8. GALOIS GROUPS

§8.1. Galois Groups of Field Extensions

Here, at last, we get right into the nitty gritty of the subject! If F, K are fields, a 1-1 and onto function θ: F $\rightarrow$ K is an **isomorphism** if:

$(x + y)^\theta = x^\theta + y^\theta$ and $(xy)^\theta = x^\theta y^\theta$ for all $x, y \in$ 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

$$a_0 + a_1\alpha + a_2\alpha^2 \rightarrow a_0 + a_1\beta + a_2\beta^2.$$

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 α^3 by 2 while in $\mathbb{Q}[\beta]$ we replace β^3 by 2. Clearly this is the same process, but using α's in one case and β's in the other. So the above linear transformation takes products to products and hence is an isomorphism of fields.

We can spell this out in detail as follows.

$$(a_0 + a_1\alpha + a_2\alpha^2)(b_0 + b_1\alpha + b_2\alpha^2)$$
$$= a_0b_0 + (a_0b_1 + a_1b_0)\alpha + (a_0b_2 + a_1b_1 + a_2b_0)\alpha^2 + (a_1b_2 + a_2b_1)\alpha^3 + a_2b_2\alpha^4$$
$$= (a_0b_0 + 2a_1b_2 + 2a_2b_1) + (a_0b_1 + a_1b_0 + 2a_2b_2)\alpha + (a_0b_2 + a_1b_1 + a_2b_0)\alpha^2$$
$$\rightarrow (a_0b_0 + 2a_1b_2 + 2a_2b_1) + (a_0b_1 + a_1b_0 + 2a_2b_2)\beta + (a_0b_2 + a_1b_1 + a_2b_0)\beta^2$$
$$= (a_0 + a_1\beta + a_2\beta^2)(b_0 + b_1\beta + b_2\beta^2).$$

We've 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 $a + b\text{i}$ and $a - b\text{i}$ have the same minimum polynomial over $\mathbb{Q}$, namely:

$$(x - a)^2 + b^2.$$

So $a + b\text{i}$ has two algebraic conjugates, namely $a + b\text{i}$ and $a - b\text{i}$.

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 $\lambda:\mathbb{C}\to\mathbb{C}$ defined by $z^{\lambda} = \bar{z}$ is an automorphism of $\mathbb{C}$ since $\overline{u+v} = \bar{u} + \bar{v}$ and $\overline{uv} = \bar{u}\,\bar{v}$ for all complex numbers u, v.

Theorem 1: The set of all automorphisms of F forms a group with respect to multiplication of maps: $x^{\theta\varphi} = (x^{\theta})^{\varphi}$ for all $x \in F$.

Proof: If $x, y \in F$ then
$$\begin{aligned}(x+y)^{\theta\varphi} &= (x^{\theta} + y^{\theta})^{\varphi}\\ &= (x^{\theta})^{\varphi} + (y^{\theta})^{\varphi}\\ &= x^{\theta\varphi} + y^{\theta\varphi}\end{aligned}$$
and
$$\begin{aligned}(xy)^{\theta\varphi} &= (x^{\theta}y^{\theta})^{\varphi}\\ &= (x^{\theta})^{\varphi}(y^{\theta})^{\varphi}\\ &= x^{\theta\varphi}y^{\theta\varphi}.\end{aligned}$$

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:

$$\mathbf{G(K/F)} = \{\theta \in \mathrm{Aut}(K) \mid x^\theta = x \text{ for all } x \in F.\}.$$

It is easily seen to be a subgroup of Aut(K).

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

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

Now $i^2 = -1$ so $(i^2)^\theta = (-1)^\theta = -1$. Thus $(i^\theta)^2 = -1$. There are thus only two possibilities for i^θ, namely $\pm i$.

If $i^\theta = i$ then for any complex number

$$(a + bi)^\theta = a^\theta + b^\theta i^\theta = a + bi$$

and so θ is the identity automorphism. On the other hand if $i^\theta = -i$ then for any complex number
$(a + bi)^\theta = a^\theta + b^\theta i^\theta = a - bi$ and so $\theta = \lambda$.
Hence $G(\mathbb{C}/\mathbb{R}) \cong \mathbf{C}_2$.

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 α^θ is an algebraic conjugate of α over F.

Proof: Suppose the minimum polynomial of α over F is $p(x)$. Then $0 = 0^\theta = p(\alpha)^\theta = p(\alpha^\theta)$.

Corollary 1: If $f(x) \in F[x]$ and $\theta \in G(F[f(x) = 0]/F)$ then θ 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 $f(x) \in F[x]$ has degree n then $G(F[f(x)]/F)$ is isomorphic to a subgroup of $\mathbf{S}_n$.
Proof: The map that takes an element of $G(F[f(x)]/F)$ 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 $F[f(x)]$.

