero. But p is prime, so $U/(p)$ and therefore $U/(p)[x]$ are integral domains, so $f(x)g(x)$ is not zero, giving a contradiction. It follows that $f(x)g(x)$ was primitive in the first place. □

Definition 9.3. Let D be the field of fractions of U, and let $p(x) \in D[x]$. There exists $a \in U[x]$ such that $ap(x) \in U[x]$ (for example, take the product of the denominators of the coefficients of $p(x)$). Define the content of $p(x)$ to be the content of $ap(x)$ divided by a.

Lemma 9.4. *The content of a polynomial $p(x) \in D[x]$ is well defined up to units, and if $p(x) = af(x)$ for $f(x) \in U[x]$ primitive, then a is the content of $p(x)$.*

Proposition 9.5 (Gauss's Lemma)**.** *Suppose $p(x) \in U[x]$ factors in $D[x]$. Then it factors in $U[x]$.*

Proof. □

Proposition 9.6 (Eisentein's Criterion)**.** *Suppose $p(x) = \sum_{k=0}^{n} a_k x^k \in U[x]$ for which there exists a prime $p \in U$ such that $p \mid a_k$ for $0 \leq k \leq n-1$ and $p^2 \nmid a_0$. Then $p(x)$ is irreducible.*

Proof. □

10 Cyclotomic Extensions

Definition 10.1. An nth root of unity is an element ζ of a field F such that $\zeta^n = 1$ for some positive integer n.

Definition 10.2. If E is a finite extension of $\mathbb{Q}$ obtained by adjoining a root of unity, it is called a *cyclotomic extension.*

Since all nth roots of unity are roots of the polynomial $x^n - 1$, there are at most n of them. Furthermore, the derivative of this polynomial is nx^{n-1}, whose only root is 0, which is clearly not a root of $x^n - 1$. Therefore, the polynomial $x^n - 1$ has no multiple roots, and we can form a splitting field E of $x^n - 1$ over a field F which contains n distinct roots of $x^n - 1$.

Furthermore, if $a^n = b^n = 1$, then $(ab)^n = 1$, so the roots of $x^n - 1$ in any field form a multiplicative group. If E has all the roots of $x^n - 1$, this is a finite group of order n, and by Corollary 8.2 is cyclic. Each element of this group has some order dividing n, and for each $k \mid n$, there are $\phi(k)$ elements of order k and k kth roots of unity.

Definition 10.3. A root of unity of order k is called a *primitive* kth root of unity.

If we adjoin a primitive nth root of unity ζ_n to a field F, then its minimal polynomial divides $x^n - 1$, so we can imbed $F(\zeta_n)$ in the splitting field E of $x^n - 1$ over F. Then all the roots of $x^n - 1$ can be expressed as powers of ζ_n, so $E = F(\zeta_n)$. Since $x^n - 1$ has no multiple roots and is therefore separable, this extension is always Galois.

It follows that if ζ_k is a primitive kth root of unity sitting inside E, then $F(\zeta_k)$ is a splitting field for $x^k - 1$ over F, i.e. the splitting field of $x^k - 1$ sits inside that of $x^n - 1$. This allows us to freely talk about kth roots of unity sitting in the splitting field of $x^n - 1$ just as if they were in the splitting field of $x^k - 1$.

Fix a primitive nth root of unity $\zeta_n \in E$. Any automorphism of E must restrict to an automorphism of the group of nth roots of unity, and such an automorphism must send primitive roots to primitive roots of unity. Furthermore, any element of $\mathrm{Gal}(E/F)$ is determined by its action on ζ_n and therefore on the subgroup of nth roots of unity. The automorphism group of a cyclic group of

order n is isomorphic to $(\mathbb{Z}/n)^\times$, so $\mathrm{Gal}(E/F)$ imbeds in this group. We have proven:

Proposition 10.4. *If F is a field, and $E = F(\zeta_n)$, where ζ_n is a primitive nth root of unity, then E/F is Galois and equal to the splitting field of $x^n - 1$ over F, and $\mathrm{Gal}(E/F)$ imbeds in $(\mathbb{Z}/n)^\times$.*

It follows that $\mathrm{Gal}(E/F)$ sends primitive nth roots of unity only to primitive nth roots of unity, and so the minimal polynomial of each primitive root of unity has only primitive nth roots of unity as roots. It follows that the product of $x - \zeta_n$ for each primitive nth root of unity ζ_n has coefficients in F. We define:

Definition 10.5. The polynomial $\Phi_n(x) = \prod(x - \zeta_n)$ over all primitive nth roots of unity ζ_n is called the nth *cyclotomic polynomial*.

