CHAPTER VIII

GALOIS THEORY

1. Automorphism groups and fixed fields

Let $K \supseteq F$ be a field extension. Denote by $G(K/F)$ the set of all automorphisms σ of K which fix F, i.e., such that $\sigma(a) = a$ for $a \in F$. It is easy to verify that $G(K/F)$ is a group. $G(K/F)$ can be defined for any extension, but it is most interesting in the case of finite normal extensions, which, from the previous chapter, we know are the same a splitting fields of specific polynomials.

Proposition. *Let K be a splitting field of a nonconstant polynomial $f(X) \in F[X]$. Then $G(K/F)$ is finite. In particular, if $x_1, \dots, x_n$ are the distinct roots of $f(X)$ in K, then $G(K/F)$ is isomorphic to a subgroup of the group of permutations of $\{x_1, ..., x_n\}$, so its order divides $n!$.*

Proof. Let σ be an automorphism of K fixing F. If $x = x_i$ is a root of $f(X)$, then $f(\sigma(x)) = \sigma(f(x))$—since σ fixes F—so $\sigma(x)$ is also a root of $f(X)$. Since $K = F(x_1, \dots, x_n)$, σ is completely determined by its effect on the set $\{x_1, \dots, x_n\}$. Since σ is one-one, it induces a permutation s of that set. It is clear that the mapping $\sigma \mapsto s$ preserves composition so it is a group monomorphism. □

Example. Let $\alpha = \sqrt{2}$ and $\beta = \sqrt{3}$. Then it is clear that $\mathbf{Q}[\alpha, \beta]$ is normal over $\mathbf{Q}$ since it is the splitting field of $(X^2 - 2)(X^2 - 3)$. We calculate $G = G(\mathbf{Q}[\alpha, \beta]/\mathbf{Q})$. Any element σ of G may be identified with a permutation of the set of roots $\{x_1 = \alpha, x_2 = -\alpha, x_3 = \beta, x_4 = -\beta\}$. Since $X^2 - 2$ is in $\mathbf{Q}[X]$ and splits in $\mathbf{Q}[\alpha, \beta]$, σ must permute its roots and similarly for $X^2 - 3$. It follows that $\sigma(\alpha) = \pm\alpha$ and $\sigma(\beta) = \pm\beta$. There are of course 4! permutations of the set of roots but the above remark tells us that any acceptable permutation (except the identity) contains either the 2-cycle $(x_1\, x_2)$ or the 2-cycle $(x_3\, x_4)$ or of course both. To simplify the notation, we just use the subscripts. That leaves 4 possible elements:

$$\mathrm{Id}, (1\,2), (3\,4), \text{ and } (1\,2)(3\,4).$$

In fact, each of these permutations does arise from some $\sigma \in G$. For, by our general theory about roots of irreducible polynomials, we know there is an automorphism $\tau : \mathbf{Q}[\alpha] \to \mathbf{Q}[\alpha]$ such that $\tau(\alpha) = -\alpha$. By normality, we may conclude that there is an automorphism of $\mathbf{Q}[\alpha, \beta]$ extending τ. Any such extension must yield either the permutation $(1\,2)$ or the permutation $(1\,2)(3\,4)$ (or both such extensions might occur.) A similar remark applies to β. If we can obtain two of the nontrivial permutations listed above, G must also contain the third since it is a group. If not, the only possible alternative is that the only realizable permutation of the roots is $(1\,2)(3\,4)$. To show that this can't happen, consider the subfield $\mathbf{Q}[\alpha\beta]$. Since $\alpha\beta$ is a root of $X^2 - 6$, it follows as above that there is an automorphism of $\mathbf{Q}[\alpha, \beta]$ sending $\alpha\beta$ to $-\alpha\beta$. However, $(1\,2)(3\,4)$ sends $\alpha\beta$ to $(-\alpha)(-\beta) = \alpha\beta$. It follows that G is isomorphic the subgroup of S_4 consisting of all four listed elements. That group, of course, is the Klein 4-group.

Notice that the reasoning above is quite involved. A common mistake made by beginners is to pick out some plausible permutations of the roots and then assert without further discussion that $G(K/F)$ consists of those permutations. But, for a permutation of the roots to come from an automorphism, it must preserve all the relations among the roots, and to prove that could be quite difficult because those relations are not generally known explicitly. Usually, it is better to use indirect reasoning as above.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TeX

Given a (usually finite normal) extension $K \supseteq F$, we have considered the group $G(K/F)$. On the other hand, if K is any field, and P is any group of automorphisms of K, we define

$$K^P = \{x \in K \mid \sigma(x) = x \text{ for all } \sigma \in P\}$$

and we call it the *fixed field* of P. (It is easy to check that it is in fact a field.) We shall see below that if P is a finite group, then $K \supseteq K^P$ is a finite normal extension, and moreover $[K : K^P] = |P|$. This is one part of the main theorem of Galois Theory. First, however, we shall list some formal properties of the two operations we have described relating groups to field extensions.

THEOREM. *Let K be a field.*

(a) *If $K \supseteq L \supseteq F$, then $G(K/L) \leq G(K/F)$.*
(b) *If $Q \geq P$ are automorphism groups of K, then $K^Q \subseteq K^P$.*
(c) *For each subfield F of K, we have $K^{G(K/F)} \supseteq F$. Moreover, if $F = K^P$ for some group of automorphisms of K, then $K^{G(K/F)} = F$.*
(d) *For each group P of automorphisms of K, we have $G(K/K^P) \geq P$. Moreover, if $P = G(K/F)$ for some subfield F, then $G(K/K^P) = P$.*

PROOF. The proofs of these facts are quite straightforward. We leave (a), (b), and (d) as exercises for the student, and concentrate on the proof of (c).