Example 6:
$G(\mathbb{Q}[x^4 = 2]/\mathbb{Q}) \cong \mathbf{D}_8 = \langle A, B \mid A^4, B^2, BA = A^{-1}B \rangle$.
The zeros of $x^4 - 2$ are $\pm\sqrt[4]{2}$, $\pm\sqrt[4]{2}\,i$.
Let $\alpha_1 = \sqrt[4]{2}$, $\alpha_2 = -\sqrt[4]{2}$, $\alpha_3 = \sqrt[4]{2}\,i$ and $\alpha_4 = -\sqrt[4]{2}\,i$.
Let A be the automorphism that maps $\sqrt[4]{2}$ to $\sqrt[4]{2}\,i$
and fixes i.
Then under A, $\alpha_1 \to \alpha_3$, $\alpha_2 \to \alpha_4$ and $\alpha_4 \to \alpha_1$ and
$\alpha_3 = \sqrt[4]{2}\,i \to (\sqrt[4]{2}\,i)i = -\sqrt[4]{2} = \alpha_2$,.
This corresponds to the permutation (1324).
The automorphism B that fixes $\sqrt[4]{2}$ and maps i to –i corresponds to the permutation (34).
Clearly $A^4 = 1$, $B^2 = 1$ and $BA = A^{-1}B$.

§8.2. 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 4: 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 I'll 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 θ to H. The domain of $\theta|_H$ is H, but on these elements the effect is the same as for θ. So $\theta|_H$ is also an isomorphism. But is it an automorphism of H? For that to happen we'd 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's in G(H/F). Let the restriction map be denoted by ρ, that is $\theta^\rho = \theta|_H$. The function ρ is a function from G(K/F) to G(H/F).

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

Then $h^{(\theta\varphi)^\rho} = h^{(\theta\varphi)|_H}$ (this is how ρ is defined)

$= h^{(\theta\varphi)}$ (restrictions give the same values)

$= (h^\theta)^\varphi$ (by the way products are defined)

$= (h^{\theta|_H})^{\varphi|_H}$ (restrictions give the same values)

$= (h^{\theta^\rho})^{\varphi^\rho}$ (this is how ρ is defined)

$= h^{\theta^\rho\varphi^\rho}$ (by the way products are defined)

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

Now ker ρ 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 ρ = 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 im ρ 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's ASSUME that they can all be so extended. In other words we'll assume that ρ is onto, or in other words, im ρ = 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 5: 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 $H = F[f(x)] = F[\alpha_1, ..., \alpha_n]$ where the α_i are the zeros of $f(x)$.
Then $F = F^\theta \leq H^\theta$ and each $\alpha_i{}^\theta \in H^\theta$ so

$$F[\alpha_1{}^\theta, ..., \alpha_n{}^\theta] \leq H^\theta.$$

But θ merely permutes the zeros of $f(x)$ so

$$F[\alpha_1{}^\theta, ..., \alpha_n{}^\theta] = F[\alpha_1, ..., \alpha_n] = H.$$

Hence $H \leq H^\theta$. But θ is an automorphism and so H and H^θ are isomorphic as vector spaces and, being finite-dimensional over **F**, we must have $H = H^\theta$.

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 φ.

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

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

It's easy to see that φ 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 6: Suppose $\alpha, \beta \in \mathbb{C}$, and that $\phi: F \to H$ is an isomorphism, where F, H are number fields. Suppose that the minimum polynomial of α over F is $p(x)$ and the minimum polynomial of β over H is $p^{\phi}(x)$. Then ϕ can be extended to an isomorphism $\theta: F[\alpha] \to H[\beta]$.

Proof: Suppose the minimum polynomial for α and β is

$$p(x) = x^n + p_{n-1}x^{n-1} + \ldots + p_0.$$

Then $p^{\varphi}(x) = x^n + p_{n-1}^{\varphi}\,x^{n-1} + \ldots + p_0^{\varphi}$.

