Chapter III. Galois Theory

The essence of Galois Theory: The systematically developed connection between two seemingly unrelated subjects, the theory of fields and the theory of groups.

More specifically, but in the same line, is the idea of studying a mathematical object by its group of automorphisms, an idea emphasized in Klein’s Erlanger Program, which has been accepted as a powerful tool in a great variety of mathematical disciplines.

The Galois Theory of field extensions combines the esthetic appeal of a theory of nearly perfect beauty with the technical development and difficulty that reveal the depth of the theory and that make possible its great usefulness primarily in algebraic number theory and related parts of algebraic geometry.

(From Roger Lyndon i: Encyclopedia of Mathematics and Its Applications)

BASIC CONCEPTS AND THEOREMS.

An automorphism of a field $L$ is a bijective mapping of $L$ onto itself which is also an isomorphism, i.e. a bijective mapping $\sigma$ that sends a sum of elements in $L$ into the sum of the corresponding elements and a product of elements in $L$ into the product of the corresponding elements: $\sigma(x + y) = \sigma(x) + \sigma(y)$ and $\sigma(xy) = \sigma(x)\sigma(y)$ for all $x, y \in L$. The set $\text{Aut}(L)$ of all automorphisms of $L$ forms a group where the product of two automorphisms $\sigma$ and $\tau$ is defined as the composition $\sigma\tau: \sigma\tau(x) := \sigma(\tau(x))$ for all $x \in L$. The neutral element in this group is the identity mapping sending every element in $L$ into itself. This mapping is denoted $1_L$ or $e$.

Example 3.1. For some fields the identity mapping is the only automorphism. For instance the field $\mathbb{Q}$ of all rational numbers has no other automorphism than the identity. (Why?)

If $S$ is an arbitrary subset of $\text{Aut}(L)$ we define the fixed set $\mathcal{F}(S)$ as $\mathcal{F}(S) = \{x \in L \mid \sigma x = x \forall \sigma \in S\}$.

It is easily seen that $\mathcal{F}(S)$ is a subfield of $L$ which is called the fixed field for $S$.

Example 3.2. Let $L = \mathbb{C}$ and $\sigma =$ complex conjugation. It is straightforward to check that $\mathcal{F}(\{\sigma\}) = \mathbb{R}$.

Let $K$ be a subfield of $L$. We define

$$\text{Aut}(L/K) = \{\sigma \in \text{Aut}(L) \mid \sigma_{\text{Res}, K} = 1_K\} = \{\sigma \in \text{Aut}(L) \mid \sigma k = k \forall k \in K\}.$$
Aut(L/K) is easily seen to be a subgroup of Aut(L). It is called the relative automorphism group for L over K.

The following is an immediate consequence of the definition:

1) \( \mathcal{F}(\text{Aut}(L/K)) \supseteq K \)
2) \( \text{Aut}(L/\mathcal{F}(S)) \supseteq S \)

In general, ”=” does not hold in 1) and 2).

**Remark 3.3.** If ”=” holds in 2) then S must be a subgroup of Aut(L). We shall later (Corollary 3.21) see that ”=” holds in 2) if S is a finite group.

For computations of relative automorphism groups the following is often quite useful:

**Lemma 3.4.** Let L/K be an arbitrary field extension and \( f(x) = x^n + a_1x^{n-1} + \cdots + a_n \) a (not necessarily irreducible) polynomial in \( K[X] \). If \( \alpha \) is an element in L and is a root of \( f(x) \), then \( \sigma(\alpha) \) is also a root of \( f(x) \) for every automorphism in \( \sigma \in \text{Aut}(L/K) \).

**Proof.** Since \( \alpha \) is a root of \( f(x) \) we get

\[
\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0
\]

By applying the automorphism \( \sigma \) on each side of the above equation we obtain

\[
(\sigma(\alpha))^n + a_1(\sigma(\alpha))^{n-1} + \cdots + a_n = 0 \quad (∗)
\]

where we have used that \( a_1, \cdots a_n \) are fixed under the automorphism \( \sigma \). But the equation (∗) just means that \( \sigma(\alpha) \) is a root of \( f(x) \). \( \square \)

**Example 3.5.** \( L = \mathbb{C}, \ K = \mathbb{R}, \ \text{Aut}(L/K) = \{1_L, \text{complex conjugation}\} \). Here \( \mathcal{F}(\text{Aut}(L/K)) = K \). Indeed, any number in L can be written uniquely as \( k_1 + k_2 \cdot i \) where \( k_1 \) and \( k_2 \) lie in \( K \) and \( i = \sqrt{-1} \). An automorphism in \( \text{Aut}(L/K) \) is uniquely determined by its value on \( i \). Since \( i \) is a root of \( x^2 + 1 \) the above lemma means that such an automorphism can only send \( i \) into \( i \) or \( -i \). On the other hand \( 1_L \) and complex conjugation are automorphisms in \( \text{Aut}(L/K) \) and a complex number is invariant under complex conjugation if and only if it is real.

**Example 3.6.** \( L = \mathbb{Q}((\sqrt{2})), \ K = \mathbb{Q}, \ \text{Aut}(L/K) = \{1_L, \sigma\} \) where \( \sigma(a + b\sqrt{2}) = a - b\sqrt{2} ; a, b \in \mathbb{Q} \). Here \( \mathcal{F}(\text{Aut}(L/K)) = K \). This can be verified by the same method as in the previous example.

**Example 3.7.** \( L = \mathbb{Q}((\sqrt{2})), \ K = \mathbb{Q}, \ \text{Aut}(L/K) = 1_L \). Indeed \( [L : K] = \deg(\text{Irr}(\sqrt{2})) = 3 \), since \( x^3 - 2 = \text{Irr}(\sqrt{2}) \). Hence every element in L has a unique representation of the form \( q_0 + q_1\sqrt{2} + q_2(\sqrt{2})^2 \), where \( q_0, q_1 \) and \( q_2 \) are rational numbers. An automorphism in \( \text{Aut}(L/K) \) is uniquely determined by its value on
\( \sqrt{3} \). Since \( L \) consists entirely of real numbers and \( \sqrt{3} \) is the only real root of \( x^3 - 2 \) the identity \( 1_L \) is the only automorphism in \( Aut(L/K) \). Hence \( \mathcal{F}(\text{Aut}(L/K)) = L \).

**Example 3.8.** \( L = \mathbb{R}, K = \mathbb{Q} \). Here is \( \text{Aut}(L/K) = 1_L \) hence: \( \mathcal{F}(\text{Aut}(L/K)) = L \). (The proof is non-trivial.)

**Example 3.9.** \( L = \mathbb{C}, K = \mathbb{Q} \), \( \text{Aut}(L/K) = \text{Aut}(\mathbb{C}) \) has the cardinality \( 2^{2^0} \) and \( \mathcal{F}(\text{Aut}(L/K)) = K \). (The proof is non-trivial.)

The above examples concern the relation 1).

**Example 3.10.** In 2) it can happen that \( \text{Aut}(L/\mathcal{F}(S)) \not\supseteq S \) even when \( S \) is a group. Let \( L = \mathbb{C}(X), K = \mathbb{C}, S = \) all “translations”

\[
S = \{ \sigma \in \text{Aut} \mathbb{C}(X) \mid \sigma \left( \frac{f(x)}{g(x)} \right) = \frac{f(x + a)}{g(x + a)} \},
\]

where \( a \) runs through \( \mathbb{C} \). Here \( \mathcal{F}(S) = \mathbb{C} \) and \( \text{Aut}(L/\mathcal{F}(S)) \not\supseteq S \) since \( x \to \frac{1}{x} \) induces an automorphism in \( \text{Aut}(\mathbb{C}(X)/C) \) which does not belong to \( S \).

