

3. Sylow Theory

This lecture is about a basic technique for understanding the structure of a non-abelian finite group.

3.1. Groups acting on sets

Let X be a set. Recall that the set of all bijections of X form a group. Its group law is composition of bijections. We denote this group by $Bij(X)$.

Definition 3.1. *Let G be a group and X a set. We say that G acts on X if we have a group homomorphism $\theta : G \rightarrow Bij(X)$. We also call such a group homomorphism, a G action on X . We call such an action trivial if $\theta(G) = \{id_X\}$, i.e. $Ker \theta = G$.*

Notations. Let $\theta : G \rightarrow Bij(X)$ be a G action on the set X . For $g \in G$ and $x \in X$, we write gx to denote $\theta(g)(x)$ when the role of θ is clear. For $g, h \in G$, since $\theta(gh)(x) = [\theta(g) \circ \theta(h)](x) = \theta(g)(\theta(h)(x))$, it follows that $(gh)x = g(hx)$, and so there is no harm in dropping the parentheses and write ghx .

Example. *The permutation group of n letters.* For $X = \{1, 2, \dots, n\}$, the group $Bij(X)$ is the symmetric group S_n , also called the group of permutations of n letters. Thus the identity map $S_n \rightarrow S_n$ defines an S_n action on X .

Example. *Conjugation.* Let G be a group. For $g \in G$, we define the map $\kappa_g : G \rightarrow G$, $\kappa_g(x) = gxg^{-1}$. We have

$$\kappa_g \circ \kappa_h = \kappa_{gh}$$

for $g, h \in G$, and $\kappa_e = id_G$. This shows that $\kappa_g^{-1} = \kappa_{g^{-1}}$ for $g \in G$, and hence $\kappa_g \in Bij(X)$.

It also shows that we have a G action on G

$$G \rightarrow Bij(G), \quad g \mapsto \kappa_g.$$

In fact, each κ_g is more than a bijection of the set G . It is a group automorphism of G , i.e. a bijective group homomorphism from G to itself, since

$$\kappa_g(xy) = g^{-1}xyg = gxg^{-1}gyg^{-1} = \kappa_g(x)\kappa_g(y).$$

for all $x, y \in G$. The set of group automorphisms of G is denoted by $Aut(G)$. This is a subgroup of the group $Bij(G)$. Thus, we have a group homomorphism

$$G \rightarrow Aut(G), \quad g \mapsto \kappa_g$$

which we denote by κ and call it the conjugation action on G .

Exercise. Check that if G is abelian, then κ above defines the trivial action on G .

Example. *Left and right multiplications.* Let G be a group, and H be a subgroup of G . For $h \in H$, we define two maps $\lambda_h, \rho_h : G \rightarrow G$, $\lambda_h(x) = hx$, $\rho_h(x) = xh^{-1}$. They define two H actions on G (exercise):

$$\lambda : H \rightarrow Bij(G), \quad h \mapsto \lambda_h,$$

$$\rho : H \rightarrow Bij(G), \quad h \mapsto \rho_h$$

which we call respectively, the left and the right multiplication actions on G .

Exercise. Check that λ and ρ are both injective group homomorphisms.

For the rest of this section, let $\theta : G \rightarrow Bij(X)$ be a G action on the set X .

Definition 3.2. *For a given $x \in X$, the set $\{gx | g \in G\} \subset X$ is called a G orbit of x , and is denoted by Gx when the role of θ is clear, or by $[x]$ when the roles of θ and G are clear. Any element of a given G orbit is called a representative of the G orbit. A G orbit with just one point is called a G fixed point. The set of all G fixed points in X is denoted by X^G .*

Proposition 3.3. *The collection of G orbits Gx form a partition of the set X . In other*

words, any two distinct G orbits are disjoint, and X is the union of the distinct G orbits in X .

Proof: Each $x \in X$ lies in at least one G orbit, namely Gx . So, X is the union of all G orbits in X . Let $x, x' \in X$. Suppose Gx and Gx' are not disjoint. Then $hx = h'x'$ for some $h, h' \in G$, which implies that $gx = gh^{-1}h'x' \in Gx'$ for all $g \in G$. This shows that $Gx \subset Gx'$. By symmetry, $Gx' \subset Gx$. So, $Gx = Gx'$. \square

Example. Under the conjugation action, $\kappa : G \rightarrow \text{Aut}(G)$, a G orbit is called a *conjugacy class* of G . Under the left multiplication action $\lambda : H \rightarrow \text{Bij}(G)$ on G by a subgroup H , an H orbit represented by $x \in G$, is the left coset Hx . Under the right multiplication action $\rho : H \rightarrow \text{Bij}(G)$ on G by a subgroup H , an H orbit represented by $x \in G$, is the right coset xH .

Example. *Left translation action on coset space.* Let G/H be the collection of all right cosets xH of H . Let K be any subgroup of G . Then K acts on the set G/H by left translation, i.e.

$$k(xH) = kxH$$

for $k \in K$ and $x \in G$. If $K = G$, then there is just one K orbit in G/H , since any coset of H is of the form xH , for some $x \in K = G$.

Exercise. Let H be subgroup of G and $g \in G$. If $gHg^{-1} \subset H$, show that $gHg^{-1} = H$. (Hint: Consider the maps $u : H \rightarrow H$, $h \mapsto ghg^{-1}$, and $v : H \rightarrow H$, $h \mapsto g^{-1}hg$, and show that they are inverses of one another.)

The G orbits are certain special *subsets* of a set X we associate to a given G action on X . Next, we associate to the G action, certain special *subgroups* of G .

Definition 3.4. For $x \in X$, the set $\{g \in G | gx = x\} \subset G$ is called the *stabilizer* of x , and is denoted by G_x .

Given $x \in X$, the stabilizer is a subgroup of G , since $g, h \in G_x$ implies that $gx = hx = x$, which implies that $gh^{-1}x = x$, i.e. $gh^{-1} \in G_x$.

Note that $x \in X$ is a G fixed point iff $G_x = G$.

Exercise. Check that under the conjugation action, $\kappa : G \rightarrow \text{Aut}(G)$, the stabilizer of $x \in G$ is the *centralizer* of x , i.e. the subgroup $C_G(x)$ of all elements in G which commute with x . In particular, $x \in G$ is a G fixed point iff $C_G(x) = G$ iff $x \in Z(G)$, where $Z(G)$ is the center of G . Check that under the left multiplication action $\lambda : H \rightarrow \text{Bij}(G)$ on G by a subgroup H , the stabilizer of any point $x \in G$ is always the trivial subgroup $\{e\}$. Likewise under the right multiplication action.

The next theorem relates G orbits in X with stabilizers in G .

Theorem 3.5. *Take a point $x \in X$. The correspondence $G/G_x \rightarrow Gx$, $gG_x \mapsto gx$, is a well-defined bijection of sets. In particular, if G is finite, then $|Gx| = [G : G_x]$.*

Proof: For $g, g' \in G$, we have

$$gG_x = g'G_x \Leftrightarrow g^{-1}g' \in G_x \Leftrightarrow g^{-1}g'x = x \Leftrightarrow gx = g'x.$$

This shows that $G/G_x \rightarrow Gx$ above is well-defined and injective. It is obviously surjective.

Our second assertion follows from $[G : G_x] = |G/G_x|$. \square .

Corollary 3.6. *If G is finite, then the cardinality of each G orbit $|Gx|$ divides $|G|$.*

Corollary 3.7. *(Class Equation) Let G be a finite group, whose action on X has exactly r distinct orbits. Let x_1, \dots, x_r be representatives of those orbits. Then*

$$|X| = \sum_{i=1}^r [G : G_{x_i}].$$

Proof: By the proposition above, X is the union of the disjoint sets Gx_1, \dots, Gx_r . So, the cardinality $|X|$ is the sum $\sum_{i=1}^r |Gx_i|$. Now, our assertion follows immediately from the theorem. \square

Corollary 3.8. *Let G be a finite group with exactly r conjugacy classes, and x_1, \dots, x_r be representatives of those conjugacy classes. Then*

$$|G| = \sum_{i=1}^r [G : C_G(x_i)]$$

Proof: Specialize the preceding corollary to the conjugation action $\kappa : G \rightarrow \text{Aut}(G)$. \square

3.2. p -groups

Throughout this section, p denotes a prime number, and $\theta : G \rightarrow \text{Bij}(X)$ a G action on the set X .

Definition 3.9. *A finite group whose order is a power of p is called a p -group.*

Since every divisor of a power of p is a power of p , every subgroup H of a p -group G is a p -group, with $[G : H]$ equal to a power of p , by Lagrange's theorem.

Theorem 3.10. (*p -Group Fixed Point Theorem*) *Let G be a p -group acting on a finite set X . Then*

$$|X^G| \equiv |X| \pmod{p}.$$

Proof: Put $f = |X^G|$. In the Class Equation, we can arrange the representatives x_1, \dots, x_r of the G orbits so that x_1, \dots, x_f are the full list of G fixed points, if any. Then $G = G_{x_i}$ for $i = 1, \dots, f$, and so

$$|X| - f = \sum_{i=f+1}^r [G : G_{x_i}].$$

For each $i > f$, since x_i is not a G fixed point, G_{x_i} is a proper subgroup of G , hence $[G : G_{x_i}] > 1$. Each such term is also divisible by p , since G is a p -group. It follows that $|X| - f \equiv 0 \pmod{p}$. \square

Corollary 3.11. *Let G be a p -group acting on a finite set X . If there is no G fixed point in X , then p divides $|X|$.*

Corollary 3.12. *Let G be a p -group. If $G \neq \{e\}$, then the center of G has at least p elements.*

Proof: We specialize the theorem to G acting on $X = G$ by conjugation. Then the set of G fixed points is $Z(G)$ (Exercise above.) But $|Z(G)|$ a power of p , since $Z(G)$ is a subgroup of the p -group G . So, $Z(G)$ has less than p elements iff $Z(G) = \{e\}$. In this case, the theorem implies that $|G| = 1$. \square

Example. By Lagrange, a group of order p is cyclic, hence abelian. Let G be a group of order p^2 . We will show that it is isomorphic to either \mathbf{Z}_{p^2} or $\mathbf{Z}_p \times \mathbf{Z}_p$.