By definition, the polynomial $\Phi_n(x)$ has degree $\phi(n)$.

Since the roots of $x^n - 1$ are those which have order k for some $k \mid n$, we get

$$x^n - 1 = \prod_{k|n} \Phi_k(x).$$

For the rest of this section, we work over the base field $\mathbb{Q}$.

Proposition 10.6. *For all n, $\Phi_n(x)$ has integer coefficients and is primitive.*

Proof. We induct on n. For $n = 1$, we have $\Phi_1(x) = x - 1$.

Suppose the proposition is true for all $n \leq m-1 \geq 1$. The polynomial $x^m - 1$ splits as $\prod_{a=1}^{m}(x - \zeta_m^a)$. By hypothesis, for each $k \mid m, k \neq m$, the polynomial $\Phi_k(x)$ has integer coefficients, content 1, and divides $x^m - 1$. The product

$$p(x) = \prod_{k|m, k\neq m} \Phi_k(x)$$

is therefore primitive with integer coefficients. We can thus write $x^m - 1 = f(x)p(x)$ for $f(x)$ primitive with integer coefficients, by Gauss's Lemma. But

$$x^m - 1 = \Phi_m(x)p(x),$$

so $\Phi_m(x) = f(x)$, and $\Phi_m(x)$ has integer coefficients and is primitive. □

Lemma 10.7. *If p^k is a power of a prime in $\mathbb{Z}$, then $\Phi_{p^k}(x)$ is irreducible.*

Proof. The primitive p^kth roots of unity are the p^kth roots of unity which are not p^{k-1}th roots of unity, so $\Phi_{p^k}(x) = \dfrac{x^{p^k} - 1}{x^{p^{k-1}} - 1} = \sum_{i=0}^{p-1} x^{ip^{k-1}}$. Now $\Phi_{p^k}(x)$ is irreducible iff $\Phi_{p^k}(x+1)$ is. Then

$$\Phi_{p^k}(x+1) = \sum_{i=0}^{p-1}(x+1)^{ip^{k-1}}.$$

The constant term of $\Phi_{p^k}(x+1)$ is p, and the leading coefficient is 1.

Taking $(x^{p^{k-1}}-1)\Phi_{p^k}(x) = x^{p^k}-1$ and reducing both sides of this equation mod p, we get $(x-1)^{p^{k-1}}\Phi_{p^k}(x) \equiv (x-1)^{p^k} \mod p$. Since $\mathbb{Z}/p[x]$ is an integral domain, we can conclude $\Phi_{p^k}(x) \equiv (x-1)^{p^k-p^{k-1}} \mod p$, so $\Phi_{p^k}(x+1) \equiv x^{p^k-p^{k-1}} \mod p$. This means that all the coefficients other than the leading coefficient of $\Phi_{p^k}(x+1)$ are divisible by p. It follows by Eisenstein's Criterion that $\Phi_{p^k}(x+1)$ and therefore $\Phi_{p^k}(x)$ are irreducible. □

By the above lemma, the extension $\mathbb{Q}(\zeta_{p^k})/\mathbb{Q}$, where ζ_{p^k} is a primitive p^kth root of unity, has degree $\phi(p^k)$. Since the extension is Galois, this is the order of its Galois group, so by Proposition 10.4, the Galois group is isomorphic to $(\mathbb{Z}/p^k)^\times$.

Theorem 10.8. *The cyclotomic polynomial $\Phi_n(x)$ is irreducible over $\mathbb{Q}$ for all positive integers n.*

Proof. Let E be the splitting field of x^n-1. Then $E = \mathbb{Q}(\zeta_n)$, where ζ_n is a primitive nth root of unity. If we can show that $E/F = |\mathrm{Gal}(E/F)| = \phi(n)$, then the minimal polynomial of ζ_n over $\mathbb{Q}$ has degree $\phi(n)$, and therefore $\Phi_n(x)$ must be this minimal polynomial, so $\Phi_n(x)$ is irreducible.

