§11.1. The Galois Correspondence

The Fundamental Theorem of Galois Theory describes a remarkable connection between the subfields between $F$ and $K$, where $K$ is any polynomial extension of $F$, and the subgroups of $G(K/F)$.

In fact there is 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 top in the picture of subfields, will be $K$ itself. This will correspond to the largest subgroup, namely $G(K/F)$ itself. At the bottom of the picture of subfields will be $F$ and this will correspond to the trivial subgroup $1$.

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

This correspondence, called the Galois correspondence, associates each subfield $L$, with $F \leq L \leq K$ with $G(K/L)$. Going back the other way the correspondence associates each subgroup $H$ of $G$ 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 $H$.

To illustrate this, in a later chapter we will establish the following as the “lattice” of subfields and subgroups in the case $F = \mathbb{Q}$ and $K = \mathbb{Q}[x^3 = 2]$
Finally we state the fundamental theorem more precisely.

**Theorem 1 (Fundamental Theorem of Galois Theory):**
Suppose $K$ is a polynomial extension of $F$ and let $G = G(K/F)$. Let $S$ be the set of subgroups of $G$ and let $T$ be the set of all subfields of $K$ that contain $F$. Then

1. $H \rightarrow G(K/H)$ is a 1-1 and onto map from the subfields of $K$ that contain $F$ to the set of subgroups of $G(K/H)$.
2. The inverse of this map takes each subgroup of $G$ to its fixed field.
3. $H_1 \leq H_2$ if and only if $G(K/H_2) \leq G(K/H_1)$.
4. $L \leq K$ is a polynomial extension of $F$ if and only if $G(K/H)$ is a normal subgroup of $G(K/F)$.
5. $|L_1:L_2| = |G(H(K/L_2))| / |G(K/L_1)|$ whenever $L_2 \leq L_1 \leq K$.

**Theorem 2:** Suppose $K$ is a polynomial extension of $F$ and $H$ is an extension of $F$. If $\varphi: K \rightarrow H$ is an isomorphism such that $F = F = F$ then $K = H$.

**Proof:** Suppose $K = F[f(x) = 0]$. Then $K = F[f^0(x) = 0] = F[f(x) = 0]$.

**Theorem 3:** Suppose $F \leq K$. Then there exist at least $|K:F|$ isomorphisms from $K$ into $C$ that fix the elements of $F$.

**Proof:** We prove this by induction on $n$. Suppose $n > 1$. Let $H$ be a proper subfield of $K$ such that $|K:H|$ is least. Let $\alpha \in K - H$. Then $H < H[\alpha] \leq K$ and so $K = H[\alpha]$.

Let $\beta$ be any algebraic conjugate of $\alpha$ over $H$ and let $\vartheta: H \rightarrow C$ be an isomorphism into $C$. By Theorem there exists $\vartheta$ such that $\alpha$ maps to $\beta$. By induction there are at least $|H:F|$ such $\beta$ and hence at least $|K:F|$ such $\vartheta$. (Since $\vartheta |_H = \alpha^0 = \alpha$ these are all distinct.

**Corollary:** If $K$ is a polynomial extension of $F$ then $|G(K/F)| \geq |K:F|$.

**Proof:** If $\varphi$ is an isomorphism of $K$ into $C$ that fixes the elements of $F$ then $K^0 = K$ and so $\varphi$ is an automorphism and so $\varphi \in G(K/F)$. There are at least $|K:F|$ such $\vartheta$ by the theorem which proves the corollary.

### §11.2. Degrees and Orders

**Theorem 4:** Suppose $p(x) \in F[x]$ is prime over $F$ and has degree $n$. Then $|G(F[p(x) = 0]/F)|$ is a multiple of $n$.

**Proof:** Let $G = g(F[f(x) = 0])$. Let the zeros of $p(x)$ be $\alpha_1$, $\alpha_2$, ..., $\alpha_n$.

For each $k$ there exists $\tau_k \in G$ that maps $\alpha_1$ to $\alpha_k$.

For each $k$ let $H_k = \{ \vartheta \in G \mid \vartheta^0 = \alpha_k \}$.