By definition, all $\sigma \in G(K/F)$ fix F. So $K^{G(K/F)} \supseteq F$.

Suppose further that $F = K^P$. Then by the *first* part of (d), we have $G(K/F) \geq P$. By (b) and the first part of (c), we have $F \subseteq K^{G(K/F)} \subseteq K^P = F$, so they are equal. □

Suppose now that K is a field, P is a *finite* group of automorphisms of K, and $F = K^P$. Let $x \in K$, and let $\{x = x_1, \ldots, x_r\}$ be the orbit of x under the action of P. Thus, $x_i = \sigma_i(x)$ for some $\sigma_i \in P$. (Of course, it will generally be the image of many such elements of P, any two of which differ by an element of the isotropy group P_x.) Let $f(X) = \prod(X - x_i)$. The coefficients of $f(X)$ are

$$\begin{aligned}
a_1 &= \sum_i x_i \text{ (sum of the roots)} \\
a_2 &= -\sum_{i<j} x_i x_j \text{ (sum of the products of roots, 2 at a time)} \\
a_3 &= \sum_{i<j<k} x_i x_j x_k \text{ (sum of the products of roots, 3 at a time)} \\
&\vdots \\
a_r &= (-1)^r x_1 x_2 ... x_r \text{ (product of the roots).}
\end{aligned}$$

The sums (without the signs) are called the elementary symmetric functions. It is clear that these quantities are fixed by any permutations of the roots. In particular, since $\sigma \in P$ must permute the elements of any orbit, it follows that σ fixes each of the coefficients a_i. Thus, $f(X) \in F[X]$ since $F = K^P$.

PROPOSITION. *With the above notation, $f(X)$ is irreducible over F.*

PROOF. Let $m(X)$ be the minimal polynomial of x over F. Then since x is a root of $f(X)$, $m(X) \mid f(X)$. On the other hand, every $\sigma(x)$ is a root of $m(X)$ since $\sigma(m(x)) = m(\sigma(x))$ (since the coefficients of $m(X)$ are fixed by σ.) Thus, each $X - x_i$ divides $m(X)$, and by unique factorization in $K[X]$ (and the fact that the $X - x_i$ are distinct, hence relatively prime linear polynomials), it follows that $m(X)$ is divisible by $f(X) = \prod(X - x_i)$. Since both are monic, the two polynomials are equal, and $f(X)$ is irreducible. □

It now follows that if P is a finite group of automorphisms of K, then K is normal over K^P. For, we have show that the minimal polynomial over K^P of any element of K splits completely in K. But we have shown more: that every such minimal polynomial splits into *distinct* linear factors $X - x_i$. Such a polynomial is called *separable* over F.

An element x in an extension $L \supseteq F$ is called *separable* over F if its minimal polynomial is separable. (If L is not normal over F, the splitting would take place in a still larger normal extension.) An extension $L \supseteq F$ is called separable if it is algebraic and each element $x \in L$ is separable over F. Note that separability over F always implies separability over an extension $E \supseteq F$ since the minimal polynomial over E divides the minimal polynomial over F in $E[X]$.

From what we have done above, if Q is a finite group of automorphisms of K, then $K \supseteq K^Q = F$ is a normal, separable extension. We will shortly show that it is also finite. By (c) of the Theorem, $K^{G(K/F)} = F$. In fact, the properties just listed to conclude that that this equality holds.

Proposition. *If $K \supseteq F$ is any finite, normal, separable extension, then $K^{G(K/F)} = F$.*

(Note: The result is true more generally for extensions of infinite degree which are algebraic, normal, and separable.))

Proof. Let $x \in K^{G(K/F)}$. The minimal polynomial $m(X)$ of x over F splits in $K[X]$ into *distinct* linear factors because of the assumptions of separability and normality. If it had degree > 1, then $m(X)$ would have at least two distinct roots $x, x' \in K$. By our basic automorphism theorems, $\sigma(x) = x'$ would define an isomorphism $\sigma : F[x] \cong F[x']$ fixing F, and we could extend it to an automorphism σ of K fixing F. Thus, we would have $\sigma \in G(K/F)$ with $\sigma(x) = x'$, and that contradicts $x \in K^{G(K/F)}$. Hence, $m(X) \in F[X]$ is linear of the form $X - x$, so $x \in F$. □

Exercises.

1. Let $\omega = e^{(2\pi i)/3}$, and let $\alpha = \sqrt[3]{2}$; let $K = \mathbf{Q}[\alpha, \omega]$. Show that $G(K/\mathbf{Q})$ is isomorphic to the full symmetric group S_3. Do this without using the Main Theorem of Galois Theory (in the next section) by showing that every permutation of the roots of $X^3 - 2$ arises from a some autormorphism of K. See the calculation done in the section of $G(\mathbf{Q}[\sqrt{2}, \sqrt{3}]/\mathbf{Q})$.

2. Let K be a field and G a group of automorphisms of K. Show that K^G is a subfield of K.

3. Let K be a field.
Prove the following parts of the Proposition in the text.
(a) If $K \supseteq L \supseteq F$, then $G(K/L) \geq G(K/F)$.
(b) If $Q \geq P$ are automorphism groups of K, then $K^Q \subseteq K^P$.
(d) For each group P of automorphisms of K, we have $G(K/K^P) \geq P$.
(d') If $P = G(K/F)$ for some subfield F, then $G(K/K^P) = P$.
In proving (d'), you may assume (a), (b), (c), and (d) have been proved. But of course don't assume (c) in proving (d), since the proof of (c) in the text depends on (d). (You shouldn't need it in any case.)

