MAIN THEOREM OF GALOIS THEORY

Theorem 1. *[Main Theorem] Let L/K be a finite Galois extension.*

(1) The group $G = Gal(L/K)$ is a group of order $[L : K]$.

(2) The maps

$$f : \{\text{subgroups of } G\} \to \{\text{subfields of } L \text{ containing } K\}$$

and

$$g : \{\text{subfields of } L \text{ containing } K\} \to \{\text{subgroups of } G\}$$

defined by

$$f(H) = L^H = \{x \in L \mid h(x) = x \ \forall h \in H\}$$

and

$$g(E) = G_E = \{g \in G \mid g(x) = x \ \forall x \in E\}$$

are mutually inverse bijections.

(3) If $L \supset E \supset K$ then $[L : E] = |G_E|$ and $[E : K] = [G : G_E]$.

(4) Moreover, E/K is a normal extension if and only if G_E is a normal subgroup of G. In that case, every element of G preserves the subfield E, and the restriction map

$$r : G \to Gal(E/K); \;\; r(g)(x) = g(x) \;\; \forall x \in E$$

defines an isomorphism

$$G/G_E \xrightarrow{\sim} Gal(E/K).$$

Theorem **??** corresponds to Theorem 84 of Rotman's book.

Outline of the proof

The theorem is proved in a series of propositions.

Proposition 2. *Let L/K be an extension of degree d, U/K any extension, $\Sigma = \{\sigma : L \to U \mid \sigma(x) = x \ \forall x \in K\}$. Then $|\Sigma| \leq d$.*

Corollary 3. *Under the hypotheses of Proposition* **??***, suppose U is a finite Galois extension. Suppose moreover that, for any $x \in L$, the minimal polynomial of x in $K[X]$ has a root in U. Then $|\Sigma| = d$.*

This corresponds roughly to Theorem 51 of Rotman's book.

Proposition 4. *Let L be any field, $G \subset Aut(L)$ a finite group of automorphisms with d elements. Let $K = L^G = \{x \in L \mid g(x) = x \, \forall g \in G\}$. Then L/K is a Galois extension and $[L : K] = d$.*

This corresponds to Theorem 79 of Rotman's book.

First we show how these three steps imply Theorem **??**, then we sketch the main steps in the proofs of the propositions.

- To prove (1) of Theorem **??**, we take $L = U$ in Corollary **??**. Then Σ is the group $Gal(L/K)$.
- We check first that $L^G = K$ in (2) of Theorem **??**. Say $K_0 = L^G$. It follows from the definitions that $L \supset K_0 \supset K$. But $[L : K_0] = |G|$ by Proposition **??**, and $[L : K] = |G|$ by Theorem **??** (1). It follows from the degree formula

$$L \supset E \supset K \Rightarrow [L : K] = [L : E][E : K] \tag{5}$$

  (applied to $E = K_0$) that $K_0 = K$.

  More generally, if $L \supset E \supset K$, L/E is Galois. Any element of $Aut(L)$ that fixes E necessarily fixes K, so $G_E = Gal(L/E)$. It then follows from the above argument that the fixed field L^{G_E} is E. This shows that $f \circ g$ is the identity in (2). Combining this with (1), we obtain (3).
- We need to show that $g \circ f$ is the identity; that is, that if $H \subset G$, then $H = G_{L^H}$. In any case we have $H \subset H_0$. Let $E = L^H$, E_0 the fixed field of $H_0 = G_{L^H}$. It follows from the definitions that (tautologically) $E \subset E_0$. But $H_0 = G_{E_0}$ by Proposition **??**, and therefore $H_0 \subset H$. Thus $H = H_0$.
- Let $\mathcal{E}$ be the set of subfields of L containing K. The group G acts on $\mathcal{E}$: if $\sigma \in G$, $E \in \mathcal{E}$, then

$$\sigma(E) = \{\sigma(x), \mid x \in E\}.$$

  Say $E \in \mathcal{E}$ is *stable* for G if, for all $\sigma \in G$, $\sigma(E) = E$. If E is stable then the restriction map defines a map from G to $Gal(E/K)$, as in (4); however, we have not yet shown that E is Galois over K.

  Let $E \in \mathcal{E}$. Let $H = G_E$. We have for any $\sigma \in G$ that

$$G_E = \{g \in G \mid g(x) = x \, \forall x \in E\} = \{g \in G \mid \sigma(g)\sigma^{-1}\sigma(x) = \sigma(x) \, \forall x \in E\}.$$

  It follows that

$$\sigma H \sigma^{-1} = G_{\sigma(E)}.$$

  In particular, E is stable for E if and only if $G_{\sigma(E)} = G_E$ if and only if H is a normal subgroup. This completes part of (4).
- Finally, it remains to be shown that E/K is normal if and only if H is normal. Suppose E is normal, say E is the splitting field of some

$Q \in K[X]$, with roots $x_1, \ldots, x_r$, $E = K(x_1, \ldots, x_r)$. Then any $\sigma \in G$ permutes the roots of Q, hence leaves E stable.

