11. Counting Automorphisms

Definition 11.1. *Let L/K be a field extension.*

An ***automorphism of*** *L/K is simply an automorphism of L which fixes K.*

Here, when we say that ϕ fixes K, we mean that the restriction of ϕ to K is the identity, that is, ϕ extends the identity; in other words we require that ϕ fixes every point of K and not just the whole subset.

Definition-Lemma 11.2. *Let L/K be a field extension.*

The ***Galois group of*** *L/K, denoted $\mathrm{Gal}(L/K)$, is the subgroup of the set of all functions from L to L, which are automorphisms over K.*

Proof. The only thing to prove is that the composition and inverse of an automorphism over K is an automorphism, which is left as an easy exercise to the reader. □

The key issue is to establish that the Galois group has enough elements.

Proposition 11.3. *Let L/K be a finite normal extension and let M be an intermediary field.*

TFAE

1. *M/K is normal.*
2. *For every automorphism ϕ of L/K, $\phi(M) \subset M$.*
3. *For every automorphism ϕ of L/K, $\phi(M) = M$.*

Proof. Suppose (1) holds. Let ϕ be any automorphism of L/K. Pick $\alpha \in M$ and set $\phi(\alpha) = \beta$. Then β is a root of the minimum polynomial m of α. As M/K is normal, and α is a root of $m(x)$, $m(x)$ splits in M. In particular $\beta \in M$. Thus (1) implies (2).

Suppose that (2) holds and let ϕ be any automorphism of L/K. As L/K is finite, then so is M/K. As ϕ is an automorphism,

$$[\phi(M) : K] = [M : K].$$

On the other hand, by hypothesis $\phi(M) \subset M$. So by the Tower Law, $[M : \phi(M)] = 1$. Hence (2) implies (3).

Now suppose that (3) holds. Let $f(x)$ be an irreducible polynomial and let $\alpha \in M$ be a root of $f(x)$. As L/K is normal, $f(x)$ splits in L. Let β be any other root of $f(x)$. Then we may find an automorphism ϕ of L that carries α to β, by (8.8). As $\phi(M) \subset M$, it follows that $\beta \in M$. But then $f(x)$ splits in M. Thus (3) implies (1). □

Lemma 11.4. *Let L/K be a separable extension and let M/K be an intermediary field.*

Then M/K and L/M are both separable.

Proof. M/K is clearly separable.

Suppose that $\alpha \in L$. Let $f(x)$ be the minimum polynomial of α over L and let $g(x)$ be the minimum polynomial over K. Then $f(x)$ divides $g(x)$. On the other hand, $g(x)$ is separable, that is, $g(x)$ has no repeated roots, as L/K is separable. Thus $f(x)$ has no repeated roots and so L/M is separable. □

Lemma 11.5. *Let L/K be a field extension, let $\alpha \in L$ be algebraic and let $M = K(\alpha)$ be the intermediary field generated by α. Suppose that the degree of M/K is d. Let $\phi\colon K \longrightarrow K'$ be any ring homorphism and let L'/K' be a normal field extension.*

Then there are at most d ring homomorphisms $\psi\colon M \longrightarrow L'$, extending ϕ, with equality if and only if α is separable and there is at least one automorphism extending ϕ.

Proof. Let $m(x)$ be the minimum polynomial of α. The degree of $m(x)$ is d. Let $m'(x)$ be the corresponding polynomial in $K'[x]$. Then $m'(x)$ has at most d roots, with equality if and only if α is separable and it has one root. On the other hand any map ψ extending ϕ is determined by its action on α and there is an automorphism carrying α to β if and only if β is a root of $m'(x)$. □

Proposition 11.6. *Let L/K be a finite field extension, let $\phi\colon K \longrightarrow K'$ be any ring homomorphism and suppose that L'/K' is normal.*

Then there are at most $[L : K]$ ring homomorphisms $\psi\colon L \longrightarrow L'$ extending ϕ with equality if and only if L/K is separable and there is at least one automorphism extending ϕ.

Proof. The proof is by induction on $[L : K]$. If $L = K$ there is nothing to prove. Otherwise pick $\alpha \in L - K$. Suppose that the degree of $M = K(\alpha)/K$ is d. By (11.5) there are at most $d = [M : K]$ ring homomorphisms $\pi\colon M \longrightarrow L'$ extending ϕ. On the other hand, as $[M : K] > 1$, by the Tower Law $[L : M] < [L : K]$, so that by induction there are at most $[L : M]$ ring homomorphisms $\psi\colon L \longrightarrow L'$ extending a given π. Since any ψ extends at least one π, there are at most $[L : K] = [L : M][M : K]$ extensions of ϕ, with equality if and only if α is separable and, by induction, $[L : M]$ is separable.

