7. GALOIS GROUPS

§7.1 Galois Groups of Field Extensions

If F, K are fields, a 1-1 and onto function \( \theta : F \rightarrow K \) is an isomorphism if:
\[
(x + y)^0 = x^0 + y^0 \quad \text{and} \quad (xy)^0 = x^0 y^0 \quad \text{for all} \quad x, y \in F.
\]

If there exists an isomorphism from F to K we say that F and K are isomorphic and write \( F \cong K \). Like isomorphic groups and isomorphic vector spaces, isomorphic fields are essentially the same in terms of their algebraic structure.

**Example 1:** Let \( \alpha = \sqrt[3]{2} \) and \( \beta = \sqrt[3]{2} \omega \). These share the same minimum polynomial \( x^3 - 2 \). As vector spaces over \( \mathbb{Q} \) these are isomorphic under the linear transformation
\[
\begin{align*}
(a_0 + a_1 \alpha + a_2 \alpha^2)(b_0 + b_1 \alpha + b_2 \alpha^2) &= a_0 b_0 + (a_0 b_1 + a_1 b_0) \alpha + (a_0 b_2 + a_1 b_1 + a_2 b_0) \alpha^2 + (a_1 b_2 + a_2 b_1) \alpha^3 + a_2 b_2 \alpha^4 \\
&= (a_0 b_0 + 2a_1 b_2 + 2a_2 b_1) + (a_0 b_1 + a_1 b_0 + 2a_2 b_2) \alpha + (a_0 b_2 + a_1 b_1 + a_2 b_0) \alpha^2 \\
&\rightarrow (a_0 b_0 + 2a_1 b_2 + 2a_2 b_1) + (a_0 b_1 + a_1 b_0 + 2a_2 b_2) \beta + (a_0 b_2 + a_1 b_1 + a_2 b_0) \beta^2 \\
&= (a_0 + a_1 \beta + a_2 \beta^2)(b_0 + b_1 \beta + b_2 \beta^2).
\end{align*}
\]
We have shown that \( \mathbb{Q}[\sqrt[3]{2}] \cong \mathbb{Q}[\sqrt[3]{2} \omega] \). The same argument will show that \( \mathbb{Q}[\sqrt[3]{2} \omega^2] \) is also isomorphic to \( \mathbb{Q}[\sqrt[3]{2}] \).

In fact the same argument can show that we get isomorphic fields if we extend a field by two numbers that have the same minimum polynomial.

If two complex numbers have the same minimum polynomial over a number field F we say that they are algebraic conjugates over F. Trivially every number is an algebraic conjugate of itself over any field.

**Example 2:** Complex conjugates are algebraic conjugates over \( \mathbb{R} \). If \( b \neq 0 \) then \( a + bi \) and \( a - bi \) have the same minimum polynomial over \( \mathbb{R} \), namely \( (x - a)^2 + b^2 \). So \( a + bi \) has two algebraic conjugates, namely \( a + bi \) and \( a - bi \).

An isomorphism from a field to itself is called an automorphism. Trivially the identity map is an automorphism, but usually there are others.

**Example 3:** The map \( \lambda : \mathbb{C} \rightarrow \mathbb{C} \) defined by \( z \mapsto \bar{z} \) is an automorphism of \( \mathbb{C} \) since
\[
\begin{align*}
u + \bar{v} &= \bar{u} + v \quad \text{and} \quad \bar{uv} &= \bar{u} \bar{v}
\end{align*}
\]
for all complex numbers \( u, v \).
**Theorem 1:** The set of all automorphisms of $F$ forms a group with respect to multiplication of maps: $x^\varphi = (x^\theta)^\varphi$ for all $x \in F$.

**Proof:** If $x, y \in F$ then $(x + y)^\varphi = (x^\theta + y^\theta)^\varphi = (x^\theta)^\varphi + (y^\theta)^\varphi = x^\theta y^\theta$ and $(xy)^\varphi = (x^\theta y^\theta)^\varphi = (x^\theta)^\varphi (y^\theta)^\varphi = x^\theta y^\theta$.

The group of all automorphisms of $F$ is called the **automorphism group** of the field and is denoted by Aut($F$). But instead of focussing on fields themselves, and all their associated automorphisms, we consider field extensions $K:F$ and the subgroup of Aut($K$) consisting of those that fix every element of $F$.

If $F$ is a subfield of $K$ we define the **Galois group** of $K$ over $F$ to be:

$$\{ \varphi \in \text{Aut}(K) \mid x^\varphi = x \text{ for all } x \in F \}.$$  

It is easily seen to be a subgroup of Aut($K$) and it is denoted by $G(K/F)$.

**Example 4:** Find $G(\mathbb{C}/\mathbb{R})$.

**Solution:** The identity map $1$ and the conjugation map $\varphi$ are clearly in $G(\mathbb{C}/\mathbb{R})$ since they fix every real number. We now show that $G(\mathbb{C}/\mathbb{R}) = \{1, \varphi\}$, that is that every automorphism of $\mathbb{C}$ which fixes $\mathbb{R}$ is either $1$ or $\varphi$.