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

$$a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} \to a_0^{\phi} + a_1^{\phi}\beta + \ldots + a_{n-1}^{\phi}\beta^{n-1}$$

is a linear transformation. For example:

$$(a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}) + (b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1})$$
$$= (a_0 + b_0) + (a_1 + b_1)\alpha + \ldots + (a_{n-1} + b_{n-1})\alpha^{n-1}$$
$$\to (a_0 + b_0)^{\varphi} + (a_1 + b_1)^{\varphi}\,\beta + \ldots + (a_{n-1} + b_{n-1})^{\varphi}\,\beta^{n-1}$$
$$= (a_0^{\varphi} + b_0^{\varphi}) + (a_1^{\varphi} + b_1^{\varphi})\,\beta + \ldots + (a_{n-1}^{\varphi} + b_{n-1}^{\varphi})\,\beta^{n-1}$$
$$= (a_0^{\varphi} + a_1^{\varphi}\,\beta + \ldots + a_{n-1}^{\varphi}\,\beta^{n-1}) + (b_0^{\varphi} + b_1^{\varphi}\,\beta + \ldots + b_{n-1}^{\varphi}\,\beta^{n-1}).$$

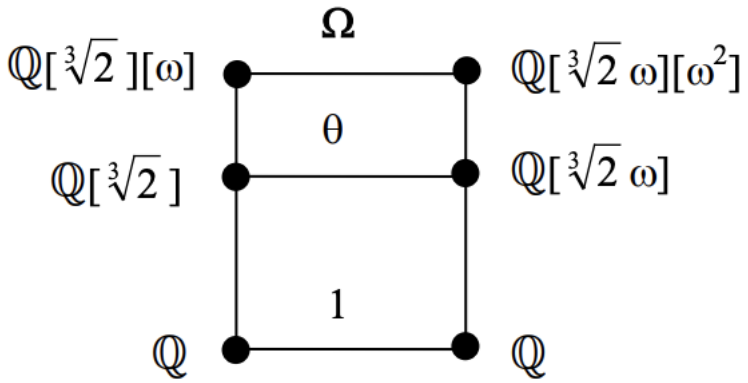
When it comes to multiplication in each of $\mathbb{Q}[\alpha]$ and $\mathbb{Q}[\beta]$ we multiply the expressions as if they are polynomials and then, in $\mathbb{Q}[\alpha]$ replace powers of α^n by $-p_{n-1}\alpha^{n-1} - ... - p_1\alpha - p_0$ while in $\mathbb{Q}[\beta]$ we replace β^n by the equivalent expression in β. Clearly this is the same process, but using α's in one case and β'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 $\mathbb{Q}$ can be extended to an isomorphism $\theta:\mathbb{Q}[\sqrt[3]{2}] \to \mathbb{Q}[\sqrt[3]{2}\,\omega]$ that takes $\sqrt[3]{2}$ to $\sqrt[3]{2}\,\omega$.

The minimum polynomial of ω over $\mathbb{Q}[\sqrt[3]{2}]$ is $x^2 + x + 1$. This is the same as its minimum poly over $\mathbb{Q}$, but conceivably it could factorise over this larger 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 ω a real number.
You have to be careful with minimum polynomials over larger fields. For example the minimum polynomial of $\sqrt[4]{2}$ over $\mathbb{Q}$ is $x^4 - 2$, but over $\mathbb{Q}[\sqrt{2}]$ it is $x^2 - \sqrt{2}$.

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



But $\mathbb{Q}[\sqrt[3]{2}\,][\omega] = \mathbb{Q}[x^3 - 2] = \mathbb{Q}[\sqrt[3]{2}\,\omega][\omega^2]$ and so we have an automorphism Ω of $\mathbb{Q}[x^3 = 2]$ that sends $\sqrt[3]{2}$ to $\sqrt[3]{2}\,\omega$ and ω to ω^2.
$(\sqrt[3]{2}\,)^{\Omega^2} = (\sqrt[3]{2}\,\omega)^{\Omega} = (\sqrt[3]{2}\,)^{\Omega}\omega^{\Omega} = (\sqrt[3]{2}\,\omega)(\omega^2) = \sqrt[3]{2}$ and
$(\omega)^{\Omega^2} = (\omega^2)^{\Omega} = (\omega)^{\Omega}\omega^{\Omega} = (\omega^2)(\omega^2) = \omega^4 = \omega$.
Hence Ω^2 is the identity automorphism.

We can map $\sqrt[3]{2}$ to $\sqrt[3]{2}$, $\sqrt[3]{2}\,\omega$ or $\sqrt[3]{2}\,\omega^2$ and ω can be sent to ω or ω^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 ω.

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.

	1	**A**	**A²**	**B**	**AB**	**A²B**
$\sqrt[3]{2} \rightarrow$	$\sqrt[3]{2}$	$\sqrt[3]{2}\,\omega$	$\sqrt[3]{2}\,\omega^2$	$\sqrt[3]{2}$	$\sqrt[3]{2}\,\omega$	$\sqrt[3]{2}\,\omega^2$
$\omega \rightarrow$	ω	ω	ω	ω^2	ω^2	ω^2

We can easily show that $A^3 = 1$, $B^2 = 1$ and $BA = A^{-1}B$. Hence $G(\mathbb{Q}[x^3 = 2]/\mathbb{Q}) \cong \langle A, B \mid A^3, B^2, BA = A^{-1}B\rangle$ which is the dihedral group of order 6, otherwise known as $\mathbf{S}_3$.

