The fundamental theorem of Galois theory

Definition 1. A polynomial in $K[X]$ (K a field) is *separable* if it has no multiple roots in any field containing K. An algebraic field extension L/K is separable if every $\alpha \in L$ is separable over K, i.e., its minimal polynomial $m_\alpha(X) \in K[X]$ is separable.

Definition 2. (a) For a field extension L/K, $\mathrm{Aut}_K L$ is the group of K-automorphisms of L.

(b) For any subset $\mathcal{H} \subset \mathrm{Aut}_K L$, the *fixed field of* $\mathcal{H}$ is the field

$$L^{\mathcal{H}} := \{\, x \in L \mid hx = x \text{ for all } h \in \mathcal{H} \,\}.$$

Remark. Suppose L/K finite. Writing $L = K[\alpha_1, \dots, \alpha_n]$, and noting that any K-automorphism of L is determined by what it does to the α's (each of which must be taken to a root of its minimal equation over K), we see that $\mathrm{Aut}_K L$ is finite.

Proposition-Definition. *For a finite field extension L/K, and $\mathcal{G} := \mathrm{Aut}_K L$, the following conditions are equivalent—and when they hold we say that L/K is a* galois extension*, with galois group $\mathcal{G}$.*

1. *L/K is normal and separable.*
2. *L is the splitting field of a separable polynomial $f \in K[X]$.*
3. $|\mathcal{G}| = [L : K]$.

$3'$. $|\mathcal{G}| \geq [L : K]$.

4. *K is the fixed field of $\mathcal{G}$.*

Proof. $1 \Leftrightarrow 2$. Assume 1. Then L, being normal, is, by definition, the splitting field of a polynomial in $K[X]$ which has no multiple factors over K, and hence is separable (since L/K is). Conversely, if 2 holds then L is normal and $L = K[\alpha_1, \dots, \alpha_n]$ with each α_i the root of the separable polynomial f, whence, by a previous result, L/K is separable.

$1 \Rightarrow 4$. Assume 1. Obviously $K \subset L^{\mathcal{G}}$, and so it will suffice to show that every $\beta \notin K$ is moved by some K-automorphism θ of L. The minimal polynomial g of β is separable, of degree ≥ 2, so there exists a root $\beta_1 \neq \beta$ of g, and a K-automorphism $\theta_1 \colon K(\beta) \xrightarrow{\sim} K(\beta_1)$ with $\theta_1\beta = \beta_1$. Since L is a splitting field of f over both $K(\beta)$ and $K(\beta_1)$, therefore (as in the proof of uniqueness of splitting fields) θ_1 extends to a θ with the desired properties.

The implication $4 \Rightarrow 1$ follows from the next Lemma, as does the implication $4 \Rightarrow 3$. As $3 \Rightarrow 3'$ is trivial, it remains to show $3' \Rightarrow 4$. But that also follows from the Lemma, which gives $[L : K] \geq [L : L^{\mathcal{G}}] = |\mathcal{G}|$, so that $|\mathcal{G}| \geq [L : K] \Rightarrow K = L^{\mathcal{G}}$.

Lemma. *For any finite group of automorphisms $\mathcal{H}$ of L, $L/L^{\mathcal{H}}$ is normal and separable, of degree $|\mathcal{H}|$. Moreover $\mathcal{H} = \mathrm{Aut}_{L^{\mathcal{H}}} L$.*

Proof. For any $\alpha \in L$, let $\alpha = \alpha_1, \alpha_2, \dots, \alpha_{n_\alpha}$ be the $\mathcal{H}$-orbit of α. Then α is a root of the separable polynomial $g_\alpha(X) = \prod_i (X - \alpha_i) \in L^{\mathcal{H}}[X]$; and so $L/L^{\mathcal{H}}$ is separable algebraic. Moreover, any α_i is a root of the minimal polynomial of α over $L^{\mathcal{H}}$. Therefore g_α is that minimal polynomial, and $[L^{\mathcal{H}}(\alpha) : L^{\mathcal{H}}] = n_\alpha$.

Any field F with $L^{\mathcal{H}} \subset F \subset L$ and $[F : L^{\mathcal{H}}] < \infty$ has a primitive element β, and then $[F : L^{\mathcal{H}}] = n_\beta \leq |\mathcal{H}|$. Hence $L/L^{\mathcal{H}}$ has finite degree, otherwise there'd be F's of arbitrarily large degree over $L^{\mathcal{H}}$. So $L/L^{\mathcal{H}}$ has a primitive element—call it α—and then $L/L^{\mathcal{H}}$ is the splitting field of the separable polynomial g_α, so that $L/L^{\mathcal{H}}$ is normal as well as separable.

