If σ and τ are automorphisms of K then the composite $\sigma\tau$ (and also the composite $\tau\sigma$, which may not be the same) is defined and is again an automorphism of K.

Proposition 1. Aut(K) is a group under composition and Aut(K/F) is a subgroup.

Proof: It is clear that Aut(K) is a group. If σ and τ are automorphisms of K which fix F then also $\sigma\tau$ and σ^{-1} are the identity on F, which shows that Aut(K/F) is a subgroup.

The following proposition is extremely useful for determining the automorphisms of algebraic extensions.

Proposition 2. Let K/F be a field extension and let $\alpha \in K$ be algebraic over F. Then for any $\sigma \in$ Aut(K/F), $\sigma\alpha$ is a root of the minimal polynomial for α over F i.e., Aut(K/F) permutes the roots of irreducible polynomials. Equivalently, any polynomial with coefficients in F having α as a root also has $\sigma\alpha$ as a root.

Proof: Suppose α satisfies the equation

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$$

where $a_0, a_1, \ldots, a_{n-1}$ are elements of F. Applying the automorphism σ we obtain (using the fact that σ is an additive homomorphism)

$$\sigma(\alpha^n) + \sigma(a_{n-1}\alpha^{n-1}) + \cdots + \sigma(a_1\alpha) + \sigma(a_0) = \sigma(0) = 0.$$

Using the fact that σ is also a multiplicative homomorphism this becomes

$$(\sigma(\alpha))^n + \sigma(a_{n-1})(\sigma(\alpha))^{n-1} + \cdots + \sigma(a_1)(\sigma(\alpha)) + \sigma(a_0) = 0.$$

By assumption, σ fixes all the elements of F, so $\sigma(a_i) = a_i, i = 0, 1, \ldots, n-1$. Hence

$$(\sigma\alpha)^n + a_{n-1}(\sigma\alpha)^{n-1} + \cdots + a_1(\sigma\alpha) + a_0 = 0.$$

But this says precisely that $\sigma\alpha$ is a root of the same polynomial over F as α. This proves the proposition.

Examples

(1) Let $K = \mathbb{Q}(\sqrt{2})$. If $\tau \in \text{Aut}(\mathbb{Q}(\sqrt{2})) = \text{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$, then $\tau(\sqrt{2}) = \pm\sqrt{2}$ since these are the two roots of the minimal polynomial for $\sqrt{2}$. Since τ fixes $\mathbb{Q}$, this determines τ completely:

$$\tau(a + b\sqrt{2}) = a \pm b\sqrt{2}.$$

The map $\sqrt{2} \mapsto \sqrt{2}$ is just the identity automorphism 1 of $\mathbb{Q}(\sqrt{2})$. The map $\sigma : \sqrt{2} \mapsto -\sqrt{2}$ is the isomorphism considered in Example 2 following Corollary 13.7. Hence $\text{Aut}(\mathbb{Q}(\sqrt{2})) = \text{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{1, \sigma\}$ is a cyclic group of order 2 generated by σ.

(2) Let $K = \mathbb{Q}(\sqrt[3]{2})$. As before, if $\tau \in \text{Aut}(K/\mathbb{Q})$, then τ is completely determined by its action on $\sqrt[3]{2}$ since

$$\tau(a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2) = a + b\tau\sqrt[3]{2} + c(\tau\sqrt[3]{2})^2.$$

Since $\tau\sqrt[3]{2}$ must be a root of $x^3 - 2$ and the other two roots of this equation are not elements of K (recall the splitting field of this polynomial is degree 6 over $\mathbb{Q}$), the only possibility is $\tau\sqrt[3]{2} = \sqrt[3]{2}$ i.e., $\tau = 1$. Hence $\text{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = 1$ is the trivial group.

In general, if K is generated over F by some collection of elements, then any automorphism $\sigma \in \mathrm{Aut}(K/F)$ is completely determined by what it does to the generators. If K/F is finite then K is finitely generated over F by algebraic elements so by the proposition the number of automorphisms of K fixing F is finite, i.e., $\mathrm{Aut}(K/F)$ is a finite group. In particular, the automorphisms of a finite extension can be considered as permutations of the roots of a finite number of equations (not every permutation gives rise to an automorphism, however, as Example 2 above illustrates). It was the investigation of permutations of the roots of equations that led Galois to the theory we are describing.

We have associated to each field extension K/F (equivalently, with a subfield F of K) a *group*, $\mathrm{Aut}(K/F)$, the group of automorphisms of K which fix F. One can also reverse this process and associate to each group of automorphisms a field extension.

Proposition 3. Let $H \leq \mathrm{Aut}(K)$ be a subgroup of the group of automorphisms of K. Then the collection F of elements of K fixed by all the elements of H is a subfield of K.

Proof: Let $h \in H$ and let $a, b \in F$. Then by definition $h(a) = a$, $h(b) = b$ so that $h(a \pm b) = h(a) \pm h(b) = a \pm b$, $h(ab) = h(a)h(b) = ab$ and $h(a^{-1}) = h(a)^{-1} = a^{-1}$, so that F is closed, hence a subfield of K.

Note that it is not important in this proposition that H actually be a *subgroup* of $\mathrm{Aut}(K)$ — the collection of elements of K fixed by all the elements of a *subset* of $\mathrm{Aut}(K)$ is also a subfield of K.