**Galois Theory Starts.**

**Definition 3.11.** \( L \supseteq K \) is called a normal extension if \( K = \mathcal{F}(\text{Aut}(L/K)) \). If moreover \( [L : K] \) is finite, \( L \) is called a finite normal extension of \( K \).

**Theorem 3.12.** If \( M \) is the splitting field over the field \( K \) for a separable polynomial \( f(x) \in K[X] \) then \( M \) is a finite normal extension of \( K \).

**Proof.** \( [M : K] < \infty \) is clear. If all roots of \( f(x) \) lie in \( K \) then \( M = K \) and there is nothing to prove. So let us assume that \( M \not\supseteq K \). We may then choose roots \( \alpha_1, \ldots, \alpha_t \) of \( f(x) \) such that \( M = K(\alpha_1, \ldots, \alpha_t) \) and \( K \not\supseteq K(\alpha_1) \not\supseteq K(\alpha_1, \alpha_2) \not\supseteq \cdots \not\supseteq K(\alpha_1, \ldots, \alpha_t) = M \). We shall prove that \( \forall \beta \in M \setminus K \exists \sigma \in \text{Aut}(M/K) \) such that \( \sigma(\beta) \neq \beta \).

Assume \( \beta \in K(\alpha_1, \ldots, \alpha_i) \setminus K(\alpha_1, \ldots, \alpha_{i-1}) \). To ease the notation we set \( L = K(\alpha_1, \ldots, \alpha_{i-1}), \gamma = \alpha_i \). Therefore \( \beta \in L(\gamma), \beta \notin L \). Thus:

\[
\text{Irr}(\gamma, L) | \text{Irr}(\gamma, K) | f(x).
\]

Since \( f(x) \) is separable, \( \text{Irr}(\gamma, K) \) and thus in particular \( \text{Irr}(\gamma, L) \) has only simple roots.

If \( n \) is the degree of \( \text{Irr}(\gamma, L) \), then \( [L(\gamma) : L] = n \) and \( \text{Irr}(\gamma, L) \) has exactly \( n \) distinct roots \( \gamma_1, \gamma_2, \ldots, \gamma_n \) where for instance \( \gamma = \gamma_1 \).

\( \beta \) can be written in the form

\[
\beta = a_0 + a_1 \gamma + \cdots + a_{n-1} \gamma^{n-1}, \quad a_0, \ldots, a_{n-1} \in L
\]

and \( \beta \notin L \Rightarrow a_i \neq 0 \) for at least one \( i \geq 1 \).
Not all the elements \(a_0 + a_1\gamma_j + \cdots + a_{n-1}\gamma_j^{n-1}, j = 1, 2, \ldots, n\) can be equal to \(\beta\). Otherwise the non-zero polynomial \(\beta - a_0 - a_1x - \cdots - a_{n-1}x^{n-1}\) of degree \(< n\) would have \(n\) distinct roots \(\gamma_1, \ldots, \gamma_n\).

Assume for instance \(a_0 + a_1\gamma_2 + \cdots + a_{n-1}\gamma_2^{n-1} \neq \beta\).

According to the uniqueness theorem for adjunction of a root of an irreducible polynomial (Theorem 2.57) there exists an isomorphism \(\varphi : L(\gamma) \rightarrow L(\gamma_2)\) for which \(\varphi_{\text{Res},L} = 1_L\) and \(\varphi(\gamma) = \gamma_2\).

$$\begin{array}{c}
M \\
\beta \\
L \\
\varphi \\
\gamma_2 \\
L(\gamma) \\
\varphi \\
L(\gamma_2) \\
\end{array}$$

Here \(\varphi(\beta) = \varphi(a_0 + a_1\gamma + \cdots + a_{n-1}\gamma^{n-1}) = a_0 + a_1\gamma_2 + \cdots + a_{n-1}\gamma_2^{n-1}\), which we just have seen is \(\neq \beta\). Now \(M\) is splitting field for \(f(x)\) over \(L(\gamma)\) and \(M\) is splitting field for \(f(x)\) over \(L(\gamma_2)\).

Since \(f(x) \in K[x] \subseteq L[x]\) the mapping of \(L(\gamma)[X] \rightarrow L(\gamma_2)[X]\) induced by \(\varphi\) will send \(f(x)\) into itself. By the theorem concerning the uniqueness of splitting fields (Theorem 2.60 in chap.2) \(\varphi\) can be prolonged to an automorphism \(\sigma : M \rightarrow M\). Clearly \(\sigma\) has the properties \(\sigma(\beta) \neq \beta\) and \(\sigma_{\text{Res},K} = 1_K\). In other words: \(\sigma\) is an automorphism in \(\text{Aut}(M/K)\) with the desired property. \(\square\)

---

**Example 3.13.** \(M = K(T), f(x) = (x - T)(x - \frac{1}{T}) = x^2 - (T + \frac{1}{T})x + 1\). \(M\) is a splitting field for \(f(x)\) over \(L = K(T + \frac{1}{T})\). Clearly \(f(x)\) is separable. \(\text{Aut}(M/L) = \{1_L\ \text{and} \ \sigma\}\) where \(\sigma(g(T)) = g(\frac{1}{T})\) for \(g(T) \in K(T)\). From this we get a theorem (which can be formulated without use of splitting fields etc.) about rational functions: a rational function \(g(T)\) satisfies the "functional equation" \(g(T) = g(\frac{1}{T})\) if and only if \(g = \) rational function of \(T + \frac{1}{T}\).

**Theorem 3.14.** If \(\mathbb{F}_p^n\) as usual denotes the finite field with \(p^n\) elements, the relative automorphism group \(\text{Aut}(\mathbb{F}_p^n / \mathbb{Z}_p)\) is cyclic of order \(n\) and is generated by the Frobenius automorphism sending every element into its \(p\)-th power.

**Proof.** By the theorem of Abel-Steinitz there exists an element \(\alpha \in \mathbb{F}_p^n\) such that \(\mathbb{F}_p^n = \mathbb{Z}_p(\alpha)\). Let \(f(x) = \text{Irr}(\alpha, \mathbb{Z}_p)\). An automorphism \(\sigma \in \text{Aut}(\mathbb{F}_p^n / \mathbb{Z}_p)\) is uniquely determined by its value on \(\alpha\); thus (by Lemma 3.4) there are at most \(n\) possibilities for \(\sigma\) since \(f(x)\) is of degree \(n\). On the other hand as we have seen in Chap.2 the mapping \(\sigma : a \mapsto a^p\) (sending every element into its \(p\)-th power) is an automorphism. Now \(\sigma^n = \) the identity \(1_L\) on \(L\) and \(\sigma^i \neq 1_L\) for \(0 < i < n\). Indeed, otherwise all elements...
of $\mathbb{F}_{p^n}$ would be roots of the polynomial $x^{p^i} - x$. But this is impossible since $\mathbb{F}_{p^n}$ has $p^n$ elements. Therefore $\text{Aut}(\mathbb{F}_{p^n}/\mathbb{Z}_p)$ consists just of the powers $\sigma, \sigma^2, \ldots, \sigma^n = 1_L$. □

**Theorem 3.15.** Every set of distinct automorphisms $\sigma_1, \ldots, \sigma_n$ of a field $L$ is independent, i.e. if $a_1, \ldots, a_n \in L$ and $a_1\sigma_1(x) + \cdots + a_n\sigma_n(x) = 0$ for all $x \in L$ then $a_1 = \cdots = a_n = 0$.

**Proof.** Induction on $n$.

The case $n = 1$ is clear: for $x = 1$ we get $a_1\sigma_1(1) = a_1 = 0$.