Let ζ_m denote a primitive mth root of unity for all positive integer m. We now prove by induction on n that $|\mathrm{Gal}(E/F)| = \phi(n)$, where $E = \mathbb{Q}(\zeta_n)$. For $n = 1$, we have $\zeta_n = 1$, so the result is trivial.

Now suppose the hypothesis is true for all $n < k > 1$. We prove the result for $n = k$.

Let E denote the splitting field of $x^k - 1$ over $\mathbb{Q}$. Suppose k factors as $p_1^{e_1}\cdots p_k^{e_k}$. Let $m = \frac{k}{p_1^{e_1}}$. Let $F/\mathbb{Q}$ denote the splitting field of x^m-1, which, by hypothesis, has degree $\phi(m)$. Note that we can imbed F in E. If $H = \mathrm{Gal}(E/K)$ and $N = \mathrm{Gal}(E/\mathbb{Q}(\zeta_{p_1^{e_1}}))$, then $H \cap N$ is the trivial subgroup, since K and $\zeta_{p_1^{e_1}}$ together generate E over $\mathbb{Q}$.

The product of two elements of a finite group with relatively prime orders has order equal to their product, and by induction, the product $\zeta_{p_1^{e_1}}\cdots\zeta_{p_k^{e_k}}$ has order n. If E_i denotes $\mathbb{Q}(\zeta_{p_i^{e_i}})$, this implies that $E_1 \cup \cdots \cup E_k = E$. Let $G_i = \mathrm{Gal}(E/E_i) \leq \mathrm{Gal}(E/\mathbb{Q})$.

□

11 Ruler and Compass Constructions

12 Noether's Equations and Hilbert's Theorem 90

Definition 12.1. If G is a finite group of automorphisms of a field E, then a mapping $G \to E^\times$ defined by $\sigma \to x_\sigma$ for $\sigma \in G$ is said to be a *solution to*

Noether's Equations if for all $\sigma, \tau \in G$, we have

$$x_\sigma \sigma(x_\tau) = x_{\sigma\tau}.$$

If x_σ is contained in the fixed field F of G for all $\sigma \in G$, then $x_\sigma x_\tau = x_{\sigma\tau}$, so we have a character of G in F. Similarly, given a character of G in F, then we have a solution of Noether's Equations contained in F.

Proposition 12.2. *$\{x_\sigma\}_{\sigma\in G}$ is a solution to Noether's Equations iff there exists $\alpha \in E$ such that $x_\sigma = \dfrac{\alpha}{\sigma(\alpha)}$ for all $\sigma \in G$.*

Proof. If $\alpha \in E$, and $x_\sigma = \dfrac{\alpha}{\sigma(\alpha)}$, then

$$\begin{aligned} x_\sigma \sigma(x_\tau) &= \left(\frac{\alpha}{\sigma(\alpha)}\right) \sigma\left(\frac{\alpha}{\tau(\alpha)}\right) \\ &= \left(\frac{\alpha}{\sigma(\alpha)}\right)\left(\frac{\sigma(\alpha)}{\sigma(\tau(\alpha))}\right) \\ &= \frac{\alpha}{\sigma(\tau(\alpha))} \\ &= x_{\sigma\tau} \end{aligned}$$

So then $\{x_\sigma\}_{\sigma\in G}$ is a solution to Noether's Equations.

Conversely, suppose $\{x_\sigma\}_{\sigma\in G}$ is a solution to Noether's Equations.

By the linear independence of characters, there exists $a \in E$ such that $\sum_{\tau\in G} x_\tau \tau(a) = \alpha \neq 0$. Then

$$\begin{aligned} x_\sigma \sigma(\alpha) &= x_\sigma \sigma\left(\sum_{\tau\in G} x_\tau \tau(a)\right) \\ &= \sum_{\tau\in G} x_\sigma \sigma(x_\tau)\sigma(\tau(a)) \\ &= \sum_{\tau\in G} x_{\sigma\tau}\sigma(\tau(a)) \\ &= \sum_{\tau\in G} x_\tau \tau(a) \\ &= \alpha \end{aligned}$$

It follows that $x_\sigma = \dfrac{\alpha}{\sigma(\alpha)}$ for all $\sigma \in G$. □