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

Theorem 7: Suppose that $\varphi: H \rightarrow K$ is an isomorphism and that $f(x) \in H[x]$ is non-zero. Then φ may be extended to an isomorphism

$$\theta: H[f(x) = 0] \rightarrow K[f^{\phi}(x) = 0]$$

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 α be one of the zeros of $f(x)$ and let $p(x)$ be the minimum polynomial of α over F. Let β be a zero of the corresponding polynomial $p^{\phi}(x)$. By Theorem 5, φ may be extended to $\sigma: H[\alpha] \rightarrow K[\beta]$ 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

$$f^{\phi}(x) = (x - \beta)g^{\phi}(x).$$

It follows from the induction hypothesis that σ may be extended further to an isomorphism

$$\theta: H[\alpha][g(x) = 0] \rightarrow K[\beta][g^{\phi}(x) = 0].$$

But $H[\alpha][g(x) = 0] = H[f(x) = 0]$ and

$$K[\beta][g^{\phi}(x) = 0] = K[f^{\phi}(x) = 0]$$

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 $\theta \in G(F[f(x) = 0]/F)$ which maps α to β.

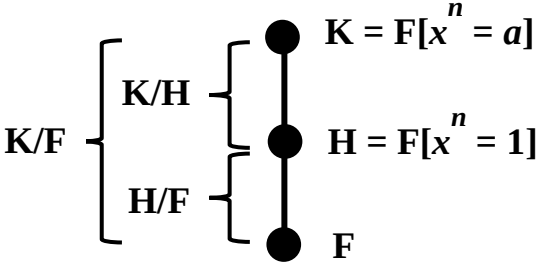
Proof: By Theorem 5 the identity automorphism on F can be extended to an isomorphism φ from $F[\alpha]$ to $F[\beta]$ that takes α to β. Since φ fixes F, $f^{\varphi}(x) = f(x)$.

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

§8.3. 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 I 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: $F[x^n = 1]/F]$ followed by $F[x^n = a]/F[x^n = 1]$. So we'll concentrate on calculating the Galois groups of each type.



Theorem 8: $G(F[x^n = 1]/F)$ 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 θ, φ permute the n'th roots of 1, $\omega^\theta = \omega^r$ and $\omega^\varphi = \omega^s$ for some integers r, s.

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

Example 9: Find $G = G(\mathbb{Q}[x^7 = 1]/\mathbb{Q})$.

Solution: Let $\omega = e^{2\pi i/7}$. If $\theta \in G$ then $\omega^\theta = \omega^r$ for some r with $0 \le r < 7$. 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 $\mathbb{Q}$, ω^r is an algebraic conjugate of ω 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 one.

$\omega \to \omega^3 \to \omega^9 = \omega^2$

$\omega^2 \to \omega^6 \to \omega^{18} = \omega^4$

$\omega^4 \to \omega^{12} = \omega^5$

$\omega^5 \to \omega^{15} = \omega$

So $G \cong \mathbf{C}_6$.

	1	$\mathbf{A^2}$	**A**	$\mathbf{A^4}$	$\mathbf{A^5}$	$\mathbf{A^3}$
$\omega \to$	ω	ω^2	ω^3	ω^4	ω^5	ω^6

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

Solution: Let $\omega = e^{2\pi i/10}$. If $\theta \in G$ then $\omega^\theta = \omega^r$ for some r with $0 \le r < 10$. 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 $\mathbf{C}_4$ or $\mathbf{C}_2 \times \mathbf{C}_2$. The case $r = 3$ gives an automorphism of order 4 so $G \cong \mathbf{C}_4$.

	1	**A**	$\mathbf{A^3}$	$\mathbf{A^2}$
$\omega \to$	ω	ω^3	ω^7	ω^9

Example 11: Find $G = G(\mathbb{Q}[x^8 = 1]/\mathbb{Q})$.
Solution: Let $\omega = e^{2\pi i/8}$. If $\theta \in G$ then $\omega^\theta = \omega^r$ for some r but only 1, 3, 5, 7 are possible. The values 3, 5 and 7 all give automorphisms of order 2 and so G must be $\mathbf{C}_2 \times \mathbf{C}_2$.

	1	**A**	**B**	**AB**
$\omega \to$	ω	ω^3	ω^5	ω^7

Now we investigate the Galois groups of Type 2 extensions.