Now $i^2 = -1$ so $(i^2)^\varphi = (-1)^\varphi = -1$. Thus $i^\varphi = \pm i$.

If $i^\varphi = i$ then for any complex number $(a + bi)^\varphi = a^\varphi + b^\varphi i^\varphi = a + bi$ and so $\varphi$ is the identity automorphism. On the other hand if $i^\varphi = -i$ then for any complex number $(a + bi)^\varphi = a^\varphi + b^\varphi (-i) = a - bi$ and so $\varphi = \lambda$.

This is an example of a general principle that numbers can only be mapped to those that share the same minimum polynomial.

**Theorem 2:** If $\theta \in G(K/F)$ and $\alpha \in K$ is algebraic over $F$ then $\alpha^\varphi$ is an algebraic conjugate of $\alpha$ over $F$.

**Proof:** Suppose the minimum polynomial of $\alpha$ over $F$ is $p(x)$.

Then $0 = 0^\varphi = p(\alpha^\varphi) = p(\alpha)^\varphi$.

**Corollary 1:** If $f(x) \in F[x]$ and $\theta \in G(F[\alpha(x) = 0]/F)$ then $\theta$ permutes the zeros of $f(x)$.

**Example 5:** Although $|\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}| = 3$, $G(\mathbb{Q}[\sqrt[3]{2}] / \mathbb{Q}) = 1$.

Note that $\mathbb{Q}[\sqrt[3]{2}] \leq \mathbb{R}$. Now $\sqrt[3]{2}$ has to be mapped to one of the cube roots of 2, but $\sqrt[3]{2}$ itself is the only one that lies within $\mathbb{Q}[\sqrt[3]{2}]$.

**Theorem 3:** If $f(x) \in F[x]$ then $G(F[\alpha(x) = 0]/F)$ is isomorphic to a subgroup of $S_n$.

**Proof:** The map that takes an element of $G(F[\alpha(x) = 0]/F)$ to the corresponding permutation on the zeros is a homomorphism. Its kernel is 1 since an automorphism that fixes all the zeros of $f(x)$ must fix every element of $F[\alpha(x) = 0]$.

**Example 6:** $|G(\mathbb{Q}[x^4 = 2]/\mathbb{Q})| \cong D_8$ which is isomorphic to a subgroup of $S_4$ of order 8.

The zeros of $x^4 - 2$ are $\pm \sqrt[4]{2}$, $\pm i \sqrt[4]{2}$. Let $\alpha_1 = \sqrt[4]{2}$, $\alpha_2 = -\sqrt[4]{2}$, $\alpha_3 = i \sqrt[4]{2}$ and $\alpha_4 = -i \sqrt[4]{2}$. The automorphism that maps $\sqrt[4]{2}$ to $i \sqrt[4]{2}$ and fixes $i$ corresponds to the permutation $(1 3 2 4)$. The automorphism that fixes $\sqrt[4]{2}$ and maps $i$ to $-i$ corresponds to the permutation $(3 4)$.
§7.2. The Heart of Galois Theory

We now come to the central idea of Galois Theory. If we have a sequence of field extensions \( F \leq H \leq K \) we have three Galois groups: \( G(K/F), G(K/H) \) and \( G(H/F) \). There is a strong connection between these three, provided the larger two fields are polynomial extensions of the smallest.

**Theorem 3:** If \( F \leq H \leq K \) and if \( H, K \) are polynomial extensions of \( F \) then \( G(H/F) \cong G(K/F)/G(K/H) \).

**Outline of the Proof:** There are a couple of technical difficulties which we will postpone so as to focus on the central idea – the concept of restricting automorphisms.

Suppose \( \theta \in G(K/F) \). Consider \( \theta|_H \), the restriction of \( \theta \) to \( H \). The domain of \( \theta|_H \) is \( H \), but on these elements the effect is the same as for \( \theta \). So \( \theta|_H \) is also an isomorphism. But is it an automorphism of \( H \)? For that to happen we would need \( H^\theta = H \). Let us ASSUME that \( H^\theta = H \). In other words we are assuming that every automorphism in \( G(K/F) \) can be restricted to an automorphism of \( H \). (Assumption 1)

So now \( \theta|_H \) is an automorphism of \( H \) and since it fixes the elements of \( F \) it is in \( G(H/F) \). Let the restriction map be denoted by \( \rho \), that is \( \theta \rho = \theta|_H \). The function \( \rho \) is a function from \( G(K/F) \) to \( G(H/F) \).

It is easy to check that \( \rho \) is a homomorphism. Suppose \( \theta, \varphi \in G(K/F) \).

\[
\rho(\theta \varphi) = \theta(\varphi|_H) = \theta(\varphi_\theta)
\]

because this is how \( \rho \) is defined

\[
= \varphi^\theta \theta
\]

because restrictions give the same values

\[
= (h^{\theta \varphi})^\theta \theta
\]

by the way products are defined

\[
= (h^{\theta \varphi})^{\theta \varphi}
\]

because restrictions give the same values

\[
= (h^\theta)^\varphi \theta
\]

because this is how \( \rho \) is defined

\[
= h^\theta \varphi \theta
\]

by the way products are defined

Hence \( \rho(\theta \varphi) = \theta(\varphi^\theta) \).

