Notes on Galois Theory I

1 First remarks

Definition 1.1. Let $E$ be a field. An automorphism of $E$ is a (ring) isomorphism from $E$ to itself. (Note that every ring homomorphism $\sigma$ from $E$ to itself is automatically injective, since $\text{Ker} \, \sigma$ is an ideal of $E$, hence either $\{0\}$ or $E$ since $E$ is a field. But $\sigma(1) = 1 \neq 0$, so $\text{Ker} \, \sigma \neq E$, hence $\text{Ker} \, \sigma = \{0\}$ and so $\sigma$ is injective. Thus $\sigma$ is an automorphism $\iff \sigma$ is surjective.) We denote the set of all automorphisms of $E$ by $\text{Aut} \, E$. Since every isomorphism is also a bijection, $\text{Aut} \, E$ is a subset of $S_E$, the group of all permutations of the set $E$. The composition of two automorphisms is an automorphism, the identity $\text{Id}_E$ is an automorphism, and the inverse of an automorphism is also an automorphism. Hence $\text{Aut} \, E$ is a subgroup of $S_E$. We shall use the same conventions for multiplication in $\text{Aut} \, E$ as we use with the symmetric group $S_E$: the product of $\sigma_1$ and $\sigma_2$ is written as $\sigma_1 \sigma_2$, instead of $\sigma_1 \circ \sigma_2$, we write $1$ for the identity automorphism $\text{Id}_E$.

Let $E$ be a finite extension of a field $F$. Define the Galois group $\text{Gal}(E/F)$ to be the subset of $\text{Aut} \, E$ consisting of all automorphisms $\sigma : E \to E$ such that $\sigma(a) = a$ for all $a \in F$. We write this last condition as $\sigma | F = \text{Id}$. It is easy to check that $\text{Gal}(E/F)$ is a subgroup of $\text{Aut} \, E$ (i.e. that it is closed under composition, $1 \in \text{Gal}(E/F)$, and, if $\sigma \in \text{Gal}(E/F)$, then $\sigma^{-1} \in \text{Gal}(E/F)$). Note that, if $F_0$ is the prime subfield of $E$ ($F_0 \cong \mathbb{Q}$ or $F_0 \cong \mathbb{F}_p$ depending on whether the characteristic is 0 or a prime $p$), then $\text{Aut} \, E = \text{Gal}(E/F_0)$. In other words, every $\sigma \in \text{Aut} \, E$ satisfies $\sigma(1) = 1$ and hence $\sigma(a) = a$ for all $a \in F_0$. A useful fact, which is left as a homework problem, is that if $E$ is a finite extension of a field $F$ and $\sigma : E \to E$ is a ring homomorphism such that $\sigma(a) = a$ for all $a \in F$, then $\sigma$ is surjective, hence an automorphism, hence is an element of $\text{Gal}(E/F)$.

If we have a sequence of fields $F \leq K \leq E$, then $\text{Gal}(E/K) \leq \text{Gal}(E/F)$ (the order is reversed).

Example 1.2. (1) If $\sigma : \mathbb{C} \to \mathbb{C}$ is complex conjugation, then $\sigma \in \text{Gal}(\mathbb{C}/\mathbb{R})$, and in fact we shall soon see that $\text{Gal}(\mathbb{C}/\mathbb{R}) = \{\text{Id}, \sigma\}$. 
(2) The group $\text{Aut } \mathbb{R} = \text{Gal}(\mathbb{R}/\mathbb{Q})$, surprisingly, is trivial: $\text{Gal}(\mathbb{R}/\mathbb{Q}) = \{\text{Id}\}$. The argument roughly goes by showing first that every automorphism of $\mathbb{R}$ is continuous and then that a continuous automorphism of $\mathbb{R}$ is the identity. In the case of $\mathbb{C}$, however, the only continuous automorphisms of $\mathbb{C}$ are the identity and complex conjugation. Nonetheless, $\text{Aut } \mathbb{C}$ and $\text{Aut } \mathbb{Q}^{\text{alg}}$ turn out to be very large groups! Most elements of $\text{Aut } \mathbb{C}$ are therefore (very badly) discontinuous.