Definition. If H is a subgroup of the group of automorphisms of K, the subfield of K fixed by all the elements of H is called the *fixed field* of H.

Proposition 4. The association of groups to fields and fields to groups defined above is inclusion reversing, namely

(1) if $F_1 \subseteq F_2 \subseteq K$ are two subfields of K then $\mathrm{Aut}(K/F_2) \leq \mathrm{Aut}(K/F_1)$, and

(2) if $H_1 \leq H_2 \leq \mathrm{Aut}(K)$ are two subgroups of automorphisms with associated fixed fields F_1 and F_2, respectively, then $F_2 \subseteq F_1$.

Proof: Any automorphism of K that fixes F_2 also fixes its subfield F_1, which gives (1). The second assertion is proved similarly.

Examples

(1) Suppose $K = \mathbb{Q}(\sqrt{2})$ as in Example 1 above. Then the fixed field of $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})) = \mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{1, \sigma\}$ will be the set of elements of $\mathbb{Q}(\sqrt{2})$ with

$$\sigma(a + b\sqrt{2}) = a + b\sqrt{2}$$

since everything is fixed by the identity automorphism. This is the equation

$$a - b\sqrt{2} = a + b\sqrt{2}.$$

which is equivalent to $b = 0$, so the fixed field of $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ is just $\mathbb{Q}$.

(2) Suppose now that $K = \mathbb{Q}(\sqrt[3]{2})$ as in Example 2 above. In this case $\mathrm{Aut}(K) = 1$, so that every element of K is fixed, i.e., the fixed field of $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ is $\mathbb{Q}(\sqrt[3]{2})$.

Given a subfield F of K, the associated group is the collection of automorphisms of K which fix F. Given a group of automorphisms of K, the associated extension is defined by taking F to be the fixed field of the automorphisms. In the first example above, starting with the subfield $\mathbb{Q}$ of $\mathbb{Q}(\sqrt{2})$ one obtains the group $\{1, \sigma\}$ and starting with the group $\{1, \sigma\}$ one obtains the subfield $\mathbb{Q}$, so there is a "duality" between the two. In the second example, however, starting with the subfield $\mathbb{Q}$ of $\mathbb{Q}(\sqrt[3]{2})$ one obtains only the trivial group and starting with the trivial group one obtains the full field $\mathbb{Q}(\sqrt[3]{2})$.

An examination of the two examples suggests that for the second example there are "not enough" automorphisms to force the fixed field to be $\mathbb{Q}$ rather than the full $\mathbb{Q}(\sqrt[3]{2})$. This in turn seems to be due to the fact that the other roots of $x^3 - 2$, which are the only possible images of $\sqrt[3]{2}$ under an automorphism, are not elements of $\mathbb{Q}(\sqrt[3]{2})$. (Although even if they were we would need to check that the additional maps we could define were *automorphisms*.) We now make precise the notion of fields with "enough" automorphisms (leading to the definition of a *Galois* extension). As one might suspect even from these two examples (and we prove in the next section) these are related to splitting fields.

We first investigate the size of the automorphism group in the case of splitting fields.

Let F be a field and let E be the splitting field over F of $f(x) \in F[x]$. The main tool is Theorem 13.27 on the existence of extensions of isomorphisms, which states that any isomorphism $\varphi : F \xrightarrow{\sim} F'$ of F with F' can be extended to an isomorphism $\sigma : E \xrightarrow{\sim} E'$ between E and the splitting field E' for $f'(x) = \varphi(f(x)) \in F'[x]$.

We now show by induction on $[E : F]$ that the number of such extensions is at most $[E : F]$, with equality if $f(x)$ is separable over F. If $[E : F] = 1$ then $E = F$, $E' = F'$, $\sigma = \varphi$ and the number of extensions is 1. If $[E : F] > 1$ then $f(x)$ has at least one irreducible factor $p(x)$ of degree > 1 with corresponding irreducible factor $p'(x)$ of $f'(x)$. Let α be a fixed root of $p(x)$. If σ is any extension of φ to E, then σ restricted to the subfield $F(\alpha)$ of E is an isomorphism τ of $F(\alpha)$ with some subfield of E'. The isomorphism τ is completely determined by its action on α, i.e., by $\tau\alpha$, since α generates $F(\alpha)$ over F. Just as in Proposition 2, we see that $\tau\alpha$ must be some root β of $p'(x)$. Then we have a diagram

$$\begin{tikzcd}
\sigma : & E \arrow[r, "\sim"] \arrow[d, dash] & E' \arrow[d, dash] \\
\tau : & F(\alpha) \arrow[r, "\sim"] \arrow[d, dash] & F'(\beta) \arrow[d, dash] \\
\varphi : & F \arrow[r, "\sim"] & F'
\end{tikzcd}$$

Conversely, for any β a root of $p'(x)$ there are extensions τ and σ giving such a diagram (this is Theorem 13.8 and Theorem 13.27). Hence to count the number of extensions σ we need only count the possible number of these diagrams.

The number of extensions of φ to an isomorphism τ is equal to the number of distinct roots β of $p'(x)$. Since the degree of $p(x)$ and $p'(x)$ are both equal to $[F(\alpha) : F]$, we see that the number of extensions of φ to a τ is at most $[F(\alpha) : F]$, with equality if the roots of $p(x)$ are distinct.

Since E is also the splitting field of $f(x)$ over $F(\alpha)$, E' is the splitting field of $f'(x)$