Clearly, any $\theta \in \mathrm{Aut}_{L^{\mathcal{H}}} L$ is determined by $\theta(\alpha)$, which is a root of g_α, so equal to $\phi(\alpha)$ for some $\phi \in \mathcal{H}$. Thus $\mathrm{Aut}_{L^{\mathcal{H}}} L$ is contained in, hence equal to, $\mathcal{H}$. Furthermore, $\phi \mapsto \phi(\alpha)$ is a bijection from $\mathcal{H}$ onto the orbit of α. So $|\mathcal{H}| = n_\alpha = [L : L^{\mathcal{H}}]$. $\square$

Corollary. *Let $L \supset F \supset K$ be fields, with L/K galois. Then:*

(i) *L/F is galois.*

(ii) *F/K is galois iff $gF = F$ for every $g \in \mathrm{Aut}_K L$; in other words, a subfield of L/K is normal over K iff it is equal to all its conjugates. When F/K is galois, restriction of automorphisms gives rise to an isomorphism*

$$\mathrm{Aut}_K L/\mathrm{Aut}_F L \xrightarrow{\sim} \mathrm{Aut}_K F.$$

Proof. (i) This is immediate from 2 of the Proposition.

(ii) If F/K is galois, then for every α in F, F contains all the roots in L of the minimal polynomial of α over K; and since $g\alpha$ must be such a root for any $g \in \mathrm{Aut}_K L$, therefore $g\alpha \in F$. Thus $gF \subset F$ for all g; and since, clearly, $[gF : K] = [F : K]$, therefore $gF = F$.

Suppose now that $gF = F$ for every g. Then the group homomorphism $\mathrm{Aut}_K L \to \mathrm{Aut}_K F$ given by restriction is *surjective* (see the proof of the theorem on uniqueness of splitting fields), whence the last assertion. It follows from this surjectivity that the fixed field K of $\mathrm{Aut}_K L$ is also the fixed field of $\mathrm{Aut}_K F$, so that F/K is galois.

Theorem. (Fundamental theorem of Galois Theory). *Let L/K be a galois extension, with galois group $\mathcal{G} := \mathrm{Aut}_K L$.*

To each subfield F of L/K (= field between K and L) associate the group $\mathcal{G}_F := \mathrm{Aut}_F L$; and to each subgroup $\mathcal{H} < \mathcal{G}$ associate the fixed field $L^{\mathcal{H}}$. Then:

(a) *These associations are inverse inclusion-reversing bijections between the set of subfields of L/K and the set of subgroups of $\mathcal{G}$.*

(b) *If $F \subset F'$ are subfields of L/K, then*

$$[F' : F] = [\mathcal{G}_F : \mathcal{G}'_F].$$

If $\mathcal{H}' < \mathcal{H} < \mathcal{G}$ are subgroups, then

$$[\mathcal{H} : \mathcal{H}'] = [L^{\mathcal{H}'} : L^{\mathcal{H}}].$$

(c) *If F is a subfield of L/K and $g \in \mathcal{G}$ then gF is a subfield of L/K and*

$$\mathcal{G}_{gF} = g\mathcal{G}_F g^{-1}.$$

If $\mathcal{H} < \mathcal{G}$ then

$$L^{g\mathcal{H}g^{-1}} = gL^{\mathcal{H}}.$$

In other words, "conjugate subfields" correspond to conjugate subgroups.

(d) *A subfield F of L/K is normal—hence galois—over K iff $\mathcal{G}_F$ is a normal subgroup of $\mathcal{G}$.*

Proof. (a) follows from 4 of the Proposition and from the Lemma (last part).

To prove the first part of (b), apply 3 of the Proposition to the galois extensions L/F and L/F' (see Corollary) to get

$$[F' : F] = [L : F]/[L : F'] = |\mathcal{G}_F|/|\mathcal{G}_{F'}| = [\mathcal{G}_F : \mathcal{G}_{F'}];$$

and using (a), deduce the second part by setting $F = L^{\mathcal{H}}$ and $F' = L^{\mathcal{H}'}$.

For the first part of (c), just note that $h \in g\mathcal{G}_F g^{-1} \iff g^{-1}hgx = x$ for all $x \in F \iff hy = y$ for all $y = gx \in gF$. The second part can easily be checked directly, or, using (a), deduced from the first part by setting $F = L^{\mathcal{H}}$.

Finally, (d) follows from (c) and the Corollary, because a normal subgroup is one equal to all its conjugates.