Proof: Every non-identity element of G has order p or p^2 , by Lagrange. If there is an element of order p^2 , then G is cyclic and is therefore isomorphic to \mathbf{Z}_{p^2} . Suppose every non-identity element of G has order p . By the preceding corollary, we can find an order p element x in the center $Z(G)$. Pick any $y \notin G - (x)$. Then $xy = yx$, and (y) has order p . It is enough to show that the elements $x^i y^j$, with $0 \leq i, j \leq p - 1$, are distinct. For then the map $G \rightarrow \mathbf{Z}_p \times \mathbf{Z}_p$, $x^i y^j \mapsto (i, j)$ defines a group isomorphism.

Suppose $0 \leq i, j, a, b \leq p - 1$ and $x^i y^j = x^a y^b$. Then $x^{i-a} = y^{b-j} \in (x) \cap (y)$ must be e , since any such element $\neq e$ would have order p and would therefore generate (x) and (y) , contradicting that $y \notin (x)$. Thus, $i = a$ and $b = j$. \square

Note that a group of order 2^3 need not be abelian. The dihedral group D_8 , the symmetry group of a square with marked corners, is an example of a non-abelian group of order 2^3 .

Theorem 3.13. (*p -Subgroup Theorem*) *Let G be a p -group of order p^n . Then G has a subgroup of order p^i , for each $i = 0, 1, \dots, n$.*

Proof: For $n = 0$, the assertion is trivially true. Assume it is true up to some n . Let G be of order p^{n+1} . By the preceding corollary, we can find an element $x \in Z(G)$, of order p^t

for some $t \geq 1$. Since $\langle x \rangle$ is a cyclic subgroup of order p^t , it contains an element y of order p . Since $H = \langle y \rangle \subset Z(G)$ is a normal subgroup of G , the projection map

$$\gamma : G \rightarrow G/H, g \mapsto gH$$

is a group homomorphism. Since $|G/H| = p^n$, the inductive assumption implies that G/H has a subgroup of order p^i , for each $i = 0, 1, \dots, n$. Let A be any of these subgroups, say of order p^i . Then by the Group Homomorphism Theorem, $\gamma^{-1}(A)$ is a subgroup of G containing $\langle y \rangle = \text{Ker } \gamma$, such that $\gamma^{-1}(A)/\langle y \rangle$ is isomorphic to A . It follows that

$$|\gamma^{-1}(A)| = |\langle y \rangle| |A| = p^{i+1}.$$

This shows that G has a subgroup of order p^{i+1} , for each $i = 0, 1, \dots, n$. It also has the subgroup $\{e\}$ of order p^0 . This completes the induction proof. \square

We will prove a stronger version and a generalization (to general finite group) using Sylow theory.

3.3. Sylow Theory

Throughout this section, unless stated otherwise, p denotes a given prime number, and G is a finite group whose order is divisible by p .

Theorem 3.14. *(Cauchy's Theorem) G contains an element of order p .*

Proof: Let X be the set of all p -tuples $(g_1, \dots, g_p) \in G^p$, such that $g_1 \cdots g_p = e$. Since each such tuple has $g_p = (g_1 \cdots g_{p-1})^{-1}$, it follows that X is in bijection with G^{p-1} . So, p divides $|X|$.

Let $(g_1, \dots, g_p) \in X$. Then $g_1 \cdots g_p = e$ implies that $g_1 = (g_2 \cdots g_p)^{-1}$, so that $(g_2 \cdots g_p)g_1 = e$. This implies $(g_2, \dots, g_p, g_1) \in X$. This shows that the map $\sigma : X \rightarrow X$, $(g_1, \dots, g_p) \mapsto (g_2, \dots, g_p, g_1)$, is well-defined. Note that $\sigma^p = \text{id}_X$, and σ is a bijection in particular. This defines an action of the cyclic group C of order p on the set X , where the generator acts by $\sigma \in \text{Bij}(X)$. Moreover, $(g_1, \dots, g_p) \in X$ is a C fixed point iff $g_1 = \cdots = g_p$, and so $g_1^p = e$ in particular.

There is at least one C fixed point, namely (e, \dots, e) . By the p -Group Fixed Point Theorem, $|X| \equiv |X^C| \pmod{p}$. Since p divides $|X|$, this shows $|X^C|$ is at least p . In particular, there is a p -tuple $(g, \dots, g) \neq (e, \dots, e)$, such that $g^p = e$. Since p is prime, the order of g must be either p or 1. Since $g \neq e$, it has order p . \square

Let G be a group (not necessarily finite) and H any subgroup of G . Put

$$N_H := \{g \in G \mid gHg^{-1} = H\}.$$

It is easy to check that N_H is a subgroup of G which contains H as a normal subgroup. N_H is called the *normalizer* of H in G . Now, H acts on the right coset space G/H , by left translation. Namely, for $h \in H$ and $x \in G$, $h(xH) = hxH$. We now describe the H fixed point set $(G/H)^H$, in terms N_H .

Theorem 3.15. $(G/H)^H = N_H/H$. In particular, if G is finite and H is a p -subgroup of G , then

$$[N_H : H] \equiv [G : H] \pmod{p}.$$

Proof: For $h \in H$, $x \in G$,

$$hxH = xH \Leftrightarrow x^{-1}hxH = H \Leftrightarrow x^{-1}hx \in H.$$

It follows that $xH \in G/H$ is an H fixed point iff $x^{-1}Hx \subset H$, which is equivalent to that $x^{-1}Hx = H$ (Exercise above.) In turn this is equivalent to that $x \in N_H$. This shows that if $xH \in G/H$, then $xH \in N_H/H$. Conversely, given a coset in N_H/H , say xH with $x \in N_H$, we have $xH \in G/H$.

Now, our second assertion follows immediately from the p -Group Fixed Point Theorem, applied to the H action on G/H . \square

Definition 3.16. If H is a normal subgroup of a group G , we write $H < G$. We say that a finite group G is **solvable**, if there is a chain of subgroups

$$\{e\} = H_0 < H_1 < \dots < H_n = G$$

such that H_i/H_{i-1} is abelian, for $i = 1, \dots, n$. In this case, we call the chain a **normal chain**. Note that for each i , H_{i-1} is assumed normal in H_i , but not necessarily in G .

The next two results strengthen the p -Subgroup Theorem.

Corollary 3.17. *Let G be a p -group and H a subgroup of index $[G : H] = p$. Then H is normal in G .*

Proof: We have $H \subset N_H \subset G$. By Lagrange, $N_H = H$ or $N_H = G$. By the preceding theorem, $[N_H : H] \equiv 0 \pmod{p}$. Thus, $N_H \neq H$, and so $N_H = G$, implying that H is normal in G . \square

Corollary 3.18. (*p -Group Solvability Theorem*) *Every p -group G is solvable. In fact, if G has order p^n , then there is normal chain of subgroups*

$$\{e\} = H_0 < H_1 < \dots < H_n = G$$

such that $[H_i : H_{i-1}] = p$ for each $i = 1, \dots, n$.

Proof: Applied to G , the p -Subgroup Theorem yields a chain of subgroups

$$\{e\} = H_0 \subset H_1 \subset \dots \subset H_n = G.$$

By the preceding corollary, H_{i-1} is normal in H_i , for each $i = 1, \dots, n$. Since the factor group H_i/H_{i-1} has order p , it is cyclic, and therefore abelian. \square

Theorem 3.19. (*First Sylow Theorem*) *Let G be a finite group whose order is divisible by p^n , but not by p^{n+1} . Then G has a subgroup of order p^n .*

Proof: By Cauchy, G has a subgroup of order p . Suppose G has a subgroup H of order p^i for some $i < n$. We will show that G has a subgroup of order p^{i+1} . Put $|G| = p^n q$. Since $i < n$, so p divides $[G : H] = p^{n-i} q$. By the lemma, p divides $[N_H : H]$, which is the order of the factor group N_H/H . By Cauchy again, this group has a subgroup K of order p . Let $\gamma : N_H \rightarrow N_H/H$, $x \mapsto xH$, be the projection homomorphism. By the Group

Homomorphism Theorem, $\gamma^{-1}(K)$ is a subgroup of N_H containing $H = \text{Ker } \gamma$, such that $\gamma^{-1}(K)/H$ is isomorphic to K . It follows that

$$|\gamma^{-1}(K)| = |H| |K| = p^{i+1}. \quad \square$$

Definition 3.20. Let G be a finite group of order divisible by p^n , but not by p^{n+1} . A subgroup of G of order p^n is called a Sylow p -subgroup of G . Thus, it is a maximal p -subgroup of G , i.e. it is not contained in any other p -subgroups of G .

Theorem 3.21. (Second Sylow Theorem) Let G be a finite group. Then any two Sylow p -subgroups of G are conjugate subgroups of G .

Proof: Let A and B be Sylow p -subgroups of G . Consider A acting on G/B by left translation. By the p -group Fixed Point Theorem,

$$|G/B| \equiv |(G/B)^A| \pmod{p}.$$

Put $|G| = p^n q$, so that $(p, q) = 1$. Since $|B| = p^n$, we have $|G/B| = q \equiv 1 \pmod{p}$, so there is at least one A fixed point in G/B , say xB , for some $x \in G$. Then $yxB = xB$ for all $y \in A$, implying that $x^{-1}Ax \subset B$. Since $|A| = p^n = |B|$, it follows that $x^{-1}Ax = B$, as desired. \square

Theorem 3.22. (Third Sylow Theorem) Let m be the number Sylow p -subgroups of G . Then $m \equiv 1 \pmod{p}$, and m divides $|G|$.

