Fixed Fields

Definition: Fixed Field

Let K/F be a field extension and let $H \leq \operatorname{Aut}(K/F)$. The *fixed field* of H, denoted $F(H)$, is given by:

$$F(H) = \{\alpha \in K \mid \forall\, \varphi \in H, \varphi(\alpha) = \alpha\}$$

$$\begin{array}{lllll}
K & \text{--------} & G(K) & \text{----} & F(\{\text{id}\}) = K \\
| & & \shortmid\!\cap & & \cup\!\shortmid \\
F & \text{--------} & G(F) & \text{----} & F(G(F)) \supseteq F
\end{array}$$

Example

Recall that for $K = \mathbb{Q}(\sqrt[3]{2})$ and $F = Q$, $G(F)$ is trivial because K is not a splitting field for $x^3 - 2$. Thus:

$$F(G(F)) = K \supset F$$

Definition

To say that a field extension K/F is *Galois* means:

$$F(G(F)) = F$$

There is no slippage - $G(F)$ only fixes F and nothing else.

Example: Quadratic Extensions

Let $[K : \mathbb{Q}] = 2$
Assume $\alpha \in K$:

$$m_{\alpha,\mathbb{Q}}(x) = x^2 + bx + c$$

for some $b, c \in \mathbb{Q}$.

$$x = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$$

If $\sqrt{b^2 - 4c} \in \mathbb{Q}$ then $[K : \mathbb{Q}] = 1$, so assume not.
Let $b = \frac{p}{q}$ and $c = \frac{h}{k}$ where $p, q, h, k \in \mathbb{Z}$ and $q, k \neq 0$:

$$\begin{aligned}
x &= \frac{-\frac{p}{q} \pm \sqrt{\left(\frac{p}{q}\right)^2 - \frac{4h}{k}}}{2} \\
&= -\frac{p}{2q} \pm \frac{1}{2}\sqrt{\frac{p^2k - 4qh}{q^2k}} \\
&= -\frac{p}{2q} \pm \frac{1}{2q^2k}\sqrt{q^2k(p^2k - 4qh)}
\end{aligned}$$

Note that $q^2k(p^2k - 4qh) \in \mathbb{Z}$, so factor out any perfect square part, calling it n^2, and whatever squarefree integer is left call it d:

$$x = -\frac{p}{2q} \pm \frac{1}{2q^2k}\sqrt{n^2d} = -\frac{p}{2q} \pm \frac{n}{2q^2k}\sqrt{d}$$

Now let $r = -\frac{p}{2q} \in \mathbb{Q}$ and $s = \frac{n}{2q^2k} \in \mathbb{Q}$:

$$x = r \pm s\sqrt{d}$$

And so $K = \mathbb{Q}(\sqrt{d})$

Now assume $\varphi \in G(\mathbb{Q})$
Since φ is a ring homomorphism that fixes $\mathbb{Q}$:

$$\varphi(x) = \phi(r \pm s\sqrt{d}) = \phi(r) \pm \phi(s\sqrt{d}) = r \pm \phi(s)\phi(\sqrt{d}) = r \pm s\phi(\sqrt{d})$$

And so φ is completely determined by what it does to $\sqrt{d}$.

Thus, there are only two $\mathbb{Q}$-automorphisms:

1). id
2). $\sqrt{d} \mapsto -\sqrt{d}$

In other words, the identity and a two-cycle.

Therefore, $\mathrm{Aut}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$

Also note that since φ only moves $\pm\sqrt{d}$:

$$F(G(\mathbb{Q})) = \mathbb{Q}$$

Thus, there there are no proper subfields of L such that $\mathbb{Q} \subset L \subset \mathbb{Q}(\sqrt{d})$.