Toward the Galois Extension Theorem

OK, lets see where we are. We have a map $\ast$ from fields to groups and a map $\dagger$ from groups to fields (more precisely, intermediate fields $L, F \subseteq L \subseteq K$, and subgroups $H \subseteq G$. We know that if we apply $\ast$ and then $\dagger$ we get back to the same $L$. This gives a bijection between intermediate fields $L$ and subgroups $H$ which may be expressed as $H = L^\ast$ though, a priori, there may be $H$ that are not of that form.

Now we look at the size relationship in the Galois Correspondence Theorem. We make strong use of the Single Generator Theorem.

**Theorem 0.1** Let $K$ be a normal extension of $F$ and let $L$ be an intermediate field. Set $r = [K : L]$ Then $L^\ast$ consists of precisely $r$ automorphisms.

**Proof:** We know from the Middle Normal Theorem that $K$ is a normal extension of $L$, which will allow us basically to ignore $F$. From the Single Generator Theorem write $K = L(\alpha)$. Let $p(x)$ be the minimal polynomial in $L[x]$ with $\alpha$ as a root so that $p(x)$ has degree $r$. In $C$ let $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_r$ denote the roots of $p(x)$. As $K : L$ is normal, $\alpha_1, \ldots, \alpha_r \in K$. As $[L(\alpha_i) : L] = r$ we must have all $L(\alpha_i) = K$. For each $1 \leq i \leq r$ as $\alpha, \alpha_i$ have the same minimal polynomial in $L[x]$ there is an isomorphism $\sigma_i : L(\alpha) \rightarrow L(\alpha_i)$ given by setting $\sigma_i(\alpha) = \alpha_i$. These are automorphisms of $K$ fixing $L$, so elements of $L^\ast$. Conversely $\sigma \in L^\ast$ is determined by $\sigma(\alpha)$ and $\sigma(\alpha)$ must also satisfy $p(x)$ and so must be one of $\alpha_1, \ldots, \alpha_r$ and so $\sigma_1, \ldots, \sigma_r$ are all of the automorphisms in $L^\ast$.

**Example:** Take $K = Q(\sqrt{2}, \sqrt{3})$. The Single Generator Theorem works and we can see $K = Q(\sqrt{2} + \sqrt{3})$. This is not certain a priori, one must check that $\sqrt{2} + \sqrt{3}$ does indeed generate $K$ which takes some linear algebra. Setting $\gamma = \sqrt{2} + \sqrt{3}$ we check that $1, \gamma, \gamma^2 = 5 + 2\sqrt{6}, \gamma^3 = 11\sqrt{2} + 9\sqrt{3}$ are indeed linearly independent. Now set, for example, $\overline{\gamma} = \sqrt{2} - \sqrt{3}$ and we want a $\sigma \in \Gamma(K : Q)$ with $\sigma(\gamma) = \overline{\gamma}$. Then $\sigma(\gamma^2) = \sigma(5 + 2\sqrt{6}) = \overline{\gamma}^2 = 5 - 2\sqrt{6}$ and $\sigma(\gamma^3) = \sigma(9 + 11\sqrt{6}) = \overline{\gamma}^3 = 11\sqrt{2} - 9\sqrt{3}$. $\sigma$ is a linear transformation from $K$ to itself. From $\sigma(\gamma^2) = \overline{\gamma}^2$ we deduce $\sigma(\sqrt{6}) = -\sqrt{6}$. Further $\gamma^3 - 9\gamma = 2\sqrt{2}$ and so $\sigma(2\sqrt{2}) = \overline{\gamma}^3 - 9\overline{\gamma} = 2\sqrt{2}$. Thus we must have $\sigma(\sqrt{2}) = \sqrt{2}$ and, finally, $\sigma(\sqrt{3}) = \sigma(\sqrt{6})/\sigma(\sqrt{2}) = -\sqrt{3}$. That is, $\sigma$ is one of the four automorphisms we knew we had.

Now we have shown the size relationship in the Galois Correspondence Theorem. The only item left is to show that the correspondence between $L$ and $L^\ast$ gives us all of the subgroups $H$. This will take an interesting side detour.