Proof: Let X be the set of all Sylow p -subgroups of G . By Cauchy, X is not empty. Pick $A \in X$, and let A act on the set X by conjugation. Clearly $A \in X$ is an A fixed point. Let $B \in X$ be an A fixed point. Then $xBx^{-1} = B$ for all $x \in A$, so $A \subset N_B$. Obviously $B \subset N_B$. This shows that A and B are Sylow p -subgroups of N_B . By Second Sylow, they are conjugate in N_B , i.e. $y^{-1}By = A$ for some $y \in N_B$. But $B = y^{-1}By$, since every $y \in N_B$ normalizes B . So, $B = A$. This shows that $A \in X$ is the only A fixed point. By the p -group Fixed Point Theorem,

$$m = |X| \equiv 1 \pmod{p}.$$

Now, let G acts on X by conjugation. By First Sylow, there is just one G orbit in X . By the Class Equation,

$$m = |X| = [G : G_A]$$

for any $A \in X$. But the right side divides $|G|$. \square

3.4. Some applications

Example. We say that a group is *simple*, if the group itself and $\{e\}$ are the only normal subgroups. Can a group G of order 20 be simple? By the Third Sylow, since $20 = 5 \cdot 4$, the number of Sylow 5-subgroup that G has, is $m \equiv 1 \pmod{5}$, and m divides 20, hence m divides 4. This shows that $m = 1$. Let H be the Sylow 5-subgroup of G . For any $g \in G$, gHg^{-1} has order 5, hence it is also a Sylow 5-subgroup of G , so it must be equal to H . This shows that H is a normal subgroup of G . So G can't be simple.

Theorem 3.23. *Let G be a group of order pq , where p, q be distinct primes with $p < q$. Then G has a single subgroup H of order q , and H is normal. If, in addition, $q \not\equiv 1 \pmod{p}$, then G is isomorphic to $\mathbf{Z}_p \times \mathbf{Z}_q$.*

Proof: By the Third Sylow, the number of Sylow q -subgroups that G has, is $m \equiv 1 \pmod{q}$, and m divides p . Since $p < q$, it follows that $m = 1$. Let H be the Sylow q -subgroup of G . Again, for any $g \in G$, gHg^{-1} is a Sylow q -subgroup of G , hence $gHg^{-1} = H$, and so H is normal in G .

Now suppose $q \equiv 1 \pmod{p}$. The number of Sylow p -subgroups that G has, is $n \equiv 1 \pmod{p}$, i.e. $n = 1 + kp$ for some $k \geq 0$, and n divides q . Since q is prime, $n = 1$ or q . Since $q \equiv 1 \pmod{p}$, we have $n = 1$. So, there is just one Sylow p -subgroup K , and it is normal in G .

Since every non-identity element in H has order q , and every non-identity element in K has order p , it follows that $H \cap K = \{e\}$. By the next lemma, G is isomorphic to $H \times K \cong \mathbf{Z}_q \times \mathbf{Z}_p$. \square

Lemma 3.24. *Let H, K be normal subgroups of a group G such that $H \cap K = \{e\}$. Then $hk = kh$ for all $h \in H, k \in K$. If, in addition, $G = HK$, then G is isomorphic to $H \times K$.*

Proof: Let $h \in H$ and $k \in K$. Note that $hkh^{-1}k^{-1} = h(kh^{-1}k^{-1}) = (hkh^{-1})k^{-1}$. The middle term is in H since H is normal, and the last term is in K since K is normal. So the first term is in $H \cap K = \{e\}$, implying that $hk = kh$.

Now, suppose $G = HK = \{hk | h \in H, k \in K\}$. Define $f : H \times K \rightarrow G, f(h, k) = hk$. Then f is a surjective group homomorphism. If $f(h, k) = e$, then $h = k^{-1} \in H \cap K$, implying that $h = k = e$. So $\text{Ker } f = \{e\}$, and so f is an isomorphism. \square

Example. Any group of order $5 \cdot 7$ is isomorphic to $\mathbf{Z}_5 \times \mathbf{Z}_7$.

4. Galois Theory

Fix a field F . In this lecture, we study structures of algebraic extensions of F by exploiting the symmetry of the roots of polynomials that we use to define those extensions. This is one of Évariste Galois's great ideas. Group Theory enters the picture via symmetry groups. Structural information about those groups will yield important information about the algebraic extensions in question, and vice versa. This lecture may be viewed as a place where Field Theory and Group Theory converge, culminating in a proof that it is impossible to express the roots of a general quintic polynomial equation in terms of its coefficients in the form of radicals. In another application, we will use Galois theory to determine all constructible regular n -gons.

4.1. Symmetry of roots

Throughout this section, F denotes a given field. When α is an element of some algebraic extension field of F , we shall often refer to it as *an element α that is algebraic over F* , without explicitly saying which algebraic extension of F is α an element of. It is convenient to keep one fixed algebraic closure \bar{F} of F in mind, and think of $\alpha \in \bar{F}$. Since any two algebraic closures of F are isomorphic, the choice \bar{F} will play no essential role in any of our discussion.

We remind the reader that a field homomorphism is a ring homomorphism from a field to a field that preserves 1. Since nonzero elements of a field is invertible, it follows that such a field homomorphism is always *injective*. For this reason, it is called an **embedding** of fields.

Definition 4.1. Let E', E be extension fields of F . We say that an embedding $\sigma : E' \rightarrow E$ **fixes** F or that it is an embedding **over** F , if $\sigma a = a$ for all $a \in F$. When $E' = E$, we call a bijective embedding $\sigma : E \rightarrow E$ over F , an **automorphism** of E over F . When F is either \mathbf{Q} or \mathbf{Z}/p , we shall drop the phrase “over F ” or “fixes F ”.

Exercise. Show that an embedding $\sigma : E' \rightarrow E$ fixes F iff σ is linear over F .

Let E', E be extensions of F , and $\sigma : F \rightarrow E$ an embedding (over \mathbf{Q} or \mathbf{Z}/p .) We say that an embedding $\sigma' : E' \rightarrow E$ **prolongs** σ to E' or that σ' **restricts** to σ , if $\sigma' a = \sigma a$ for all $a \in F$. Therefore, an embedding $E' \rightarrow E$ over F prolongs the **inclusion map** $F \rightarrow E, a \mapsto a$, to E' . We now examine in a few situations, conditions under which such a prolongation exists, and count how many there are.

Exercise. Explain why there cannot be an embedding $\mathbf{Q}(\sqrt{2}) \rightarrow \mathbf{Q}(\sqrt{3})$.

An extension field of F of the form $F(\alpha)$ is called a **simple extension** of F . The next theorem tells us when we can or cannot prolong the inclusion map to the simple algebraic extension $E' = F(\alpha)$, and how many ways we can do so.

Theorem 4.2. (*Embedding Theorem*) Let α be an element that is algebraic over F , $g \in F[x]$ the irreducible polynomial of α , and E an extension of F . Then for every root β of g contained in E , there is a unique embedding $\sigma' : F(\alpha) \rightarrow E$ over F such that $\sigma' \alpha = \beta$. Moreover, every prolongation $F(\alpha) \rightarrow E$ over F is determined by a root of g in this way.

Example. There are exactly two embeddings $\mathbf{Q}(i) \rightarrow \mathbf{C}$, since the irreducible polynomial of i over \mathbf{Q} is $x^2 + 1$, which has exactly two roots $\pm i$ in \mathbf{C} . The embeddings map i to $\pm i$ respectively.

We now prove a slightly more general and useful version of the Embedding Theorem, in which the inclusion map $F \rightarrow E$ is replaced by an arbitrary embedding. Consider an embedding $\sigma : F \rightarrow E$. Its image σF is a subfield of E which is isomorphic to F . So, we have a ring isomorphism

$$F[x] \rightarrow \sigma F[x], \quad f = \sum_{i=0}^n a_i x^i \mapsto \sigma f = \sum_{i=0}^n \sigma(a_i) x^i.$$

Theorem 4.3. (*Embedding Theorem'*) Let α be an element that is algebraic over F , $g \in F[x]$ the irreducible polynomial of α , E an extension of F , and $\sigma : F \rightarrow E$ a given embedding. Then for every root β of σg contained in E , there is a unique prolongation $\sigma' : F(\alpha) \rightarrow E$ of σ such that $\sigma'\alpha = \beta$. Moreover, every prolongation $F(\alpha) \rightarrow E$ of the σ is determined by a root of σg in this way.

Proof: By Kronecker, the evaluation map $F[x] \rightarrow F(\alpha)$, $f \mapsto f(\alpha)$, induces an isomorphism $\phi_\alpha : F[x]/(g) \rightarrow F(\alpha)$ over F . The embedding $\sigma : F \rightarrow E$ induces the ring homomorphism $F[x] \rightarrow E$, $f \mapsto \sigma f(\beta)$, whose kernel is the maximal ideal (g) . So, we have an embedding $\sigma'' : F[x]/(g) \rightarrow E$. Composing σ'' with ϕ_α^{-1} , we get an embedding $\sigma' : F(\alpha) \rightarrow E$. By definition,

$$\sigma' f(\alpha) = \sigma'' \circ \phi_\alpha^{-1} f(\alpha) = \sigma''[f + (g)] = \sigma f(\beta).$$

Specializing to $f = a \in F$ constant, we get $\sigma'a = \sigma a$. So, σ' prolongs σ to $F(\alpha)$. Specializing to $f = x$, we get $\sigma'\alpha = \beta$.