4. Let K be a field.
(a) Let $K \supseteq L \supseteq F$. Show that for each $\tau \in G(K/F)$, $G(K/\tau(L)) = \tau G(K/L)\tau^{-1}$.
(b) Similarly, if τ is an autormorphism of K and H is a group of automorphisms of K, show that $K^{H'} = \tau(K^H)$ for $H' = \tau H \tau^{-1}$.

5. Let $K = k(X)$ be the field of rational functions in an indeterminate X over a field k of characteristic 0. Show that $\sigma : X \mapsto -X$ and $\tau : X \mapsto 1 - X$ define automorphisms of K. Show that σ and τ are both of order 2, but $\tau\sigma$ is of infinite order. Show that the fixed field of the cyclic group H generated by $\tau\sigma$ is k. Note that $K \supseteq k$ is not an algebraic extension.

2. Galois's Main Theorem

Theorem. *(First Basic Lemma on degree) Let Q be a finite group of automorphisms of the field K, and let $F = K^Q$. Then $K \supseteq F$ is finite, and $[K : F] \leq |Q|$.*

Proof. Let $n = |Q|$. We shall show that any $n + 1$ elements of K are linearly dependent over F. Let $Q = \{\sigma_1 = \mathrm{Id}, \ldots, \sigma_n\}$, and let $\{x_1, \ldots, x_{n+1}\}$ be a subset of K with $n + 1$ elements. Consider the system of equations

$$\begin{aligned}
\sigma_1(x_1)t_1 + \sigma_1(x_2)t_2 + \dots + \sigma_1(x_{n+1})t_{n+1} &= 0\\
\sigma_2(x_1)t_1 + \sigma_2(x_2)t_2 + \dots + \sigma_2(x_{n+1})t_{n+1} &= 0\\
&\vdots\\
\sigma_n(x_1)t_1 + \sigma_n(x_2)t_2 + \dots + \sigma_n(x_{n+1})t_{n+1} &= 0
\end{aligned}$$

Since there are more unknowns than equations, there exists a nontrivial solution vector $[t_1, \dots, t_{n+1}]$ in K^{n+1}. We shall show that there exists a solution vector $[t_1, \dots, t_{n+1}]$ in F^{n+1}, so the first equation will give the desired dependence relation.

Suppose that among all nontrivial solution vectors $[t_1, \dots, t_{n+1}]$ we choose one with the number s of non-zero t_i minimal. Moreover, suppose, for convenience, that $t_1, \dots, t_s \neq 0$ (and the remaining $t_i = 0$.) Finally, if necessary divide by t_s to be able to assume that $t_s = 1$. Let $\sigma \in Q$, and apply σ to the entire system of equations with these t_i. The rows of the coefficient matrix are just permuted so that we get essentially the same system of equations but with solution vector $[\sigma(t_1), \dots, \sigma(t_s) = 1, 0, \dots, 0]$. Since the system is homogeneous, it follows that the vector of differences

$$[\sigma(t_1) - t_1, \dots, \sigma(t_s) - t_s = 0, 0, \dots, 0]$$

is also a solution. However, this contradicts the minimality of s unless all the differences are zero, i. e.

$$\begin{aligned}
\sigma(t_1) &= t_1\\
\sigma(t_2) &= t_2\\
&\vdots\\
\sigma(t_{n+1}) &= t_{n+1}
\end{aligned}$$

(Of course, some of these equations just assert that $0 = 0$.) Since this must be true for all $\sigma \in Q$, it follows that the t_i chosen as above are in $F = K^Q$. □

As above, let Q be a finite group of automorphisms of the field K, and let $F = K^Q$. We want to show that $[K : F] \geq |Q|$ so that in view of what we just proved, the two are equal. To do this we need a theorem originally due to Dedekind and in its abstract form attributed to E. Artin. Let K be a field. For any set M, we may make the set $\mathrm{Map}(M, K)$ of functions $f : M \to K$ into a vector space over K by defining

$$(af)(m) = af(m) \qquad a \in K, m \in M.$$

THEOREM. *(Artin's Theorem on Characters). Let M be a group and K a field. The set* $\mathrm{Hom}(M, K^*)$ *viewed as a subset of* $\mathrm{Map}(M, K)$ *is a linearly independent set.*

PROOF. Abbreviate $S = \mathrm{Hom}(M, K^*)$. As the theorem suggests, any function into K^* can certainly be viewed as a function into K, so we may view S as a subset of $\mathrm{Map}(M, K)$.

Consider dependence relations

$$\sum_{\sigma \in S} x_\sigma \sigma = 0 \tag{1}$$

where of course all but a finite number of the coefficients are zero. Assume there is a non-trivial relation and choose such a relation for which the number of coefficients $x_\sigma \neq 0$ is minimal. Note that there must be at least two such coefficients since no $\sigma = 0$. (Each takes values in K^*.)