Definition 12.3. If E/F is a Galois extension, and $\alpha \in E$, we define the *norm* $N_{E/F}(\alpha)$ to be

$$\prod_{\sigma\in \mathrm{Gal}(E/F)} \sigma(\alpha).$$

It follows that $\tau(N_{E/F}(\alpha)) = N_{E/F}(\alpha)$ for all $\tau \in \mathrm{Gal}(E/F)$, so $N_{E/F}(\alpha) \in F$. In addition, for $\alpha, \beta \in E$, we have $N_{E/F}(\alpha\beta) = N_{E/F}(\alpha)N_{E/F}(\beta)$.

Corollary 12.4 (Hilbert's Theorem 90)**.** *Suppose E/F is Galois with cyclic Galois group of order n generated by σ. Suppose $a \in E$ has norm 1. Then there exists $\alpha \in E$ such that $a = \dfrac{\alpha}{\sigma(\alpha)}$.*

Proof. Let $x_{\sigma^k} = \prod_{i=0}^{k-1} \sigma^i(a)$ for all integers $k \geq 0$. Note that this is well-defined since $N_{E/F}(a) = 1$, so

$$\begin{aligned}
\prod_{i=0}^{n+k-1} \sigma^i(a) &= N_{E/F}(a) \prod_{i=n}^{n+k-1} \sigma^i(a) \\
&= \prod_{i=n}^{n+k-1} \sigma^i(a) \\
&= \prod_{i=0}^{k-1} \sigma^{i+n}(a) \\
&= \prod_{i=0}^{k-1} \sigma^i(a).
\end{aligned}$$

Then

$$\begin{aligned}
x_{\sigma^k}\sigma^k(x_{\sigma^l}) &= \left(\prod_{i=0}^{k-1} \sigma^i(a)\right) \sigma^k \left(\prod_{i=0}^{k-1} \sigma^i(a)\right) \\
&= \left(\prod_{i=0}^{k-1} \sigma^i(a)\right) \left(\prod_{i=0}^{k-1} \sigma^{i+k}(a)\right) \\
&= \left(\prod_{i=0}^{k-1} \sigma^i(a)\right) \left(\prod_{i=k}^{l+k-1} \sigma^{i+k}(a)\right) \\
&= x_{\sigma^{l+k}},
\end{aligned}$$

so we have a solution to Noether's Equations. Then there exists α such that $a = x_\sigma = \dfrac{\alpha}{\sigma(\alpha)}$ by Proposition 12.2. □

Corollary 12.5. *Suppose E/F is Galois with cyclic Galois group of prime order p, and suppose that F contains a primitive pth root of unity. Then E is the splitting field of a polynomial of the form $x^p - a$ where $a \in F$.*

Proof. Suppose ζ is a primitive pth root of unity. Then $N_{E/F}(\zeta) = \zeta^p = 1$, and therefore there is an $\alpha \in E$ such that $\zeta = \dfrac{\alpha}{\sigma(\alpha)}$. Then $\left(\dfrac{\alpha}{\sigma(\alpha)}\right)^p = \zeta^p = 1$, so

$\alpha^p = \sigma(\alpha^p)$, so $\alpha^p \in E$, but $\alpha \notin F$ since $\dfrac{\alpha}{\sigma(\alpha)} = \zeta \neq 1$. Since $[E : F]$ is prime and $[F(\alpha) : F] > 1$, we must have $F(\alpha) = E$, so the roots of $x^p - \alpha^p$ generate E, and this polynomial splits in E because E/F is Galois, so E is the splitting field of $x^p - \alpha^p$. □

13 Solvability of Equations by Radicals

For the purposes of this section only, all fields are assumed to be perfect. In particular, everything is separable, and all finite normal extensions are Galois.

Definition 13.1. A group G is said to be *solvable* if there exists a chain of subgroups $0 = G_0 \leq G_1 \leq \cdots \leq G_n = G$ such that for $1 \leq i \leq n$, G_{i-1} is normal in G_i, and G_i/G_{i-1} is Abelian.

Note that Abelian groups are trivially solvable.