On the other hand, since $F(\alpha)$ is generated by α over F , any embedding $\sigma' : F(\alpha) \rightarrow E$ is determined by its value on F and at α . So, if σ' prolongs σ , then it is determined by the value $\sigma'\alpha$ alone. Moreover, if $g = \sum_{i=0}^n a_i x^i$ then $g(\alpha) = \sum_{i=0}^n a_i \alpha^i = 0$. Applying σ' to this yields $\sum_{i=0}^n \sigma a_i (\sigma'\alpha)^i = 0$, which says that $g(\sigma'\alpha) = 0$. So, $\sigma'\alpha \in E$ is necessarily a root of σg . \square

Given an extension field E of F , an automorphism of E over F prolongs the inclusion map $F \rightarrow E$, to E . The set of all such automorphisms form a group under composition. It is called **the Galois group** of E over F , and is denoted by $\text{Gal } E/F$. We will write the **composition** $\sigma \circ \tau$ of $\sigma, \tau \in \text{Gal } E/F$ simply as $\sigma\tau$.

Proposition 4.4. Let $\sigma \in \text{Gal } E/F$, and $f \in F[x]$ any polynomial. If $\alpha \in E$ is a root of f , then so is $\sigma\alpha$. This defines an action of the group $\text{Gal } E/F$ on the set of roots of f in E .

Proof: Let $\alpha \in E$ be a root of f . Then as before, $\sigma\alpha \in E$ is a root of f . Let X be the set of roots of f in E , and define the map

$$\text{Gal } E/F \rightarrow \text{Bij}(X), \quad \sigma \mapsto \phi_\sigma$$

where $\phi_\sigma(\alpha) = \sigma\alpha$, for $\alpha \in X$. This map is a group homomorphism. For if $\sigma, \tau \in \text{Gal } E/F$, then $\phi_{\sigma\tau} = \phi_\sigma \circ \phi_\tau$, and $\phi_e = \text{id}_X$. \square

Example. By the example above, they are exactly two automorphisms $\mathbf{Q}(i) \rightarrow \mathbf{Q}(i) \subset \mathbf{C}$. They map i to $\pm i$ respectively. Thus $\text{Gal } \mathbf{Q}(i)/\mathbf{Q}$ has just two elements $\{e, \sigma\}$.

Definition 4.5. An extension field E' of F is called a **splitting field** of the polynomial $g \in F[x]$ over F , if $E' = F(\alpha_1, \dots, \alpha_n)$ and if $g = c(x - \alpha_1) \cdots (x - \alpha_n)$ for some $c \in F$.

Given a polynomial $g \in F[x]$, a splitting field of g always exists as a subfield of an algebraic closure \bar{F} of F . For since \bar{F} contains all roots $\alpha_1, \dots, \alpha_n$ of g , $F(\alpha_1, \dots, \alpha_n) \subset \bar{F}$ is a splitting field of g . We can also apply Kronecker, repeatedly if necessarily, to construct a splitting field of g over F .

Example. For the irreducible $g = x^2 - 2$ over \mathbf{Q} , once is enough, since $\mathbf{Q}(\sqrt{2})$ is a splitting field of g over \mathbf{Q} . Consider $g = x^4 - 2$, which is also irreducible over \mathbf{Q} (by Eisenstein.) Applying Kronecker once would yield either $\mathbf{Q}(\sqrt[4]{2})$ or $\mathbf{Q}(i\sqrt[4]{2})$, neither is a splitting field of g over \mathbf{Q} . Applying Kronecker once more would yield $\mathbf{Q}(\sqrt[4]{2}, i\sqrt[4]{2})$ which is a splitting field of g .

Note that the same field E can be a splitting field of many different polynomials. For example, $\mathbf{Q}(i)$ is a splitting field of $(x - i)(x + i)$ and $(x - i - 1)(x + i - 1)$ over \mathbf{Q} . But for a given polynomial $g \in F[x]$, a splitting field of g is essentially unique, as we now show.

Theorem 4.6. (*Uniqueness of Splitting Field*) Let $g \in F[x]$, and E', E be two splitting fields of g . Then there is a field isomorphism $\sigma : E' \rightarrow E$ over F . Moreover, if $h \in F[x]$ is an irreducible factor of g , then any such isomorphism maps the roots of h in E' , to those in E .

Proof: Our second assertion follows immediately from the Embedding Theorem. Let $g = c(x - \alpha_1) \cdots (x - \alpha_n)$, where $\alpha_1, \dots, \alpha_n \in E'$. Since E contains a root of g , (hence a root of an irreducible factor of g), the Embedding Theorem implies that there is an embedding $\sigma_1 : F(\alpha_1) \rightarrow E$ over F , such that $\sigma_1\alpha_1$ is a root of g . Repeat this argument for the field

$F(\alpha_1)$, and the root α_2 of $g \in F(\alpha_1)[x]$ in E , we get an embedding $\sigma_2 : F(\alpha_1, \alpha_2) \rightarrow E$ over $F(\alpha_1)$ (hence over F), and $\sigma_2\alpha_2$ is a root of g in E . Continuing this way, we get an embedding $\sigma : F(\alpha_1, \dots, \alpha_n) = E' \rightarrow E$ over F , and $\sigma\alpha_1, \dots, \sigma\alpha_n$ are roots of g in E .

Now σ induces a ring homomorphism $E[x] \rightarrow E'[x]$ such that $x \mapsto x$. Since σ is linear over F , $g \mapsto g$ under this ring homomorphism. It follows that $g = c(x - \sigma\alpha_1) \cdots (x - \sigma\alpha_n)$, and so $\sigma\alpha_1, \dots, \sigma\alpha_n$ are *all* the roots of g in E . It follows that $E = F(\sigma\alpha_1, \dots, \sigma\alpha_n)$. In particular σ is surjective, hence bijective. \square

From now on, we shall speak of **the splitting field** E of a polynomial g over F . We can think of E as the field generated by the roots of g in some fixed algebraic closure \bar{F} of F . The preceding theorem shows that any other choice of algebraic closure will produce an isomorphic splitting field of g .

Here are two easy consequences of the Embedding Theorem.

Corollary 4.7. *The Galois group of any finite extension over F is a finite group.*

Proof: We will show that if $\alpha_1, \dots, \alpha_n$ elements which are algebraic over F , and E is any field, then the set of embeddings $\sigma : F(\alpha_1, \dots, \alpha_n) \rightarrow E$ over F can be parameterized by a finite set of data. Let σ be any such embedding. Then σ is determined by the values $\sigma\alpha_1, \dots, \sigma\alpha_n$. By restrictions, it also defines an embedding $F(\alpha_i) \rightarrow E$ for each i . By the Embedding Theorem, $\sigma\alpha_i$ must be a root of the irreducible polynomial of α_i over F , for each i . So, there are only finitely many possible values $\sigma\alpha_i$ can take, for each i . This shows that there are at most finitely many embeddings σ . Now specializing to the case a finite extension $E = F(\alpha_1, \dots, \alpha_n)$ of F , this shows that there are at most finitely many automorphisms of E over F . \square

Since a splitting field of a polynomial is generated, over F , by the roots of the polynomial, it is a finite extension of F .

Corollary 4.8. *The Galois group of the splitting field of any polynomial over F is a finite group.*

Exercise. Show that $Gal(\mathbf{Q}(\pi)/\mathbf{Q})$ is infinite. (Hint: The automorphism σ of $\mathbf{Q}(\pi)$ over \mathbf{Q} , defined by $\sigma\pi = \pi + 1$, has infinite order.)

Next, we give a crude description of the Galois group of a splitting field of an arbitrary monic polynomial $g \in F[x]$. Let

$$g = h_1^{\mu_1} \cdots h_k^{\mu_k}$$

be its factorization into pairwise distinct monic irreducible h_1, \dots, h_k over F , and $\mu_1, \dots, \mu_k \geq 1$. Let E be the splitting field of g , and X_i be the set of roots of h_i in E , for $i = 1, \dots, k$. By the preceding theorem (applied to $E' = E$), an automorphism $\sigma \in \text{Gal}(E/F)$ maps X_i to X_i bijectively, hence it defines a bijection on X_i , which we denote by σ_i , for each i . From the first paragraph of the proof of the preceding theorem, we see that for $\sigma, \tau \in \text{Gal}(E/F)$, we have $(\sigma\tau)_i = \sigma_i\tau_i$, and $e_i \in \text{Bij}(X_i)$ is the identity map on X_i . This shows that we have a group homomorphism

$$\phi_g(E/F) : \text{Gal}(E/F) \rightarrow \text{Bij}(X_1) \times \cdots \times \text{Bij}(X_k), \quad \sigma \mapsto (\sigma_1, \dots, \sigma_k).$$

Proposition 4.9. *The group homomorphism $\phi_g(E/F)$ is injective.*

Proof: Let $\sigma \in \text{Gal}(E/F)$. If $(\sigma_1, \dots, \sigma_k) = (e_1, \dots, e_k)$, then $\sigma(\alpha) = \alpha$ for each root α of g . Since E is generated over F by all the roots of g , and σ is linear over F , it follows that $\sigma = \text{id}_E$. So, $\phi_g(E/F)$ is injective. \square

Example. $\phi_g(E/F)$ is not surjective in general. Consider $g = x^4 - 2$, which is irreducible over \mathbf{Q} (Eisenstein criterion.) Let $E \subset \mathbf{C}$ be the splitting field of g . The set of roots of g is $X = \{\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}\}$. So, $\text{Bij}(X)$ consists of all permutations of X . But if $\sigma \in \text{Gal}(E/\mathbf{Q})$, then σ is not an arbitrary permutation of X , since $\sigma(-\sqrt[4]{2}) + \sigma\sqrt[4]{2} = 0$. The permutation must respect any algebraic relations that the roots have in E . We will see later that, $\text{Gal}(E/\mathbf{Q})$ has order 4 in this case, which is much smaller than $4!$.