Let $k \in M$. Then

$$\sum x_\sigma \sigma(km) = \sum x_\sigma \sigma(k)\sigma(m) = 0$$

for all $m \in M$. Thus,

$$\sum x_\sigma \sigma(k)\sigma = 0.$$

Similarly, for any given $\tau \in S$, we have

$$\tau(k)\sum x_\sigma \sigma = \sum x_\sigma \tau(k)\sigma = 0.$$

Hence,

$$\sum x_\sigma(\sigma(k) - \tau(k))\sigma = 0. \tag{2}$$

Choose τ such that $x_\tau \neq 0$. Then in (2), $x_\tau((\tau(k) - \tau(k)) = 0$, so at least one more coefficient is zero than in (1). This leads to a contradiction unless *all* the coefficients in (2) are zero, i. e.

$$\sigma(k) = \tau(k)$$

for all σ such that $x_\sigma \neq 0$. However, there is at least one $\sigma \neq \tau$ with $x_\sigma \neq 0$ since at least two of the coefficients in (1) had to be non-zero. Hence, we can choose k such that $\sigma(k) \neq \tau(k)$, which is also a contradiction. So there were no dependence relations to start. □

Consider now the group $\mathrm{Aut}(K)$ of all field automorphisms of K. $\mathrm{Aut}(K)$ is a subset of $\mathrm{Hom}(K, K)$ which in turn is a subset of $\mathrm{Map}(K, K)$. However, any element of $\mathrm{Hom}(K, K)$ necessarily takes 0 into 0 so it is completely determined by its effect on K^*. Thus, $\mathrm{Hom}(K, K)$ can in fact be identified with a subset of $\mathrm{Map}(K^*, K)$. If we make this identification, then $\mathrm{Hom}(K, K)$ becomes a K-subspace of $\mathrm{Map}(K^*, K)$ using the same definition of K-action as given above. (Check that xf is a homomorphism if f is!)

Corollary. *Let K be a field. Then $\mathrm{Aut}(K)$ is a linearly independent subset of $\mathrm{Hom}(K, K)$. In other words, any set of distinct automorphisms of K is linearly independent over K.*

Proof. Given the above identifications, $\mathrm{Aut}(K)$ is a subset of $\mathrm{Hom}(K^*, K^*)$ which in turn is a linearly independent subset of $\mathrm{Map}(K^*, K)$. Since $\mathrm{Aut}(K)$ is in fact contained in $\mathrm{Hom}(K, K)$, it is a linearly independent subset of the latter subspace. □

Corollary. *(2nd Basic Lemma on Degree). Let $K \supseteq F$ be a finite field extension. Then $[K : F] \geq |G(K/F)|$. In particular, if Q is a finite group of automorphisms of K, and $F = K^Q$ then $[K : F] \geq |Q|$.*

Proof. Note that $\mathrm{Hom}_F(K, K)$ is in fact a K-subspace of $\mathrm{Hom}(K, K)$ if we view the former as a K-vector space through $(xf)(y) = xf(y)$. For, if f is F-linear, then

$$(xf)(ay) = xf(ay) = xaf(y) = axf(y) = a(xf)(y)$$

for $x, y \in K$ and $a \in F$. However, if $[K : F] = n$, then we may write

$$K = Fx_1 \oplus Fx_2 \oplus \cdots \oplus Fx_n.$$

In view of this, it is easy to see that

$$\begin{aligned} \mathrm{Hom}_F(K, K) &\cong \mathrm{Hom}_F(Fx_1, K) \oplus \mathrm{Hom}_F(Fx_2, K) \oplus \cdots \oplus \mathrm{Hom}_F(Fx_n, K) \\ &\cong K \oplus K \oplus \cdots \oplus K \ (n \text{ times}) \end{aligned}$$

and in fact these are isomorphisms of vector spaces over K. It follows that $\dim_K \mathrm{Hom}_F(K, K) = n$. Since $G(K/F) \subseteq \mathrm{Hom}_F(K, K)$ and its elements are linearly independent over K the first result follows. The second follows because from the previous section $G(K/K^Q) \geq Q$. □

We are now ready to state the main theorem of Galois theory which relates intermediate fields of a finite, normal, separable extension $K \supseteq F$ to subgroups of $G(K/F)$. Note that if K is any field, and Q is a finite group of automorphisms of K, then we have shown that $K \supseteq F = K^Q$ *is a finite, normal separable, extension*. Conversely, we have shown that if $K \supseteq F$ is finite, normal, and separable, then $G(K/F)$ is finite and $K^{G(K/F)} = F$. Hence, we can either start with a subfield F of K for which $K \supseteq F$ is finite, normal, and separable or we may start with a finite group Q of automorphisms of K.

Theorem. *(Galois's Main Theorem). Let $K \supseteq F$ be a finite, normal, separable extension. Let $G = G(K/F)$.*

(A) *(i) For each subgroup H of G, we have $G(K/K^H) = H$.*
(ii) For each subfield L with $K \supseteq L \supseteq F$, we have $K^{G(K/L)} = L$

Hence, $H \mapsto K^H$ and $L \mapsto G(K/L)$ provide a one-to-one correspondence between subgroups of $G(K/F)$ and intermediate subfields L.

(B) *If the subgroup H corresponds to the intermediate subfield L, then $[K : L] = |H|$. In particular, $[K : F] = |G(K/F)|$.*

(C) *If the subgroup H corresponds to the intermediate subfield L, then H is normal in $G \Leftrightarrow L \supseteq F$ is a normal extension. Moreover, in that case*

$$G/H \cong G(L/F).$$

Proof. We first prove (A) and (B).

(i) Let $L = K^H$. Then we know that $G(K/L) \supseteq H$ on purely formal grounds. Hence, the first and second basic lemmas on degree show

$$[K : L] \geq |G(K/L)| \geq |H| \geq [K : L].$$

It follows that $G(K/L) = H$ as claimed and incidentally their common order its $[K : L]$ which proves (B).

(ii) Since $K \supseteq F$ is finite, normal and separable, the same is true of $K \supseteq L$. However, for such extensions we have already proved that $K^{G(K/L)} = L$.