This proves the inequality and that there is equality if L/K is separable. On the other hand, note that if there is equality, then simply varying α, we see that every element of L/K is separable, so that L/K is separable. □

Corollary 11.7. *Let L/K be a finite extension and let M be an intermediary extension.*

Then L/K is separable if and only if L/M and M/K are separable.

Proof. By (11.4) it suffices to prove that if L/M and M/K are separable, then L/K is separable. Let N/K be a normal closure of L/K. By (11.6) there are $[M : K]$ ring homomorphisms $\pi\colon M \longrightarrow N$, whose restriction to K is the identity, and for each such π there are then $[L : M]$ ring homomorphisms $\psi\colon L \longrightarrow N$ extending π. There are thus at least $[L : K] = [L : M][M : K]$ ring homomorphisms $\psi\colon L \longrightarrow N$ extending the identity. It follows by (11.6) that L/K is separable. □

Corollary 11.8. *Let L/K be a finite extension, and suppose that $L = K(\alpha_1, \alpha_2, \dots, \alpha_n)$.*

Then L/K is separable if and only if each α_i is separable.

Proof. Let M_i be the intermediary field generated by the first i α's, $\alpha_1, \alpha_2, \dots, \alpha_i$. The result then follows by (11.7) and an obvious induction. □

Definition 11.9. *Let L/K be a field extension.*

*We say that L/K is **Galois** if it is normal and separable.*

It is easy to give some nice characterisations of finite Galois extensions.

Lemma 11.10. *Let L/K be a finite field extension.*

Then L/K is Galois if and only if it is the splitting field of a separable polynomial $f(x) \in K[x]$.

Proof. Easy. □

Lemma 11.11. *Let L/K be a separable extension, and let N/K be a normal closure.*

Then N/K is Galois.

Proof. Note that the normal closure of a separable field extension L/K is the splitting field of a separable polynomial, as each irreducible factor of the polynomial has a root in L. The result follows by (11.10). □

Theorem 11.12. *Let L/K be a finite extension.*

Then L/K is Galois if and only if there are $[L : K]$ automorphisms of L/K.

Proof. Suppose that L/K is Galois. Then the result follows by (11.3) and (11.6).

Now suppose that there are $[L : K]$ automorphisms of L/K. Let N/K be a normal closure. Then there are at most $[L : K]$ ring homomorphisms $\psi\colon L \longrightarrow N$. It follows that L/K is separable, by (11.6) and that every ring homomorphism is in fact an automorphism, so that L/K is normal, by (11.3). □

Definition 11.13. *Let L be a field and let G be a collection of automorphisms of L. The **fixed field** of G, denoted L^G, is the set of all elements of L which are fixed by every element of G.*

Note that if X is a set of automorphisms of L and G is the subgroup of the group of all functions from L to L generated by X then $L^X = L^G$. So we might as well assume that G is a group, when dealing with fixed fields.

Lemma 11.14. *Let $L/M/K$ be a field extension, let G be a group of automorphisms of L and let H be a subgroup. Then*

(1) $G \subset \operatorname{Gal}(L/L^G)$.
(2) $K \subset L^{\operatorname{Gal}(L/K)}$.
(3) $L^G \subset L^H$.
(4) $\operatorname{Gal}(L/M) \subset \operatorname{Gal}(L/K)$.

Proof. Easy. □

Let G be a group of automorphisms of L and let K be the fixed field. Our object is to prove that in fact the two associations,

$$G \longrightarrow L^G \qquad \text{and} \qquad M \longrightarrow \operatorname{Gal}(L/M),$$

set-up an order reversing correspondence between the subgroups of G and the intermediary fields $L/M/K$. The key point will be to establish that L/K is Galois, that is, we want

$$[L:K] = |G|.$$

Definition 11.15. *Let R be a ring. R^* denotes the group of units, under multiplication.*

If R is a field, then $R^* = R - \{0\}$.

Definition 11.16. *Let G be a group and let K be a field. A **character** is a group homomorphism*

$$G \longrightarrow K^*.$$

Recall that given any set X and an R-module M, the set of all functions from X to M has the structure of an R-module.

Lemma 11.17. *Let G be a group and let K be a field.*
Then any set of characters is linearly independent.

Proof. Suppose not. Then we may find characters $\chi_1, \chi_2, \dots, \chi_n$ and scalars $a_1, a_2, \dots, a_n \in K$ such that

$$\sum_{i=1}^{n} a_i \chi_i = 0,$$

where not all a_i are zero. We pick $n > 0$ minimal with this property. In particular $a_i \neq 0$ for all i. $n \neq 1$, as otherwise $0 = a_1\chi_1(1) = a_1$. As $\chi_1 \neq \chi_n$ we may find $h \in G$ such that $\chi_1(h) \neq \chi_n(h)$.