Let $H = H_1$. Clearly $H \leq G$ and $H_k = H\tau_k$.

So there are $n$ right cosets of $H$ in $G$. Hence $|G| = n|H|$ and so $n$ divides $|G|$.

**Theorem 5:** Suppose $K$ 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 $\alpha$ over $F$ and let $r = \deg p(x)$.

Let the zeros of $p(x)$ be $\alpha = \alpha_1$, $\alpha_2$, ..., $\alpha_r$.

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

Let $|K:F[\alpha_i]| = s$. Since $|F[\alpha]:F| = r$, $rs = n$.  

114
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 $i, j, \theta_i \theta_j \in G(K/F)$. We complete the proof by showing:
1. Every element of $G(K/F)$ has the form $\theta_i \theta_j$ for some $i, j$.
2. The $n = rs$ possibilities $\theta_i \theta_j$ are distinct.

1. Suppose $\varphi \in G(K/F)$. Then $\alpha^\varphi = \alpha_j$ for some $j$.
Hence $\varphi \tau_j^{-1}$ fixes $\alpha$ and so is equal to $\theta_i$ for some $i$.
So $\varphi = \theta_i \tau_j$.

2. 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 $\alpha$.
Hence $\alpha^\tau_j = \alpha^\tau_k$ and so $\alpha_j = \alpha_k$ and $\theta_i = \theta_h$.

**Example 9:** Let $F = \mathbb{Q}$ and $K = \mathbb{Q}[x^4 = 2] = \mathbb{Q}[\sqrt[4]{2}, \mathbf{i}]$.
Now $|K:Q[i]| = 4$ since the minimum polynomial of $\sqrt[4]{2}$ over $\mathbb{Q}[i]$ is $x^4 - 2$.
$|Q[i]:Q| = 2$ so $|K:Q| = 8$. $G(K/Q)$ is the dihedral group of order 8.

<table>
<thead>
<tr>
<th>$\sqrt[4]{2}$</th>
<th>1</th>
<th>a</th>
<th>$a^2$</th>
<th>$a^3$</th>
<th>b</th>
<th>ab</th>
<th>$a^2b$</th>
<th>$a^3b$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\sqrt[4]{2}$</td>
<td>$\sqrt[4]{2}$</td>
<td>$\frac{-\sqrt[4]{2}}{2}$</td>
<td>$\frac{-\sqrt[4]{2}}{2}i$</td>
<td>$\frac{-\sqrt[4]{2}}{2}$</td>
<td>$\sqrt[4]{2}$</td>
<td>$\sqrt[4]{2}$i</td>
<td>$\sqrt[4]{2}$i</td>
<td>$\sqrt[4]{2}$i</td>
</tr>
<tr>
<td>1</td>
<td>$\sqrt[4]{2}$</td>
<td>$\sqrt[4]{2}$i</td>
<td>$\sqrt[4]{2}$i</td>
<td>$\sqrt[4]{2}$i</td>
<td>$\sqrt[4]{2}$i</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>i</td>
<td>$\sqrt[4]{2}$i</td>
<td>$\sqrt[4]{2}$i</td>
<td>$\sqrt[4]{2}$i</td>
<td>$\sqrt[4]{2}$i</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

$G(K/Q) \cong \langle a, b \mid a^4 = b^2 = 1, ba = a^{-1}b \rangle$.

We can illustrate the proof by taking $\alpha = i, p(x) = x^2 + 1$, $\alpha_1 = i, \alpha_2 = -i$.
We can take $\tau_1$ to be any of 1, $a$, $a^2$ or $a^3$ and $\tau_2$ can be any of the second four automorphisms in the above table. 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 $\theta_1 = 1$, $\theta_2 = a$, $\theta_3 = a^2$ and $\theta_4 = a^3$.
Then, for example, $\theta_0 \tau_2 = a^2 b$. By taking all $\theta_0 \tau_j$ we get all 8 elements of $G(K/F)$.