(C) Suppose first that $L \supseteq F$ is a normal intermediate extension. If σ is an automorphism of K which fixes F, then the general characterization of normality assures us that $\sigma(L) = L$. Hence, we may define an automorphism σ' of L by restricting σ to L. The map $\sigma \rightsquigarrow \sigma'$ clearly defines a homomorphism of $G(K/F) \to G(L/F)$. It is an epimorphism since because of the normality of $K \supseteq F$, any automorphism σ' of L which fixes F can be extended to an automorphism σ of K. The kernel of this epimorphism is the set of all automorphisms σ of K which restrict to the identity on L, i.e. which fix L. Thus the kernel is $G(K/L)$ so that subgroup of $G(K/F)$ is normal and $G(K/F)/G(K/L) \cong G(L/K)$.

To prove the converse we need the following simple Lemma.

Lemma. *Let $K \supseteq L \supseteq F$. Then for each $\tau \in G(K/F)$, we have*

$$G(K/\tau(L)) = \tau G(K/L)\tau^{-1}.$$

Proof of Lemma. Left to the student as an exercise.

The converse now follows because if $G(K/L)$ is normal in $G(K/F)$, we may conclude that $G(K/\tau(L)) = G(K/L)$ so that the Galois correspondence tells us that $\tau(L) = L$. Since this holds true for every automorphism of K (normal over F) fixing F, it follows from our general characterization of normality that $L \supseteq F$ is normal. □

Notes.

1. The initial example of a finite, normal, separable extension was $K \supseteq F = K^Q$ where Q is a finite group of automorphisms of K. In this case, it is in fact true that $G(K/F) = Q$, the original group of automorphisms used to define F. For, generally, $G(K/K^Q) \geq Q$, while $|G(K/K^Q| = [K : K^Q] = |Q|$ by the two basic inequalities on degree. Hence, $G(K/F) = Q$ if $F = K^Q$./

2. Unfortunately, we don't usually encounter extensions by considering fixed fields of groups of automorphisms. Also, we don't yet know that the splitting field of a separable polynomial is separable, which the way we might more naturally expect to encounter a finite normal extension. We will investigate criteria for separability in the next section. In particular, we will establish that *every* extension of a field of characteristic 0, e.g., $\mathbf{Q}$, is separable.

Example 1. Let $K = \mathbf{Q}[\sqrt{2}, \sqrt{3}]$. We saw before that $G(K/\mathbf{Q})$ consists of 4 elements id, σ, τ, $\sigma\tau$ where $\sigma(\sqrt{2}) = -\sqrt{2}, \sigma(\sqrt{3}) = \sqrt{3}, \tau(\sqrt{2}) = \sqrt{2}, \tau(\sqrt{3}) = -\sqrt{3}$. The lattice of subgroups of G is

$$\begin{tikzcd}
 & \{\mathrm{Id}\} \arrow[d, dash] & \\
\{\mathrm{Id}, \sigma\} & \{\mathrm{Id}, \tau\} \arrow[d, dash] & \{\mathrm{Id}, \sigma\tau\} \\
 & G = \{\mathrm{Id}, \sigma, \tau, \sigma\tau\} &
\end{tikzcd}$$

The corresponding lattice of subfields is

$$\begin{tikzcd}
 & \mathbf{Q}[\sqrt{2}, \sqrt{3}] \arrow[d, dash] & \\
\mathbf{Q}[\sqrt{3}] & \mathbf{Q}[\sqrt{2}] \arrow[d, dash] & \mathbf{Q}[\sqrt{6}] \\
 & \mathbf{Q} &
\end{tikzcd}$$

(Note that it is customary to write the lattice of subgroups *upside-down* so that each subgroup appears in the position of the subfield it fixes.) In this case the group is abelian, and all the intermediate subfields are normal. The factor groups (i.e. the groups of the intermediate extensions) are cyclic of order 2.

Example 2. As in an earlier discussion in $\mathbf{C}$, let $\omega = e^{(2\pi i/3)}$, and let $\alpha = \sqrt[3]{2}$ be the real cube root of 2. Then we have the lattice of subfields of $K = \mathbf{Q}[\alpha, \omega]$

$$\begin{tikzcd}
 & & K = \mathbf{Q}[\alpha, \omega] & \\
2 & & & \\
 & \mathbf{Q}[\alpha] & & \mathbf{Q}[\omega] \\
3 & & & \\
 & & \mathbf{Q} &
\end{tikzcd}$$

The numbers on the left give the indicated degrees. For, α is a root of $X^3 - 2$ which is irreducible over $\mathbf{Q}$ so α is of degree 3 over $\mathbf{Q}$, and ω is a root of $X^2 + X + 1$ so $[K : \mathbf{Q}[\alpha]] \le 2$. Since ω is not real, it is not in $\mathbf{Q}[\alpha]$ so that degree is 2. It follows that the total degree is 6, hence by Galois's Main Theorem, $|G(K/\mathbf{Q})| = 6$. It follows that $G(K/\mathbf{Q}) \cong$ the full permutation group of the roots $\{\alpha, \alpha\omega, \alpha\omega^2\} \cong S_3$. Let $\sigma \in G$ correspond to the three cycle $(\alpha\, \alpha\omega\, \alpha\omega^2)$. It is easy to see that $\sigma(\alpha) = \alpha\omega$ and $\sigma(\omega) = \omega$. (Can you "construct" such an automorphism directly by using appropriate extension theorems?) Let τ correspond to the transposition $(\alpha\omega\, \alpha\omega^2)$. It is not hard to see that $\tau(\alpha) = \alpha$ and $\tau(\omega) = \omega^2$. We know the subgroups of G. There is a unique (hence normal) subgroup $\{\mathrm{Id}, \sigma, \sigma^2\}$ of order 3 and index 2. Its fixed field is clearly $\mathbf{Q}[\omega]$ which it follows is the only intermediate field of degree 2 over $\mathbf{Q}$. There are 3 subgroups of order 2: $\{\mathrm{Id}, \tau\}$ with fixed field $\mathbf{Q}[\alpha]$, $\{\mathrm{Id}, \tau\sigma\}$ with fixed field $\mathbf{Q}[\alpha\omega]$, and $\{\mathrm{Id}, \tau\sigma^2\}$ with fixed field $\mathbf{Q}[\alpha\omega^2]$. These are the *only intermediate subfields* of K. (Can you see what $\mathbf{Q}[\alpha + \omega]$ and $\mathbf{Q}[\alpha\omega + \alpha\omega^2]$ are?) We leave it to the student to draw the complete lattice diagrams for subgroups and subfields.