Now \( \ker \rho \) consists of those elements of \( G(K/F) \) that become the identity map when we restrict to \( H \), that is they are precisely the elements of \( G(K/H) \).

So \( \ker \rho = G(K/H) \). By the First Isomorphism Theorem for groups we conclude that \( G(K/H) \) is a normal subgroup of \( G(K/F) \) and \( G(K/F)/G(K/H) \cong \text{im} \rho \).

Now \( \text{im} \rho \) is the subgroup of \( G(H/F) \) consisting of those automorphisms that are the restriction of some element of \( G(K/F) \). In other words they are those automorphisms of \( H \) that can be extended to an automorphism in \( G(K/F) \). Let us ASSUME that they can all be so extended. In other words we will assume that \( \rho \) is onto, or in other words, \( \text{im} \rho = G(H/F) \). (Assumption 2)

Subject to these assumptions we have now completed the proof.

These assumptions are:
(1) Every element of \( G(K/F) \) can be restricted to an element of \( G(H/F) \).
(2) Every element of \( G(H/F) \) can be extended to an element of \( G(K/F) \).

These can be proved using the assumption that both \( H \) and \( K \) are polynomial extensions of \( F \).

**ASSUMPTION 1**

**Theorem 4:** Suppose \( F \leq H \leq K \) where \( H \) is a polynomial extension of \( F \).

Then \( H^\theta = H \) for all \( \theta \in G(K/F) \).

**Proof:** Suppose \( H = F[f(x) = 0] = F[\alpha_1, ..., \alpha_n] \) where the \( \alpha_i \) are the zeros of \( f(x) \).
Then \( F = F^0 \leq H^0 \) and each \( \alpha_i^0 \in H^0 \) so \( F[\alpha_1^0, \ldots, \alpha_n^0] \leq H^0 \).

But \( 0 \) merely permutes the zeros of \( f(x) \) so \( F[\alpha_1^0, \ldots, \alpha_n^0] = F[\alpha_1, \ldots, \alpha_n] \leq H \).

Hence \( H \leq H^0 \). But \( 0 \) is an automorphism and so \( H \) and \( H^0 \) are isomorphic as vector spaces and being finite-dimensional over \( F \) we must have \( H = H^0 \).

If \( f(x) \in F[x] \) and \( \varphi:F \to H \) is an isomorphism we define \( f^\varphi(x) \in H[x] \) to be the polynomial that is obtained by acting on all the coefficients of \( f(x) \) by \( \varphi \).

**Example 7:** Let \( F = \mathbb{Q}[\sqrt{2}] \) and \( H = \mathbb{Q}[\sqrt[3]{2}, \omega] \) and let \( \varphi:F \to H \) be the isomorphism we encountered in example 1, that takes \( \sqrt{2} \) to \( \sqrt[3]{2} \) and \( \omega = \sqrt[3]{4} \omega \).

If \( f(x) = \sqrt{2} x^3 + (1 + \sqrt{2})x + \sqrt{4} \) then \( f^\varphi(x) = \sqrt[3]{2} \omega x^3 + (1 + \sqrt[3]{2} \omega)x + \sqrt[3]{4} \omega^2 \).

It is easy to see that \( \varphi \) extends to an isomorphism between \( F[x] \) and \( H[x] \) and that if \( p(x) \in F[x] \) is prime over \( F \) then \( p^\varphi(x) \) is prime over \( H \).

**ASSUMPTION 2**

**Theorem 5:** Suppose \( \phi:F, H \) are number fields and \( \phi:F \to H \) is an isomorphism.

Suppose that the minimum polynomial of \( \alpha \) over \( F \) is \( p(x) \) and the minimum polynomial of \( \beta \) over \( H \) is \( q(x) \). Then \( \phi \) can be extended to an isomorphism \( \psi:F[\alpha] \to H[\beta] \).

**Proof:** Suppose the minimum polynomial for \( \alpha \) and \( \beta \) is \( p(x) = x^n + \sum_{i=1}^{n-1} p_{n-i} x^{n-i} + \ldots + p_0 \).

Then \( p^\phi(x) = x^n + \sum_{i=1}^{n-1} p_{n-i}^\phi x^{n-i} + \ldots + p_0^\phi \).

As vector spaces both \( F[\alpha] \) and \( H[\beta] \) have dimension \( n \) and the map

\[
\begin{align*}
   a_0 + a_1 \alpha + \ldots + a_{n-1} \alpha^{n-1} &\to a_0^\phi + a_1^\phi \beta + \ldots + a_{n-1}^\phi \beta^{n-1} \\
   (a_0 + b_0) + (a_1 + b_1) \alpha + \ldots + (a_{n-1} + b_{n-1}) \alpha^{n-1} &\to (a_0^\phi + b_0^\phi) + (a_1^\phi + b_1^\phi) \beta + \ldots + (a_{n-1}^\phi + b_{n-1}^\phi) \beta^{n-1} \\
   (a_0^\phi + b_0^\phi) + (a_1^\phi + b_1^\phi) \beta + \ldots + (a_{n-1}^\phi + b_{n-1}^\phi) \beta^{n-1} &\to (a_0^\phi + a_1^\phi \beta + \ldots + a_{n-1}^\phi \beta^{n-1}) + (b_0^\phi + b_1^\phi \beta + \ldots + b_{n-1}^\phi \beta^{n-1}).
\end{align*}
\]

