Automorphism Groups

Definition: Automorphism

Given a field extension K/F, to say that φ is an *F-automorphism* of K/F means that $\varphi : K \to K$ is a bijective ring homomorphism such that $\forall\, \alpha \in F, \varphi(\alpha) = \alpha$.

In other words, φ fixes (acts trivially on) F — it may fix more that F, but at least F is guaranteed.

Theorem

Let $G = G(F) = \mathrm{Aut}(K/F)$ be the set of F-automorphisms of K/F:

G is a group under the operation of function composition.

Proof

Assume $\varphi_1, \varphi_2 \in G$
Assume $\alpha \in F$
$\varphi_1(\alpha) = \alpha$ and $\varphi_2(\alpha) = \alpha$
$(\varphi_1\varphi_2)(\alpha) = \varphi_1(\varphi_2(\alpha)) = \varphi_1(\alpha) = \alpha$
So $\varphi_1\varphi_2 \in G$

Therefore G is closed under the operation.

Function composition is associative.

Assume $\varphi \in G$ and $\alpha \in F$
$\iota_K(\alpha) = \alpha$, so $\iota_K \in G$
$\iota_K\varphi = \varphi\iota_K = \varphi$

Therefore G has identity ι_K.

Assume $\varphi \in G$ and $\alpha \in F$
$\varphi(\alpha) = \alpha$
φ is bijective, so φ^{-1} exists
$\varphi^{-1}(\alpha) = \varphi^{-1}(\varphi(\alpha)) = (\varphi^{-1}\varphi)(\alpha) = \iota_K(\alpha) = \alpha$
So $\varphi^{-1} \in G$

Therefore G is closed under inverses.

Therefore G is a group under the operation of function composition.

Theorem

Let $F \subseteq L \subseteq K$ be an inclusion of fields:

$$G(L) = \mathrm{Aut}(K/L) \leq \mathrm{Aut}(K/F) = G(F)$$

Proof

Assume $\alpha \in L$
$\iota_L(\alpha) = \alpha$
$\iota_L \in G(L)$

$\therefore G(L) \neq \emptyset$

Assume $\varphi \in G(L)$
Assume $\alpha \in F$, and thus $\alpha \in L$
$\varphi(\alpha) = \alpha$, so $\varphi \in G(F)$

$\therefore G(L) \subseteq G(F)$

Assume $\varphi_1, \varphi_2 \in G(L)$
Assume $\alpha \in L$

$$\begin{aligned}
(\varphi_1\varphi_2^{-1})(\alpha) &= \varphi_1(\varphi_2^{-1}(\alpha)) \\
&= \varphi_1(\varphi_2^{-1}(\varphi_2(\alpha))) \\
&= \varphi_1((\varphi_2^{-1}\varphi_2)(\alpha))) \\
&= \varphi_1(\iota_L(\alpha)) \\
&= \varphi_1(\alpha) \\
&= \alpha
\end{aligned}$$

So $\varphi_1\varphi^{-1} \in G(L)$

Therefore, by the subgroup test, $G(L) \leq G(F)$.

The result is a so-called “reverse inclusion”:

$$\begin{tikzcd}[arrows=-]
K \arrow[r, dashed] \arrow[d] & G(K) = \mathrm{Aut}(K/K) = \{\mathrm{id}\} \arrow[d, phantom, sloped, "\supseteq"] \\
L \arrow[r, dashed] \arrow[d] & G(L) = \mathrm{Aut}(K/L) \arrow[d, phantom, sloped, "\supseteq"] \\
F \arrow[r, dashed] & G(F) = \mathrm{Aut}(K/F)
\end{tikzcd}$$

Note that the larger the field, the smaller the group. This makes sense because if there are more group elements then the number of automorphisms that fix all of the group elements is less.