

5. THE FUNDAMENTAL THEOREM OF GALOIS THEORY

Theorem 5.1. (The Fundamental Theorem of Galois Theory).

Let L/K be a finite Galois extension. Then there is an inclusion reversing bijection between the subgroups of the Galois group $\text{Gal}(L/K)$ and intermediary subfields $L/M/K$. Given a subgroup H , let $M = L^H$ and given an intermediary field $L/M/K$, let $H = \text{Gal}(L/M)$.

Proof. This will be an easy consequence of all that has gone before. To prove that there is a correspondence it suffices to prove that given a subgroup H of G , if we let $M = L^H$ and then set $K = \text{Gal}(L/M)$, then $K = H$. As we have already proved that

$$H \subset K,$$

and $G = [L : K]$ is finite, it suffices to prove that the cardinality of K and is at most the cardinality of H . But

$$|H| = [L : M],$$

and there are at most $[L : M]$ automorphisms of L/M , so that

$$|K| \leq [L : M] = |H|.$$

Thus $H = K$, and the composition one way is the identity.

Now suppose that we start with $L/M/K$. Let $H = \text{Gal}(L/M)$ and let $N = L^H$. We already know that

$$M \subset N,$$

and so by the Tower Law it suffices to prove that

$$[L : N] \geq [L : M].$$

As L/K is Galois, then so is L/M . But then

$$[L : M] = |H|.$$

As H is a set of automorphisms of L/N , we have

$$[L : N] \geq |H| = [L : M].$$

Thus $M = N$ and the composition the other way is the identity. Thus we do have bijective correspondence. We have already seen that this correspondence is inclusion reversing. \square

The rest of the course will be addressed to deriving consequences of the Fundamental Theorem. We start by observing,

Theorem 5.2. *Let L/K be a finite separable extension.*

Then L/K is primitive.

Proof. It suffices to prove that there are only finitely many intermediary fields. To this end, we are certainly free to enlarge L . Replacing L by its normal closure, we may as well assume that L/K is Galois. In this case the Galois group G is finite and so there are clearly only finitely many subgroups of G . But by the Galois correspondence there are then only finitely many intermediary fields. \square

It is traditional in the statement of the Fundamental Theorem to characterise when M/K is normal in terms of the associated subgroup H of G .

Definition 5.3. Let G be a group and let S be a set. A **group action** is a function

$$G \times S \longrightarrow S,$$

denoted by

$$(g, s) \longrightarrow g \cdot s$$

such that

- (1) The identity e of G acts as the identity on S ,

$$e \cdot s = s,$$

for every $s \in S$.

- (2) For every g and h in G and $s \in S$,

$$(gh) \cdot s = g \cdot (h \cdot s).$$

Definition-Lemma 5.4. Let G act on a set S . Define a relation \sim on S by the rule $s \sim t$ iff there is an element $g \in G$ such that $g \cdot s = t$.

\sim is an equivalence relation. The equivalence classes of the action are called **orbits**. The action is said to be **transitive** if there is only one orbit (necessarily the whole of S).

Proof. We only need to check that \sim is an equivalence relation. Suppose $s \in S$. Then $s = e \cdot s$, so that $s \sim s$ and so \sim is reflexive.

Suppose that $s \sim t$. Then $s = g \cdot t$. Let $h = g^{-1}$. Then

$$\begin{aligned} h \cdot s &= h \cdot (g \cdot t) \\ &= (h \cdot g) \cdot t \\ &= e \cdot t \\ &= t. \end{aligned}$$

Thus $t \sim s$ and so \sim is symmetric.

Finally suppose that $r \sim s$ and $s \sim t$. Then there are g and $h \in G$ such that

$$s = g \cdot r \quad \text{and} \quad t = h \cdot s.$$

Then

$$\begin{aligned}t &= h \cdot s \\ &= h \cdot (g \cdot r) \\ &= (hg) \cdot r,\end{aligned}$$

and so $r \sim t$. But then \sim is transitive and hence it is an equivalence relation. \square

Definition 5.5. Suppose that the group G acts on the set S . Let $x \in S$. The **stabiliser** H of x in G is the subgroup of all elements of G that fix x .

Example 5.6. Let G be a group and let H be a subgroup. Let S be the set of all left cosets of H in G . Define an action of G on S ,

$$G \times S \longrightarrow S$$

as follows. Given $gH \in S$ and $g' \in G$, set

$$g' \cdot (gH) = (g'g)H.$$

It is easy to check that this action is well-defined. Clearly there is only one orbit and the stabiliser of the trivial left coset H is H itself.