When it comes to multiplication in each of \( \mathbb{Q}[\alpha] \) and \( \mathbb{Q}[\beta] \) we multiply the expressions as if they are polynomials and then, in \( \mathbb{Q}[\alpha] \) replace powers of \( \alpha^n \) by \( -p_{n-1} \alpha^{n-1} - \ldots - p_1 \alpha - p_0 \) while in \( \mathbb{Q}[\beta] \) we replace \( \beta^n \) by the equivalent expression in \( \beta \). Clearly this is the same process, but using \( \alpha \)'s in one case and \( \beta \)'s in the other. So the above linear transformation takes products to products and hence is an isomorphism of fields.

**Example 8:** Find \( G(\mathbb{Q}[x^3 = 2]/\mathbb{Q}) \).

Let \( \alpha = \sqrt[3]{2}, \beta = \sqrt[3]{2} \omega, F = \mathbb{Q}[\sqrt[3]{2}] \) and \( H = \mathbb{Q}[\sqrt[3]{2}, \omega] \) in theorem 5. The identity automorphism of \( Q \) can be extended to an isomorphism \( \theta:Q[\sqrt[3]{2}] \to Q[\sqrt[3]{2}, \omega] \) that takes \( \sqrt[3]{2} \) to \( \sqrt[3]{2} \omega \).

The minimum polynomial of \( \omega \) over \( \mathbb{Q}[\sqrt[3]{2}] \) is \( p(x) = x^2 + x + 1 \). This is the same as its minimum poly over \( 
\]
field. But to do so would mean that it would have linear factors and hence zeros in \( \mathbb{Q}[\sqrt[3]{2}] \). But that would mean that \( \omega \in \mathbb{Q}[\sqrt[3]{2}] \) which would make \( \omega \) a real number. You have to be careful with minimum polynomials over larger fields. For example the minimum polynomial of \( \sqrt[3]{2} \) over \( \mathbb{Q} \) is \( x^3 - 2 \), but over \( \mathbb{Q}([\sqrt[3]{2}] \) it is \( x^2 - \sqrt[3]{2} \).

In this case \( p^0(x) = p(x) \). Now take \( \alpha = \omega, \beta = \omega^3, F = \mathbb{Q}[\sqrt[3]{2}], H = \mathbb{Q}([\sqrt[3]{2}] \omega). Then \( \theta \) can be extended to an isomorphism \( \Omega: \mathbb{Q}([\sqrt[3]{2}] [\omega] \to \mathbb{Q}([\sqrt[3]{2} \omega])\omega^2) \) that sends \( \omega \) to \( \omega^3 \).

$$\begin{array}{c}
\Omega \\
\mathbb{Q}[\sqrt[3]{2}] [\omega] \\
\mathbb{Q}[\sqrt[3]{2}] \\
\mathbb{Q} \\
\mathbb{Q}[\sqrt[3]{2}] [\omega^2] \\
\mathbb{Q}[\sqrt[3]{2} \omega] \\
\mathbb{Q}[\sqrt[3]{2} \omega^2] \\
\mathbb{Q} \\
\end{array}$$

But \( \mathbb{Q}([\sqrt[3]{2}] [\omega] = \mathbb{Q}[x^3 - 2] = \mathbb{Q}([\sqrt[3]{2}] [\omega^2]) \) and so we have an automorphism \( \Omega \) of \( \mathbb{Q}[x^3 = 2] \) that sends \( \sqrt[3]{2} \) to \( \sqrt[3]{2} \omega \) and \( \omega \) to \( \omega^3 \).

\( (\sqrt[3]{2})^\omega = (\sqrt[3]{2} \omega)^\omega = (\sqrt[3]{2} \omega)^\omega \omega = (\sqrt[3]{2} \omega)(\omega^2) = \sqrt[3]{2} \) and

\( (\omega)^\omega = (\omega^2)^\omega = (\omega)^\omega \omega^\omega = (\omega^2)(\omega^2) = \omega^4 = \omega. \)

Hence \( \Omega^2 \) is the identity automorphism.

Now we can map \( \sqrt[3]{2} \) to \( \sqrt[3]{2} \), \( \sqrt[3]{2} \omega \) or \( \sqrt[3]{2} \omega^2 \) and \( \omega \) can be sent to \( \omega \) or \( \omega^2 \) and all 6 combinations are possible. Hence \( G(\mathbb{Q}[x^3 = 2] / \mathbb{Q}) \) has order 6. We can describe the 6 automorphisms in a table, where we write down their effect on \( \sqrt[3]{2} \) and \( \omega \).

Remember that since \( \mathbb{Q}[x^3 = 2] = \mathbb{Q}([\sqrt[3]{2}, \omega] \) each automorphism is determined by its effect on these two generators.

