Automorphism Groups for Simple Extensions

Theorem

Consider the simple field extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ with minimum polynomial $m_{\alpha,\mathbb{Q}}(x)$ and let $\varphi \in \mathrm{Aut}(\mathbb{Q}(\alpha)/\mathbb{Q})$:

1). φ is completely determined by $\varphi(\alpha)$

2). φ permutes the roots of $m_{\alpha,\mathbb{Q}}(x)$

Proof

Assume $f(x) \in \mathbb{Q}[x]$
$f(\alpha) = \sum_{k=1}^{n} c_k \alpha^k$, where $c_k \in \mathbb{Q}$
But φ fixes $\mathbb{Q}$, so $\varphi(c_k) = c_k$, and so:

$$\begin{aligned}
\varphi(f(\alpha)) &= \varphi\left(\sum_{k=1}^{n} c_k \alpha^k\right) \\
&= \sum_{k=1}^{n} \varphi(c_k \alpha^k) \\
&= \sum_{k=1}^{n} \varphi(c_k)\varphi(\alpha^k) \\
&= \sum_{k=1}^{n} c_k \varphi(\alpha)^k
\end{aligned}$$

Now, assume $y \in \mathbb{Q}(\alpha)$
$\exists\, f(x), g(x) \in \mathbb{Q}[x]$ such that $y = \frac{f(\alpha)}{g(\alpha)}$

$$\begin{aligned}
\varphi(y) &= \varphi\left(\frac{f(\alpha)}{g(\alpha)}\right) \\
&= \varphi\left(f(\alpha)g(\alpha)^{-1}\right) \\
&= \varphi(f(\alpha))\varphi(g(\alpha)^{-1}) \\
&= \varphi(f(\alpha))\varphi(g(\alpha))^{-1} \\
&= f(\varphi(\alpha))g(\varphi(\alpha)))^{-1} \\
&= \frac{f(\varphi(\alpha))}{g(\varphi(\alpha))}
\end{aligned}$$

Therefore, φ is completely determined by $\varphi(\alpha)$

Let $m(x) = m_{\alpha,\mathbb{Q}}(x)$
Assume α is a root of $m(x)$
$m(\alpha) = 0$
$\varphi(m(\alpha)) = m(\varphi(\alpha))$
But $\varphi(m(\alpha)) = \varphi(0) = 0$

So $m(\varphi(\alpha)) = 0$

Therefore $\varphi(\alpha)$ maps to some other (possibly the same) root of $m_{\alpha,\mathbb{Q}}(x)$.

Example

$\mathbb{C}/\mathbb{R} = \mathbb{R}[i]/\mathbb{R}$

$m_{i,\mathbb{R}}(x) = x^2 + 1$ with roots $\pm i$

$i \mapsto i$
$i \mapsto -i$

$\mathrm{Aut}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}, \bar{z}\}$ and $|\mathrm{Aut}(\mathbb{C}/\mathbb{R})| = 2$

Example

$\mathbb{Q}(\omega)/\mathbb{Q}$

$m_{\omega,\mathbb{Q}}(x) = x^3 - 1$ with roots $1, \omega, \omega^2$

Note that $1 \mapsto 1$ always
$\omega \mapsto \omega$
$\omega \mapsto \omega^2$

$\mathrm{Aut}(\mathbb{Q}(\omega)/\mathbb{Q}) = \{\mathrm{id}, \omega \mapsto \omega^2\} \cong \mathbb{Z}/(2)$

Example

$\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$

$m_{\sqrt[3]{2},\mathbb{Q}} = x^3 - 2$ with root $\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$

Thus, two of the roots are not in $\mathbb{Q}(\sqrt[3]{2})$ and thus $\mathbb{Q}(\sqrt[3]{2})$ is not a splitting field for $m_{\sqrt[3]{2},\mathbb{Q}}(x)$. Thus, the only possibility for φ is $\sqrt[3]{2} \mapsto \sqrt[3]{2}$.

$\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \mathrm{id}$ (trivial)

Example

$\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$

Now the extension is a splitting field and $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$ contains all possible permutations of the three roots, so:

$$\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}) \cong S_3$$

Example of a 3-cycle: $\sqrt[3]{2} \mapsto \omega\sqrt[3]{2} \mapsto \omega^2\sqrt[3]{2} \mapsto \sqrt[3]{2}$

Example of a 2-cycle: $\sqrt[3]{2}$ fixed, $\omega\sqrt[3]{2} \mapsto \omega^2\sqrt[3]{2} \mapsto \omega\sqrt[3]{2}$