Exercises.

1. Draw the complete lattices of subfields and subgroups in Example 2. Identify the subfields $\mathbf{Q}[\omega - \omega^2]$ and $\mathbf{Q}[\alpha + \omega]$.

2. Assume that all field extensions in characteristic zero are separable; in particular, all extensions of $\mathbf{Q}$ are separable.

Consider the splitting field in K $\mathbf{C}$ of the rational polynomial $X^4 - 2$.

(a) Let α be a *real* fourth root of 2. Show that $K = \mathbf{Q}[\alpha, i]$ is that splitting field. Show that $[\mathbf{Q}[i] : \mathbf{Q}] = 2$ and $[\mathbf{Q}[\alpha] : \mathbf{Q}] = 4$. Show that $\mathbf{Q}[i] \cap \mathbf{Q}[\alpha] = \mathbf{Q}$ and conclude $[\mathbf{Q}[\alpha, i] : \mathbf{Q}] = 8$. Conclude also that $[\mathbf{Q}[\alpha, i] : \mathbf{Q}[i]] = 4, [\mathbf{Q}[\alpha, i] : \mathbf{Q}[alpha] = 2]$.

(b) The four roots of $X^4 - 2$ are $\alpha, i\alpha, -\alpha, -i\alpha$. Show that there exists an automorphism σ of K fixing i and such that $\sigma(\alpha) = i\alpha$. Show that the orbit of α under the subgroup generated by σ consists of the above roots, and conclude σ has order four.

(c) Show there exists and automorphism τ of K fixing α and such that $\tau(i) = -i$. Show that τ has order two and that $\tau\sigma\tau^{-1} = \tau\sigma\tau = \sigma^3$.

(d) Determine all subgroups of $G(K/\mathbf{Q})$ and the corresponding lattice of subfields of K. Identify which are normal and which are not.

3. Prove or disprove the following: A normal extension of a normal extension is normal.

3. More about separability

As defined above, a polynomial is separable if it splits in its splitting field into *distinct* linear factors; otherwise it is called *inseparable*. In the inseparable case, there are *repeated* roots, i.e. in its splitting field, $f(X)$ has factors of the form $(X - u)^2$. It turns out that an irreducible polynomial can be inseparable only in very special circumstances. To deal with this issue, we need the *formal* derivative of a polynomial. If $f(X) \in F[X]$ with $f(X) = \sum a_i X^i$, we define $Df(X) = \sum i a_i X^{i-1}$. (The formal term $0a_0X^{-1}$ is interpreted as 0.) This formal derivative has the usual formal properties of a derivative.

Proposition. *D(f(X) + g(X)) = Df(X) + Dg(X).*

$$D(f(X)g(X)) = Df(X)g(X) + f(X)Dg(X)$$

Proof. Calculate $f(X + H)$ in $F[X, H] = F[X][H]$ and notice that $Df(X)$ is the coefficient of H. The rules follow easily from this fact. □

Proposition. *Let y be a root of $f(X) \in F[X]$ in some extension $E \supseteq F$. (i) $(X - y)^2$ divides $f(X)$ in $E[X]$ if and only if $f(y) = Df(y) = 0$. (ii) An irreducible polynomial $f(X) \in F[X]$ is inseparable if and only if $DF(X)$ is the zero polynomial.*

Proof.

(i) Assume first that y is a multiple root. Then

$$f(X) = (X - y)^2 g(X) \text{ in } E[X].$$

Hence $DF(X) = 2(X - y)g(X) + (X - y)^2 Dg(X)$ and so $Df(y) = 0$.

Conversely, assume that y is not a repeated root. Then

$$f(X) = (X - y)g(X) \text{ where } g(y) \neq 0.$$

Hence $Df(X) = g(X) + (X - y)Dg(X)$ so $Df(y) = g(y) \neq 0$.

(ii) If $f(X)$ is inseparable, it has a multiple root in some splitting field. If y is such a root, by (i) $Df(y) = 0$. If $f(X)$ is irreducible, it follows that it is the minimal polynomial of any one of its roots, so $f(X) \mid Df(X)$. Since $\deg Df(X) < \deg f(X)$, that is not possible unless $Df(X)$ is the zero polynomial. Conversely, if $Df(X)$ is the zero polynomial, then every root in any extension is multiple by (i). □

Corollary. *If F is a field of characteristic 0, then every irreducible polynomial, hence every algebraic extension, is separable.*

Proof. $Df(X) = \sum i a_i X^{i-1} = 0$ in $F[X]$ if and only if $a_i = 0$ for all $i > 0$ not divisible by the characteristic p of F. (If $i \equiv 0 \bmod p$ then $ia_i = 0$ is possible without $a_i = 0$.) If the characteristic is 0, we are done. □

Example. We show how to construct an inseparable extension. Let $F = \mathbf{F}_p(T)$ be the field of rational functions in an indeterminate T with coefficients in the field $\mathbf{F}_p$ with p elements. The polynomial $X^p - T \in F[X]$ is irreducible. For, suppose x is a root of $X^p - T$ in some extension of F. Then

$$(X - x)^p = X^p - x^p = X^p - T.$$

(Use the binomial theorem and the fact that the binomial coefficients

$$\binom{p}{i} \equiv 0 \bmod p \text{ for } 0 < i < p.)$$

Hence, the minimal polynomial of x must be a power $(X - x)^i$. Were $i < p$, it would follow that $x \in F$. For, in that case the coefficient $-ix$ of X^{i-1} is in F. So, since $i < p$, $x \in F$. However, $x^p = T$, and it is not hard to see that T is not a power of any element of F. It follows that $F[x] \supseteq F$ is of degree p, the minimal polynomial of x factors there as $(X - x)^p$, and $F[x] \supset F$ is certainly not a separable extension. (But it is normal. Why?)