The next three theorems are special to characteristic 0 fields. These theorems will be our main technical tools for proving the Fundamental Theorem of Galois Theory.

Theorem 4.10. (*Distinct Root Theorem*) *In characteristic 0, irreducible polynomials have no multiple roots.*

Proof: Let α be a root of the degree n polynomial $f = cx^n + \cdots$. Then α is a multiple root of f iff $f'(\alpha) = 0$. Suppose f is irreducible. Then $n \geq 1$ and f' has leading term

$ncx^{n-1} \neq 0$. (This is where characteristic 0 is crucial.) So, $f'(\alpha)$ can't be zero, or else it contradicts that f is a lowest degree polynomial having α as a root. Thus, α is not a multiple root of f . \square

Theorem 4.11. (*Counting Embeddings Theorem*) *Let F be a field of characteristic 0, and E be a finite extension of degree n over F . Let $\sigma : F \rightarrow \bar{F}$ be an embedding. Then the number of embeddings $\tau : E \rightarrow \bar{F}$ which prolong σ to E , is n .*

Proof: Suppose first $E = F(\alpha)$, and let f be the irreducible polynomial of α over F , of degree n . Then f has n distinct roots, by the preceding theorem. So, our assertion follows from the Embedding Theorem. In general, we can write

$$E_0 = F \subset E_1 = F(\alpha_1) \subset \cdots \subset E_r = F(\alpha_1, \dots, \alpha_r) = E.$$

Let $n_i = [E_i : E_{i-1}]$. Applying the argument above to $E_2 = E_1(\alpha_2)$, we find that there are exactly n_2 embeddings $\sigma_2 : E_2 \rightarrow \bar{F}$ which prolong a given $\sigma_1 : E_1 \rightarrow \bar{F}$. This gives $n_1 n_2$ embeddings $E_2 \rightarrow \bar{F}$ which prolong $\sigma : F \rightarrow \bar{F}$. Conversely, if $\tau : E_2 \rightarrow \bar{F}$ is a given embedding, then the restriction $\tau|_{E_1}$ is one of the n_1 embeddings $E_1 \rightarrow \bar{F}$. So τ must be one of the n_2 embeddings $\sigma_2 : E_2 \rightarrow \bar{F}$ which prolong $\tau|_{E_1}$. So, the $n_1 n_2$ embeddings $E_r \rightarrow \bar{F}$ we have found, account for all possible embeddings. Continuing this way by induction, we find that there are exactly $n_1 n_2 \cdots n_r$ embeddings $E_r \rightarrow \bar{F}$ which prolong $\sigma : F \rightarrow \bar{F}$. By the Degree Factorization Theorem, $n = [E : F] = n_1 \cdots n_r$. \square

Theorem 4.12. (*Primitive Element Theorem*) *In characteristic 0, every finite extension is a simple extension.*

Proof: Since every finite extension is finitely generated over F , it suffices to prove that if α, β are algebraic over F , then $F(\alpha, \beta) = F(\gamma)$ for some γ . For then the general case can be obtained by reducing the number of generators, one at a time, this way. Put $E = F(\alpha, \beta)$, $n = [E : F]$. By the preceding theorem, there are exactly n distinct embeddings $\sigma_1, \dots, \sigma_n : E \rightarrow \bar{F}$ which prolong the inclusion map $F \rightarrow \bar{F}$. Clearly, each σ_i is determined by the values $\sigma_i \alpha$ and $\sigma_i \beta$. It follows that the polynomial

$$f = \prod_{i=1}^n \prod_{j \neq i} [\sigma_j \alpha - \sigma_i \beta + x(\sigma_j \beta - \sigma_i \beta)]$$

is nonzero because each factor is nonzero. Since f has only a finite number of roots, and F is infinite (since $\mathbf{Q} \subset F$), we can find $c \in F$ such that $f(c) \neq 0$. It follows that $\sigma_i(\alpha + c\beta)$ are distinct, for $i = 1, \dots, n$.

We claim that $E = F(\gamma)$, where $\gamma = \alpha + c\beta$. Since $\gamma \in E$, we have $E \supset F(\gamma)$. By restrictions, we have embeddings $\sigma_i|_{F(\gamma)}$ from $F(\gamma)$ to \bar{F} which prolong the inclusion $F \rightarrow \bar{F}$. We have shown that $\sigma_1\gamma, \dots, \sigma_n\gamma$ are distinct. So, the embeddings $\sigma_i|_{F(\gamma)}$ are distinct. By the Counting Embeddings Theorem, $[F(\gamma) : F] \geq n$. Since $[E : F] = n$, it follows that $F(\gamma) = E$. \square

Corollary 4.13. *In characteristic 0, there is a bijection between the set of monic irreducible polynomials over F and the set isomorphism classes of finite extensions over F .*

Proof: For each monic irreducible $g \in F[x]$, we have a finite extension $F[x]/(g)$ of F , by Kronecker. For a given finite extension E over F , we have $E = F(\gamma)$ for some element γ , by the Primitive Element Theorem. So, there is a unique monic irreducible g over F such that $F[x]/(g) \rightarrow F(\gamma)$, $f + (g) \mapsto f(\gamma)$, is an isomorphism over F . Moreover, if $\tau : E' \rightarrow E$ is a given isomorphism over F (i.e. it fixes F), then we can write $E' = F(\gamma')$ and $E = F(\tau\gamma')$ for some γ' . Since τ fixes F , it follows that γ' and $\tau\gamma'$ have the same irreducible polynomial. This shows that two finite extensions which are isomorphic over F , corresponds to the same monic irreducible polynomial. \square

Note that the second and third theorems relies crucially on the first theorem. In prime characteristic, we must replace the first theorem by an assumption that the irreducible polynomial being considered has no multiple roots. The resulting extension is called a **separable extension**.

4.2. Galois theory

Throughout this section, F denotes a field, and \bar{F} a given algebraic closure of F . All algebraic extensions of F are regarded as subfields of \bar{F} .

Let K be an extension of F . Let G be a subgroup of $\text{Gal } K/F$. Then G acts on the field K by automorphisms. Denote the set of G fixed points by K^G . Let E be any intermediate field between K and F , i.e. $K \geq E \geq F$. We call E a subfield of K/F .

Exercise. Check that K^G is a subfield of K that contains F , and that $\text{Gal } K/E$ is a subgroup of $\text{Gal } K/F$. K^G is called **the fixed field** of G .

There are two obvious mappings:

$$G \mapsto K^G$$

$$E \mapsto \text{Gal } K/E.$$

The first mapping assigns to each subgroup G of $\text{Gal } K/F$, the subfield K^G of K/F . The second mapping assigns to each subfield E of K/F , the subgroup $\text{Gal } K/E$ of $\text{Gal } K/F$. The two mappings have the following basic properties, which are easy consequences of the definitions. For subgroups G, G_1, G_2 of $\text{Gal } K/F$ and subfields E_1, E_2 of K/F , we have

i. $G_1 \supset G_2 \implies K^{G_1} \subset K^{G_2}$

ii. $E_1 \supset E_2 \implies \text{Gal } K/E_1 \subset \text{Gal } K/E_2$

iii. $K^{\text{Gal } K/E} \supset E$

iv. $\text{Gal } K/K^G \supset G$.

Under some hypothesis on K , the main theorem of Galois theory says that these mappings are bijections. The main hypothesis is formalized in the next definition.

Definition 4.14. We say that a finite extension K of F is **normal** if every embedding $\sigma : K \rightarrow \bar{F}$ over F maps K to K . In other words, there is exactly one copy of K that contains F , inside \bar{F} .

Theorem 4.15. Let K be a normal extension of F , and g be an irreducible polynomial over F . If K contains one root of g , then it contains all roots of g .

Proof: Let $\alpha \in K$ be a root of g , and β be any other root of g . By the Embedding Theorem, we have an embedding $\sigma : K \rightarrow \bar{F}$ with $\sigma\alpha = \beta$. Since K is normal, $\sigma K = K$, and so $\beta \in K$. \square

Theorem 4.16. (*Normality Criterion*) In characteristic 0, a finite extension K of F is normal iff K is the splitting field of a polynomial over F .

Proof: Suppose K is the splitting field of $g \in F[x]$. Then K is generated over F by the roots of g , say $K = F(\alpha_1, \dots, \alpha_n)$. Let $\sigma : K \rightarrow \bar{F}$ be an embedding. By the Embedding Theorem, each $\sigma\alpha_i$ is also a root of g . So, $\sigma K \subset K$. But K is finite dimensional over F , and σ is injective. So $\sigma K = K$. This shows that K is normal.

Conversely, suppose K is normal over F . By the Primitive Element Theorem, we have $K = F(\gamma)$ for some γ . Let g be the irreducible polynomial of γ over F . By the preceding theorem, K contains all roots of g , and so K is the splitting field of g over F .

□

Remark 4.17. Let K be a finite normal extension over F , and E be any intermediate field, i.e. $K \geq E \geq F$. Any embedding $\sigma : K \rightarrow \bar{F} = \bar{E}$ over E is an embedding over F , and so $\sigma K = K$. It follows that K is normal over E as well.

Example. An intermediate field in a normal extension over F need not be normal over F . Then field $E = \mathbf{Q}(\sqrt[4]{2})$ has degree 4 over \mathbf{Q} , since $x^4 - 2$ is the irreducible polynomial of $\sqrt[4]{2}$ over \mathbf{Q} . But E is not normal over \mathbf{Q} , since E does not contain the root $i\sqrt[4]{2}$ of $x^4 - 2$. In fact, the embedding $\sigma : E \rightarrow \bar{\mathbf{Q}}$ with $\sigma\sqrt[4]{2} = i\sqrt[4]{2}$, does not map E to E . Now $K = E(i) \geq E \geq F$, and K has degree 8 and is normal over \mathbf{Q} because it is the splitting field of $x^4 - 2$.