(3) We have seen in the homework that $\text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{\text{Id}, \tau\}$, where $\tau(\sqrt{2}) = -\sqrt{2}$ and hence $\tau(a + b\sqrt{2}) = a - b\sqrt{2}$ for all $a, b \in \mathbb{Q}$.

(4) More generally, let $F$ be any field of characteristic not equal to 2 and suppose that $t \in F$ is not a perfect square in $F$, i.e. that the polynomial $x^2 - t$ has no root in $F$ and hence is irreducible in $F[x]$. Let $E = F(\sqrt{t})$ be the degree two extension of $F$ obtained by adding a root of $x^2 - t$, which we naturally write as $\sqrt{t}$. Then we leave it as a homework problem to check that $\text{Gal}(E/F) = \{1, \sigma\}$, where $\sigma(a + b\sqrt{t}) = a - b\sqrt{t}$.

(5) We have seen in the homework that $\text{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{\text{Id}\}$. Let $\sigma \in \text{Aut } E$. We define the fixed field

$$E^\sigma = \{\alpha \in E : \sigma(\alpha) = \alpha\}.$$ 

It is straightforward to check that $E^\sigma$ is a subfield of $E$ (since, if $\alpha, \beta \in E^\sigma$, then by definition $\sigma(\alpha \pm \beta) = \sigma(\alpha) \pm \sigma(\beta) = \alpha \pm \beta$, and similarly for multiplication and division (if $\beta \neq 0$), so that $E^\sigma$ is closed under the field operations. Clearly $E^\sigma \leq E$, and, if $F_0$ is the prime subfield of $E$, then $F_0 \leq E^\sigma$. We can extend this definition as follows: if $X$ is any subset of $\text{Aut } E$, we define the fixed field

$$E^X = \{\alpha \in E : \sigma(\alpha) = \alpha \text{ for all } \sigma \in X\}.$$ 

Since $E^X = \bigcap_{\sigma \in X} E^\sigma$, it is easy to see that $E^X$ is again a subfield of $E$. We are usually interested in the case where $X = H$ is a subgroup of $\text{Aut } E$. It is easy to see that, if $H$ is the subgroup generated by a set $X$, then $E^H = E^X$. In particular, for a given element $\sigma \in \text{Aut } E$, if $\langle \sigma \rangle$ is the cyclic subgroup generated by $\sigma$, then $E^{\langle \sigma \rangle} = E^\sigma$: this is just the statement that $\sigma(\alpha) = \alpha \iff$ for all $n \in \mathbb{Z}$, $\sigma^n(\alpha) = \alpha$. (More generally, if $\sigma_1, \sigma_2 \in X$ and $\alpha \in E^X$, then by definition $\sigma_1(\alpha) = \sigma_2(\alpha) = \alpha$, and thus $\sigma_1 \sigma_2(\alpha) = \sigma_1(\sigma_2(\alpha)) = \sigma_1(\alpha) = \alpha$. Since $\langle X \rangle$, the subgroup generated by
$X$, is just the set of all products of powers of elements of $X$, we see that
\[ \alpha \in E^X \implies \alpha \in E^{(X)}, \]
and hence that $E^X \leq E^{(X)}$. On the other hand, as $X \subseteq \langle X \rangle$, clearly $E^{(X)} \leq E^X$, and hence $E^X = E^{(X)}$.