Theorem 9: If F contains the number α and the n'th roots of unity then $G = G(F[x^n = \alpha]/F)$ is abelian.
Proof: If β is one n'th root of α 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 $F[x^n = \alpha] = F[\beta]$.

Let $\theta, \varphi \in G$. Since θ, φ permute the n'th roots of α, $\beta^\theta = \beta\omega^r$ and $\beta^\varphi = \beta\omega^s$ for some integers r, s.
Now $\beta^{\theta\varphi} = (\beta\omega^r)^\varphi = (\beta^\varphi)(\omega^r)^\varphi = (\beta\omega^s)\omega^r = \beta\omega^{s+r}$ while $\omega^{\varphi\theta} = \omega^{r+s}$. Hence $\theta\varphi = \varphi\theta$, and so G is abelian.

Example 12: 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, ω, ω^2, ω^3, ω^4, ω^5 and ω^6, and all belong to $\mathbb{Q}[\omega]$.

If $\theta \in G$, $\sqrt[7]{2}\,\theta = \sqrt[7]{2}\,\omega^r$ for some r with $0 \le r < 7$.

	1	**A**	$\mathbf{A^2}$	$\mathbf{A^3}$
$\sqrt[7]{2}$ →	$\sqrt[7]{2}$	$\sqrt[7]{2}\,\omega$	$\sqrt[7]{2}\,\omega^2$	$\sqrt[7]{2}\,\omega^3$

	$\mathbf{A^4}$	$\mathbf{A^5}$	$\mathbf{A^6}$
$\sqrt[7]{2}$ →	$\sqrt[7]{2}\,\omega^4$	$\sqrt[7]{2}\,\omega^5$	$\sqrt[7]{2}\,\omega^6$

So $G \cong \mathbf{C}_7$.

We now compute in general the Galois groups of radical extensions of Types 1 and 2.

Theorem 10: $G(\mathbb{Q}[x^n - 1]/\mathbb{Q}) \cong \mathbb{Z}_n^{\#}$, where $\mathbb{Z}_n^{\#}$ is the group of units (elements with multiplicative inverses) in the ring of integers modulo n.

Proof: Let $\theta = e^{2\pi i/n}$. Under an automorphism θ must map to a power of θ of the same order. This requires the power to be coprime with n. Conversely for every integer r that is coprime to n, θ^r will have the same order as θ and hence the same minimum polynomial. So the Galois group G consists of the automorphisms θ_r that map θ to θ^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 θ_r maps θ to θ^r and θ_s maps this to $(\theta^s)^r = \theta^{rs}$. Hence $\theta_r\theta_s = \theta_{rs}$, so the map $\Phi(r) = \theta_r$ is an isomorphism from $\mathbb{Z}_n^{\#}$ to G.

The Euler φ-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 $\varphi(n)$ can be easily computed if we have a factorisation of n.

Theorem 11: (1) If m, n are coprime then

$$\varphi(mn) = \varphi(m)\,\varphi(n).$$

(2) If p is prime then $\varphi(p^n) = p^{n-1}(p - 1)$ for all n.

Proof: (1) If m, n are coprime then $\mathbb{Z}_{mn}^{\#} \cong \mathbb{Z}_m^{\#} \times \mathbb{Z}_n^{\#}$, so just count the numbers of elements.

(2) There are p^n integers in $\{0, 1, 2, ..., p^n - 1\}$ and those that are not coprime with p^n are the p^{n-1} multiples of p, giving $\varphi(p^n) = p^n - p^{n-1}$.

Example 13: $\varphi(700) = \varphi(2^4 5^2 7) = \varphi(2^4).\varphi(5^2).\varphi(7)$
$= 2^3.5.4.6 = 960.$

Hence the Galois group of $\mathbb{Q}[x^{700} - 1]$ over $\mathbb{Q}$ is an abelian group of order 960.

In the case of $\mathbb{Q}[x^p - 1]$, where p is prime, we can be even more specific.

Theorem 12: If p is prime the Galois group of $\mathbb{Q}[x^p - 1]$ over $\mathbb{Q}$ is the cyclic group $\mathbf{C}_{p-1}$.
Proof: In Chapter 13 we'll prove that $\mathbb{Z}_p$ is a field and that $\mathbb{Z}_p^{\#}$, excluding just 0, is cyclic.

§8.4. 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 $\mathbf{S}_n$. If the polynomial is prime we can say a little more.

Theorem 13: 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 $K_i = \{\theta \in G \mid \alpha_1^{\theta} = \alpha_i\}$ and let $K = K_1$.
Clearly $K \leq G$. Moreover, since α_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's 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 $|G|$.