For the rest of the section, we shall assume that F has **characteristic 0**.

Definition 4.18. A finite normal extension E of F , is called a **Galois extension** of F .

Theorem 4.19. (*Fixed Field Theorem*) Let K be a Galois extension of F . Then F is the fixed field of $\text{Gal } K/F$.

Proof: Let E be the fixed field of $\text{Gal } K/F$. Trivially, $F \subset E$. Suppose $\alpha \in E, \notin F$. By the Embedding Theorem, there is an embedding $\sigma : F(\alpha) \rightarrow \bar{F}$ which prolongs the inclusion

map $F \rightarrow \bar{F}$ and has $\sigma\alpha \neq \alpha$. By the Prolongation Theorem, we can extend this to an isomorphism $\bar{F} \rightarrow \bar{F}$, which restricts to an embedding $\sigma' : K \rightarrow \bar{F}$. Since K is normal over F , we have $\sigma'K = K$, i.e. $\sigma' \in \text{Gal } K/F$. It follows that σ' fixes E , and so $\sigma'\alpha = \alpha$. But σ' prolongs $\sigma : F(\alpha) \rightarrow \bar{F}$, implying that $\sigma'\alpha = \sigma\alpha$. This implies that $\sigma\alpha = \alpha$, a contradiction. Thus $E = F$. \square

Theorem 4.20. (*Galois Degree Theorem*) *Let K be a Galois extension of degree n over F . Then $\text{Gal } K/F$ has order n .*

Proof: By the Primitive Element Theorem, we can write $K = F(\gamma)$ for some γ , of degree $n = [K : F]$ over F . Let g be the irreducible polynomial of K over F . Since K is Galois over F , automorphisms in $\text{Gal } K/F$ correspond 1-1 with embeddings $K = F(\gamma) \rightarrow \bar{F}$. By the Embedding Theorem, the latter correspond 1-1 with the roots of g , which are distinct, by the Distinct Root Theorem. It follows that they are exactly n elements in $\text{Gal } K/F$. \square

Theorem 4.21. (*Fundamental Theorem of Galois Theory*) *Let K be a Galois extension of F . Let Γ be the set of subgroups of $\text{Gal } K/F$, and Φ the set of subfields of K/F . Then the mappings*

$$\begin{aligned} \Gamma &\rightarrow \Phi, G \mapsto K^G \\ \Phi &\rightarrow \Gamma, E \mapsto \text{Gal } K/E \end{aligned}$$

are inverses of each other.

Proof: Let E be an intermediate field between K and F . We saw that K is Galois over E . By the Fixed Field Theorem, E is the fixed field of $\text{Gal } K/E$. It follows that if two intermediate fields E, E' are distinct, then $\text{Gal } K/E, \text{Gal } K/E'$ are distinct. So, the mapping $E \mapsto \text{Gal } K/E$ is injective.

Let G be a subgroup of $\text{Gal } K/F$. Then K is Galois over the intermediate field $E = K^G$, as before. Obviously we have $G \subset \text{Gal } K/E$. Let $\sigma_1, \dots, \sigma_r$ be the elements of G . By the Primitive Element Theorem, we can write $K = E(\gamma)$ for some γ . Put

$$f = (x - \sigma_1\gamma) \cdots (x - \sigma_r\gamma).$$

Observe that $\sigma f = f$ for any $\sigma \in G$. So, each of the coefficients of f is fixed by G , i.e. $f \in K^G[x] = E[x]$. So, K is generated by a root γ of a polynomial in $E[x]$ of degree r , implying that $[K : E] \leq r$. By the Galois Degree Theorem, we have $|\text{Gal } K/E| \leq |G|$, implying that $G = \text{Gal } K/E$. This shows that the mapping $E \mapsto \text{Gal } K/E$ is surjective. The surjectivity proof also shows that $G \mapsto K^G$ is the inverse of this mapping. \square

Corollary 4.22. *For $G, G_1, G_2 \in \Gamma$, we have*

$$(a) \ G_1 \supset G_2 \Leftrightarrow K^{G_1} \subset K^{G_2}.$$

$$(b) \ |G| = [K : K^G]$$

$$(c) \ |\text{Gal } K/F : G| = [K^G : F].$$

Proof: (a) That $G_1 \supset G_2 \implies K^{G_1} \subset K^{G_2}$ is trivial. Conversely, suppose

$$K^{G_1} \subset K^{G_2}.$$

Then every automorphism of K that fixes K^{G_2} also fixes K^{G_1} , implying that

$$\text{Gal } K/K^{G_1} \supset \text{Gal } K/K^{G_2}.$$

By the Fundamental Theorem, we have $G_1 = \text{Gal } K/K^{G_1}$ and $G_2 = \text{Gal } K/K^{G_2}$, and so $G_1 \supset G_2$.

(b) Again, by the Fundamental Theorem, $G = \text{Gal } K/K^G$. Since K is Galois over the intermediate field K^G , by the Galois Degree Theorem $|G| = |\text{Gal } K/K^G| = [K : K^G]$.

(c) By the Galois Degree Theorem and the Degree Factorization Theorem,

$$|\text{Gal } K/F| = [K : F] = [K : K^G][K^G : F].$$

But the left side is $|G| |\text{Gal } K/F : G|$. Now (c) follows from (b). \square

We omit the proof of the following theorem, which requires a little more technical preparation and a use of the Fundamental Theorem.

Theorem 4.23. *Let G be a subgroup of $\text{Gal } K/F$, as before. Then G is normal in $\text{Gal } K/F$ iff K^G is normal over F . In this case,*

$$\text{Gal } K^G/F \cong (\text{Gal } K/F)/G.$$

The one-to-one correspondence $\Gamma \leftrightarrow \Phi$ in the Fundamental Theorem is called the **Galois Correspondence** for the Galois extension K of F . This correspondence translates back and forth between information about subgroups of $\text{Gal } K/F$, and information about subfields of K/F . For finite Galois extension K over F , $\text{Gal } K/F$ is a finite group. So, if we can identify this group, we can in principle find all its subgroups and determine when any two subgroups $G_1, G_2 \in \Gamma$ have the relation $G_1 \supset G_2$. The complete list of such subgroup inclusions is called the **group diagram** for E/F . Corollary (a) to the Fundamental Theorem says that from the group diagram, we can get a complete list of subfields of K/F , namely, $\Phi = \{K^G | G \in \Gamma\}$, and determine when any two subfields have the relation $K^{G_1} \subset K^{G_2}$. The complete list of such subfield inclusions is called the **field diagram** for E/F .

Example. Let $K = \mathbf{Q}(\sqrt{2}, \sqrt{3})$, which has degree 4 over $F = \mathbf{Q}$. Clearly K is the splitting field of $g = (x^2 - 2)(x^2 - 3)$, and so K is Galois over F by the Normality Criterion. By the Galois Degree Theorem, $\text{Gal } K/F$ has order $[K : F] = 4$. Let $\sigma \in \text{Gal } K/F$. By the Embedding Theorem, $\sigma\sqrt{2} \in \{\pm\sqrt{2}\}$ and $\sigma\sqrt{3} \in \{\pm\sqrt{3}\}$. Since K is generated over F by $\sqrt{2}, \sqrt{3}$, it follows that σ is determined by its values at these two points of K . This shows that $\text{Gal } K/F = (\sigma_1, \sigma_2)$, where

$$\begin{aligned}\sigma_1\sqrt{2} &= -\sqrt{2}, & \sigma_1\sqrt{3} &= \sqrt{3} \\ \sigma_2\sqrt{2} &= \sqrt{2}, & \sigma_2\sqrt{3} &= -\sqrt{3}.\end{aligned}$$

The group diagram for K/F is given by

$$G = \text{Gal } K/F \supset (\sigma_1), (\sigma_2), (\sigma_1\sigma_2) \supset (e).$$

Note that all three intermediate subgroups are normal in G . To work out the field diagram, we consider the subfields of K/F fixed by these groups. Now an element of K can be uniquely written in the form $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$, with $a, b, c, d \in \mathbf{Q}$. It is easy to work out the elements that are fixed by σ_1 , and those fixed by σ_2 . The field diagram is

$$K^G = \mathbf{Q} \subset K^{(\sigma_1)} = \mathbf{Q}(\sqrt{3}), K^{(\sigma_2)} = \mathbf{Q}(\sqrt{2}), K^{(\sigma_1\sigma_2)} = \mathbf{Q}(\sqrt{6}) \subset \mathbf{Q}(\sqrt{2}, \sqrt{3}) = K.$$

4.3. Cyclotomic fields

Throughout this section, F denotes a field, n a positive integer which is not divisible by char F , and \bar{F} a fixed algebraic closure of F .

Definition 4.24. *The n th cyclotomic extension of F is the splitting field of $x^n - 1$.*

Thus a cyclotomic extension of F can be obtained from F by adjoining to F the roots $\alpha \in \bar{F}$ of $x^n - 1$, which we call n th roots of unity.