We shall usual apply this in the following situation: given a subgroup $H$ of $\text{Gal}(E/F)$, we have defined the fixed field
\[ E^H = \{ \alpha \in E : \sigma(\alpha) = \alpha \text{ for all } \sigma \in H \}. \]
Then $E^H$ is a subfield of $E$ and by definition $F \leq E^H$ for every $H$. Thus $F \leq E^H \leq E$. Finally, this construction is order reversing in the sense that, if $H_1 \leq H_2 \leq \text{Gal}(E/F)$, then
\[ F \leq E^{H_2} \leq E^{H_1} \leq E. \]

Thus, given a field $K$ with $F \leq K \leq E$, we have a subgroup $\text{Gal}(E/K)$ of $\text{Gal}(E/F)$, and given a subgroup $H \leq \text{Gal}(E/F)$ we get a field $E^H$ with $F \leq E^H \leq E$. In general, there is not much one can say about the relationship between these two constructions beyond the straightforward fact that
\[ H \leq \text{Gal}(E/E^H); \]
\[ K \leq E^{\text{Gal}(E/K)}. \]

Here, to see the first inclusion, note that
\[ E^H = \{ \alpha \in E : \sigma(\alpha) = \alpha \text{ for all } \sigma \in H \}. \]
Thus, for $\sigma \in H$, $\sigma \in \text{Gal}(E/E^H)$ by definition, hence $H \leq \text{Gal}(E/E^H)$. The inclusion $K \leq E^{\text{Gal}(E/K)}$ is similar.

Our first goal in these notes is to study finite extensions $E$ of a field $F$, and to find conditions which enable us to conclude that $\text{Gal}(E/F)$ is as large as possible. In fact, we will see that the maximum size is $[E : F]$, i.e. that $\#(\text{Gal}(E/F)) \leq [E : F]$. The “best” case is when equality holds. This study has two parts: First, we describe how to find homomorphisms $\sigma : E \rightarrow L$, where $L$ is some extension of $F$, with the property that $\sigma(a) = a$ for all $a \in F$. Then we give a condition where, in case $E$ is a subfield of $L$, the image of $\sigma$ is automatically contained in $E$, and thus $\sigma$ is an automorphism of $E$. We will discuss the motivation for Galois theory shortly, once we have established a few more basic properties of the Galois group.
2 Automorphisms and roots of polynomials

Recall the following basic fact about complex roots of polynomials with real coefficients, which says that complex roots of a real polynomial occur in conjugate pairs:

Lemma 2.1. Let \( f \in \mathbb{R}[x] \) is a polynomial with real coefficients and let \( \alpha \) be a complex root of \( f \). Then \( f(\bar{\alpha}) = 0 \) as well.

Proof. Suppose that \( f = \sum_{i=0}^{n} a_i x^i \) with \( a_i \in \mathbb{R} \). Then, for all \( \alpha \in \mathbb{C} \),

\[
0 = \sigma(0) = \sum_{i=0}^{n} a_i \alpha^i = \sum_{i=0}^{n} \bar{a}_i (\bar{\alpha})^i = \sum_{i=0}^{n} a_i (\bar{\alpha})^i = f(\bar{\alpha}).
\]

Hence \( f(\bar{\alpha}) = 0 \).

As a result, assuming the Fundamental Theorem of Algebra, we can describe the irreducible elements of \( \mathbb{R}[x] \):

Corollary 2.2. The irreducible polynomials \( f \in \mathbb{R}[x] \) are either linear polynomials or quadratic polynomials with no real roots.

Proof. Let \( f \in \mathbb{R}[x] \) be a nonconstant polynomial which is an irreducible element of \( \mathbb{R}[x] \). By the Fundamental Theorem of Algebra, there exists a complex root \( \alpha \) of \( f \). If \( \alpha \in \mathbb{R} \), then \( x - \alpha \) is a factor of \( f \) in \( \mathbb{R}[x] \) and hence \( f = c(x - \alpha) \) for some \( c \in \mathbb{R}^* \). Thus \( f \) is linear. Otherwise, \( \alpha \notin \mathbb{R} \), and hence \( \bar{\alpha} \neq \alpha \). Then \( (x - \alpha)(x - \bar{\alpha}) \) divides \( f \) in \( \mathbb{C}[x] \). But