Concerning $n - 1 \rightarrow n$:

Assume that

$$a_1\sigma_1(x) + a_2\sigma_2(x) + \cdots + a_n\sigma_n(x) = 0 \ \forall x \in L.$$  \hfill (*)

For every $b \in L$ we have $a_1\sigma_1(bx) + a_2\sigma_2(bx) + \cdots + a_n\sigma_n(bx) = 0 \ \forall x \in L$ or

$$a_1\sigma_1(b)\sigma_1(x) + a_2\sigma_2(b)\sigma_2(x) + \cdots + a_n\sigma_n(b)\sigma_n(x) = 0 \ \forall x \in L.$$  

By multiplication of (*) by $\sigma_1(b)$ we get

$$a_1\sigma_1(b)\sigma_1(x) + a_2\sigma_1(b)\sigma_2(x) + \cdots + a_n\sigma_1(b)\sigma_n(x) = 0 \ \forall x \in L$$

and thus

$$a_2(\sigma_2(b) - \sigma_1(b))\sigma_2(x) + \cdots + a_n(\sigma_n(b) - \sigma_1(b))\sigma_n(x) = 0 \ \forall x \in L.$$  

If we choose $b \in L$ such that $\sigma_n(b) \neq \sigma_1(b)$ the inductive assumption yields $a_n = 0$. We insert this in (*) and applying again the inductive assumption we see that $a_1 = \cdots = a_{n-1} = 0$. □

**Theorem 3.16.** Let $\sigma_1, \ldots, \sigma_n$ be distinct automorphisms of $L$ and let $K$ be a subfield of $\mathcal{F}(\{\sigma_1, \ldots, \sigma_n\})$. Then: $[L : K] \geq n$.

**Proof.** By way of contradiction assume $[L : K] = r < n$. Let $\omega_1, \ldots, \omega_r$ be a basis for $L$ viewed as a vector space over $K$. The system of homogeneous linear equations

$$x_1\sigma_1(\omega_1) + \cdots + x_n\sigma_n(\omega_1) = 0$$  \hfill (**)

$$x_1\sigma_1(\omega_r) + \cdots + x_n\sigma_n(\omega_r) = 0$$

has a proper solution (i.e. not all the $x_i$’s are 0) since $r < n$ (a well-known theorem from linear algebra\(^1\)). Any element $\beta \in L$ can be written $\beta = a_1\omega_1 + \cdots + a_r\omega_r$, where $a_1, \ldots, a_r \in K$. Because of (**) we have

$$x_1\sigma_1(\beta) + \cdots + x_n\sigma_n(\beta) = 0.$$  

This gives us the desired contradiction in view of Theorem 3.15. □

\(^1\)A system of homogeneous linear equations has a proper solution if the number of unknowns is bigger than the number of equations.
**Theorem 3.17.** Let $G$ be a group of automorphisms of $L$. Then $[L : F(G)] = |G|$ (in the sense that if one of the sides is finite so is the other and in that case the cardinalities coincide).

**Proof.** In view of the preceding theorem it is enough to consider the case where $G$ is finite. Assume $G$ has order $n < \infty$. Again by the preceding theorem it is enough to show that $[L : F(G)] \leq n$. To prove this we must show that any $(n+1)$ elements of $L$ are linearly dependent over $F(G)$.

For this we need two lemmas

**Lemma 3.18.** For every $x \in L$ “the trace” $S(x) := \sum_{\sigma \in G} \sigma(x)$ is an element in $F(G)$.

**Proof.** For every $\sigma' \in G$ we get $\sigma'(S(x)) = \sum_{\sigma \in G} \sigma'\sigma(x) = \sum_{\sigma \in G} \sigma(x) = S(x)$. $\square$

**Lemma 3.19.** There exists an element $x \in L$ for which $S(x) \neq 0$.

**Proof.** Apply Theorem 3.15 about the independence of distinct automorphisms. $\square$

We now return to the proof of theorem 3.17. Let $G = \{\sigma_1, \ldots, \sigma_n\}$.

We must show that any $n+1$ elements $\omega_1, \ldots, \omega_{n+1}$ of $L$ are linearly dependent over $K$.

The system of homogeneous linear equations

\[
\begin{align*}
 x_1\sigma_1^{-1}(\omega_1) + \cdots + x_{n+1}\sigma_1^{-1}(\omega_{n+1}) &= 0 \\
 \vdots & \\
 x_1\sigma_n^{-1}(\omega_1) + \cdots + x_{n+1}\sigma_n^{-1}(\omega_{n+1}) &= 0
\end{align*}
\]

has a proper (i.e. non-zero) solution $(x_1, \ldots, x_{n+1})$ in $L$. We may assume that $x_1 \neq 0$ and by multiplication by a suitable element in $L$ we can (because of Lemma 3.19) obtain that $S(x_1) \neq 0$.

By applying the automorphisms $\sigma_1, \ldots, \sigma_n$ on the above system of equations and taking sums we get

\[
S(x_1)\omega_1 + \cdots + S(x_{n+1})\omega_{n+1} = 0
\]

in other words: $\omega_1, \ldots, \omega_{n+1}$ are linearly dependent over $F(G)$. $\square$

**Remark 3.20.** If $G$ is infinite then $[L : F(G)]$ is also infinite, but in general the cardinality of $G$ is bigger than that of $[L : F(G)]$. For instance let $\overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$ and let $G$ be Aut($\overline{\mathbb{Q}}/\mathbb{Q}$). It can be proved that $G$ is uncountable (actually has the cardinality $2^{\aleph_0}$) while $[\overline{\mathbb{Q}} : \mathbb{Q}] = \aleph_0$. 
Corollary 3.21. If $G$ is a finite group of automorphisms of $L$ then: $\text{Aut}(L/\mathcal{F}(G)) = G$.

Proof. It is clear that $\text{Aut}(L/\mathcal{F}(G)) \supseteq G$.

Let us now prove the inverse inclusion. Let $G$ be a finite group of order $n$ consisting of the elements $\sigma_1, \ldots, \sigma_n$. Then $[L : \mathcal{F}(G)] = n$. If there were some automorphism $\sigma'$ of $L$, $\sigma'$ not lying in $G$, but fixing $\mathcal{F}(G)$ then $\mathcal{F}(G)$ would be equal to $\mathcal{F}(\sigma', \sigma_1, \ldots \sigma_n)$. But this would contradict Theorem 3.16 since $[L : \mathcal{F}(G)] = n$. □

Corollary 3.22. Distinct finite automorphism groups of $L$ have distinct fixed fields.

Proof. Let $G_1$ and $G_2$ be two finite automorphism groups of $L$. If $\mathcal{F}(G_1) = \mathcal{F}(G_2)$ the above corollary implies that $G_1 = \text{Aut}(L/\mathcal{F}(G_1)) = \text{Aut}(L/\mathcal{F}(G_2)) = G_2$. □

We recall the notion "finite normal extension". $L/K$ is a finite normal extension if $[L : K] < \infty$ and $K = \mathcal{F}($Aut$(L/K))$. Aut$(L/K)$ is called the Galois group for $L/K$ and is denoted Gal$(L/K)$. In principle we could denote the Galois group of a normal extension $L/K$ by Aut$(L/K)$. But it is customary to use the notation Gal$(L/K)$ for a normal extension.

In view of Theorem 3.17 the order of the Galois group Gal$(L/K)$ equals the dimension $[L : K]$.

Furthermore we note that a finite extension $L/K$ is normal $\iff K$ = fixed field for a group of automorphisms of $L$.

Remark 3.23. From the above we can also conclude the following. Let $L/K$ be a finite extension. Then $|\text{Aut}(L/K)| \leq [L : K]$ and $|\text{Aut}(L/K)| = [L : K]$ if and only if $L/K$ is normal.

Example 3.24. $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is normal while $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is not normal. (Cf. Examples 3.6 and 3.7).