Proposition 4.25. *The set of roots of $x^n - 1$ in \bar{F} is a cyclic group of order n . In particular, it has exactly $\varphi(n)$ elements of order n .*

Proof: It is easy to check that 1 is a root, and if α, β are roots, then so is $\alpha\beta^{-1}$. Thus the set of roots of $x^n - 1$ form a group under field multiplication. Let α be a root. By long division, we get

$$g(x) = (x^n - 1)/(x - \alpha) = x^{n-1} + \alpha x^{n-2} + \cdots + \alpha^{n-1}.$$

So, $g(\alpha) = n\alpha^{n-1} \neq 0$ since n is not divisible by $\text{char } F$. This shows that $x^n - 1$ has n distinct roots. Now, recall the fact that any multiplicative finite group in a field is cyclic. So, the roots form a group isomorphic to \mathbf{Z}_n . The number elements of order n is the number $\varphi(n)$ of integers k , with $1 \leq k \leq n$, which are coprime with n . \square

Each order n element of the group of roots of $x^n - 1$ is called a *primitive n th root of unity* over F .

Corollary 4.26. *The n th cyclotomic extension of F is $F(\alpha)$, where α is any primitive n th root of unity over F .*

Definition 4.27. *Let $\alpha_i, i = 1, \dots, \varphi(n)$, be the primitive n th roots of unity over F . We call*

$$\Phi_n = \prod_{i=1}^{\varphi(n)} (x - \alpha_i) \in \bar{F}[x]$$

the n th cyclotomic polynomial over F .

Let R_n be the set of primitive n th roots of unity in \bar{F} . Then $\Phi_n = \prod_{\alpha \in R_n} (x - \alpha)$. Since set of all roots of $x^n - 1$ in \bar{F} is a cyclic group of order n , it follows that

$$x^n - 1 = \prod_{d|n} \Phi_d$$

and that

$$\Phi_n = \frac{x^n - 1}{\prod_{d|n, d < n} \Phi_d}.$$

This allows us to compute the Φ_n recursively by the division algorithm. We have $\Phi_1 = x - 1$, and

$$\Phi_2 = \frac{x^2 - 1}{x - 1} = x + 1, \quad \Phi_3 = \frac{x^3 - 1}{x - 1} = x^2 + x + 1.$$

Note that if F has characteristic 0, then in each step, we are dividing monic polynomial in $\mathbf{Z}[x]$ by a divisor which is a monic polynomial in $\mathbf{Z}[x]$, and so the result is also a monic polynomial in $\mathbf{Z}[x]$. If F has characteristic $p > 0$, then the computation can be done over \mathbf{Z}_p , under the assumption that $(p, n) = 1$. Note that when p divides n , then over any field F of characteristic p , every root of $x^n - 1$ is a multiple root because its derivative is identically zero.

To summarize, we have

Theorem 4.28. (*Cyclotomic Polynomial*) $\Phi_n \in \mathbf{Z}[x]$ if $\text{char } F = 0$, and $\Phi_n \in \mathbf{Z}_p[x]$ if $\text{char } F = p > 0$.

Exercise. Show that if p is prime, then $\Phi_p = x^{p-1} + x^{p-2} + \cdots + 1$ over F , with $\text{char } F \neq p$.

We now restrict ourselves to the case $F = \mathbf{Q}$.

Lemma 4.29. (*Gauss Lemma*) Let $f_1, f_2 \in \mathbf{Z}[x]$, such that the coefficients of each f_i have no common factor in \mathbf{Z} . Then the coefficient of $f_1 f_2$ have no common factor in \mathbf{Z} .

Proof: Let p be a prime. The projection map $\mathbf{Z} \rightarrow \mathbf{Z}/p$ induces a ring homomorphism $\mathbf{Z}[x] \rightarrow \mathbf{Z}/p[x]$, $f \mapsto \bar{f}$. Suppose p is a common factor of the coefficients of $f_1 f_2$. Then $\overline{f_1 f_2} = \bar{f}_1 \bar{f}_2 = \bar{0}$. Since \mathbf{Z}/p is a field, $\mathbf{Z}/p[x]$ is a domain. So, $\bar{f}_1 = \bar{0}$ or $\bar{f}_2 = \bar{0}$, contradicting the assumption that the coefficients of each f_i have no common factor in \mathbf{Z} .

□

Lemma 4.30. *Let ζ be a primitive n th root of unity in $\bar{\mathbf{Q}} \subset \mathbf{C}$. Then the primitive n th roots of unity are exactly those ζ^k , with $1 \leq k \leq n$ and $(k, n) = 1$.*

Proof: By the primitivity assumption, ζ has order n and so $\{\zeta, \dots, \zeta^n\}$ is the group of all the n th roots of unity in $\bar{\mathbf{Q}}$. Since ζ is a generator, for $k \geq 1$, ζ^k is a generator iff $(k, n) = 1$.

□

Theorem 4.31. *(Cyclotomic Degree) Let ζ be a primitive n th root of unity in $\bar{\mathbf{Q}} \subset \mathbf{C}$. Then*

$$[\mathbf{Q}(\zeta) : \mathbf{Q}] = \varphi(n).$$

Proof: Since ζ is a root Φ_n , which is a polynomial in $\mathbf{Q}[x]$ by the Cyclotomic Polynomial Theorem, it follows that the degree of ζ over \mathbf{Q} is at most $\deg \Phi_n = \varphi(n)$. Let f be the irreducible polynomial of ζ over \mathbf{Q} . Then $\deg f \leq \varphi(n)$, and f divides $x^n - 1$, say

$$x^n - 1 = fh.$$

We can find positive integers a, b such that $af, bh \in \mathbf{Z}[x]$, and that the coefficients of each of them has no common factors in \mathbf{Z} . By the Gauss Lemma, the coefficients of $afbh = ab(x^n - 1)$ have no common factors in \mathbf{Z} , implying that $ab = 1$, which implies that $f, h \in \mathbf{Z}[x]$.

Let p be a prime with $(p, n) = 1$. Then ζ^p is a primitive n th root of unity, and so, by the lemma, every other primitive n th root of unity can be obtained from it by raising it repeatedly to some prime q power, with $(q, n) = 1$. It is enough to show that ζ^p is root of f . For this shows that every primitive n th root of unity is root of f , implying that $\deg f \geq \varphi(n)$, which implies that $\deg f = \varphi(n)$, completing the proof.

Suppose ζ^p is not a root of f . Then ζ^p is a root of h , and so ζ is root of $h(x^p)$. Since f is the irreducible polynomial of ζ , f divides $h(x^p)$, say

$$h(x^p) = f(x)g(x).$$

Since $a^p \equiv a \pmod p$ for any $a \in \mathbf{Z}$, and since the binomial coefficients $\binom{p}{k}$ is divisible by p for $0 < k < p$ (exercise,) it follows that $(u + v)^p \equiv u^p + v^p \pmod p$ for any $u, v \in \mathbf{Z}[x]$. Applying this repeatedly to $h(x)^p$, we find

$$h(x^p) \equiv h(x)^p \pmod p$$

and we get

$$\bar{h}(x)^p = \bar{f}(x)\bar{g}(x)$$

where $\bar{f}, \bar{g}, \bar{h} \in \mathbf{Z}/p[x]$ are reductions of $f, g, h \pmod p$. This shows that \bar{h} and \bar{f} have common polynomial factors in the ring $\mathbf{Z}/p[x]$, implying that $\bar{f}(x)\bar{h}(x)$ has multiple roots.

But

$$x^n - \bar{1} = \bar{f}(x)\bar{h}(x)$$

has no multiple roots, as can be seen by differentiation of the left side (and using the fact that $(p, n) = 1$.) This contradiction shows that ζ^p is a root of f . \square

Corollary 4.32. Φ_n is the irreducible polynomial of each primitive n th root of unity in $\bar{\mathbf{Q}}$.

Theorem 4.33. (Cyclotomic Group) Let ζ be a primitive n th root of unity in $\bar{\mathbf{Q}} \subset \mathbf{C}$. Then $\text{Gal } \mathbf{Q}(\zeta)/\mathbf{Q}$ is isomorphic to the group \mathbf{Z}_n^\times of invertible elements in the ring \mathbf{Z}_n , hence it has order $\varphi(n)$.

Proof: Fix a primitive n th root of unity $\zeta \in \bar{\mathbf{Q}}$. Then ζ, \dots, ζ^n are all the n th roots of unity, and $E_n = \mathbf{Q}(\zeta, \dots, \zeta^n) = \mathbf{Q}(\zeta)$. Any primitive n th root of unity is a root of the irreducible polynomial Φ_n over \mathbf{Q} , by the corollary. So, by the Embedding Theorem, given any primitive n th root of unity β , there is a unique $\sigma_\beta \in \text{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$ such that $\sigma_\beta \zeta = \beta$. It follows that the map

$$\mathbf{Z}_n^\times = \{d \mid 1 \leq d \leq n, (d, n) = 1\} \rightarrow \text{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q}), \quad d \mapsto \sigma_{\zeta^d}$$

is bijective. It is easy to check that this is a group homomorphism, using that $\zeta^n = 1$. \square

Example. $x^4 + 1$ is the only irreducible monic factor of $x^8 - 1$ over \mathbf{Q} of degree $4 = \varphi(8)$. So, it must be equal to Φ_8 . Its splitting field is $\mathbf{Q}(e^{i\pi/4})$ which has Galois group isomorphic

to the group $\{1, 3, 5, 7\} \subset \mathbf{Z}_8$, under multiplication mod 8. Since every element of this 4-element group square to 1, it is isomorphic to $\mathbf{Z}_2 \times \mathbf{Z}_2$.

Example. Let p be a prime. Then \mathbf{Z}_p^\times is $\{1, 2, \dots, p-1\} \subset \mathbf{Z}_p$, which is a cyclic group since it is a finite multiplicative subgroup of a field.

4.4. Constructible polygons

Throughout this section, n denotes a positive integer, and $\zeta = e^{2\pi i/n}$.

Recall that the regular n -gon is constructible iff $\cos \frac{2\pi}{n}$ is constructible. Since $\sin^2\theta + \cos^2\theta = 1$, $\cos \theta$ is constructible iff $\sin \theta$ is constructible, since the field k of real constructible numbers is closed under taking square roots of positive elements. Put

$$\zeta = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}.$$

Then the regular n -gon is constructible iff ζ is constructible.