\[
(x - \alpha)(x - \bar{\alpha}) = x^2 - (\alpha + \bar{\alpha})x + \alpha \bar{\alpha} = x^2 - (2 \text{Re} \alpha)x + |\alpha|^2 \in \mathbb{R}[x],
\]

hence \( (x - \alpha)(x - \bar{\alpha}) \) divides \( f \) in \( \mathbb{R}[x] \). Thus \( f = c(x - \alpha)(x - \bar{\alpha}) \) for some \( c \in \mathbb{R}^* \) and \( f \) is an irreducible quadratic polynomial.

We can generalize Lemma 2.1 as follows:

Lemma 2.3. Let \( E \) be an extension field of a field \( F \), and let \( f \in F[x] \). Suppose that \( \alpha \in E \) and that \( f(\alpha) = 0 \). Then, for every \( \sigma \in \text{Gal}(E/F) \), \( f(\sigma(\alpha)) = 0 \) as well.

Proof. If \( f = \sum_{i=0}^{n} a_i x^i \) with \( a_i \in F \) for all \( i \), then

\[
0 = \sigma(0) = \sigma \left( \sum_{i=0}^{n} a_i \alpha^i \right) = \sum_{i=0}^{n} a_i (\sigma(\alpha))^i,
\]

hence \( \sigma(\alpha) \) is a root of \( f \) as well.
In fact, it will be useful to prove a more general version. We suppose that we are given the following situation: \( E \) is an extension field of a field \( F \), \( K \) is another field, and \( \varphi: E \to K \) is a homomorphism (automatically injective). Let \( F' = \varphi(F) \) and let \( \sigma: F \to F' \) be the corresponding isomorphism. Another way to think of this is as follows:

**Definition 2.4.** Suppose that \( E \) is an extension field of the field \( F \), that \( L \) is an extension field of the field \( K \), and that \( \sigma: F \to K \) is a homomorphism. An extension of \( \sigma \) is a homomorphism \( \varphi: E \to L \) such that, for all \( a \in F \), \( \varphi(a) = \sigma(a) \). We also say that the restriction of \( \varphi \) to \( F \) is \( \sigma \), and write this as \( \varphi|F = \sigma \).

The situation is summarized in the following diagram:

\[
\begin{array}{ccc}
E & \xrightarrow{\varphi} & L \\
\downarrow & & \downarrow \\
F & \xrightarrow{\sigma} & K
\end{array}
\]

Given \( f = \sum_{i=0}^{n} a_i x^i \in F[x] \), define a new polynomial \( \sigma(f) \in K[x] \) by the formula

\[
\sigma(f) = \sum_{i=0}^{n} \sigma(a_i) x^i.
\]

In other words, \( \sigma(f) \) is the polynomial obtained by applying the isomorphism \( \sigma \) to the coefficients of \( f \).

**Lemma 2.5.** In the above situation, \( \alpha \in E \) is a root of \( f \in F[x] \) if and only if \( \varphi(\alpha) \in L \) is a root of \( \sigma(f) \in K[x] \).

**Proof.** In fact, for \( \alpha \) an arbitrary element of \( E \), and using the definitions and the fact that \( \varphi \) is a field automorphism, we see that

\[
\varphi(f(\alpha)) = \varphi(\sum_{i=0}^{n} a_i \alpha^i) = \sum_{i=0}^{n} \varphi(a_i) \varphi(\alpha)^i = \sum_{i=0}^{n} \sigma(a_i) \varphi(\alpha)^i = \sigma(f)(\varphi(\alpha)).
\]

Thus, as \( \varphi \) is injective, \( f(\alpha) = 0 \iff \varphi(f(\alpha)) = 0 \iff \sigma(f)(\varphi(\alpha)) = 0 \). \( \square \)