Example 3.25. $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ is normal. Indeed $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is the splitting field of the separable polynomial $(x^2 - 2)(x^2 - 3)$, so we can apply Theorem 3.12. Since $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ the Galois group Gal$(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ has order 4. There are two groups of order 4: Kleins 4-group and the cyclic group of order 4. To determine which of these groups is isomorphic to the Galois group we note that an automorphism in Gal$(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ is uniquely determined by its values on $\sqrt{2}$ and $\sqrt{3}$. Since $\sqrt{2}$ is a root of $x^2 - 2$ and $\sqrt{3}$ is a root of $x^2 - 3$. Lemma 3.4 implies that an automorphism must send $\sqrt{2}$ into $\sqrt{2}$ or $-\sqrt{2}$ and $\sqrt{3}$ into $\sqrt{3}$ or $-\sqrt{3}$. Thus there are at most 4 possibilities. Since the Galois group has order 4 each of these possibilities can be realized as an automorphism in exactly one way. They can be listed in this way: the identity which fixes both $\sqrt{2}$ and $\sqrt{3}$, an automorphism $\sigma_1$ which fixes $\sqrt{2}$ and sends $\sqrt{3}$ to $-\sqrt{3}$, an automorphism $\sigma_2$ which fixes $\sqrt{3}$ and sends $\sqrt{2}$ to $-\sqrt{2}$ and an automorphism $\sigma_3$ which sends $\sqrt{2}$ to $-\sqrt{2}$ and $\sqrt{3}$ to $-\sqrt{3}$. It is easily checked that $\sigma_1^2 = \sigma_2^2 = \sigma_3^2 = \text{the identity}$. Hence the Galois group is isomorphic to Kleins 4-group.
We now give an extremely important characterization of the finite normal extensions.

**Theorem 3.26.** Let $L/K$ be a finite extension. Then $L/K$ is normal $\iff L =$ splitting field for a separable polynomial $f(x)$ over $K$.

**Proof.** “$\Longrightarrow$” has already been proved in Theorem 3.12.

“$\iff$” here we need the following which is very important in its own right.

**Theorem 3.27.** Let $L/K$ be a finite normal extension. If an irreducible polynomial $p(x)$ in $K[x]$ has some root $\alpha \in L$, then all roots of $p(x)$ lie in $L$ and all of them are simple, and they are just the distinct elements among $\{\sigma(\alpha) \mid \sigma \in \text{Aut}(L/K)\}$. In particular $p(x)$ is separable.

**Proof.** W.l.o.g we may assume that $p(x)$ is monic, hence $p(x) = \text{Irr}(\alpha, K)$. Let $\sigma_1(\alpha), \ldots, \sigma_j(\alpha)$ be the distinct elements in the set $\{\sigma(\alpha) \mid \sigma \in \text{Aut}(L/K)\}$. For every automorphism $\tau \in \text{Aut}(L/K)$ we have $\{\tau \sigma_1(\alpha), \ldots, \tau \sigma_j(\alpha)\} = \{\sigma_1(\alpha), \ldots, \sigma_j(\alpha)\}$.

Let $\hat{\tau}$ be automorphism of $L[x]$ induced by $\tau$. ($\hat{\tau}$ (a polynomial in $L[x]$) = the polynomial obtained by replacing the coefficients by their images under $\tau$). For the polynomial $f(x) := [x - \sigma_1(\alpha)] \cdots [x - \sigma_j(\alpha)]$ we get

$$
\hat{\tau}f(x) = [x - \tau \sigma_1(\alpha)] \cdots [x - \tau \sigma_j(\alpha)] = f(x).
$$

This holds for all $\tau \in \text{Gal}(L/K)$, hence $f(x)$ has coefficients in $\mathcal{F}(\text{Gal}(L/K)) = K$. $f(x)$ is thus a polynomial in $K[x]$ and $f(\alpha) = 0$ and so $p(x) = \text{Irr}(\alpha, K)|f(x)$.

On the other hand (by Lemma 3.4) $p(\alpha) = 0 \Rightarrow p(\sigma(\alpha)) = 0 \forall \sigma \in \text{Gal}(L/K)$. Consequently each of the elements $\sigma_1(\alpha), \ldots, \sigma_j(\alpha)$ is a root of $p(x)$ and this implies that $f(x) = [x - \sigma_1(\alpha)] \cdots [x - \sigma_j(\alpha)] | p(x)$. But $f(x)$ and $p(x)$ are monic polynomials for which $f(x) \mid p(x)$ og $p(x) \mid f(x)$. This means $f(x) = p(x)$. \hfill $\square$

Now we return to the proof of “$\iff$” in Theorem 3.26.

Theorem 3.27 implies in particular that every finite normal extension is separable. By Abel-Steinitz’s theorem there exists an $\alpha$ in $L$ such that $L = K(\alpha)$. By Theorem 3.27 the polynomial $p(x) = \text{Irr}(\alpha, K)$ splits into linear factors inside $L$, and no proper subfield of $L$ containing $K$ has this property; consequently $L$ is the splitting field for \text{Irr}(\alpha, K) and \text{Irr}(\alpha, K)$ is separable. \hfill $\square$

We give yet another characterization of finite normal extensions.

**Theorem 3.28.** A finite extension $L/K$ is normal if and only if $L/K$ is separable and every irreducible polynomial in $K[x]$ having some root in $L$ has all its roots in $L$.

**Proof.** “only if” has already been proved.

“if”: By Abel-Steinitz’s theorem $L = K(\alpha)$ for a suitable $\alpha \in L$. Therefore $L$ is the splitting field for the separable polynomial $p(x) = \text{Irr}(\alpha, K)$. \hfill $\square$
Remark 3.29. Some authors call a finite extension $L/K$ normal if every irreducible polynomial in $K[x]$ having some root in $L$ has all its roots in $L$, while an extension which is normal in the sense of these notes is called a Galois extension. For perfect fields, in particular for fields of characteristic 0, the two definitions coincide.

**Theorem 3.30.** Assume $M/K$ is a finite normal extension and $L$ is an intermediate extension, i.e. $M \supseteq L \supseteq K$, then $M/L$ is a finite normal extension.

**Proof.** $M/K$ finite normal $\Rightarrow M =$ splitting field for a separable polynomial $f(x)$ over $K \Rightarrow M =$ splitting field for $f(x)$ over $L \Rightarrow M/L$ is a finite normal extension $\Box$

**Example 3.31.** If $M/K$ is a finite normal extension and $L$ is an intermediate field, i.e. $M \supseteq L \supseteq K$, then $L$ may not be a normal extension of $K$. A counterexample can be gotten by taking $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt[3]{2})$ and $M =$ the splitting field for $x^3 - 2$ over $\mathbb{Q}$. By theorem 3.12 $M/\mathbb{Q}$ is normal, while $L/\mathbb{Q}$ (cf. Example 3.24) is not normal.

**THE FUNDAMENTAL THEOREM OF GALOIS THEORY.**

By means of the previous results we are now in a position to prove

**Theorem 3.32.** The Fundamental Theorem of Galois Theory. Let $M/K$ be a finite normal extension with Galois group $G = \text{Gal}(M/K)$. (Here is $[M : K] = |G|$ (cf. Theorem 3.17)). There exists a $(1-1)$ correspondence between the subgroups of $G$ and the intermediate fields of $M/K$ (i.e. subfields of $M$ containing $K$). The $(1-1)$ correspondence is obtained in the following way:

To an intermediate field $L$ we associate $T(L) = \text{Gal}(M/L)$ (which is a subgroup of $G$); to a subgroup $H$ of $G$ we associate the fixed field $F(H)$ ($K \subseteq F(H) \subseteq M$). Then:

1) $F(T(L)) = L$, $T(F(H)) = H$ (this gives the $(1-1)$ correspondence mentioned above)
2) $|T(L)| = [M : L]$; $|L : K| = [G : T(L)]$.
3) $L_1 \subseteq L_2 \Leftrightarrow T(L_1) \supseteq T(L_2)$; $H_1 \subseteq H_2 \Leftrightarrow F(H_1) \supseteq F(H_2)$.
4) For an intermediate field $L$ holds: $L/K$ is normal $\Rightarrow T(L) \triangleleft G$.
5) If $L/K$ is normal [so by 4] $T(L) \triangleleft G$ then $\text{Gal}(L/K) \cong G/T(L)$ and every automorphism of $\text{Gal}(L/K)$ can be extended to an automorphism of $\text{Gal}(M/K)$.