Suppose ζ is constructible. Then $[\mathbf{Q}(\zeta) : \mathbf{Q}]$ is a power of 2, by the 2-Power Theorem. It follows that $\varphi(n)$ is a power of 2, by the Cyclotomic Degree Theorem. We claim that then n must have the form

$$n = 2^e p_1 \cdots p_r$$

where $e \geq 0$ and p_1, \dots, p_r are distinct Fermat primes, i.e. primes of the form $2^{2^k} + 1$. (This includes the case when n is just a power of 2 and $r = 0$.) First, we can write

$$n = 2^e p_1^{m_1} \cdots p_r^{m_r}$$

where $e \geq 0$, $m_1, \dots, m_r \geq 1$ and p_1, \dots, p_r are distinct primes. By elementary counting, we can show that

$$\varphi(n) = 2^{e-1} p_1^{m_1-1} \cdots p_r^{m_r-1} (p_1 - 1) \cdots (p_r - 1).$$

This is a power of 2 iff $m_1 = \cdots = m_r = 1$ and $p_i - 1$ is a power of 2 for each i .

Suppose p is a prime such that $p-1$ is a power of 2, say 2^m . If m is an odd number, then polynomial $x^m + 1$ is divisible by the polynomial $x + 1$, say $x^m + 1 = (x + 1)h(x)$ where $h(x)$ has integer coefficients. Likewise, if m is divisible by an odd number $k > 1$, then $x^m + 1 = (x^{m/k} + 1)h(x)$ where $h(x) \in \mathbf{Z}[x]$. It follows that if m is divisible by an

odd number $k > 1$, then $p = 2^m + 1$ is divisible by $2^{m/k} + 1 < p$, which is a contradiction. Thus, in order for a prime p to have the form $2^m + 1$, it is necessary (but not sufficient!) that m is itself a power of 2, i.e. p is necessarily a Fermat prime. To summarize, we have shown that

if $\zeta = e^{2\pi i/n}$ is constructible, then $n = 2^e p_1 \cdots p_r$ for some $e \geq 0$ and distinct Fermat primes p_1, \dots, p_r (possibly $r = 0$.)

Exercise. Show that the regular 7-gon is not constructible.

We now proceed to prove the converse. Suppose $n = 2^e p_1 \cdots p_r$, for some $e \geq 0$ and distinct Fermat primes p_1, \dots, p_r . Then $\varphi(n) = [\mathbf{Q}(\zeta) : \mathbf{Q}]$ is a power of 2, as we have just seen. By the Cyclotomic Group Theorem, $G = \text{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$ has order exactly $N = \varphi(n)$. By the p -Group Solvability Theorem, there is a chain of 2-subgroups

$$\{e\} = H_0 < H_1 < \cdots < H_N = G$$

such that $[H_j : H_{j-1}] = 2$ for each $j = 1, \dots, N$. Since $\mathbf{Q}(\zeta)$ is the splitting field of $x^n - 1$ over \mathbf{Q} , which has no multiple roots, it follows that $\mathbf{Q}(\zeta)$ is normal (and automatically separable since we are in characteristic 0) over \mathbf{Q} , i.e. $\mathbf{Q}(\zeta)$ is a Galois extension of \mathbf{Q} . So we can apply **the Fundamental Theorem of Galois Theory** to find a chain of extension fields

$$\mathbf{Q} = K_0 < K_1 < \cdots < K_N = \mathbf{Q}(\zeta)$$

such that $[K_j : K_{j-1}] = 2$ for each $j = 1, \dots, N$. It follows that $K_j = K_{j-1}(\alpha_{j-1})$ where α_{j-1} is a root of a degree 2 polynomial in $K_{j-1}[x]$. By the Property Q of the field of constructible numbers K (as proved in a homework assignment,) it follows that $\alpha_1, \dots, \alpha_N \in K$, which implies that $\zeta \in K$. This concludes the proof of

Theorem 4.34. (Gauss) *The regular n -gon is constructible iff $n = 2^e p_1 \cdots p_r$ for some $e \geq 0$ and distinct Fermat primes p_1, \dots, p_r (possibly $r = 0$.)*

Exercise. Show that the regular 17-gon is constructible. C.F. Gauss gave an explicit construction of this in his famous book *Disquisitiones Arithmeticae*. He liked the picture so much that he decided to have it carved on his tomb stone!

4.5. Galois Solvability Criterion

Throughout this section, F denotes a field of characteristic 0. All algebraic extensions of F are regarded as subfields of a fixed algebraic closure \bar{F} of F .

Definition 4.35. We say that K is an **extension by radicals** over F , if there exist $\alpha_1, \dots, \alpha_r \in K$ such that $K = F(\alpha_1, \dots, \alpha_r)$ and $\alpha_i^{n_i} \in F(\alpha_1, \dots, \alpha_{i-1})$ for $i = 1, \dots, r$. For $g \in F[x]$, we say that the equation $g(x) = 0$ is **solvable by radicals** over F , if there is an extension by radicals K over F such that K contains the splitting field of g .

In other words, a polynomial equation $g(x) = 0$ is solvable by radical over F , if we can express each root of g by a finite number of field operations and extractions of certain n th roots, starting from elements of the base field F .

Definition 4.36. Let $g \in F[x]$ be a polynomial that has distinct roots in its splitting field E over F . We call $\text{Gal } E/F$ the **Galois group** of g .

Theorem 4.37. (Galois Solvability Criterion) An equation $g(x) = 0$ is solvable by radicals over F of characteristic 0 iff its Galois group is solvable.

The proof uses the Galois Correspondence along with a number of technical results involving splitting fields of $x^n - a$ over extensions of F . We omit the proof.

4.6. Insolvability of the quintic

We now explain the crowning achievement of E. Galois – proving that a general degree 5 polynomial equation cannot be solved by radicals – using a theory he had created.

Let $y_1, \dots, y_k \in \mathbf{R}$. Then $\mathbf{Q}(y_1, \dots, y_k)$ is a countable set, and so \mathbf{R} has uncountable dimension over $\mathbf{Q}(y_1, \dots, y_k)$. In particular, there exists $y \in \mathbf{R}$ which is transcendental over $\mathbf{Q}(y_1, \dots, y_k)$. Choose $y_1, \dots, y_5 \in \mathbf{R}$ so that y_{k+1} is transcendental over $\mathbf{Q}(y_1, \dots, y_k)$,

for $k = 1, \dots, 4$. It follows that there is an isomorphism from $\mathbf{Q}(y_1, \dots, y_k)$ to the field of rational functions in 5 variables $\mathbf{Q}(x_1, \dots, x_5)$, with $y_i \mapsto x_i$. Put

$$g = (x - y_1) \cdots (x - y_5) = \sum_{i=0}^5 (-1)^i s_{5-i} x^i$$

where

$$\begin{aligned} s_0 &= 1 \\ s_1 &= \sum_j y_j \\ s_2 &= \sum_{j < k} y_j y_k \\ &\vdots \\ s_5 &= y_1 y_2 y_3 y_4 y_5. \end{aligned}$$

The $s_1, \dots, s_k \in \mathbf{Q}[y_1, \dots, y_k]$ are called **elementary symmetric functions** in 5 variables. Each such polynomial $s_i(y_1, \dots, y_5)$ has the symmetry property that it remains unchanged when we interchange any two of the y 's. Consider the field extensions

$$\mathbf{Q} \leq F = \mathbf{Q}(s_1, \dots, s_5) \leq E = \mathbf{Q}(y_1, \dots, y_5).$$

Since $F(y_1, \dots, y_5) = E$, it follows that E is the splitting field of the polynomial $g \in F[x]$ over F .

Lemma 4.38. *Gal E/F is isomorphic to the symmetric group S_5 .*

Proof: The Embedding Theorem gives us an injective group homomorphism $\phi_g : \text{Gal } E/F \rightarrow \text{Bij}(\{y_1, \dots, y_5\}) \cong S_5$. We will show that it is also surjective. Let $\sigma \in S_5$, a permutation of the set $\{x_1, \dots, x_5\}$. Then σ induces an automorphism on $\mathbf{Q}(x_1, \dots, x_5)$, hence on E , $\hat{\sigma} : E \rightarrow E$ such that for each i , $\hat{\sigma} y_i = y_{\sigma(i)}$ and

$$\hat{\sigma} s_i(y_1, \dots, y_5) = s_i(y_{\sigma(1)}, \dots, y_{\sigma(5)}) = s_i(y_1, \dots, y_5)$$

by the symmetry property of the polynomial s_i . It follows that $\sigma \alpha = \alpha$ for all $\alpha \in F = \mathbf{Q}(s_1, \dots, s_5)$. So, $\hat{\sigma} \in \text{Gal } E/F$. By definition, the bijection $\phi_g(\hat{\sigma}) \in \text{Bij}(\{y_1, \dots, y_5\})$ is given by $\phi_g(\hat{\sigma}) : y_i \mapsto \hat{\sigma} y_i = y_{\sigma(i)}$. In other words, $\phi_g(\hat{\sigma}) = \sigma$. This shows that ϕ_g is surjective.

□

Theorem 4.39. (*Galois*) *It is impossible to solve a general degree 5 equation by radicals.*

Proof: Since S_5 has exactly three normal subgroups $\{e\}$, A_5 and S_5 , and A_5 is simple, the only normal chain of subgroups we can form is

$$S_5 > A_5 > \{e\}.$$

But $A_5/\{e\} = A_5$ is not abelian, it follows that S_5 is not solvable. By **the Galois Solvability Criterion**, the extension $E > F$ is not solvable, which means that the polynomial g , whose the splitting field over F is E , is not solvable by radicals. \square