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>a</th>
<th>a^2</th>
<th>b</th>
<th>ab</th>
<th>a^2b</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \sqrt[3]{2} )</td>
<td>( \sqrt[3]{2} )</td>
<td>( \sqrt[3]{2} \omega )</td>
<td>( \sqrt[3]{2} \omega^2 )</td>
<td>( \sqrt[3]{2} )</td>
<td>( \sqrt[3]{2} \omega )</td>
<td>( \sqrt[3]{2} \omega^2 )</td>
</tr>
<tr>
<td>( \omega )</td>
<td>( \omega )</td>
<td>( \omega )</td>
<td>( \omega )</td>
<td>( \omega )</td>
<td>( \omega )</td>
<td>( \omega )</td>
</tr>
</tbody>
</table>

We can easily show that \( a^3 = 1, b^2 = 1 \) and \( ba = a^{-1} b \).
Hence \( G(\mathbb{Q}[x^3 = 2] / \mathbb{Q}) = \langle a, b | a^3 = b^2 = 1, ba = a^{-1} b \rangle \) which is the dihedral group of order 6, otherwise known as \( S_3 \).

In general we can extend isomorphisms in this way until we reach a polynomial extension and the isomorphism becomes an automorphism.

**Theorem 6:** Suppose that \( \varphi: H \to K \) is an isomorphism and that \( f(x) \in H[x] \) is non-zero. Then \( \varphi \) may be extended to an isomorphism \( \theta: H[f(x) = 0] \to K[f(x) = 0] \)

**Proof:** We proceed by induction on \( n \), the degree of \( f(x) \).

The theorem is trivial for \( n = 0 \). Suppose that \( n \geq 1 \) and that the theorem holds for polynomials of lower degree. Let \( \alpha \) be one of the zeros of \( f(x) \) and let \( p(x) \) be the minimum polynomial of \( \alpha \) over \( F \). Let \( \beta \) be a zero of the corresponding polynomial \( p^\theta(x) \). By Theorem 5 \( \varphi \) may be extended to \( \sigma: H[\alpha] \to K[\beta] \) such that \( \alpha^\sigma = \beta \).
Now \( f(x) = (x - \alpha)g(x) \) for some \( g(x) \in H[\alpha][x] \) that is, with coefficients in \( H[\alpha] \) and \( f^\theta(x) = (x - \beta)g^\theta(x) \). It follows from the induction hypothesis that \( \sigma \) may be extended further to an isomorphism \( 0: H[\alpha][g(x) = 0] \to K[\beta][g^\theta(x) = 0] \). But \( H[\alpha][g(x) = 0] = H[f(x) = 0] \) and \( K[\beta][g^\theta(x) = 0] = K[f^\theta(x) = 0] \) and so the proof is complete.

**Corollary:** Suppose \( f(x) \in F[x] \) and \( \alpha, \beta \in F[f(x) = 0] \) are algebraic conjugates over \( F \). Then there exists \( 0 \in G(F[f(x) = 0])/F) \) which maps \( \alpha \) to \( \beta \).

**Proof:** By Theorem 5 the identity automorphism on \( F \) can be extended to an isomorphism \( \varphi \) from \( F[\alpha] \) to \( F[\beta] \) that takes \( \alpha \) to \( \beta \). Since \( \varphi \) fixes \( F, f^\varphi(x) = f(x) \).

Take \( H = F[\alpha] \) and \( K = F[\beta] \) in Theorem 6. Then \( \varphi \) can be extended to an isomorphism of \( F[\alpha][f(x) = 0] = F[\beta][f(x) = 0] \), that is, an automorphism of \( F[f(x) = 0] \).

§7.3. Galois Groups of Radical Extensions

There are two special types of radical extension. We can extend a field by the \( n \)th roots of unity. This we shall call a **type 1 radical extension**. Or we can extend a field that already contains the \( n \)th roots of unity by the \( n \)th roots of some other element. We shall call this a **type 2 extension**.

Any radical extension that is not of one or other of these special types can be split into a type 1 extension followed by a type 2 extension: \( F \leq F[x^n = 1] \leq F[x^n = \alpha] \). So we shall concentrate on calculating the Galois groups of each type.

**Theorem 7:** \( G(F[x^n = 1]/F) \) is abelian.

**Proof:** The \( n \)th roots of 1 are 1, \( \omega, \omega^2, \ldots, \omega^{n-1} \) where \( \omega = e^{2\pi i/n} \).

Hence \( F[x^n = 1] = F[\omega] \). Let \( \theta, \varphi \in G(F[\omega]/F) \). Since \( \theta, \varphi \) permute the \( n \)th roots of 1, \( \omega^r = \omega^s \) and \( \omega^r = \omega^s \) for some integers \( r, s \).

Now \( \omega^r = (\omega^r)^s = \omega^{rs} \) while \( \omega^{rs} = \omega^{rs} \). Hence \( 1 = \varphi^{-1} \theta \varphi \) fixes \( \omega \) and the elements of \( F \) and so must be the identity.

**Example 10:** Find \( G = G(\mathbb{Q}[x^7 = 1]/\mathbb{Q}) \).

**Solution:** Let \( \omega = e^{2\pi i/7} \). If \( \theta \in G \) then \( \omega^r = \omega^s \) for some \( r, s \) with \( 0 \leq r < 7 \). But \( r = 0 \) is clearly not possible since \( x^7 - 1 = (x - 1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1) \).