§8.5. The Galois Correspondence

Suppose K is a polynomial extension of the field F and G = G(K/F) is the Galois group of this polynomial extension. Consider the fields that lie between F and K, including those fields themselves, and the subgroups of G. The Fundamental Theorem of Galois Theory describes a remarkable connection between these subfields and these subgroups.

It states that there's a 1-1 order reversing correspondence between these subfields and these subgroups. This means that if we draw a picture of the subgroups of G(K/F), where we place larger subgroups above smaller ones, with lines indicating that one subgroup is contained inside another, and then turn the picture upside down, we get a picture of the subfields between F and K.

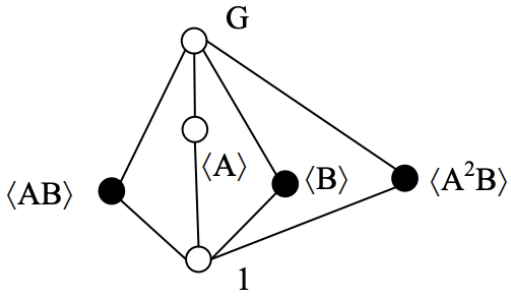
At the bottom of the subfield picture will be F itself. This will correspond to the largest subgroup, namely G itself. At the top of the subfield picture will be K and this will correspond to the trivial subgroup 1.

Where one of the subfields is contained inside another the degree of the extension will be the index of the corresponding subgroups. Under this correspondence, polynomial extensions correspond to normal subgroups. In our examples we represent polynomial extensions and normal subgroups by white dots and others by black dots.

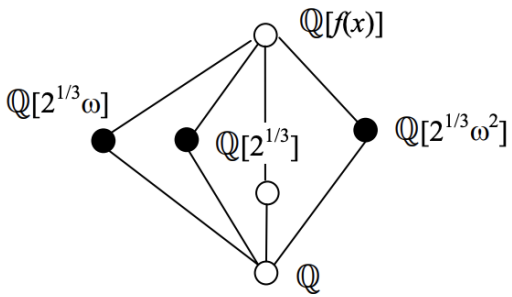
Finally, the Fundamental Theorem says something about quotient groups of the Galois group. This is probably the most important part of the theorem.

The correspondence, called the **Galois Correspondence**, associates each double field extension $F \leq L \leq K$ with $G(K/L)$. Going back the other way the correspondence associates each subgroup H of $G(K/L)$ with the fixed field of H. The **fixed field** of H is the set of all elements of K that are fixed by every element of H.

Example 14: To illustrate this recall the situation for $f(x) = x^3 - 2$. The lattice of subgroups of the Galois group and the lattice of subfields of the splitting field are as follows:

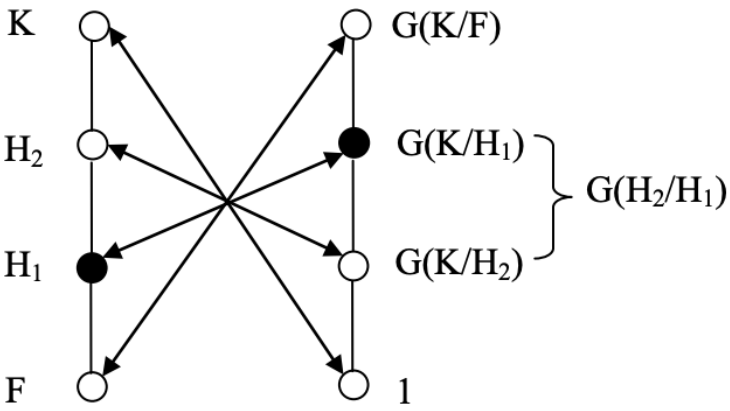


SUBGROUPS OF $G(\mathbb{Q}[x^3 = 2]/\mathbb{Q})$



SUBFIELDS OF $\mathbb{Q}[x^3 = 2]$

Theorem 14 (FUNDAMENTAL THEOREM OF GALOIS THEORY):
Suppose K is a polynomial extension of F. Then:
(1) $H \rightarrow G(K/H)$ is a 1-1 and onto correspondence between the subfields of K that contain F and the set of subgroups of G(K/F), taking each subgroup of G(K/F) to its fixed field.
(2) $H_1 \leq H_2 \leq K$ if and only if $G(K/H_2) \leq G(K/H_1)$.
(3) $|H_2:H_1| = |G(K/H_1):G(K/H_2)|$ whenever $H_1 \leq H_2 \leq K$.
(4) $H \leq K$ is a polynomial extension of F if and only if G(K/H) is normal in G(K/F).
(5) If H_2 is a polynomial extension of H_1 then $G(K/H_1)/G(K/H_2) \cong G(H_2/H_1)$.