A second basic observation is then the following:
Corollary 2.6. Let $E$ be an extension field of the field $F$ and let $f \in F[x]$. Suppose that $\alpha_1, \ldots, \alpha_n$ are the (distinct) roots of $f$ that lie in $E$, i.e. \{\alpha \in E : f(\alpha) = 0\} = \{\alpha_1, \ldots, \alpha_n\}$ and, for $i \neq j$, $\alpha_i \neq \alpha_j$. Then $\text{Gal}(E/F)$ acts on the set $\{\alpha_1, \ldots, \alpha_n\}$, and hence there is a homomorphism $\rho : \text{Gal}(E/F) \to S_n$, where $S_n$ is the symmetric group on $n$ letters. If moreover $E = F(\alpha_1, \ldots, \alpha_n)$, then $\rho$ is injective, and hence identifies $\text{Gal}(E/F)$ with a subgroup of $S_n$. In particular, in this case $\#(\text{Gal}(E/F)) \leq n!$.

Proof. It follows from Lemma 2.3 that, if $\alpha_i$ is a root of $f$, then so is $\sigma(\alpha_i)$. Thus $\text{Gal}(E/F)$ acts on the set $\{\alpha_1, \ldots, \alpha_n\}$, where the action is given by $\sigma \cdot \alpha_i = \sigma(\alpha_i)$. It is easy to check that this is an action, since

$$\sigma_1 \cdot (\sigma_2 \cdot \alpha_i) = \sigma_1 \cdot (\sigma_2(\alpha_i)) = \sigma_1(\sigma_2(\alpha_i)) = \sigma_1 \circ \sigma_2(\alpha_i) = \sigma_1 \sigma_2(\alpha_i).$$

Hence that there is an associated homomorphism $\rho : \text{Gal}(E/F) \to S_n$, defined by

$$\sigma(\alpha_i) = \alpha_{\rho(\sigma)(i)}.$$ 

To see that $\rho$ is injective if $E = F(\alpha_1, \ldots, \alpha_n)$, it suffices to show that, if $\sigma \in \text{Gal}(E/F)$ and $\sigma(\alpha_i) = \alpha_i$ for all $i$, then $\sigma = \text{Id}$. To see this, recall that $E^\sigma$ is the fixed field of $\sigma$. Since $\sigma \in \text{Gal}(E/F)$, $F \leq E^\sigma$. If in addition $\sigma(\alpha_i) = \alpha_i$ for all $i$, then $E^\sigma$ is a subfield of $E$ containing $F$ and $\alpha_i$ for all $i$, and hence $E = F(\alpha_1, \ldots, \alpha_n) \leq E^\sigma \leq E$. It follows that $E^\sigma = E$, i.e. that $\sigma(\alpha) = \alpha$ for all $\alpha \in E$. This says that $\sigma = \text{Id}$. \qed

Lemma 2.7. Every finite extension $E$ of a field $F$ is of the form $E = F(\alpha_1, \ldots, \alpha_n)$, where the $\alpha_i$ are the roots in $E$ of some polynomial $f \in F[x]$, not necessarily irreducible.

Proof. We have seen that every finite extension $E$ of $F$ is of the form $F(\beta_1, \ldots, \beta_k)$ for some $\beta_i \in E$, necessarily algebraic over $F$. For each $i$, let $f_i = \text{irr}(\beta_i, F)$ and let $\alpha_1, \ldots, \alpha_n$ be the the set of all elements of $E$ which are a root of some $f_i$. (This is a finite set since each $f_i$ has only finitely many roots.) Let $f$ be the product $f_1 \cdots f_n$. An element $\alpha \in E$ is a root of $f$ $\iff$ $\alpha$ is a root of $f_i$ for some $i$, so that the set of roots of $f$ is $\{\alpha_1, \ldots, \alpha_n\}$. Also, for all $i$, $\beta_i$ is a root of $f_i$ and hence $\beta_i \in \{\alpha_1, \ldots, \alpha_n\}$. Thus $E = F(\beta_1, \ldots, \beta_k) \leq F(\alpha_1, \ldots, \alpha_n) \leq E$, so that $E = F(\alpha_1, \ldots, \alpha_n)$ is as claimed. \qed

Corollary 2.8. Let $E$ be a finite extension of the field $F$. Then $\text{Gal}(E/F)$ is finite.