Lemma 5.7. Let G be a group acting transitively on a set S and let H be the stabiliser of a point $s \in S$. Let L be the set of left cosets of H in G . Then there is an isomorphism of actions (where isomorphism is defined in the obvious way) of G acting on S and G acting on L , as in 5.6. In particular

$$|S| = \frac{|G|}{|H|}.$$

Proof. Define a map

$$f: L \longrightarrow S$$

by sending the left coset gH to the element $g \cdot s$. We first have to check that f is well-defined. Suppose that $gH = g'H$. Then $g' = gh$, for some $h \in H$. But then

$$\begin{aligned}g' \cdot s &= (gh) \cdot s \\ &= g \cdot (h \cdot s) \\ &= g \cdot s.\end{aligned}$$

Thus f is indeed well-defined. f is clearly surjective as the action of G is transitive. Suppose that $f(gH) = f(g'H)$. Then $gH = g's$. In this

case $h = g^{-1}g'$ stabilises s , so that $g^{-1}g' \in H$. But then g and g' are in the same left coset and $gH = g'H$. Thus f is injective as well as surjective, and the result follows. \square

Lemma 5.8. *Let G be a group and let S be a set. Let $s \in S$ and let $t = g \cdot s$. Let H be the stabiliser of s and K be the stabiliser of t .*

Then

$$K = gHg^{-1}.$$

Proof. Suppose that $k \in gHg^{-1}$. Then $k = ghg^{-1}$. Thus

$$\begin{aligned} k \cdot t &= (ghg^{-1})t \\ &= g \cdot (h \cdot (g^{-1} \cdot t)) \\ &= g \cdot (h \cdot s) \\ &= g \cdot s \\ &= t. \end{aligned}$$

Thus $k \in K$ and so

$$gHg^{-1} \subset K.$$

On the other hand, as $s = g^{-1} \cdot t$, by the same token we have

$$g^{-1}Kg \subset H,$$

so that

$$K \subset gHg^{-1}.$$

As we have an inclusion both ways, the result follows. \square

Theorem 5.9. (The Fundamental Theorem of Galois Theory).

Let L/K be a finite Galois extension. Then there is an inclusion reversing bijection between the subgroups of the Galois group $\text{Gal}(L/K)$ and intermediary subfields $L/M/K$. Given a subgroup H , let $M = L^H$ and given an intermediary field $L/M/K$, let $H = \text{Gal}(L/M)$.

Furthermore M/K is normal iff H is normal in G . In this case the Galois group of M/K is isomorphic to G/H .

Proof. We have already established the existence of the correspondence.

Recall that M/K is normal iff for every $\phi \in G$, $\phi(M) = M$. Suppose that M/K is normal. Define a map

$$f: G \longrightarrow \text{Gal}(M/K)$$

by sending ϕ to the restriction ψ of ϕ to M . As M/K is normal, ψ is indeed define an automorphism of M/K . It is easy to check that f is a homomorphism of groups. Clearly H is the kernel, so that H

is indeed normal. It follows that G/H is isomorphic to a subgroup of $\text{Gal}(M/K)$. But

$$\begin{aligned} |\text{Gal}(M/K)| &= [M : K] \\ &= [L : K]/[L : M] \\ &= |G|/|H|, \end{aligned}$$

where we used the Tower Law and the fact that L/M and L/K are Galois extensions, so that in fact $\text{Gal}(M/K) \simeq G/H$.

Now suppose that H is normal. Note that G acts on L , in an obvious way. Suppose that $m \in M$ and let $\phi \in G$. Set $n = \phi(m)$. As H stabilises m , then $H = \phi H \phi^{-1}$ stabilises n . But, by the correspondence already established, the only elements of L stabilised by all of H , are in fact elements of M . Thus $n \in M$, and $\phi(M) \subset M$. But then M/K is normal. \square

We now turn to the problem of computing Galois groups, in explicit cases. It turns out that this is a relatively straightforward problem.

Example 5.10. *Let $L = \mathbb{C}/\mathbb{R}$. Then L/K is Galois (indeed it is quadratic) and the Galois group has order two. $L = \mathbb{R}(i)$. i is a root of $x^2 + 1$, irreducible, and any automorphism of L/K must send i to another root. There are only two possible roots, $\pm i$. One gives the identity, the other is complex conjugation.*

Similarly for any other quadratic extension.

We compute the Galois group of $x^4 - 2$ over $K = \mathbb{Q}$. By this we mean we look at the splitting field L/K of $x^4 - 2$ and compute this Galois group.

We first start by computing the splitting field. First we need to attach a fourth root of 2. Suppose that we call this α . We get $M = K(\alpha)$ and as $x^4 - 2$ is irreducible this is a degree four extension. Then we add a primitive fourth root of 1. Call this i , so that $i^2 = -1$. We can always pick α so that it is real. Then $i \notin M$, so that L/M is a degree two extension. Thus, by the Tower law, we have a degree eight extension. Now L/K is Galois, as $x^4 - 2$ is separable (characteristic zero).