**Proof.**

ad 1) $F(T(L)) = L$ follows from Theorem 3.30 and $T(F(H)) = H$ follows from Corollary 3.21.

ad 2) This follows immediately from Theorem 3.17.

ad 3) The two arrows $\Rightarrow$ from the left to the right are trivial. Let us now consider the inverse implications. Assume $T(L_1) \supseteq T(L_2)$. Applying the (trivial) implication $\Rightarrow$ on this inclusion we get $F(T(L_1)) \subseteq F(T(L_2))$, which by
1) just means that \( L_1 \subseteq L_2 \). The other arrow \( \Leftarrow \) is obtained by a similar argument.

ad 4) For this we need two sublemmas.

**Sublemma 3.33.** An intermediate field \( L \) is normal over \( K \) if and only if \( \sigma L = L \) for all \( \sigma \in G \).

**Proof.** “only if”: It is enough to show that \( \sigma L \subseteq L \) for all \( \sigma \in G \) (why?).

Let \( \alpha \in L \), \( p(x) = \text{Irr}(\alpha, K) \) then \( \sigma(\alpha) \) (cf. Lemma 3.4) is also a root of \( p(x) \) for all \( \sigma \in G \). Theorem 3.27 implies that \( \sigma(\alpha) \) is an element in \( L \) i.e.: \( \sigma(\alpha) \in L \) for all \( \alpha \in L \) and for all \( \sigma \in G \).

“if”: Since \( M/K \) is normal, \( M/K \) is separable, in particular \( L/K \) is separable. By Abel-Steinitz’s theorem \( L = K(\alpha) \) for a suitable \( \alpha \in L \). The roots of \( p(x) = \text{Irr}(\alpha, K) \) are (by Theorem 3.27) exactly the elements \( \sigma(\alpha) \), \( \sigma \in G \).

Since \( \sigma L = L \) all these roots lie in \( L \), which therefore is the splitting field for the separable polynomial \( p(x) \) over \( K \), hence \( L/K \) is normal by Theorem 3.12. \( \square \)

**Sublemma 3.34.** \( T(\sigma L) = \sigma T(L)\sigma^{-1} \) for every intermediate field \( L \) and every automorphism \( \sigma \) in \( G = \text{Gal}(M/K) \).

**Proof.** By the definitions we have

\[
T(\sigma L) = \{ \tau \in G | \tau \sigma \ell = \sigma \ell \ \forall \ell \in L \} = \{ \tau \in G | \sigma^{-1} \tau \sigma \ell = \ell \ \forall \ell \in L \}
\]

\[
= \{ \tau \in G | \sigma^{-1} \tau \sigma \in T(L) \} = \{ \tau | \tau \in \sigma T(L)\sigma^{-1} \} = \sigma T(L)\sigma^{-1}.
\]

We now apply the sublemmas to prove 4). By Sublemma 3.33 we know that \( L/K \) is normal if and only if \( \sigma L = L \) for all \( \sigma \in G \). Since \( T \) is injective the latter equality holds if and only if \( T(\sigma L) = T(L) \) for all \( \sigma \in G \). By Sublemma 3.34 \( T(\sigma L) = \sigma T(L)\sigma^{-1} \). Hence \( T(\sigma L) = T(L) \) for all \( \sigma \in G \) if and only if \( T(L) \) is a normal subgroup of \( G \).

ad 5) Assume that \( L/K \) is normal and thus \( T(L) \triangleleft G \).

We define a mapping \( \varphi : G = \text{Gal}(M/K) \mapsto \text{Gal}(L/K) \) by \( \varphi(\sigma) = \sigma_{\text{Res},L} \). Sublemma 3.34 implies that \( \sigma_{\text{Res},L} \) really is an automorphism for \( L \) (which is the identity on \( K \) i.e.: \( \sigma_{\text{Res},L} \in \text{Gal}(L/K) \)). Therefore \( \varphi \) is a well defined homomorphism from \( G \) into \( \text{Gal}(L/K) \).

For the kernel of this homomorphism we find \( \text{Ker} \varphi = \{ \sigma \in G \mid \sigma_{\text{Res},L} = 1_L \} = \text{Gal}(M/L) = T(L) \). Therefore we get an isomorphism \( G/T(L) \cong \varphi G \subseteq \text{Gal}(L/K) \).

Now by 2) we have \( |G/T(L)| = [L : K] \).

Theorem 3.17 says that \( |\text{Gal}(L/K)| = [L : K] \); therefore \( \varphi G \) is a subgroup of \( \text{Gal}(L/K) \) having the same order as \( \text{Gal}(L/K) \). Consequently \( \varphi G = \text{Gal}(L/K) \). \( \square \)

**Exercise 3.35.** Let \( M/L \) and \( L/K \) be finite normal extensions. Show by an example that \( M/K \) is not necessarily a normal extension. (Consider e.g. \( M = \mathbb{Q}(\sqrt{2}), L = \mathbb{Q}(\sqrt{2}) \) and \( K = \mathbb{Q} \).)

**Exercise 3.36.** Let \( M/L \) and \( L/K \) be finite normal extensions and assume furthermore that every automorphism in \( \text{Gal}(L/K) \) can be extended to an automorphism
of $M$. Prove that this implies that $M/K$ is a normal extension. (Compare this with 5) in the fundamental theorem of Galois theory.)

**Exercise 3.37.** Let $M/\mathbb{Q}$ be a finite normal extension. Show that complex conjugation induces an automorphism in $\text{Gal}(M/\mathbb{Q})$ (which is the identity if $M$ is contained in the field of real numbers; otherwise it is an automorphism of order 2). (Hint: use e.g. Theorem 3.27.)

---

**Theorem 3.38. Supplement to the Fundamental Theorem of Galois Theory.** Let $M/K$ be a finite normal extension. For two intermediate fields $L_1, L_2$ there exists a smallest field (“the compositum”) containing $L_1$ and $L_2$, denoted $\{L_1, L_2\}$ or just $L_1L_2$. Correspondingly for two subgroups $H_1, H_2$ of a given group there is a smallest group, (“the compositum”), denoted $\{H_1, H_2\}$ containing $H_1$ and $H_2$. With the notations from the fundamental theorem of Galois theory the following holds:

$$
T\{L_1, L_2\} = T(L_1) \cap T(L_2),
T(L_1 \cap L_2) = \{T(L_1), T(L_2)\},
\mathcal{F}(H_1 \cap H_2) = \{\mathcal{F}H_1, \mathcal{F}H_2\},
\mathcal{F}\{H_1, H_2\} = \mathcal{F}H_1 \cap \mathcal{F}H_2.
$$

**Proof.** We just check the first one:

$$T(\{L_1, L_2\}) \supseteq T(L_1) \Rightarrow T(L_1) \supseteq T(\{L_1, L_2\}) \quad \Rightarrow T(\{L_1, L_2\}) \subseteq T(L_1) \cap T(L_2)
$$

$$\{L_1, L_2\} \supseteq L_2 \Rightarrow T(L_2) \supseteq T(\{L_1, L_2\})
$$

Furthermore

$$\mathcal{F}(T(L_1) \cap T(L_2)) \supseteq \mathcal{F}(T(L_1)) = L_1 \quad \Rightarrow \mathcal{F}(T(L_1) \cap T(L_2)) \supseteq \{L_1, L_2\}
$$

$$\mathcal{F}(T(L_1) \cap T(L_2)) \supseteq \mathcal{F}(T(L_2)) = L_2
$$

$$\Rightarrow T(L_1) \cap T(L_2) \subseteq T(\{L_1, L_2\}). \quad \square
$$

**Corollary 3.39.** With the notations from above the following holds: $L_1/K$ normal and $L_2/K$ normal $\Rightarrow L_1 \cap L_2/K$ normal and $\{L_1, L_2\}/K$ normal.

