1 Group Actions and Fixed Fields

Let us consider a Galois extension K/F with Galois group $G = \mathrm{Gal}(K/F)$. The fundamental theorem of Galois theory establishes a one-to-one correspondence between intermediate fields E (with $F \subseteq E \subseteq K$) and subgroups $H \leq G$. This correspondence is given by:

$$E \mapsto \mathrm{Gal}(K/E) \quad \text{and} \quad H \mapsto K^H,$$

where $K^H = \{x \in K \mid \sigma(x) = x \ \forall \sigma \in H\}$ denotes the fixed field of H.

1.1 The Galois Correspondence for Normal Subgroups

Suppose $H \trianglelefteq G$ is a normal subgroup. Then the fixed field $E = K^H$ is a Galois extension of F, and we have:

$$\mathrm{Gal}(E/F) \cong G/H.$$

This isomorphism is natural and reflects the fact that the quotient group G/H acts faithfully on E.

1.2 A Key Lemma on Group Actions

We now prove an important lemma concerning the action of G on K.

Lemma 1 *Let G act on K, and let $H \leq G$. For any $a \in K$, the following are equivalent:*

1. *$a \in K^H$, i.e., $h(a) = a$ for all $h \in H$.*
2. *The orbit $G \cdot a$ is contained in K^H.*

We prove both directions.

(1) $\Rightarrow$ (2)**:** Assume $a \in K^H$. Let $g \in G$ and $h \in H$. Since H is normal in G (in the context of Galois extensions, though the lemma holds more generally), we have $hg = gh'$ for some $h' \in H$. Then:

$$h(g(a)) = (hg)(a) = (gh')(a) = g(h'(a)) = g(a),$$

since $h'(a) = a$. Thus $g(a) \in K^H$ for all $g \in G$, so $G \cdot a \subseteq K^H$.

(2) $\Rightarrow$ (1)**:** Assume $G \cdot a \subseteq K^H$. In particular, taking $g = e$ (the identity), we have $a \in K^H$. More formally, for any $h \in H$, $h(a) \in G \cdot a \subseteq K^H$, so $h(a)$ is fixed by all elements of H. But then $h(a) = h'(h(a))$ for all $h' \in H$, which implies $a = h(a)$ by applying h^{-1}. Hence $a \in K^H$.

1.3 An Application to Field Elements

Let us apply this lemma in the context of Galois theory. Suppose K/F is Galois with group G, and $H \trianglelefteq G$. Let $E = K^H$. For any $a \in K$, consider the following:

Since $H \trianglelefteq G$, for any $g \in G$ and $h \in H$, there exists $h' \in H$ such that $gh = h'g$. Then:

$$h(g(a)) = (hg)(a) = (h'g)(a) = h'(g(a)).$$

If $g(a) \in E$, then $h'(g(a)) = g(a)$, so $h(g(a)) = g(a)$. This shows that $g(a)$ is fixed by H, hence $g(a) \in E$. Therefore, G permutes the elements of E.

Moreover, if $a \in E$, then for any $g \in G$, we have $g(a) \in E$ as above. This implies that the minimal polynomial of a over F splits completely in E, which is consistent with E/F being Galois.

1.4 Conclusion

The interplay between group actions and field theory is fundamental in Galois theory. The lemma proved above illustrates how the structure of the Galois group G and its subgroups controls the behavior of field elements under automorphisms. This leads to the powerful correspondence between intermediate fields and subgroups, which is the cornerstone of Galois theory.