Lemma 13.2. *Suppose $f : G_1 \to G_2$ is a surjective homomorphism, and $K_2 \trianglelefteq H_2 \leq G$. Let K_1 and H_1 denote the preimages of K_2 and H_2 respectively under f. Then $K_1 \trianglelefteq H_1$, and $H_1/K_1 \cong H_2/K_2$. In particular, $|H_1/K_1| = |H_2/K_2|$.*

Proof. Restrict f to H_1, and compose it with the natural map $H_2 \to H_2/K_2$. Call this map g. Since f is surjective, H_1 hits all of H_2 and therefore all of H_2/K_2. An element of H_1 goes to 0 under g iff its image under f is in K_2, that is to say, iff it is in K_1. Therefore, $H_1/K_1 \cong H_2/K_2$. □

Proposition 13.3. *Suppose G is solvable. Then any quotient or subgroup of G is also solvable.*

Proof. Suppose $H \leq G$. We have a chain of subgroups $0 = G_0 \leq G_1 \leq \cdots \leq G_n = G$ such that for $1 \leq i \leq n$, G_{i-1} is normal in G_i, and G_i/G_{i-1} is Abelian. Let $H_i = G_i \cap H$ for $0 \leq i \leq n$.

If f_i denotes the inclusion of H_i into G_i, and g_i denotes the natural map of G_i onto G_i/G_{i-1} for $1 \leq i \leq n$. An element of H_i is in the kernel iff it is in $H_i \cap G_{i-1} = H \cap G_{i-1} = H_{i-1}$, so the image is isomorphic to H_i/H_{i-1}, and this group must be Abelian because it is a subgroup of G_i/G_{i-1}. It follows that H is solvable by the chain of subgroups $0 = H_0 \leq H_1 \leq \cdots \leq H_n = H$.

Suppose $f : G \to H$ is surjective, i.e. H is a quotient of G. We have a chain of subgroups $0 = G_0 \leq G_1 \leq \cdots \leq G_n = G$ such that for $1 \leq i \leq n$, G_{i-1} is normal in G_i, and G_i/G_{i-1} is Abelian. Let $H_i = f(G_i)$ for $0 \leq i \leq n$. Then $H_0 = 0$, and $H_n = H$. Furthermore, if $h_1 = f(g_1) \in H_i$, and $h_2 = f(g_2) \in H_{i-1}$, where $g_1 \in G_i$ and $g_2 \in G_{i-1}$, then $h_1 h_2 h_1^{-1} = f(g_1 g_2 g_1^{-1}) \in H_{i-1}$ since $g_1 g_2 g_1^{-1} \in G_{i-1}$ because $G_{i-1} \trianglelefteq G_i$. Therefore, $H_{i-1} \trianglelefteq H_i$.

Let g_i denote the natural map $H_i \to H_i/H_{i-1}$ for $1 \leq i \leq n$. Let f_i denote f restricted to G_i, and let $h_i = g_i \circ f_i$ for $1 \leq i \leq n$. Then this map is surjective, and G_{i-1} is contained in its kernel, so there exists a surjective homomorphism $G_i/G_{i-1} \to H_i/H_{i-1}$, meaning that H_i/H_{i-1} is Abelian since

G_i/G_{i-1} is. Then the chain of subgroups $0 = H_0 \leq H_1 \leq \cdots \leq H_n = H$ gives us that H is solvable. $\square$

Proposition 13.4. *Suppose $N \trianglelefteq G$, and N and G/N are solvable. Then G is solvable.*

Proof. Since G/N is solvable, we have a chain of subgroups $0 = G_0 \leq G_1 \leq \cdots \leq G_n = G/N$ such that for $1 \leq i \leq n$, G_{i-1} is normal in G_i, and G_i/G_{i-1} is Abelian. If we let H_i be the preimage of G_i under the natural map $G \to G/N$ for $0 \leq i \leq n$, then H_i/H_{i-1} is Abelian for $1 \leq i \leq n$ by Lemma 13.2. Note that $H_0 = N$, and $H_n = G$. Let $0 = K_0 \leq K_1 \leq \cdots \leq K_n = N$ be a similar chain of subgroups in N. Then the sequence of subgroups $0 = K_0 \leq K_1 \leq \cdots \leq K_n = N = H_0 \leq H_1 \leq \cdots \leq H_n = G$ implies that G is solvable. $\square$

Proposition 13.5. *The following are equivalent for a group G:*

1. *G is solvable.*
2. *There exists a chain of subgroups $0 = G_0 \leq G_1 \leq \cdots \leq G_n = G$ such that for $1 \leq i \leq n$, G_{i-1} is normal in G_i, and G_i/G_{i-1} is cyclic.*
3. *There exists a chain of subgroups $0 = G_0 \leq G_1 \leq \cdots \leq G_n = G$ such that for $1 \leq i \leq n$, G_{i-1} is normal in G_i, and G_i/G_{i-1} is cyclic of prime order.*

Proof. It is clear that $3 \to 2 \to 1$.