---

**WHAT DO GALOIS GROUPS LOOK LIKE?**

We shall now prove a theorem which is quite useful for the explicit computation of the Galois group for a normal extension that is given as the splitting field of a separable polynomial.
**Theorem 3.40.** Let $M$ be the splitting field over a field $K$ for a polynomial $p(x)$ having degree $n$ and no multiple roots. Then there is an isomorphism $\varphi$ from the Galois group $\text{Gal}(M/K)$ onto a subgroup of the symmetric group $S_n$. Hence the following holds: $[M : K] \leq n!$ and even $[M : K] | n!$. If $p(x)$ is irreducible in $K[x]$ then $\varphi \text{Gal}(M/K)$ is a transitive subgroup of $S_n$. Hence: $n \leq [M : K] \leq n!$ and even $n | [M : K] | n!$.

**Proof.** We can write $M = K(\alpha_1, \ldots, \alpha_n)$ where $\alpha_1, \ldots, \alpha_n$ are the distinct roots of $p(x)$. An automorphism $\sigma \in \text{Gal}(M/K)$ is uniquely determined by its values on $\alpha_1, \ldots, \alpha_n$. According to Lemma 3.4 the elements $\sigma(\alpha_i), 1 \leq i \leq n$, are roots of $p(x)$. This means that $\left( \begin{array}{c} \alpha_1, \ldots, \alpha_n \\ \sigma(\alpha_1), \ldots, \sigma(\alpha_n) \end{array} \right)$ is a permutation of the roots $\alpha_1, \ldots, \alpha_n$.

Furthermore the mapping $\text{Gr}(M/K) \xrightarrow{\varphi} S_n$, $\varphi \sigma = \left( \begin{array}{c} \alpha_1, \ldots, \alpha_n \\ \sigma(\alpha_1), \ldots, \sigma(\alpha_n) \end{array} \right)$ is an homomorphism from $\text{Gal}(M/K)$ into $S_n$; since $\sigma$ is uniquely determined by its values on $\alpha_1, \ldots, \alpha_n$ we conclude that $\phi$ is injective. If $p(x)$ is assumed to be irreducible in $K[x]$ Theorem 3.27 implies that $\varphi(\text{Gal}(M/K))$ is a transitive subgroup of $S_n$. The transitivity theorem (Theorem 2.47 in Chap.II) implies $n | [M : K]$, since $M$ contains for instance $K(\alpha_1)$ which has dimension $n$ over $K$.

**Theorem 3.41.** Let $M$ be the splitting field over a field $K$ for a polynomial $p(x)$ having degree $n$ and no multiple roots. Assume moreover that the characteristic of $K$ is $\neq 2$. If $\varphi$ is the isomorphism introduced in Theorem 3.40 the image $\varphi \text{Gal}(M/K)$ is a subgroup of the alternating group $A_n$ if and only if the discriminant $\text{discrim}(p)$ is the square of an element in $K$.

**Proof.** $M = K(\alpha_1, \ldots, \alpha_n)$ where $\alpha_1, \ldots, \alpha_n$ are the distinct roots of $p(x)$. We consider the mapping $\varphi : \text{Gal}(M/K) \rightarrow S_n$ introduced in Theorem 3.40.

Assume $\varphi(\text{Gal}(M/K)) \subseteq A_n$. Then $\Delta(\alpha_1, \ldots, \alpha_n) = \prod_{i>j} (\alpha_i - \alpha_j)$ is invariant under all automorphisms in $\text{Gal}(M/K)$; therefore $\Delta(\alpha_1, \ldots, \alpha_n) \in K$. Hence $\text{discrim}(p) = (\Delta(\alpha_1, \ldots, \alpha_n))^2$ is the square of an element in $K$.

Next assume that $\varphi \text{Gal}(M/K) \not\subseteq A_n$. Then there is an automorphism $\sigma \in \text{Gal}(M/K)$ such that $\sigma \Delta(\alpha_1, \ldots, \alpha_n) = -\Delta(\alpha_1, \ldots, \alpha_n)$. Since the characteristic of $K$ is $\neq 2$ the element $\Delta(\alpha_1, \ldots, \alpha_n)$ cannot lie in $K$; thus $\text{discrim}(p)$ is not the square of an element in $K$.

**Example 3.42.** Let $M$ be the splitting field for $x^3 - 2$ over $\mathbb{Q}$. $x^3 - 2$ is irreducible (by Eisenstein’s criterion) and separable (all polynomials over $\mathbb{Q}$ are separable). By theorem 12 the Galois group $\text{Gal}(M/\mathbb{Q})$ is (isomorphic to) a transitive subgroup of $S_3$. Since $M = \mathbb{Q}(\sqrt[3]{2}, \varepsilon)$ where $\varepsilon$ is the 3rd root of unity $e^{\frac{2\pi i}{3}} = \frac{-1 + \sqrt{3}i}{2}$ and $\varepsilon$ is a root of the polynomial $x^2 + x + 1$, it is an easy consequence of the transitivity theorem that the dimension $[M : \mathbb{Q}] = 6$. Therefore $\text{Gal}(M/\mathbb{Q}) \simeq S_3$. It is an instructive exercise to write down all subgroups of $\text{Gal}(M/\mathbb{Q}) \simeq S_3$ and the corresponding fixed
By the fundamental theorem of Galois theory one then gets a diagram of all subfields of $M$.

**Exercise 3.43.** Show that every normal extension $M/Q$ with $S_3$ as Galois group can be obtained as the splitting field over $Q$ for an irreducible cubic polynomial $f(x)$ in $Q[x]$. Let $L$ be the fixed field of a transposition in $S_3$. Notice that $[L:Q]=3$; by Abel-Steinitz’s theorem there is an $\alpha \in L$ so that $L=Q(\alpha)$. As $f(x)$ one can use $\text{Irr}(\alpha, Q)$.

**Example 3.44.** Let $M$ be the splitting field for $x^4-2$ over $Q$. Here $M=Q(\sqrt[4]{2}, i)$ which implies that $[M:Q]=8$. We want to find $\text{Gal}(M/Q)$. First notice that without any computation we can predict that it must be the dihedral group $D_4$ of order 8. Indeed, by Theorem 3.40 $\text{Gal}(M/Q)$ is a subgroup of $S_4$ of order 8. But by Sylow’s theorems any subgroup of $S_4$ of order 8 is (isomorphic to) $D_4$.

We now study what the automorphisms in the Galois group look like, i.e. how the automorphisms act explicitly on the numbers in $M$.