But remember, for this to work we need K to be a polynomial extension of F. If it isn't then the situation can be quite different. For example $\mathbb{Q}[2^{1/3}]$ is not a polynomial extension of $\mathbb{Q}$. It has degree 3 over $\mathbb{Q}$ and two subfields,

$\mathbb{Q}[2^{1/3}]$ itself and $\mathbb{Q}$. But $G(\mathbb{Q}[2^{1/3}]/\mathbb{Q})$ is the trivial group because the only zero of $x^3 - 2$ that is in $\mathbb{Q}[2^{1/3}]$ is $2^{1/3}$.

Parts (2), (4) and (5) were proved in Theorem 3 of chapter 7. But we have not yet established the 1-1 correspondence. If $F \leq L \leq K$ we can map L to G(K/L). In the reverse direction we can map a subgroup H of G(K/L) to its fixed field. It's not obvious that the fixed field of G(K/L) will take us back to L.

Suppose that the fixed field of G(K/L) is L_0. It's clear that $L \leq L_0$ but it's conceivable that the automorphisms of K that fix the elements of L will also fix some other elements. We have to show that this can never be the case.

§8.6. Orders and Degrees

Here we'll show that the degree of a polynomial extension is the order of the corresponding Galois group.

Theorem 15: Suppose that K is a polynomial extension of F. Then $|G(K/F)| = |K:F|$.
Proof: We prove this by induction on $n = |K:F|$.
It is trivial if $n = 1$. Suppose $n > 1$.
Let $\alpha \in K - F$. Let $p(x)$ be the minimum polynomial of α over F and let $r = \deg p(x)$.
Let the zeros of $p(x)$ in F be $\alpha = \alpha_1, \alpha_2, ..., \alpha_r$.

For each i the identity automorphism of F can be extended to an isomorphism from $F[\alpha]$ to $F[\alpha_i]$ such that α maps to α_i and this can be extended to $\tau_i \in G(K/F)$.

Let $|K/F[\alpha]| = s$.

Since $|H[\alpha]/F| = r$ we have $rs = n$.

Since $s < n$ we may assume that $|G(K/F[\alpha])| = s$.

Let $G(K/F[\alpha]) = \{\theta_1, \theta_2, ..., \theta_s\}$.

Then for all i, j, $\theta_i\tau_j \in G(K/F)$.

We complete the proof by showing:

(1) Every element of G(K/F) has the form $\theta_i\tau_j$ for some i, j.

Suppose $\varphi \in G(K/F)$. Then $\alpha^{\varphi} = \alpha_j$ for some j.

Hence $\varphi\tau_j^{-1}$ fixes α and so is equal to θ_i for some i and so $\varphi = \theta_i\tau_j$.

(2) The rs possibilities $\theta_i\tau_j$ are distinct.

Suppose $\theta_i\tau_j = \theta_h\tau_k$.

Then $\tau_j\tau_k^{-1} = \theta_h\theta_i^{-1}$ and so $\tau_j\tau_k^{-1}$ fixes α.

Hence $\alpha^{\tau_j} = \alpha^{\tau_k}$ and so $\alpha_j = \alpha_k$ which means that $j = k$.

So $\theta_i = \theta_h$ and so $i = h$.

Example 15: Let $F = \mathbb{Q}$ and $K = \mathbb{Q}[x^4 = 2] = \mathbb{Q}[\sqrt[4]{2}, i]$. Now $|K/\mathbb{Q}[i]| = 4$ since the minimum polynomial of $\sqrt[4]{2}$ over $\mathbb{Q}[i]$ is $x^4 - 2$. $|\mathbb{Q}[i]/\mathbb{Q}| = 2$ so $|K/\mathbb{Q}| = 8$. $G(K/\mathbb{Q})$ is the dihedral group of order 8.

	1	**A**	**A^2**	**A^3**
$\sqrt[4]{2} \rightarrow$	$\sqrt[4]{2}$	$\sqrt[4]{2}\,i$	$-\sqrt[4]{2}$	$-\sqrt[4]{2}\,i$
$\mathbf{i} \rightarrow$	i	i	i	i

	B	**AB**	**A^2B**	**A^3B**
$\sqrt[4]{2} \rightarrow$	$\sqrt[4]{2}$	$\sqrt[4]{2}\,i$	$-\sqrt[4]{2}$	$-\sqrt[4]{2}\,i$
$\mathbf{i} \rightarrow$	–i	–i	–i	–i

$$G(K/\mathbb{Q}) \cong \langle A, B \mid A^4, B^2, BA = A^{-1}B \rangle.$$

We can illustrate the proof by taking:

$$\alpha = i,\ p(x) = x^2 + 1,\ \alpha_1 = i,\ \alpha_2 = -i.$$

We can take τ_1 to be any power of A and τ_2 can be any of the A^rB. Suppose we take $\tau_1 = A^3$ and $\tau_2 = B$.