Thus $|G| = 8$. We look for generators and relations. Note first that N/K , where $N = \mathbb{Q}(i)$ is a Galois extension. Thus there is an automorphism π of N given by complex conjugation. L/N is a splitting field for $x^4 - 2$, generated by α thus we can extend π to τ by sending α to α . Thus one automorphism of L/K is given by τ , where the action of τ on generators is

$$\tau(\alpha) = \alpha \quad \text{and} \quad \tau(i) = -i.$$

Second note that there is an automorphism σ of L/K which sends α to any other root, in particular $i\alpha$. Now σ need not fix i . If it does not, then $\tau\sigma$ fixes i and sends α to $i\alpha$. But then the cube send α to $i\alpha$. Thus we may assume

$$\sigma(\alpha) = i\alpha \quad \text{and} \quad \sigma(i) = i.$$

Now $\sigma^4 = 1$ and $\tau^2 = 1$. In particular σ and τ generate two subgroups of G , of order four and two. It follows that σ and τ are generators of G . What are the relations? It suffices to compute the conjugate of σ by τ , $\tau\sigma\tau$. This sends i to i and α to $-i\alpha$. Thus $\tau\sigma\tau^{-1} = \sigma^3$. Thus G has presentation

Generators: σ and τ .

Relations: $\sigma^4 = \tau^2 = e$, $\tau\sigma\tau^{-1} = \sigma^3$.

We recognise this as D_4 , the Dihedral group of order eight, the symmetries of the square. In fact we can even see the square. The action of G is determined by its action on the four roots $\pm\alpha$ and $\pm i\alpha$, which are arranged in a square on the argand diagram.

Now we list all the possible subgroups and intermediate fields. We have already computed all possible subgroups of D_4 in 111A. Let H be a subgroup. Then the order of H divides the order of G , so that the order of H is 1, 2, 4 or 8. The cases 1 and 8 are easy and obvious, the trivial subgroup and the whole of D_4 .

Suppose that the order of H is two. Then H is generated by an element of order two. There are five of these, the two diagonal flips, the two side flips, and rotation by 180° . Thus H is one of

$$\langle \tau \rangle, \quad \langle \sigma^2 \tau \rangle, \quad \langle \sigma \tau \rangle, \quad \langle \sigma^3 \tau \rangle, \quad \langle \sigma^2 \rangle.$$

Now suppose that the order of H is four. One possibility is $\langle \sigma \rangle$. Otherwise we have to combine two elements of order two together. Now note that any subgroup of G of order 4 has index 2 and any subgroup of index two is normal. Thus if H is a subgroup of order 4 then it is normal in G . But a subgroup H of G is normal iff it is a union of conjugacy classes. Now the diagonal flips and the side flips are conjugates of each other, so we can combine two side flips, or two diagonal flips, but we cannot mix side and diagonal flips. Thus the subgroups of order 4 are

$$\langle \sigma \rangle, \quad \langle \tau, \sigma^2 \rangle, \quad \langle \sigma \tau, \sigma^2 \rangle.$$

Now we list the corresponding fixed fields. Two extremes are \mathbb{Q} and $\mathbb{Q}(\alpha, i)$, corresponding to G and $\{e\}$. If M/\mathbb{Q} is quadratic then the corresponding subgroup H has order 4 and index 2. Thus we are looking

for three subfields of degree two,

$$\mathbb{Q}(i), \quad \mathbb{Q}(\sqrt{2}), \quad \mathbb{Q}(i\sqrt{2}).$$

A little thought shows that in fact these fields are in the order corresponding to the subgroups of order 4.

Now let us search for the intermediate fields of order four. These correspond to subgroups of order two, so we are looking for five such fields. One obvious one is $\mathbb{Q}(\alpha)$, corresponding to τ . Similarly $\mathbb{Q}(i\alpha)$ corresponds to $\sigma^2\tau$. Also there is $\mathbb{Q}(i, \sqrt{2})$ corresponding to σ^2 . Now we need to compute the intermediate field associated to $\sigma\tau$. There is not much to do but write down the general element of L and see when it is fixed by $\sigma\tau$. Note that we know M contains $\mathbb{Q}(i\sqrt{2})$, so we only need to write down a basis for $\mathbb{Q}(\alpha, i)/\mathbb{Q}(i\sqrt{2})$, which is easily seen to be

$$1, \quad \alpha, \quad i, \quad i\alpha.$$

So the general element of $\mathbb{Q}(\alpha, i)$ is

$$a + b\alpha + ci + d(i\alpha)$$

and this is sent to

$$a + b\alpha - ci + d(i\alpha).$$

So $c = 0$ and $b = d$. Thus the corresponding fixed field is $\mathbb{Q}((1+i)\alpha)$. Similarly the other field of degree four is $\mathbb{Q}((1-i)\alpha)$.

