The Final Piece

**Theorem 0.1** Let $F \subset K$ be subfields of $C$ with $K$ a normal extension of $F$ and $G = \Gamma(K : F)$. Let $H$ be a subgroup of $G$, set $L = H^+$ and $H^+ = L^*$. Then $H = H^+$.

Set $[K : L] = r$. Let $|H| = s$. By the Single Generator Theorem write $K = L(\gamma)$. We already know $H \subset H^+$ and that $|H^+| = r$. Thus $s \leq r$. We shall show $r \leq s$.

Set $f(x) = \prod_{\sigma \in H} (x - \sigma(\gamma))$ (1)

Write $f(x) = x^s + \sum_{i=1}^{s} a_i x^{s-i}$ (2)

We shall show that all $a_i \in L$.

We take $a_2$ as an illustrative example. We multiply out so that

$$a_2 = \sum_{\rho, \theta} \rho(\gamma)\theta(\gamma)$$ (3)

where $\rho, \theta$ run over all unordered pairs of elements of $H$. Let $\sigma \in H$. Then

$$\sigma(a_2) = \sigma \left[ \sum_{\rho, \theta} \rho(\gamma)\theta(\gamma) \right] = \sum_{\rho, \theta} (\rho \sigma)(\gamma)(\theta \sigma)(\gamma)$$ (4)

As $\rho, \theta$ range over unordered pairs of elements of $H$, so do $\rho \sigma, \theta \sigma$. Why? They both have the same size and for any $\rho, \theta$, $\{ (\rho \sigma^{-1}) \sigma, (\theta \sigma^{-1}) \sigma \}$ is equal to $\{ \rho, \theta \}$. Thus (4) gives that $\sigma(a_2) = a_2$. This holds for all $\sigma \in H$. Therefore $a_2 \in H^+ = L$.

The general case is similar. For $1 \leq u \leq s$ we can write

$$a_u = (-1)^u \sum_{X} \prod_{\rho \in X} \rho(\gamma)$$ (5)

where $X$ ranges over all the subsets of $H$ of size $u$. Let $\sigma \in H$. Then

$$\sigma(a_u) = \sigma \left[ (-1)^u \sum_{X} \prod_{\rho \in X} \rho(\gamma) \right] = (-1)^u \sum_{X} \prod_{\rho \in X} (\rho \sigma)(\gamma)$$ (6)
Let us define $X\sigma$ as the set of $\rho\sigma, \rho \in X$. Then

$$\sigma(a_u) = (-1)^u \sum_{X} \prod_{\eta \in X\sigma} \eta(\gamma)$$

(7)

As in the $u = 2$ case, as $X$ ranges over all the subsets of $H$ of size $u$ so does $X\sigma$ so that $\sigma(a_u) = a_u$.

We have shown that all $a_u \in L$ so that $f(x) \in L[x]$ so that $\gamma = e(\gamma)$ satisfies a polynomial in $L[x]$ of degree $s$. But $K = L(\gamma)$ so $r = [K : L]$ is the degree of the minimal polynomial $g(x) \in L[x]$ satisfied by $\gamma$. Hence $r \leq s$.

Hence $r = s$. Hence for any $H^-$, setting $L = (H^-)^\dagger, L^* = H^-$. Hence the Galois Correspondence Theorem has been proven.