$G(K/F[\alpha]) = \{1, A, A^2, A^3\}$ so we can take:

$$\theta_1 = 1,\ \theta_2 = A,\ \theta_3 = A^2 \text{ and } \theta_4 = A^3.$$

Then, for example, $\theta_3\tau_2 = A^2B$. By taking all $\theta_i\tau_j$ we get all 8 elements of G(K/F).

Theorem 16: Suppose $F \le L \le K$ where K is a polynomial extension of F.
Then $|G(K/L)| = |K/L|$ and L is the fixed field of G(K/L).
Proof: Since K is a polynomial extension of F then so is L.
[If $K = F[f(x)]$ where $f(x) \in F[x]$ then $f(x) \in L[x]$ and $K = L[f(x)]$.] So by Theorem 2, $|G(K/L)| = |K/L|$.
If L_0 is the fixed field of G(K/L) then

$$L \leq L_0 \text{ and } G(K/L_0) = G(K/L).$$

But this means that $|K/L_0| = |K/L|$ and so $L_0 = L$.

EXERCISES FOR CHAPTER 8

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 $\varphi(88000)$.

Exercise 4: Find the Galois group of $x^{100} - 1$ over $\mathbb{Q}$.

SOLUTIONS FOR CHAPTER 8

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 $2^{1/6}\alpha^5$

where $\alpha = e^{2\pi i/6}$ that is, $\pm 2^{1/6}$, $\pm 2^{1/6}\omega$ and $\pm 2^{1/6}\omega^2$. Every automorphism in $G(\mathbb{Q}[x^6 = 2]/\mathbb{Q}[\omega])$ must map $2^{1/6}$ to one of these and must fix ω. 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) $G(\mathbb{Q}[x^6 = 2]/\mathbb{Q})/ G(\mathbb{Q}[x^6 = 2]/\mathbb{Q}[\omega]) \cong G(\mathbb{Q}[\omega]/\mathbb{Q})$

$\cong \mathbf{C}_2$.

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 $G(\mathbb{Q}[x^2 + x + 2 = 0]/\mathbb{Q}) \cong \mathbf{C}_2$.

(ii) $\mathbb{Q}[x^8 = 1] = \mathbb{Q}[\alpha]$ where $\alpha = e^{2\pi i/8}$. Under an automorphism α must be mapped to α, α^3, α^5 or α^7. So $G(\mathbb{Q}[x^8 = 1]/\mathbb{Q})$ has 4 elements whose effects on α are as follows:

	1	**A**	**B**	**C**
$\alpha \rightarrow$	α	α^3	α^5	α^7

Clearly $A^2 = B^2 = C^2$ so $G(\mathbb{Q}[x^5 = 1]/\mathbb{Q}) \cong \mathbf{C}_2 \times \mathbf{C}_2$.

(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:

	1	**A**	**B**	**C**
$\sqrt{3} \rightarrow$	$\sqrt{3}$	$\sqrt{3}$	$-\sqrt{3}$	$-\sqrt{3}$
$\mathbf{i} \rightarrow$	i	$-$i	i	$-$i

Again the Galois group is isomorphic to $\mathbf{C}_2 \times \mathbf{C}_2$.

Exercise 3:
$\varphi(88000) = \varphi(64.125.11) = \varphi(2^6.5^3.11)$
$= \varphi(2^6).\varphi(5^3).\varphi(11) = 2^5.5^2.4.10 = 32000.$

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 $|\mathbb{Z}_{25}^{\#}| = \varphi(25) = 20$.
So $\mathbb{Z}_{25}^{\#}$ is either isomorphic to $\mathbf{C}_4 \times \mathbf{C}_5$ or $\mathbf{C}_2 \times \mathbf{C}_2 \times \mathbf{C}_5$. To decide which we need to look at the orders of the elements. Mod 25 we have $24 = -1$, which has order 2. If there's another element of order 2 then the Galois group is isomorphic to $\mathbf{C}_2 \times \mathbf{C}_2 \times \mathbf{C}_5$.

Consider the equation $x^2 \equiv 1 (\text{mod } 25)$. 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 $\mathbb{Z}_{25}^{\#} \cong \mathbf{C}_4 \times \mathbf{C}_5 \cong \mathbf{C}_{20}$. It follows that the Galois group is isomorphic to $\mathbf{C}_2 \times \mathbf{C}_{20}$.