**Theorem 6:** If $K$ is a field then $\text{Aut}(K)$ is a linearly independent set over $K$.

**Proof:** Suppose $\text{Aut}(K)$ is linearly dependent.
Then for some $n$ there exist $\theta_1, ..., \theta_n \in \text{Aut}(K)$ and $\lambda_1, ..., \lambda_n \in K$, all of which are non-zero, such that $\lambda_1 \theta_1 + ... + \lambda_n \theta_n = 0$ ............ (1)
Choose such an equation for which $n$ is least. Clearly $n \geq 2$.
For all $x \in K$, $\lambda_1 x^{\theta_1} + \lambda_2 x^{\theta_2} + ... + \lambda_n x^{\theta_n} = 0$ ............ (2)
Since $\theta_1 \neq \theta_2$ there exists $y \in K$ such that $y^{\theta_1} \neq y^{\theta_2}$.
Replacing $x$ in (2) by $xy$ we get:
For all $x \in K$, $\lambda_1 x^{\theta_1} y^{\theta_1} + \lambda_2 x^{\theta_2} y^{\theta_2} + ... + \lambda_n x^{\theta_n} y^{\theta_n} = 0$ ............ (3)
But multiplying (2) by $y^{\theta_1}$ we get:
For all $x \in K$, $\lambda_1 x^{\theta_1} y^{\theta_1} + \lambda_2 x^{\theta_2} y^{\theta_1} + ... + \lambda_n x^{\theta_n} y^{\theta_1} = 0$ ............ (4)
Subtracting (4) from (3) we get:
For all $x \in K$, $\lambda_2 (y^{\theta_2} - y^{\theta_1}) x^{\theta_2} + ... + \lambda_n (y^{\theta_n} - y^{\theta_1}) x^{\theta_n} = 0$ ............ (5)
Hence $\lambda_2 (y^{\theta_2} - y^{\theta_1}) \theta_2 + ... + \lambda_n (y^{\theta_n} - y^{\theta_1}) \theta_n = 0$ ............ (6)
The coefficient of $\theta_2$ is non-zero. Removing any zero coefficients we get a shorter equation like (1), a contradiction.
Theorem 7: Suppose $H$ is a finite subgroup of $\text{Aut}(K)$ and let $F$ be the fixed field of $H$. Then $|K:F| \geq |H|$.  

**Proof:** Suppose $|K:F| = m$ and suppose $|H| = n$. 
Let $\alpha_1, ..., \alpha_m$ be a basis for $K$ over $F$ and let $H = \{0_1, ... 0_n\}$. 
Let $A = (\alpha_i^{0_j})$, an $m \times n$ matrix over $K$. 
Suppose $m < n$. Then the columns of $A$ are linearly dependent over $K$. 
Hence there exist $\lambda_i$'s in $K$, not all zero, such that: 
$$\sum_{j=1}^{n} \lambda_j (\alpha_i^{0_j}) = 0$$ for all $i$. 

Let $x \in K$. Then $x = \sum_{i=1}^{m} \mu_i \alpha_i$ for some $\mu_i \in F$. 

For all $j$, $x^{0_j} = \sum_{i=1}^{m} \mu_i^{0_j} \alpha_i^{0_j} = \sum_{i=1}^{m} \mu_i \alpha_i^{0_j}$. 

Hence $\sum_{j=1}^{n} \lambda_j x^{0_j} = \sum_{j=1}^{n} \sum_{i=1}^{m} \lambda_j \mu_i \alpha_i^{0_j} = \sum_{i=1}^{m} \mu_i \sum_{j=1}^{n} \lambda_j \alpha_i^{0_j} = 0$ for all $x \in K$. 

Thus $\sum_{j=1}^{n} \lambda_j 0_j = 0$, contradicting the fact that the $0_j$ are linearly independent.

Theorem 8: Suppose $K$ is a polynomial extension of $F$. Then $|K:F| = |G(K/F)|$ and $F$ is the fixed field of $G(K/F)$.  

**Proof:** $|G(K/F)| \leq |K:K_0| \leq |K:F|$ where $K_0$ is the fixed field of $G(K/F)$. 
But $|G(K/F)| \geq |K:F|$. 
Hence $|G(K/F)| = |K:F|$ and $K_0 = F$.  

116