We will first show by induction that any Abelian group A has chain of subgroups as in 3. For $|A| = 1$ it trivially holds.

Suppose it is true for all $|A| \leq k \geq 1$. Suppose $|A| = k + 1$. Since $k + 1 \geq 2$, there is a prime $p \mid |A|$, and by Cauchy's Theorem, there is a subgroup N of A of order p. Then $N \trianglelefteq A$ since A is Abelian, and $|A/N| = \dfrac{k+1}{p} < k + 1$. We therefore have, by hypothesis, a chain of subgroups $0 = G_0 \leq G_1 \leq \cdots \leq G_n = A/N$ such that for $1 \leq i \leq n$, G_{i-1} is normal in G_i, and G_i/G_{i-1} is cyclic of prime order (or trivial). If we let N_i be the preimage of G_i under the natural map $A \to A/N$ for $0 \leq i \leq n$, then we have that N_i/N_{i-1} is cyclic of prime order for $1 \leq i \leq n$ by Lemma 13.2. Furthermore, $N_0/0 = N$ is cyclic of order p, so we have our desired chain of subgroups $0 \leq N_0 \leq N_1 \leq \cdots \leq N_n = A$.

Now suppose G is solvable with a chain of subgroups $0 = G_0 \leq G_1 \leq \cdots \leq G_n = G$ such that for $1 \leq i \leq n$, G_{i-1} is normal in G_i, and G_i/G_{i-1} is Abelian. Let $0 = H_{i0} \leq H_{i1} \leq \cdots \leq H_{ir_i} = G_i/G_{i-1}$ for $1 \leq i \leq n$, where $H_{ij}/H_{i(j-1)}$ is cyclic of prime order for $1 \leq j \leq r_i$. For $1 \leq i \leq n$ and $0 \leq j \leq r_i$, let K_{ij} be the preimage of H_{ij} under the natural map $G_i \to G_i/G_{i-1}$. Then $K_{i0} = G_{i-1}$, $K_{ir_i} = G_i$, and $K_{ij}/K_{i(j-1)}$ is cyclic of prime order for $1 \leq i \leq n$ and $1 \leq j \leq r_i$. It follows that $0 = G_0 = G_{10} \leq G_{11} \leq \cdots \leq G_{1r_1} = G_1 = G_{20} \leq G_{21} \leq \cdots \leq \cdots \leq G_{n0} \leq G_{n1} \leq \cdots \leq G_{nr_n} = G_n = G$ is the desired chain of subgroups. $\square$

Definition 13.6. An extension E/F is said to be *radical* if there is a sequence of intermediate fields $F = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_{n-1} \subseteq E_n = E$ such that for $1 \leq i \leq n$, the extension E_i is the splitting field over E_{i-1} of a polynomial $x^r - a$ for $a \in E_{i-1}$. Such an extension is Galois by Proposition 7.4.

Definition 13.7. A polynomial $p(x)$ is said to be *solvable by radicals* over F iff the splitting field E of $p(x)$ can be imbedded in a radical extension of F.

Lemma 13.8. *A radical extension has a solvable Galois group.*

Proof. □

Theorem 13.9. *The roots of a polynomial $p(x) \in F[x]$ can be obtained by adjoining radicals iff $\mathrm{Gal}(E/F)$, where E is the splitting field of $p(x)$, is solvable.*

Proof. If E can be imbedded in a radical extension R of F. Then $\mathrm{Gal}(E/F)$ is a quotient of $\mathrm{Gal}(R/F)$, which is solvable, so by Proposition 13.3, $\mathrm{Gal}(E/F)$ is solvable.