An automorphism in $\text{Gal}(M/Q)$ is uniquely determined by its values on $\sqrt[4]{2}$ and $i$. For the values on $\sqrt[4]{2}$ there are (cf. Lemma 3.4) the following possibilities $\sqrt[4]{2}$, $-\sqrt[4]{2}$, $i\sqrt[4]{2}$, $-i\sqrt[4]{2}$. For the values on $i$ there are the possibilities $+i$ and $-i$. Since $\text{Gal}(M/Q)$ has order 8 any one of the above 8 combinations can be realized by exactly one automorphism in $\text{Gal}(M/Q)$. The Galois group consists of the following automorphisms:

$$
\sigma, \sigma^2, \sigma^3, \sigma^4 = e, \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3,
$$

where

$$
\begin{align*}
\sigma(\sqrt[4]{2}) &= \sqrt[4]{2}i, \\
\sigma^2(\sqrt[4]{2}) &= -\sqrt[4]{2}; \\
\sigma^3(\sqrt[4]{2}) &= -i\sqrt[4]{2}; \\
\sigma^4(\sqrt[4]{2}) &= \sqrt[4]{2} \\
\sigma(i) &= i; \\
\sigma^2(i) &= -i; \\
\sigma^3(i) &= i; \\
\sigma^4(i) &= i \\
\tau(\sqrt[4]{2}) &= \sqrt[4]{2}, \\
\tau\sigma(\sqrt[4]{2}) &= -i\sqrt[4]{2}; \\
\tau\sigma^2(\sqrt[4]{2}) &= -\sqrt[4]{2}; \\
\tau\sigma^3(\sqrt[4]{2}) &= i\sqrt[4]{2} \\
\tau(i) &= -i; \\
\tau\sigma(i) &= -i; \\
\tau\sigma^2(i) &= -i; \\
\tau\sigma^3(i) &= -i.
\end{align*}
$$

Here we have $\tau^2 = e, \sigma\tau = \tau\sigma^{-1}$.

By direct computation one finds all subgroups of $\text{Gal}(M/Q)$:

$\{e\}$

$\{e, \tau\sigma\}$

$\{e, \tau\sigma^3\}$

$\{e, \tau\}$

$\{e, \tau\sigma^2\}$

$\{e, \sigma^2\}$

$\{e, \sigma^2, \tau\sigma\}$

$\{e, \sigma^2, \tau\sigma^3\}$

$\{e, \sigma, \sigma^2, \sigma^3\}$

$\{e, \sigma^2, \tau, \tau\sigma^2\}$

$\text{Gal}(M/K)$
From the fundamental theorem of Galois theory we then know that the mutual positions of the subfields of $M$ are as in the above diagram. Explicit computations show that the subfields are:

$$Q(\sqrt{2}(1 - i)) \quad Q(\sqrt{2}(1 + i)) \quad Q(\sqrt{2}, i)$$

Let us for instance check that the fixed field of $\{e, \sigma, \sigma^2, \sigma^3\}$ is $Q(i)$. It is clear that $Q(i) \subseteq F(\{e, \sigma, \sigma^2, \sigma^3\})$ From 2) in the fundamental theorem of Galois theory we know that the dimension of $F(\{e, \sigma, \sigma^2, \sigma^3\})$ over $Q$ is 2. The dimension $[Q(i) : Q]$ is also 2. Therefore the fixed field must be exactly $Q(i)$. The determination of the other fixed fields can be done similarly. The hardest ones are the fixed fields of $\{e, \tau \sigma\}$ and $\{e, \tau \sigma^3\}$. It is clear that $L := Q(\sqrt{2}(1 - i)) \subseteq F(\{e, \tau \sigma\})$. To show equality it suffices to verify that the dimension of $M$ over $L$ is $\leq 2$. For this one should just observe that $M = L(i)$.

An analogous argument shows that the fixed field of $\{e, \tau \sigma^3\}$ is $Q(\sqrt{2}(1 + i))$.

Which subfields of $M$ are normal over $Q$?

How can the commutator subgroup of $\text{Gal}(M/Q)$ be interpreted in terms of Galois theory?

**Exercise 3.45**. Let $f(x)$ be an irreducible polynomial in $Q[x]$ of degree $n$. Assume that the number $r$ of real roots of $f(x)$ satisfies $0 < r < n$. Let $M$ be the splitting field for $f(x)$ over $Q$ (viewed as a subfield of the complex number field $C$). Show that $L = M \cap \mathbb{R}$ is a non-normal extension of $Q$ and that $[L : Q] \geq n$.

1) Show that $[M : Q] \geq 2n$.

Now let $f(x)$ be $x^4 - 2x^3 - 2x + 1$.

2) Show that $f(x) = x^4 - 2x^3 - 2x + 1$ is irreducible over $Q$ (consider $f(x + 1)$).

3) Show that $f(x)$ has exactly 2 real roots.

4) Let $M$ be the splitting field for $f(x)$ over $Q$. Find $[M : Q]$ and $\text{Gal}(M/Q)$.

(Hint: Observe that a number $\alpha$ is a root of $f(x)$ if and only if $1/\alpha$ is a root of $f(x)$. Hence the roots of $f(x)$ have the form $\alpha, 1/\alpha, \beta, 1/\beta$ for suitable numbers $\alpha$ and $\beta$.)
THE TRANSLATION THEOREM AND APPLICATIONS.

Theorem 3.46. Translation Theorem. Let $M$ and $L$ be extension fields of a field $K$, both of them being contained in a common extension field of $K$. Assume $M/K$ is a finite normal extension while $L$ is an arbitrary extension of $K$. Then the compositum $ML$ is a normal extension of $L$ and $\text{Gal}(ML/L) \cong \text{Gal}(M/M \cap L)$. In particular $[ML:L] = [M : M \cap L]$.

Furthermore, by associating $N \rightarrow NL$, $(M \cap L \subseteq N \subseteq M)$ and $\Lambda \rightarrow \Lambda \cap M$, $(L \subseteq \Lambda \subseteq ML)$ we get a $(1-1)$ correspondence between the fields $N$ between $M \cap L$ and $M$ and between the fields $\Lambda$ between $L$ and $ML$. The correspondence is established by the following

$$NL \cap M = N \text{ and } (\Lambda \cap M)L = \Lambda.$$ 

Proof. Since $M/K$ is finite normal, $M = K(\alpha)$ for a suitable $\alpha \in M$, and $p(x) = \text{Irr}(\alpha, K)$ is separable. $ML = L(\alpha)$ is splitting field for $p(x)$ over $L$; hence $ML/L$ is a finite normal extension.

The mutual positions of the fields can be illustrated this way:

```
M ----------------- ML
|                   |
|                   |
M \cap L -------- L
|                   |
K
```

If $\sigma$ is an automorphism in $\text{Gal}(ML/L)$ the restriction $\sigma_{\text{Res},M}$ will be an automorphism in $\text{Gal}(M/K)$ since $\sigma M \subseteq M$ (use e.g. Theorem 3.27). The mapping $\varphi : \text{Gal}(ML/L) \mapsto \text{Gal}(M/K)$ defined by $\varphi \sigma = \sigma_{\text{Res},M}$ is a homomorphism. Since $\sigma$ is uniquely determined by its value on $\alpha$, the mapping $\varphi$ is injective.

$\varphi \text{Gal}(ML/L)$ is a subgroup of $\text{Gal}(M/K)$ and is therefore by the fundamental theorem of Galois theory determined by $\mathcal{F}(\varphi \text{Gal}(ML/L))$. According to the definitions we get

$$\mathcal{F}(\varphi \text{Gal}(ML/L)) = \{m \in M | \sigma(m) = m \land \sigma \in \text{Gal}(ML/L)\} = \{m \in M | m \in \mathcal{F}(\text{Gal}(ML/L) = L) = M \cap L \}.$$ 

Therefore we get $\varphi \text{Gal}(ML/L) = \text{Gal}(M/M \cap L)$. The injectivity of $\varphi$ yields the isomorphism mentioned in the translation theorem and in particular that $[ML:L] = [M : M \cap L]$.