Now we turn to the problem of computing Galois groups over finite fields. It turns out that this problem is almost completely trivial.

Definition 5.11. Let R be a ring of characteristic p . The map

$$\Phi: R \longrightarrow R$$

defined as

$$\Phi(a) = a^p,$$

is a ring homomorphism, called the **Frobenius** map.

Theorem 5.12. Let L/K be an extension of finite fields.

Then L/K is Galois. Moreover the Galois group is cyclic, generated by a power of Frobenius.

Proof. We already know that $L \simeq \mathbb{F}_q$, $K \simeq \mathbb{F}_r$, where q and r are powers of p , $q = p^n$ and $r = p^m$, where $m|n$ and $d = n/m$ is the degree of the extension. Moreover L is the splitting field of the polynomial $x^q - x$ and the non-zero elements of L are precisely the roots of unity. As Φ is injective and L is finite, Φ is clearly an automorphism of L .

The fixed field of Φ^k is the set of all elements of L such that

$$a^t = a,$$

where $t = p^k$, that is all roots of the polynomial

$$x^t - x.$$

But then Φ^m fixes K and the smallest power of Φ^m that fixes L is d . Thus

$$\langle \Phi^m \rangle$$

is a subgroup of the Galois group of order d . As the Galois group has order d the result follows. \square

Example 5.13. Let us compute the Galois group of $f(x) = x^4 + x + 1$ over the field \mathbb{F}_2 . The problem essentially boils down to factoring f .

f certainly does not have any linear factors as it has no roots. Suppose then that f were reducible. Then

$$x^4 + x + 1 = (x^2 + ax + b)(x^2 + cx + d),$$

where a, b, c and $d \in \mathbb{F}_2$. Looking at the coefficient of x^3 , we have $c = -a = a$ and looking at the constant coefficient we have $bd = 1$, so that $b = d = 1$. Thus we would have

$$x^4 + x + 1 = (x^2 + ax + 1)(x^2 + ax + 1) = x^4 + ax^2 + 1,$$

a contradiction.

Thus $x^4 + x + 1$ is irreducible. Let L be a splitting field and let α be a root of f . Then $M = \mathbb{F}_2(\alpha)$ is normal, as all extensions of finite fields are normal. Thus $L = M$ and L/\mathbb{F}_2 has degree four. Thus the Galois group is cyclic of order 4.

Lemma 5.14. Let $f(x) \in \mathbb{R}[x]$ have odd degree.

Then $f(x)$ has a real root.

Proof. We may as well suppose that $f(x)$ is monic. We may write

$$f(x) = x^n + \sum a_i x^i,$$

Let $m = \max |a_i|$, and pick $x > nm$. Then

$$\begin{aligned} f(x) &\geq x^n - \left| \sum a_i x^i \right| \\ &\geq x^n - \sum |a_i| x^i \\ &\geq x^n - nm x^{n-1} \\ &\geq x^{n-1}(x - nm) > 0. \end{aligned}$$

Similarly $f(x) < 0$, for $x < -nm$. Thus $f(x)$ must have a zero by the Intermediate Value Theorem. \square

Theorem 5.15. (*Fundamental Theorem of Algebra*) \mathbb{C} is the algebraic closure of \mathbb{R} .

In particular \mathbb{C} is algebraically closed.

Proof. Let L/\mathbb{C} be a finite extension. It suffices to prove that $L = \mathbb{C}$. Passing to a normal closure we may assume that L/\mathbb{R} is Galois. Let G be the Galois group. Let H be a Sylow 2-subgroup. Let $M = L^H$ be the corresponding fixed field.

Then M/\mathbb{R} has odd degree. Let $\alpha \in M$ and let $f(x)$ be the minimum polynomial of α . Then $f(x)$ has odd degree. But then $f(x)$ has a root in \mathbb{R} . As $f(x)$ is irreducible, its degree must be one. But then $\alpha \in \mathbb{R}$ and so $M = \mathbb{R}$. Thus L/\mathbb{R} has degree a power of two. Similarly for L/\mathbb{C} .

Suppose that G is not the trivial group. By Sylow's Theorem there is a subgroup H of G of index two. But then there would be an extension M/\mathbb{C} of degree two. As the characteristic is zero, there would then be an element $\alpha \in M$ such that $\alpha^2 \in \mathbb{C}$. But \mathbb{C} is certainly closed under taking square roots, a contradiction.

Thus G is trivial and $L = \mathbb{C}$. □