We now analyze the general structure of a monic, irreducible polynomial $f(X)$ over a field F of characteristic p. We have seen above that if $f(X)$ is inseparable, then (since $Df(X) = 0$) all coefficients $a_i = 0$ for $i \equiv 0 \bmod p$. Hence, in fact $f(X)$ is a polynomial in $X^p : f(X) = g(X^p)$ for some $g(X) \in F[x]$. Clearly, $g(X)$ is also irreducible. (However, we could easily start with an irreducible $g(X)$ but not have $g(X^p)$ irreducible.) If $g(X)$ is inseparable, then we can repeat the argument with it. Iterating in this way we conclude that $f(X) = g(X^{p^e})$ for some irreducible, separable $g(X) \in F[X]$.

Let $g(X) = \prod(X - x_i)$ in its splitting field where because of separability, the roots $x_1, x_2, \dots, x_r$ are distinct. Then

$$f(X) = g(X^{p^{e)}}) = \prod_{i=1}^{r}(X^{p^e} - x_i).$$

For each i, adjoin a root y_{i_e} of $X^{p^e} - x_i$. Since $(X - y_i)^{p^e} = X^{p^e} - y_i^{p^e} = X^{p^e} - x_i$, it follows that the unique factorization of $f(X)$ in its splitting field is

$$f(X) = g(X^{p^e}) = \prod_{i=1}^{r}(X - y_i)^{p^e}.$$

Hence, $f(X) = h(X)^{p^e}$ where $h(X)$ has coefficients in the splitting field of $f(X)$ and splits there into distinct linear factors.

A field F is called *perfect* if every irreducible polynomial in $F[X]$ (hence every algebraic extension of F) is separable. Thus, fields of characteristic 0 are perfect.

Theorem. *Every finite field is perfect.*

Proof. Let F be a finite field of characteristic p, and consider the function $\phi : F \to F$ defined by $\phi(x) = x^p$. $(x + y)^p = x^p + y^p$ because of the argument given above about binomial coefficients, and clearly $(xy)^p = x^p y^p$. Hence, ϕ is a field monomorphism of F into itself. Since F is finite ϕ must also be an epimorphism, i.e. it is an isomorphism of F onto itself. (ϕ is often called a Frobenius map although this confuses it with a related but more complicated notion in algebraic number theory bearing the same name.)

Let $f(X) \in F[X]$ be an irreducible polynomial. As noted above, if $f(X)$ is inseparable, it must be of the form

$$f(X) = a_0 X^{pk} + a_1 X^{p(k-1)} + \cdots + a_{k-1} X^p + a_k.$$

Since ϕ is an epimorphism, we have $a_i = b_i^p$ with $b_i \in F$ for each $i = 0, 1, \dots, k$. It follows that

$$f(X) = (b_0 X^k + b_1 X^{k-1} + \cdots + b_k)^p$$

contradicting the irreducibilty of $f(X)$. Hence, every irreducible polynomial over F is separable. □

The above arguments show that any extension of a field of characteristic zero or of a finite field is separable. Another way to be sure that an extension is separable is to obtain it as a splitting field of a separable polynomial. That would allow us for example to apply Galois Theory to at least some extensions of $\mathbf{F}_p(X)$, although not every extension of that field is separable.

Theorem. *Let $f(X) \in F[X]$ be a separable polynomial, and let K be a splitting field for $f(X)$. Then $K \supseteq F$ is a separable extension. In particular, Galois's Main Theorem applies to it.*

Proof. We proceed by induction on $[K : F]$.

Choose a root $x \in K$ of $f(X)$ and let $m(X)$ be its minimal polynomial. Let $\{x = x_1, x_2, \dots, x_r\}$ be the orbit of x under the action of $G(K/F)$. Since $x_i \mapsto x_j$ defines an F-isomorphism $F[x_i] \to F[x_j]$ which can be extended to an automorphism of K, we know that this orbit is the set of all distinct roots of $m(X)$. Since $f(X)$ is separable, each of its factors is separable, hence $m(X)$ is separable. It follows that $r = \deg m(X) = [F[x] : F]$. On the other hand, an element of $G(K/F)$ fixes $F[x]$ if and only if it fixes x so that the stabilizer of x is just $G(K/F[x])$. Hence, $(G(K/F) : G(K/F[x]) = r = [F[x] : F]$. By induction, viewing $f(X)$ as a polynomial in $F[x][X]$, we may assume $K \supseteq F[x]$ is separable so $|G(K/F[x])| = [K : F[x]]$ by Galois's Main Theorem. Thus, we have

$$|G(K/F)| = [K : F[x]][F[x] : F] = [K : F].$$

However, also by Galois's Main Theorem,

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

($K \supseteq K^{G(K/F)}$ is separable, and $G(K/K^{(G/F)}) = G(K/F)$.) Since $K^{G(K/F)} \supseteq F$ in any case, we may conclude that $F = K^{G(K/F)}$ so the extension is separable. □

Corollary. *Let $K \supseteq E \supseteq F$ where K is a finite, normal extension of F. Then $E \supseteq F$ is separable if and only if the number of distinct isomorphisms $\sigma : E \to K$ fixing F is $[E : F]$.*

Proof. We leave this as a challenging exercise for the student. It amounts to showing that $(G(K/F) : G(K/E)) = [E : F]$.