Conversely, suppose $\mathrm{Gal}(E/F)$ is solvable. Let $K = E(\zeta_n)$, where n is the product of the prime factors of $|\mathrm{Gal}(E/F)|$, and ζ_n is a primitive nth root of unity. Note that K/F is Galois by Proposition 7.4, since K/E and E/F are both Galois, the former by Proposition 10.4. If we let $L = F(\zeta_n)$, then there is an injection from $\mathrm{Gal}(K/L)$ into $\mathrm{Gal}(E/F)$ by restricting to E, since if an element of $\mathrm{Gal}(K/L)$ is constant on E, then it is constant on K too. It follows that $|\mathrm{Gal}(K/L)| \mid |\mathrm{Gal}(E/F)|$. In addition, $\mathrm{Gal}(K/L)$ must be solvable.

By Proposition 13.5, we have a chain of subgroups $0 = G_0 \leq G_1 \leq \cdots \leq G_n = \mathrm{Gal}(K/L)$ such that for $1 \leq i \leq n$, G_{i-1} is normal in G_i, and G_i/G_{i-1} is cyclic of prime order. For $0 \leq i \leq n$, let $K_i = K^{G_i}$, so that $K_0 = K$, and $K_n = L$. Then K_{i+1}/K_i is a Galois extension of prime order p for $0 \leq i \leq n-1$. This prime order divides $\mathrm{Gal}(L/K)$ and therefore $\mathrm{Gal}(E/F)$, so by assumption, L, and therefore K_i, contains a primitive pth root of unity. By Corollary 12.5, K_{i+1} is the splitting field of a polynomial $x^p - a$ for $a \in K_i$. Since L is the splitting field of $x^n - 1$ over F, it follows that K/F is a radical extension by the sequence of intermediate fields $F \subseteq L \subseteq K_{n-1} \subseteq \cdots, \subseteq K$. Then since E/F can be imbedded in K/F, the polynomial $p(x)$ is solvable by radicals. □

Lemma 13.10. *The groups A_n and S_n are not solvable for $n \geq 5$.*

Proof. □

Corollary 13.11. *There exists a polynomial over $\mathbb{Q}$ of degree 5 which is not solvable by radicals.*

Proof. The polynomial $x^5 - 10x - 5$ is irreducible by Eiseinstein's criterion. If we adjoin one root, we get an extension of $\mathbb{Q}$ of degree 5, so its splitting field has degree divisible by 5. Then the Galois group must have an element of order 5, and the only elements of order 5 in S_5 are the 5-cycles, so the Galois group contains a 5-cycle. In addition, this polynomial has exactly 2 imaginary root, so complex conjugation is an automorphism which permutes these two. Since the

Galois group contains a 2-cycle and a 5-cycle on the roots of the polynomial, it must contain all permutations of the roots and be isomorphic to S_5. But S_5 is not solvable, so the roots of this polynomial cannot be imbedded in a radical extension of $\mathbb{Q}$, and hence cannot be expressed in terms of iterations of radicals of elements of $\mathbb{Q}$. □

14 Kummer Theory

We begin by stating without proof:

Theorem 14.1 (Fundamental Theorem of Finite Abelian Groups)**.** *A finite Abelian group can be uniquely represented as a product of cyclic groups*

$$C_{q_1} \oplus \cdots \oplus C_{q_t},$$

where $q_i \mid q_{i+1}$ *for* $1 \leq i \leq t-1$.

Definition 14.2. If σ_1 and σ_2 are two characters from a group G into a field F, we define their product to be the character sending each $g \in G$ to $\sigma_1(g)\sigma_2(g)$. In this way, the characters form a group, with identity equal to the character sending all of G to $1 \in F$.

Proposition 14.3. *If A is a finite Abelian group of exponent m, and the field F contains a primitive mth root of unity, then the group of characters from A into F is isomorphic to A.*

Proof. First assume A is cyclic of order m, and let $\zeta_m \in F$ be a primitive mth root of unity. □

15 Artin-Schreier Extensions

16 Primitive Element and Normal Basis Theorems

17 Credits

Thanks to Emil Artin, Israel Herstein, and Mark Krusemeyer, who, directly or indirectly, helped me understand Galois theory. In particular, this treatment of Galois theory is rather similar to the one presented in Emil Artin's books.

Thanks to Waffle Wofsey for providing me with a template for this LaTeX code.