We shall give an explicit bound for the order of $\text{Gal}(E/F)$ later.
**Remark 2.9.** The homomorphism $\rho: \text{Gal}(E/F) \to S_n$ given in Corollary 2.6 depends on a choice of labeling of the roots of $f$ as $\alpha_1, \ldots, \alpha_n$. A different choice of labeling the roots corresponds to an element $\tau \in S_n$, and it is easy to check that listing the roots as $\alpha_{\tau(1)}, \ldots, \alpha_{\tau(n)}$ replaces $\rho$ by $\tau \cdot \rho \cdot \tau^{-1}$, i.e., by $i_\tau \circ \rho$, where $i_\tau: S_n \to S_n$ is the inner automorphism given by conjugation by $\tau$. In particular, the image of $\rho$ is well-defined up to conjugation. As we shall see, it also depends on which polynomial $f$ we choose, in a more essential way.

**Example 2.10.** (1) In case $F = \mathbb{R}$ and $E = \mathbb{C}$, let $f = x^2 + 1$ with roots $\pm i$. Since $\mathbb{C} = \mathbb{R}(i)$, there is an injective homomorphism $\text{Gal}(\mathbb{C}/\mathbb{R}) \to S_2$, where $S_2$ is viewed as the set of permutations of the two element set $\{i, -i\}$. Hence $\#(\text{Gal}(\mathbb{C}/\mathbb{R})) = 2$. Since complex conjugation $\sigma$ is an element of $\text{Gal}(\mathbb{C}/\mathbb{R})$ which exchanges $i$ and $-i$, $\text{Gal}(\mathbb{C}/\mathbb{R})$ has order two and is equal to $\{1, \sigma\}$.

(2) Similarly, with $F = \mathbb{Q}$ and $E = \mathbb{Q}(\sqrt{2})$, $\text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ is isomorphic to a subgroup of $S_2$, where $S_2$ is now viewed as the set of permutations of the two element set $\{\sqrt{2}, -\sqrt{2}\}$. Hence $\#(\text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})) = 2$, and since (by a homework problem) $\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$ is an automorphism of $\mathbb{Q}(\sqrt{2})$ which is the identity on $\mathbb{Q}$, $\text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ has order two and is equal to $\{1, \sigma\}$. More generally, if $F$ is a field, not of characteristic 2, $t \in F$ is not a square, and $E = F(\sqrt{t})$, then $\text{Gal}(E/F) = \{1, \sigma\} \cong S_2$, where $\sigma(a + b\sqrt{t}) = a - b\sqrt{t}$.