Since \( x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \) is prime over \( \mathbb{Q}, \omega^r \) is an algebraic conjugate of \( \omega \) for \( r = 1, 2, 3, 4, 5 \) and 6. Since the Galois group is an abelian group of order 6 it must be cyclic so we look for a value of \( r \) that gives an automorphism of order 6 and discover that when \( r = 3 \) we get an automorphism of order 6.

\( \omega \rightarrow \omega^3 \rightarrow \omega^9 = \omega^2 \rightarrow \omega^6 \rightarrow \omega^{18} = \omega^4 \rightarrow \omega^{12} = \omega^5 \rightarrow \omega^{15} = \omega \)

We can describe the automorphisms as follows.

| \( \omega \rightarrow \omega \rightarrow \omega^2 \rightarrow \omega^3 \rightarrow \omega^4 \rightarrow \omega^5 \rightarrow \omega^6 \) |

So \( G \cong C_6 \).

**Example 11:** Find \( G = G(\mathbb{Q}[x^{10} = 1]/\mathbb{Q}) \).

**Solution:** Let \( \omega = e^{2\pi i/10} \). If \( \theta \in G \) then \( \omega^r = \omega^s \) for some \( r, s \) with \( 0 \leq r < 10 \). But \( r \) must be coprime with 10 so only \( r = 1, 3, 7, 9 \) are possible. \( G \) is an abelian group of order 4 and so must be \( C_4 \) or \( C_2 \times C_2 \). The case \( r = 3 \) gives an automorphism of order 4 so \( G \cong C_4 \).
Example 12: Find $G = G(\mathbb{Q}[x^8 = 1]/\mathbb{Q})$.
Solution: Let $\omega = e^{2\pi i/8}$. If $0 \in G$ then $\omega^r = \omega^s$ for some $r = 1, 3, 5, 7$ are possible. The values $3, 5$ and $7$ all give automorphisms of order $2$ and so $G$ must be $C_2 \times C_2$.

<table>
<thead>
<tr>
<th>$\omega \rightarrow$</th>
<th>$1$</th>
<th>$a$</th>
<th>$a^3$</th>
<th>$a^7$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\omega$</td>
<td>$\omega$</td>
<td>$\omega^3$</td>
<td>$\omega^7$</td>
<td>$\omega^9$</td>
</tr>
</tbody>
</table>

Theorem 8: If $F$ contains the number $\alpha$ and the $n$’th roots of unity then $G = G(\mathbb{F}[\alpha^n = \alpha]/F)$ is abelian.
Proof: If $\beta$ is one $n$’th root of $\alpha$ then the other $n$’th roots are $\beta \omega, \beta \omega^2, \ldots, \beta \omega^{n-1}$ where $\omega = e^{2\pi i/n}$. Thus $F[\omega^n = \alpha] = F[\beta]$.
Let $0, \varphi \in G$. Since $0, \varphi$ permute the $n$’th roots of $\alpha$, $\beta^0 = \beta \omega^r$ and $\beta^s = \beta \omega^s$ for some integers $r, s$. Now $\beta^{r+s} = (\beta \omega^r)(\beta \omega^s) = (\beta \omega^r)\omega^s = \beta \omega^{r+s}$ while $\omega^{s+0} = \omega^s$. Hence $0^s \varphi^r \varphi$ fixes $\beta$ and the elements of $F$ and so must be the identity.

Example 13: Find $G = G(\mathbb{Q}[x^7 = 2]/\mathbb{Q}[\omega])$ where $\omega = e^{2\pi i/7}$.
Solution: The $7$’th root of unity are $1, \omega, \omega^2, \omega^3, \omega^4, \omega^5$ and $\omega^6$, all belong to $\mathbb{Q}[\omega]$. If $0 \in G$, $\sqrt[7]{2} \rightarrow \sqrt[7]{2} \omega^r$ for some $r$ with $0 \leq r < 7$.

<table>
<thead>
<tr>
<th>$\sqrt[7]{2} \rightarrow$</th>
<th>$\sqrt[7]{2}$</th>
<th>$\sqrt[7]{2} \omega$</th>
<th>$\sqrt[7]{2} \omega^2$</th>
<th>$\sqrt[7]{2} \omega^3$</th>
<th>$\sqrt[7]{2} \omega^4$</th>
<th>$\sqrt[7]{2} \omega^5$</th>
<th>$\sqrt[7]{2} \omega^6$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\omega$</td>
<td>$\omega$</td>
<td>$\omega^3$</td>
<td>$\omega^7$</td>
<td>$\omega^9$</td>
<td>$\omega^{11}$</td>
<td>$\omega^{13}$</td>
<td>$\omega^{15}$</td>
</tr>
</tbody>
</table>

So $G \cong C_7$.

We now compute precisely the Galois groups of a certain type of radical extension.