Corollary. *Let $L \supseteq E \supseteq F$ where $[L : F] < \infty$. L is separable over F if and only if L is separable over E and E is separable over F.*

Proof. The "only if" has already been discussed; in any event it is fairly clear.

Suppose conversely that $L \supseteq E$ and $E \supseteq F$ are separable. We may construct a normal closure $K \supseteq F$ containing L. By the previous corollary,

$$\begin{aligned}(G(K/F) : G(K/L)) &= (G(K/F) : G(K/E))(G(K/E) : G(K : L)) \\ &= [E : F][L : E] = [L : F].\end{aligned}$$

Hence, $L \supseteq F$ is separable. □

Exercises.

1. Prove the Corollary in the section.

Let $K \supseteq E \supseteq F$ where K is a finite, normal extension of F. Then $E \supseteq F$ is separable if and only if the number of distinct isomorphisms $\sigma : E \to K$ fixing F is $[E : F]$.

See the note on the proof for a hint.

2. Let $K \supseteq F$ be an extension of fields of characteristic $p \neq 0$. Let F' be the subset of all elements of K such that $x^q \in F$ for q a power of p (depending generally on x).

(a) Show that F' is a subfield of K containing F.

(b) Suppose K is finite and normal over F. Show that any automorphism of K which fixes F also fixes F'.

(c) Show that $K^{G(K/F)} = F'$.

4. Primitive elements

Theorem. *If $E \supseteq F$ is a finite separable extension, then $E = F(x)$ for some x.*

x is called a *primitive* element. Note that this result eliminates quite a bit of potential complication. If we had proved it earlier, we could have shortened some of the proofs a bit. Earlier developments of Galois theory depended strongly on this result. However, from our current point of view, the result is seen to be a lucky side effect rather than a fundamental fact which reveals the basic structure of the theory.

Proof of the Theorem. The proof is based on the following result.

Lemma. *$E \supseteq F$ is algebraic and $E = F(x)$ if and only if there are only a finite number of intermediate fields between E and F.*

It is clear that the lemma implies the theorem. For, if $E \supseteq F$ is finite and separable, then $E = F(x_1, x_2, \dots, x_n)$ for appropriate elements $x_1, x_2, \dots, x_n$ in E, and if we adjoin the remaining roots of the minimal polynomials of these elements we obtain a finite normal separable extension K of F with $K \supseteq E \supseteq F$. By Galois's main theorem, there are only finitely many intermediate fields between K and F so the same is true of E and F, hence by the lemma $E \supseteq F$ has a primitive element.

Proof of the Lemma. Suppose that $E = F(x)$ where x is algebraic over F. Let $m(X) \in F[X]$ be the minimal polynomial of x. If L is any intermediate field, let $g(X) \in L[X]$ be the minimal polynomial of x over L. Let $g(X) = X^k + u_1X^{k-1} + \dots + u_{k-1}X + u_k$ where $u_1, \dots, u_k \in L$. $E = F(x) = L(x)$ so $[E : L] = k$. However, $g(X)$ is certainly an irreducible polynomial in $L' = F(u_1, \dots, u_k)$ still with x as root, so we also have $[E : L'] = k$. It follows that $L = L' = F(u_1, \dots, u_k)$. Since (in E) $m(X)$ has only finitely many *monic* factors (by unique factorization), it follows that there can only be finitely many L.

Conversely, suppose there are only finitely many intermediate fields between E and F. Then E is a finite extension of F. For, if we choose x_1 not in F, x_2 not in $F(x_1)$, x_3 not in $F(x_1, x_2)$, etc. that process must eventually stop or we would obtain infinitely many subfields; hence $E = F(x_1, x_2, \dots, x_n)$ for appropriate elements $x_1, x_2, \dots, x_n$ in E. Moreover, each element x of E is algebraic over F, since otherwise $F(x)$, $F(x^2), F(x^3), \dots, F(x^i), \dots$ is easily seen to be a *strictly* decreasing chain of intermediate subfields. Thus, $E = F(x_1, x_2, \dots, x_n)$ is finite over F.

To show $E = F(x)$ for some x, we separate out two cases: F is finite and F is infinite. If F is finite, the result follows from the characterization of finite fields in the next chapter. If F is infinite, we argue by induction on $[E : F]$ as follows. Choose $y \in E, y \notin F$; there are certainly only finitely many subfields between E and $F(y)$, so we can conclude by induction that $E = F(y)(z) = F(y, z)$ for some z. Consider the intermediate fields $F(ay + bz)$ for $a, b \in F$. They can't all be different so we can find two such intermediate fields

$$F(ay + bz) = F(a'y + b'z) = L$$

where we may assume $ab' - a'b \neq 0$ since F is infinite. If we put

$$ay + bz = t$$
$$a'y + b'z = t'$$

we can solve (using Cramer's Rule) for y and z in terms of t and t' which are in L, so it follows that $y, z \in L$. Hence $F(y, z) \subseteq L$, i.e. $E = F(y, z) = L = F(t) = F(t')$. □

Exercises.

1. Let K be the subfield of $\mathbf{C}$ which is the splitting field of $X^4 - 2$. Find $\gamma \in K$ such that $K = \mathbf{Q}[\gamma]$. Find the minimum polynomial of γ.