To prove the second half of the translation theorem we have to show

1) $NL \cap M = N$ 
2) $(\Lambda \cap M)L = \Lambda$. 
ad 1)

\[ M \rightarrow\rightarrow\rightarrow ML \]
\[ N \rightarrow\rightarrow NL \]
\[ M \cap L \rightarrow L \]
\[ \rightarrow\rightarrow K \]

It is clear that \( NL \cap M \supseteq N \). Now \( M/N \) is normal, and since \( ML = M(NL) \) the first half of the translation theorem yields: \([ML : NL] = [M : NL \cap M]\). Since \([M : M \cap L] = [ML : L]\) we get: \([NL \cap M : M \cap L] = [NL : L]\).

Let \( N = (M \cap L)(\beta) \) for a suitable \( \beta \) in \( N \); then: \([N : M \cap L] = \text{degree}(\text{Irr}(\beta, M \cap L)) \geq \text{degree}(\text{Irr}(\beta, L)) = [L(\beta) : L] = [NL : L]\). From this we conclude: \([N : M \cap L] \geq [NL \cap M : M \cap L]\). This taken together with \( NL \cap M \supseteq N \) gives us \([N : M \cap L] = [NL \cap M : M \cap L]\) and thus \( NL \cap M = N \).

ad 2)

\[ M \rightarrow\rightarrow\rightarrow ML \]
\[ M \cap \Lambda \rightarrow\rightarrow\rightarrow\rightarrow\rightarrow\rightarrow\rightarrow\Lambda \]
\[ \rightarrow\rightarrow (M \cap \Lambda)L \]
\[ M \cap L \rightarrow L \]
\[ \rightarrow\rightarrow K \]

It is clear that \( \Lambda \supseteq (M \cap \Lambda)L \). From the proof of 1) follows (with \( N = M \cap \Lambda \)) that \([ (M \cap \Lambda)L : L] = [M \cap \Lambda : M \cap L]\). According to the first half of the translation theorem we get

\([M : M \cap \Lambda] = [ML : \Lambda] \text{ og } [M : M \cap L] = [ML : L]\),

and from theorem 2.47 in chap. II (the transitivity theorem) we then get

\([M \cap \Lambda : M \cap L] = [\Lambda : L]\)
Consequently \([ (M \cap \Lambda) L : L] = [\Lambda : L]\). Combining this with \(\Lambda \supseteq (M \cap \Lambda) L\) we conclude \(\Lambda = (M \cap \Lambda) L\).

\[\square\]

**Theorem 3.47.** Theorem about the compositum of finite normal extensions. Let \(L\) and \(M\) be finite normal extensions of a field \(K\) and assume that \(L\) and \(M\) are contained in a common extension field. The compositum \(LM\) is a finite normal extension of \(K\) and the Galois group \(\text{Gal}(LM/K)\) is isomorphic to a subgroup of the direct product \(\text{Gal}(L/K) \times \text{Gal}(M/K)\). There is an isomorphism \(\text{Gal}(LM/K) \simeq \text{Gal}(L/K) \times \text{Gal}(M/K)\) if \(L \cap M = K\).

**Proof.** By Theorem 3.26 there exist separable polynomials \(f(x)\) and \(g(x) \in K[x]\) such that \(L\) (resp. \(M\)) is the splitting field over \(K\) for \(f(x)\) (resp. \(g(x)\)). Let \(\alpha_1, \ldots, \alpha_s\) (resp. \(\beta_1, \ldots, \beta_t\)) be the roots of \(f(x)\) (resp. \(g(x)\)). Then \(LM = K(\alpha_1, \ldots, \alpha_s, \beta_1, \ldots, \beta_t)\) is the splitting field over \(K\) for \(f(x)g(x)\) and thus a finite normal extension of \(K\), (cf. Theorem 3.26). Lemma 3.4 implies that \(\sigma L = L\) and \(\sigma M = M\) for any \(\sigma\) in \(\text{Gal}(LM/K)\). Hence there is a well defined homomorphic mapping \(\text{Gal}(LM/K) \rightarrow \text{Gal}(L/K) \times \text{Gal}(M/K)\) determined by

\[\sigma \in \text{Gal}(LM/K) \mapsto (\sigma_{\text{Res},L}, \sigma_{\text{Res},M}).\]

Since \(\sigma\) is uniquely determined by its values on \(\alpha_1, \ldots, \alpha_s, \beta_1, \ldots, \beta_t\) the above mapping is injective.

If \(L \cap M = K\) we conclude from the Translation theorem that

\[|\text{Gal}(LM/K)| = [LM : K] = [L : K][M : K] = |\text{Gal}(L/K) \times \text{Gal}(M/K)|\]

so the injective mapping

\[\text{Gal}(LM/K) \mapsto \text{Gal}(L/K) \times \text{Gal}(M/K)\]

becomes surjective and thus an isomorphism.

\[\square\]

**Corollary 3.48.** Let \(M_1, \ldots, M_t\) be finite normal extensions of \(K\) and assume that for each \(i = 1, \ldots, t\) the intersection of \(M_i\) and the compositum of the remaining fields \(M_j\), \(1 \leq j, i \neq j\), is \(K\). Then the compositum of the fields \(M_1, \ldots, M_t\) is a normal extension of \(K\) whose Galois group is \(\simeq \text{Gal}(M_1/K) \times \cdots \times \text{Gal}(M_t/K)\).

**Exercise 3.49.** Construct a finite normal extension \(M/\mathbb{Q}\), whose Galois group is \(\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\).

**Example 3.50.** Let \(b\) be a real algebraic number and \(i = \sqrt{-1}\). Applying the translation theorem (with \(K = \mathbb{Q}\), \(M = \mathbb{Q}(i)\) and \(L = \mathbb{Q}(b)\)) we conclude that \([\mathbb{Q}(i, b) : \mathbb{Q}(b)] = [\mathbb{Q}(i) : \mathbb{Q}] = 2\), hence \([\mathbb{Q}(i, b) : \mathbb{Q}] = 2[\mathbb{Q}(b) : \mathbb{Q}]\). To find the relation between \([\mathbb{Q}(ib) : \mathbb{Q}]\) and \([\mathbb{Q}(b) : \mathbb{Q}]\) we have to distinguish between two cases:
i) $i \notin \mathbb{Q}(ib)$

and

ii) $i \in \mathbb{Q}(ib)$.

In the case i) we use the translation theorem ($K = \mathbb{Q}$, $M = \mathbb{Q}(i)$ and $L = \mathbb{Q}(ib)$).

Since $i \notin \mathbb{Q}(ib)$ the intersection $\mathbb{Q}(i) \cap \mathbb{Q}(ib)$ is $\mathbb{Q}$; therefore $[\mathbb{Q}(i,b) : \mathbb{Q}(ib)] = [\mathbb{Q}(i) : \mathbb{Q}] = 2$ and thus $[\mathbb{Q}(i,b) : \mathbb{Q}(i)] = [\mathbb{Q}(ib) : \mathbb{Q}]$. Hence $[\mathbb{Q}(b) : \mathbb{Q}] = [\mathbb{Q}(ib) : \mathbb{Q}]$.

In the case ii) $\mathbb{Q}(i,b) = \mathbb{Q}(ib)$ since $i \in \mathbb{Q}(ib)$. Therefore we get $[\mathbb{Q}(ib) : \mathbb{Q}] = 2[\mathbb{Q}(b) : \mathbb{Q}]$.

**Exercise 3.51.** Let $\alpha$ be a complex number written as $\alpha = a + ib$, where $i = \sqrt{-1}$ and $a$ and $b$ are real numbers. Prove that $\alpha$ is an algebraic number if and only if $a$ and $b$ are algebraic numbers.

Let $n$ be the degree of $\alpha$ over $\mathbb{Q}$.

Show that the degree of $a$ is a most $n(n - 1)/2$ and that the degree of $b$ is at most $n(n - 1)$.

If $i \in \mathbb{Q}(ib)$ then the degree of $b$ is at most $n(n - 1)/2$. 