Theorem 9: $G(\mathbb{Q}[x^n - 1]/\mathbb{Q}) \cong \mathbb{Z}_n^\#$, where $\mathbb{Z}_n^\#$ is the group of units (elements with multiplicative inverses) in the ring of integers modulo $n$.
Proof: Let $0 = e^{2\pi i/n}$. Under an automorphism $0$ must map to a power of $0$ of the same order. This requires the power to be coprime with $n$. Conversely for every integer $r$ that is coprime to $n$, $0^r$ will have the same order as $0$ and hence the same minimum polynomial. So the Galois group $G$ consists of the automorphisms $0_r$ that map $0$ to $0^r$, where $r$ is coprime to $n$. The corresponding elements of $\mathbb{Z}_n$ are precisely those that have inverses under multiplication.

If $r, s$ are coprime to $n$, the automorphism $0_r$ maps $0$ to $0^r$ and $0_s$, maps this to $(0^r)^s = 0^{rs}$. Hence $0_r0_s = 0_{rs}$ and so the map $\Phi(r) = 0_r$ is an isomorphism from $\mathbb{Z}_n^\#$ to $G$.

The Euler $\phi$-function is the number of integers from $1$ to $n - 1$ that are coprime with $n$. It is therefore the order of the group $\mathbb{Z}_n^\#$ and hence the order of the Galois group $G(\mathbb{Q}[x^n - 1]/\mathbb{Q})$.

The value of $\phi(n)$ can be easily computed if we have a factorisation of $n$.
If $m, n$ are coprime then $\mathbb{Z}_{mn}^\# \cong \mathbb{Z}_m^\# \times \mathbb{Z}_n^\#$ and hence $\phi(mn) = \phi(m)\phi(n)$. It remains to be able to compute $\phi(p^r)$ for any prime $p$ and any positive integer $r$. The relevant formula is $\phi(p^r) = p^{r-1}(p - 1)$ because there are $p^r$ integers in $\{0, 1, 2, ..., p^r - 1\}$ and those that are not coprime with $p^r$ are the $p^{r-1}$ multiples of $p$, giving $\phi(p^r) = p^r - p^{r-1}$.

69
Example 14: \( \phi(700) = \phi(2^4 5^2 7) = \phi(2^4)\phi(5^2)\phi(7) = 2^3 \cdot 5 \cdot 4 \cdot 6 = 960. \)
Hence the Galois group of \( \mathbb{Q}[x^{700} - 1] \) over \( \mathbb{Q} \) is an abelian group of order 960.

In the case where \( n \) is prime we can be even more specific.

Theorem 10: If \( p \) is prime the Galois group of \( \mathbb{Q}[x^p - 1] \) over \( \mathbb{Q} \) is the cyclic group \( C_{p-1} \).
Proof: In chapter 13 we will prove that \( \mathbb{Z}_p \) is a field and that \( \mathbb{Z}_p^\# \), excluding just 0, is cyclic.

§7.4. The Order of a Galois Group

The automorphisms of a polynomial extension permute the zeros of the polynomial so if \( f(x) \in F[x] \) has degree \( n \) then \( G(F[f(x)])/F \) is isomorphic to a subgroup of \( S_n \). If the polynomial is prime we can say a little more.

Theorem 9: Let \( G = G(F[p(x)]/F) \) where \( p(x) \) is a prime polynomial over \( F \) of degree \( n \). Then \( n \) divides \( |G| \).
Proof: Let the zeros of \( p(x) \) be \( \alpha_1, \alpha_2, ..., \alpha_n \).
For each \( i \) let \( K_i = \{ \theta \in G | \alpha_1^\theta = \alpha_i \} \) and let \( K = K_1 \).
Clearly \( K \leq G \). Moreover, since \( \alpha_1 \) can be mapped to any of its conjugates under some automorphism in \( G \), the \( K_i \) are non-empty.
For each \( i \) choose \( \theta_i \in K_i \). It is easy to check that for each \( i \), \( K_i = K \theta_i \), that is they are right cosets of \( K \) in \( G \). Every element of \( G \) is in one of these cosets and so \( |G:K| = n \).
Hence, by Lagrange’s Theorem, \( n \) divides \(|G| \).

EXERCISES FOR CHAPTER 7

Exercise 1:
(i) Find \( G(\mathbb{Q}[2^{1/6}]/\mathbb{Q}) \);
(ii) Find \( G(\mathbb{Q}[x^6 = 2]/\mathbb{Q}[(\omega)]) \);
(iii) Find the order of \( G(\mathbb{Q}[x^6 = 2]/\mathbb{Q}) \).

Exercise 2: Find each of the following Galois groups.
(i) \( G(\mathbb{Q}[x^2 + x + 2 = 0]/\mathbb{Q}) \);
(ii) \( G(\mathbb{Q}[x^8 = 1]/\mathbb{Q}) \);
(iii) \( G(\mathbb{Q}[x^4 - 2x^2 - 3 = 0]/\mathbb{Q}) \).

Exercise 3: Find \( \phi(88000) \).

