Math 306: Main Theorems of Galois Theory

Here are the main theorems we will encounter on the way to proving the Fundamental Theorem of Galois Theory. If a theorem can be found in our book, its number is given in parentheses.

Theorem 1: Let $i\colon K \to K'$ be an isomorphism. Suppose that m_α and m_β are minimal polynomials for α over K and β over K', respectively, and that $m_\beta = i(m_\alpha)$. Then there is an isomorphism $j\colon K(\alpha) \to K'(\beta)$ with $j(\alpha) = \beta$.

Theorem 2 (5.13): There is a K-isomorphism $i\colon K(\alpha) \to K(\beta)$ if α and β are roots of the same minimal polynomial $f \in K[x]$.

Theorem 3 (9.5): Let $i\colon K \to K'$ be an isomorphism. Suppose that $f \in K[x]$ and Σ is the splitting field for f. If $K' \to L$ is a monomorphism such that $i(f)$ splits in $L[x]$, then there is a monomorphism $j\colon \Sigma \to L$ such that $j|_K = i$.

Theorem 4 (9.6): Let $i\colon K \to K'$ be an isomorphism. Suppose that Σ is a splitting field for $f \in K[x]$ and Σ' a splitting field for $i(f) \in K'[x]$. Then there is an isomorphism $j\colon \Sigma \to \Sigma'$ such that $j|_K = i$.

Theorem 5 (9.9): A finite extension $L\colon K$ is normal iff it is a splitting field for some $f \in K[x]$.

Theorem 6 (11.3): Let $L\colon K$ be finite and normal with $K \subseteq M \subseteq L$. If $\tau \in \mathrm{Mon}_K(M, L)$, then there is $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma|_M = \tau$.

Theorem 7 (11.4): If $L\colon K$ is finite and normal, and if α and β are zeros in L of the same irreducible polynomial $p \in K[x]$, then there is $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(\alpha) = \beta$.

Theorem 8: Let $L\colon K$ be finite and normal, and let α and β be zeros in L of the same irreducible polynomial $f \in K[x]$, giving an isomorphism $\tau\colon K(\alpha) \to K(\beta)$ with $\tau(\alpha) = \beta$. Suppose that $g \in K(\alpha)[x]$ is irreducible with root γ and $\tau_*(g) \in K(\beta)[x]$ has root β. Then there is $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(\alpha) = \beta$ and $\sigma(\gamma) = \delta$.

Theorem 9: Suppose that α is algebraic over K and that $K(\alpha)\colon K$ is normal. If $f \in K[x]$ is the minimum polynomial for α and β is a root of f, then there is a unique $\sigma \in \mathrm{Gal}(K(\alpha)/K)$ such that $\sigma(\alpha) = \beta$.

Theorem 10 (10.1): Every set of distinct monomorphisms $K \to L$ is linearly independent over L.

Theorem 11 (10.6): If H is a subgroup of $\mathrm{Gal}(L/K)$ and $|H| < \infty$, then $[L\colon H^\dagger] = |H|$.

Theorem 12 (11.6): If $L\colon K$ is finite, then the normal closure of $L\colon K$ is unique up to isomorphism.

Theorem 13 (11.9): Let $L\colon K$ be finite. The following are equivalent:

1. $L\colon K$ is normal;
2. There is a normal $N\colon K$ with $N \supset L$ such that every K-monomorphism $\tau\colon L \to N$ is a K-automorphism of L;
3. For every $M\colon K$ with $M \supset L$, every K-monomorphism $\tau\colon L \to M$ is a K-automorphism of L.

Theorem 14 (11.10): Let $L\colon K$ be a finite separable extension. Then there are precisely n distinct K-monomorphisms of L into a normal closure N, where $n = [L\colon K]$.

Theorem 15 (11.11): Let $L\colon K$ be separable and normal with $[L\colon K] = n$. Then $|\mathsf{Gal}(L/K)| = n$.

Theorem 16 (11.12): Let $L\colon K$ be finite of degree n. If $L\colon K$ is normal and separable, then $K = G^\dagger$, where $G = \mathsf{Gal}(L/K)$.

Theorem 17 (11.13): Suppose that $K \subseteq L \subseteq M$, where $M\colon K$ is finite. If $[L\colon K] = n$, then the number of K-monomorphisms from L to M is at most n.

Theorem 18 (11.14): If $L\colon K$ is finite and $G = \mathsf{Gal}(L/K)$ with $G^\dagger = K$, then $L\colon K$ is normal and separable.

Theorem 19 (12.1) – Fundamental Theorem of Galois Theory: Let $[L\colon K] = n$, separable and normal. Recall that $* : \mathcal{F} \to \mathcal{G}$. Then

1. $|\mathsf{Gal}(L/K)| = n$
2. $*$ and $\dagger$ are inverses (this is the *Galois correspondence*)
3. If $K \subseteq M \subseteq L$, then $[L\colon M] = |M^*|$ and $[M\colon K] = |G|/|M^*|$
4. $M\colon K$ is normal iff M^* is normal in G
5. If $M\colon K$ is normal, then $\mathsf{Gal}(M/K) \cong G/M^*$