(3) Let $F = \mathbb{Q}$ and $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Every element of $\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ permutes the roots of $(x^2 - 2)(x^2 - 3)$, i.e. the set $\{\pm \sqrt{2}, \pm \sqrt{3}\}$. Since $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\pm \sqrt{2}, \pm \sqrt{3})$, $\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ is isomorphic to a subgroup of $S_4$. Explicitly, let us label $\alpha_1 = \sqrt{2}$, $\alpha_2 = -\sqrt{2}$, $\alpha_3 = \sqrt{3}$, and $\alpha_4 = -\sqrt{3}$. Since $\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ actually permutes the set $\{\pm \sqrt{2}\}$ and $\{\pm \sqrt{3}\}$ individually, we see that the image of $\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ is contained in the subgroup $\{1, (12), (34), (12)(34)\} \cong S_2 \times S_2$ of $S_4$. In fact, we claim that $\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ is isomorphic to the full subgroup $\{1, (12), (34), (12)(34)\}$. To see this, apply (2) above to the case $F = \mathbb{Q}(\sqrt{3})$ and $t = 2$. We have seen in the homework that $\sqrt{2} \notin \mathbb{Q}(\sqrt{3})$, i.e., that the polynomial $x^2 - 2$ is irreducible in $\mathbb{Q}(\sqrt{3})[x]$. Then by (2) there is an element $\sigma_1 \in \text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{3})) \leq \text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ such that $\sigma_1(\sqrt{2}) = -\sqrt{2}$, and $\sigma_1(\sqrt{3}) = \sqrt{3}$ by construction. Thus $\sigma_1$ corresponds to the permutation $(12) \in S_4$. Exchanging the roles of 2 and 3, we see that there is a $\sigma_2 \in \text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{2})) \leq \text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ such that $\sigma_2(\sqrt{2}) = \sqrt{2}$, and $\sigma_2(\sqrt{3}) = -\sqrt{3}$. Thus $\sigma_2$ corresponds to the permutation $(34)$. Finally, the product $\sigma_3 = \sigma_1\sigma_2$ satisfies: $\sigma_3(\sqrt{2}) = -\sqrt{2}$, $\sigma_3(\sqrt{3}) = -\sqrt{3}$, and thus corresponds to the permutation $(12)(34)$. 


Finally, note that $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ is a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$. In this basis, the elements of $\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ are diagonalized, with eigenvalues $\pm 1$.

(4) For a very closely related example, let $\alpha = \sqrt{2} + \sqrt{3}$ with $\text{irr}(\alpha, \mathbb{Q}, x) = x^4 - 10x^2 + 1$. Then we have seen that $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. By (4) above, $\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = \text{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) = \{1, \sigma_1, \sigma_2, \sigma_3\}$, where

$\sigma_1(\sqrt{2}) = -\sqrt{2}; \quad \sigma_1(\sqrt{3}) = \sqrt{3};$

$\sigma_2(\sqrt{2}) = \sqrt{2}; \quad \sigma_2(\sqrt{3}) = -\sqrt{3};$

$\sigma_3(\sqrt{2}) = -\sqrt{2}; \quad \sigma_3(\sqrt{3}) = -\sqrt{3}.$

Applying $\sigma_i$ to $\alpha$ and using Lemma 2.3, we see that all of the elements $\pm \sqrt{2} \pm \sqrt{3}$ of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ are roots of $\text{irr}(\alpha, \mathbb{Q}, x) = x^4 - 10x^2 + 1$. Since there are four such elements and $x^4 - 10x^2 + 1$ has degree four, the roots of $\text{irr}(\alpha, \mathbb{Q}, x) = x^4 - 10x^2 + 1$ are exactly $\alpha = \beta_1 = \sqrt{2} + \sqrt{3}$, $\beta_2 = -\sqrt{2} + \sqrt{3}$, $\beta_3 = \sqrt{2} - \sqrt{3}$, and $\beta_4 = -\sqrt{2} - \sqrt{3}$. In particular, the polynomial $x^4 - 10x^2 + 1$ factors into linear factors in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$:

$$x^4 - 10x^2 + 1 = (x - \beta_1)(x - \beta_2)(x - \beta_3)(x - \beta_4).$$

The action of the Galois group on the set $\{\beta_1, \beta_2, \beta_3, \beta_4\}$ then identifies the $\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = \text{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) = \{1, \sigma_1, \sigma_2, \sigma_3\}$

with the subgroup

$$\{1, (12)(34), (13)(24), (14)(23)\}$$

of $S_4$. We can thus identify the same Galois group $\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = \text{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ with two different (but of course isomorphic) subgroups of $S_4$. Note that $H$ is not in fact conjugate to $S_2 \times S_2$ since $H$ acts transitively on $\{1, 2, 3, 4\}$ but $S_2 \times S_2$ does not.

