Fields to Groups and Back Again II

Let us fix some finite extension $F \subset K$ of subfields of $C$ and set $G$ to be the Galois Group $\Gamma(K : F)$. However, we now assume $K$ is a Normal Extension of $F$. Recall that we have already defined the map * from intermediate fields to subgroups and the map † from subgroups to intermediate fields.

**Theorem 0.1** Let $F \subset K$ be subfields of $C$ with $K$ a Normal extension of $F$ and set $G$ to be the Galois Group $\Gamma(K : F)$. Then for any intermediate field $L$

\[(L^*)\dagger = L\]  \hspace{1cm} (1)

**Proof:** We already know $L \subset (L^*)\dagger$. Now suppose $\beta \in K$ and $\beta \notin L$. Our goal is to show $\beta \notin (L^*)\dagger$. Recall that as $K$ is a normal extension of $F$, $K$ is a normal extension of $L$.

Let $p(x)$ be the minimal polynomial for $\beta \in L[x]$ and let $\beta_1$ be another root of $p(x)$. As $K$ is a normal extension of $L$, $\beta_1 \in K$. Thus there is an isomorphism $\sigma : L(\beta) \to L(\beta_1)$ which fixed $L$ and has $\sigma(\beta) = \beta_1$. Applying the Full Isomorphism Extension Theorem we extend $\sigma$ to an isomorphism $\sigma^{++}$ with domain $K$. But as $\sigma^{++}$ fixes $L$ and $K$ is normal over $L$, the range of $\sigma^{++}$ must be $K$. That is, $\sigma^{++}$ is an automorphism of $K$ which fixes all $\alpha \in L$ but does not fix $\beta$. So $\beta \notin (L^*)\dagger$. End of Proof.

This has a perhaps surprising followup.

**Theorem 0.2** Let $F \subset K$ be subfields of $C$ with $K$ a normal extension of $F$. Then there are only finitely many intermediate fields $L$.

**Proof:** From Theorem 0.2, $L$ is determined by $L^*$ but as $G = \Gamma(K : F)$ is finite there can be only finitely many subgroups $H$, only finitely many possible $L^*$.

**Theorem 0.3** Let $K$ be a finite extension of $F$, both subfields of $C$. Then there are only finitely many intermediate fields $L$.

**Proof:** Extend $K$ to $K^+$ so that $K^+$ is a normal extension of $F$. From Theorem 0.2 there are only finitely many intermediate fields between $F$ and $K^+$ and thus only finitely many intermediate fields between $F$ and the smaller $K$. 

1
**Theorem 0.4** Let $F$ be a subfield of $C$ and $\alpha, \beta \in C$, both algebraic over $F$. Then there exists $\gamma \in C$ with

$$F(\gamma) = F(\alpha, \beta)$$

**Proof:** As $\alpha, \beta$ are algebraic over $F$, $F(\alpha, \beta)$ is a finite extension of $F$. Now for each integer $i$ set $F_i = F(\alpha + i\beta)$. Each of these are subfields of $F(\alpha, \beta)$ but by Theorem 0.3 there are only finitely many such subfields so there must be $i \neq j$ with $F_i = F_j$. Thus $F_i$ contains $\alpha + i\beta$ and $\alpha + j\beta$. But then it contains $\alpha = \frac{1}{j-i}(\alpha + i\beta) - i(\alpha + j\beta)$ and $\beta = \frac{1}{j-i}((\alpha + j\beta) - (\alpha + i\beta))$. Thus $F_i$ must be all of $F(\alpha, \beta)$ and so we can take $\gamma = \alpha + i\beta$.

**Theorem 0.5** Single Generator Theorem. Let $K$ be a finite extension of $F$, both subfields of $C$. Then there is an element $\gamma \in K$ such that $K = F(\gamma)$.

**Proof:** We claim that for any $\alpha_1, \ldots, \alpha_r \in C$, all algebraic over $F$, there exists a $\gamma \in C$ with $F(\gamma) = F(\alpha_1, \ldots, \alpha_r)$. This comes from repeatedly applying Theorem 0.4 to replace two of the generators by one. (Formally we apply induction on $r$.) Now as $K$ is a finite extension of $F$ we can write $K = F(\alpha_1, \ldots, \alpha_r)$ for some finite set of $\alpha$’s and then replace them by a single $\gamma$. 