We have

$$\sum_{i=1} a_i\chi_i(g) = 0,$$

for every $g \in G$. In particular this equation holds with hg in place of g. It follows that

$$\begin{aligned} 0 &= \sum_{i=1} a_i\chi_i(hg) \\ &= \sum_{i=1} a_i\chi_i(h)\chi_i(g). \end{aligned}$$

Now multiply the first equation by $\chi_n(h) \neq 0$, to get two equations with the same last term,

$$\sum_{i=1} a_i\chi_i(h)\chi_i(g) = 0$$

$$\sum_{i=1} a_i\chi_n(h)\chi_i(g) = 0.$$

If we subtract the second equation from the first we get an equation of the form

$$\sum_{i=1} b_i\chi_i(g) = 0.$$

where $b_i = a_i(\chi_i(h) - \chi_n(g))$. As this is valid for all $g \in G$, we have

$$\sum_{i=1} b_i\chi_i = 0.$$

By assumption $b_1 \neq 0$, so that we have a smaller non-trivial linear dependence, a contradiction. □

Lemma 11.18. *Any set of automorphisms of a field L are linearly independent.*

Proof. Any automorphism ϕ determines and is determined by the obvious character

$$\chi \colon L^* \longrightarrow L^*$$

so that the result is an immediate consequence of (11.17). □

Lemma 11.19. *Let L be a field and let X be any set of automorphisms of L, with fixed field $K = L^X$.*

Then

$$[L : K] \geq |X|,$$

where we only require the LHS to be infinite if the RHS is infinite.

Proof. Suppose not. Then L/K would be finite. Let $l_1, l_2, \dots, l_m$ be a basis. By assumption we could find $\sigma_1, \sigma_2, \dots, \sigma_n$ automorphisms of L/K with $n > m$. Consider the system of $m \times n$ equations

$$\sum_j \sigma_j(l_i)x_j = 0.$$

As there are n unknowns and $m < n$ equations, there is a non-trivial solution $a_1, a_2, \dots, a_n \in K$ (just apply Gaussian elimination). I claim that

$$\sum_j a_j \sigma_j = 0.$$

Let $l \in L$. Then we may find $b_1, b_2, \dots, b_m \in K$ such that

$$l = \sum_i b_i l_i.$$

In this case

$$\begin{aligned}\sum_j a_j \sigma_j(l) &= \sum_j a_j \sigma(\sum_i b_i l_i) \\ &= \sum_j \sum_i a_j b_i \sigma(l_i) \\ &= \sum_i b_i \left(\sum_j a_j \sigma(l_j) \right) \\ &= 0,\end{aligned}$$

which establishes the claim. But this contradicts the fact that any set of automorphisms is linearly independent. □

Lemma 11.20. *Let L be any field and let G be any finite group of automorphisms of L, with fixed field K.*

Then

$$[L : K] = |G|.$$

In particular L/K is Galois.

Proof. We have already seen that

$$[L : K] \geq |G|.$$

Suppose that $[L : K] > |G|$. Suppose that the elements of G are $\sigma_1, \sigma_2, \dots, \sigma_m$. Then we may find $l_1, l_2, \dots, l_n$ an independent set of elements of L, with $n > m$. As the set of equations

$$\sum_j \sigma_i(l_j)x_j = 0,$$

has m equations and $n > m$ unknowns, we may find a non-trivial solution $a_1, a_2, \dots, a_n \in L$. Possibly rearranging, we may assume that σ_1 is the identity. Thus the first equation reads

$$\sum a_j l_j = 0.$$

As we are assuming that $l_1, l_2, \dots, l_n$ are independent over K, it follows that not every $a_j \in K$. Amongst all such solutions, we choose one with the smallest number r of a_j non-zero. We may assume that $a_j = 0$ if and only if $j > r > 0$. Rescaling we may assume that $a_r = 1$. As not all $a_j \in K$, we may assume that $a_1 \notin K$. In particular $r > 1$.

As K is the fixed field of G and $a_1 \notin K$, we may find an element of G that does not fix a_1, say σ. As the map

$$G \longrightarrow G$$

given by multiplication on the left by σ is a bijection, it follows that as σ_i runs over the elements of G, so does $\sigma \circ \sigma_i$. So consider applying σ to each of the equations above. As σ is a ring homomorphism it follows that we get a new solution to these equations

$$\sum_j b_j \sigma_i(l_j) = 0,$$

where $b_j = \sigma(a_j)$. By hypothesis $b_1 \neq a_1$. Multiplying the first set of equations by b_1 and the second set by a_1 and subtracting one set from another, we obtain a solution

$$\sum_i \sigma_i(l_j) c_i = 0,$$

where $c_r \neq 0$ but $c_1 = 0$. But this contradicts our original choice of $a_1, a_2, \dots, a_n$. $\square$