(5) Let $F = \mathbb{Q}$ and $E = \mathbb{Q}(\sqrt[3]{2})$. There is just one root of $x^3 - 2$ in $\mathbb{Q}(\sqrt[3]{2})$, namely $\sqrt[3]{2}$, and hence (as we have already seen) $\text{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{1\}$. On the other hand, if $\omega = \frac{1}{2}(-1 + \sqrt{-3})$, then $\omega^3 = 1$, hence $\omega^2 = \omega^{-1} = \bar{\omega}$. Moreover, the roots of $x^3 - 2$ in $\mathbb{C}$ are $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = \omega \sqrt[3]{2}$, and $\alpha_3 = \omega^2 \sqrt[3]{2}$, since if $\alpha$ is a root of $x^3 - 2$, then $\alpha/\sqrt[3]{2}$ is a cube root of unity as

$$\frac{\alpha}{\sqrt[3]{2}} = \sqrt[3]{2} = 2/2 = 1.$$

Moreover $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) = \mathbb{Q}(\sqrt[3]{2}, \omega)$. By Corollary 2.6, there is an injective homomorphism from $\text{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$ to $S_3$. As we shall see, this
homomorphism is in fact an isomorphism. Here we just note that complex conjugation defines a nontrivial element $\sigma$ of $\text{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$ of order 2. In fact as $\sqrt[3]{2}$ is real, $\sigma(\alpha_1) = \alpha_1$, and $\sigma(\alpha_2) = \omega \sqrt[3]{2} = \omega^2 \sqrt[3]{2} = \alpha_3$. Thus $\sigma$ corresponds to $(23) \in S_3$. If we can show that there exists an element $\varphi$ of $\text{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$ such that $\varphi(\sqrt[3]{2}) = \omega \sqrt[3]{2}$, then necessarily $\varphi$ corresponds to either $(12)$ or $(123)$. Since $S_3$ is generated by $(12)$ and $(23)$ and also by $(123)$ and $(23)$, in either case we see that the homomorphism from $\text{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$ to $S_3$ is also surjective and hence an isomorphism.

(6) Again let $F = \mathbb{Q}$ and $E = \mathbb{Q}(\sqrt[4]{2})$. There are two roots of $x^4 - 2$ in $\mathbb{Q}(\sqrt[4]{2})$, namely $\pm \sqrt[4]{2}$. Thus $\text{Gal}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q})$ has order at most 2 and in fact has order 2 by applying (4) to the case $F = \mathbb{Q}(\sqrt[2]{t})$ and $t = \sqrt[2]{2}$ with $\sqrt[4]{t} = \sqrt[4]{2}$. To improve this situation, consider the field $\mathbb{Q}(\sqrt[4]{2}, i)$, which contains all four roots $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ of the polynomial $x^4 - 2$, namely $\pm \sqrt[4]{2}$ and $\pm i \sqrt[4]{2}$. Since clearly $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = \mathbb{Q}(\sqrt[4]{2}, i)$, $\text{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$ is isomorphic to a subgroup of $S_4$. However, it cannot be all of $S_4$. For example, if $\sigma \in \text{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$ and $\sigma(\alpha_1) = \alpha_i$ for some $i$, then since $\alpha_2 = -\alpha_1$, then $\sigma(\alpha_2) = -\alpha_i$: this says that not every permutation of $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ can occur. In fact, if $\sigma \in \text{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$, then there are at most 4 possibilities for $\sigma(\sqrt[4]{2})$, since $\sigma(\sqrt[4]{2})$ has to be a root of $x^4 - 2$ and hence can only be $\alpha_i$ for $1 \leq i \leq 4$. But there are also at most 2 possibilities for $\sigma(i)$, which must be a root of $x^2 + 1$ and hence can only be $\pm i$. Since $\sigma$ is specified by its values on $\sqrt[4]{2}$ and on $i$, there are at most 8 possibilities for $\sigma$ and hence $\#(\text{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})) \leq 8$. We will see that in fact $\#(\text{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})) = 8$ and $\text{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}) \cong D_4$, the dihedral group of order 8.