Exercise 4: Find the Galois group of \( x^{100} - 1 \) over \( \mathbb{Q} \).
SOLUTIONS FOR CHAPTER 7

Exercise 1:
(i) Under an automorphism $2^{1/6}$ must be mapped to a $6^{th}$ root of 2. Now $\mathbb{Q}[2^{1/6}]$ is a subfield of $\mathbb{R}$ and the only real $6^{th}$ roots of 2 are $2^{1/6}$ and $-2^{1/6}$. Both of these are possible and so $G(\mathbb{Q}[2^{1/6}]/\mathbb{Q})$ is a cyclic group of order 2.

(ii) The algebraic conjugates of $2^{1/6}$ over $\mathbb{Q}$ are $2^{1/6}, 2^{1/6}\alpha, 2^{1/6}\alpha^2, 2^{1/6}\alpha^3, 2^{1/6}\alpha^4, 2^{1/6}\alpha^5$ and $2^{1/6}\alpha^6$ where $\alpha = e^{2\pi i/6}$ that is, $\pm 2^{1/6}, \pm 2^{1/6}\alpha$ and $\pm 2^{1/6}\alpha^2$. Every automorphism in $G(\mathbb{Q}[x^6 = 2]/\mathbb{Q}[\omega])$ must map $2^{1/6}$ to one of these and must fix $\omega$. They are all powers of the one that sends $2^{1/6}$ to $-2^{1/6}\omega$. Hence $G(\mathbb{Q}[x^6 = 2]/\mathbb{Q}[\omega]) \cong C_6$.

(iii) $G(\mathbb{Q}[x^6 = 2]/\mathbb{Q})/G(\mathbb{Q}[x^6 = 2]/\mathbb{Q}[\omega]) \cong G(\mathbb{Q}[\omega]/\mathbb{Q}) \cong C_2.$

Hence $|G(\mathbb{Q}[x^6 = 2]/\mathbb{Q})| = 12$.

Exercise 2:
(i) The zeros of $x^2 + x + 2$ are $\frac{-1 \pm \sqrt{1 - 8}}{2} = \frac{-1 \pm \sqrt{-7}i}{2}$ so $\mathbb{Q}[x^2 + x + 2] = \mathbb{Q}[\sqrt{-7}i]$. Hence $G(\mathbb{Q}(x^2 + x + 2)/\mathbb{Q}) \cong C_2$.

(ii) $\mathbb{Q}[x^8 = 1] = \mathbb{Q}[\alpha]$ where $\alpha = e^{2\pi i/8}$. Under an automorphism $\alpha$ must be mapped to $\alpha, \alpha^3, \alpha^5$ or $\alpha^7$.

So $G(\mathbb{Q}[x^8 = 1]/\mathbb{Q})$ has 4 elements whose effects on $\alpha$ are as follows:

<table>
<thead>
<tr>
<th>$\alpha$</th>
<th>$1$</th>
<th>$A$</th>
<th>$B$</th>
<th>$C$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\alpha$</td>
<td>$\alpha$</td>
<td>$\alpha^3$</td>
<td>$\alpha^5$</td>
<td>$\alpha^7$</td>
</tr>
</tbody>
</table>

Clearly $A^2 = B^2 = C^2$ so $G(\mathbb{Q}[x^5 = 1]/\mathbb{Q}) \cong C_2 \times C_2$.

(iii) $x^4 - 2x^2 - 3 = (x^2 - 3)(x^2 + 1)$ so $\mathbb{Q}[x^4 - 2x^2 - 3 = 0] = \mathbb{Q}[\sqrt{3}, i]$. So $G(\mathbb{Q}[x^4 - 2x^2 - 3 = 0]/\mathbb{Q})$ has 4 elements whose effects on $\sqrt{3}$ and $i$ are as follows:

| $\sqrt{3}$ | $\sqrt{3}$ | $\sqrt{3}$ | $-\sqrt{3}$ | $-\sqrt{3}$ |
| $i$ | $i$ | $-i$ | $i$ | $-i$ |

Again the Galois group is isomorphic to $C_2 \times C_2$.

Exercise 3: $\phi(88000) = \phi(64.125.11) = \phi(2^6.5^3.11) = \phi(2^6)\phi(5^3)\phi(11) = 2^4.2^2.4.10 = 32000$.

Exercise 4: $G(\mathbb{Q}[x^{100} - 1]/\mathbb{Q}) \cong \mathbb{Z}_{100}^* \cong \mathbb{Z}_4^# \times \mathbb{Z}_{25}^#.$
Now $\mathbb{Z}_4^# = \{1, 3\} \cong C_2$ and $|\mathbb{Z}_{25}^#| = \phi(25) = 20$. So $\mathbb{Z}_{25}^#$ is either isomorphic to $C_4 \times C_5$ or $C_2 \times C_2 \times C_5$. To decide we need to look at the orders of the elements.

Mod 25, 24 = -1 has order 2. If there is another element of order 2 then the Galois group is isomorphic to $C_2 \times C_2 \times C_5$.

Consider the equation $x^2 = 1(mod 25)$. This would mean that 25 divides $(x - 1)(x + 1)$. We need to find such an $x$ where $x - 1$ and $x + 1$ are each divisible by 5. This is clearly impossible, so $\mathbb{Z}_{25}^# \cong C_4 \times C_5 \cong C_{20}$. It follows that the Galois group is isomorphic to $C_2 \times C_{20}$.