If now $E \in \mathcal{E}$ is stable for G, say $E = K(x_1, \ldots, x_r)$. Say P_i is the minimal polynomial of x_i, $Q = \prod_i P_i$. Let $E' \supset E$ be the splitting field of Q in L. By the first part of this proof, E' is stable, hence $Gal(L/E')$ is the kernel of the restriction map $G \to Gal(E'/K)$. But

$$|Gal(E'/K)| = [E' : K] = \frac{[L : K]}{[L : E']} = |G|/|Gal(L/E')|$$

and by counting we see that the restriction map is surjective. It follows that E is invariant under all of $Gal(E'/K)$. which permutes the roots of Q.

On the other hand, we have seen that $Gal(E'/K)$ acts transitively on the roots of any irreducible polynomial that splits over E'. Since each P_i has at least one root in E, and since $Gal(E'/K)$ stabilizes E and acts transitively on the roots of P_i, it follows that all the roots of each P_i are contained in E. Thus $E' = E$.

Proofs of Proposition ?? and Corollary ?? (sketch)

First assume $L = K(y)$ for a single element y, and let $P \in K[X]$ be the minimal monic polynomial of y over K. Thus there is a unique isomorphism $K[X]/(P) \xrightarrow{\sim} L$ taking X to y, and $\deg(P) = d$. Then the set Σ is in bijection with homomorphisms $h : K[X] \to U$ such that $h(P) = 0$, in other words such that $h(X)$ is a root of P. In other words, Σ is in bijection with roots of P in U; since $\deg(P) = d$, there are at most d such roots. Moreover, if U is a Galois extension of K, then it is normal and separable, and then there are exactly d roots of P.

Now by induction on d, we may assume $L = E(y)$ where $L \supsetneq E \supset K$ and Proposition **??** and Corollary **??** are known with L replaced by E. For each $\tau : E \to U$ extending the inclusion of K in U, we let $\Sigma_\tau = \{\sigma \in \Sigma \mid \sigma(x) = \tau(x)\ \forall x \in E\}$. Let T be the set of such τ. Then $\Sigma = \coprod_{\tau \in T} \Sigma_\tau$ (disjoint union), so $|\Sigma| = \sum_\tau |\Sigma_\tau|$. Each Σ_τ has cardinality at most $d_E = [L : E]$ by the first part of the proof, with equality if U is a Galois extension of K, since it is then also a Galois extension of E. Moreover, the set T of τ has cardinality at most $[E : K]$ by induction, with equality if U is a Galois extension. Thus in general

$$|\Sigma| = \sum_{\tau \in T} |\Sigma_\tau| \leq \sum_\tau d_E = [L : E]|T| \leq [L : E][E : K] = [L : K].$$

This completes the proof of Proposition **??**. Moreover, if U is a Galois extension of K then all the inequalities are equalities; this completes the proof of Corollary **??**.

PROOF OF PROPOSITION ?? (SKETCH)

The proof has three parts.

(a) First we prove that L/K is a Galois extension. Let $x \in L$, $P \in K[X]$ its minimal polynomial. We need to show that P is split and separable in $L[X]$. For this it suffices to show that P divides a split separable polynomial in $L[X]$.

Let $\{x_1, \ldots, x_n\}$ be the G orbit of x, i.e. the set of elements of the form $g(x)$ with $g \in G$; say $x = x_1$. The x_i are all distinct though it is possible that $g_1(x) = g_2(x)$ for different g_i. Write $Q = \prod_{i=1}^{n}(X - x_i) \in L[X]$. Because the elements of g permute the x_i, $g(Q) = Q$ for all $g \in G$. This implies that the coefficients of Q as a polynomial are all fixed by G, hence belong to $L^G = K$. Thus $Q \in K[X]$. On the other hand, $Q(x) = Q(x_1) = 0$, thus Q is divisible by the minimal polynomial P of x. Since the roots of Q are distinct, this implies that P is separable; since Q is split in $L[X]$, this implies that L is also split in $L[X]$.

(b) We prove that $[L : K] = m \geq n = |G|$. (This is not necessarily the same n as in (a).) Let $x_1, \ldots, x_m$ be a basis for L/K. For each $g \in G$, let $v(g) = (g(x_1), \ldots, g(x_m)) \in L^m$ (think of this as a column vector. By Dedekind's lemma on linear independence of embeddings, the set $\{v(g), g \in G\}$ are linearly independent; if not, there would be a linear relation $\sum a_g g(x_i) = 0$ for $i = 1, \ldots, m$, hence $\sum a_g g(x) = 0$ for all $x \in L$, which contradicts Dedekind's lemma. It follows that $m \geq n$.

(c) We prove that $m \leq n$. If not, say $x_1, \ldots, x_{n+1}$ are linearly independent elements of L. Write $w(g) = (g(x_1), \ldots, g(x_{n+1})) \in L^{n+1}$ and consider the $n \times n + 1$ matrix with rows $w(g)$. The columns are linearly dependent over L, thus there exist $y_i, i = 1, \ldots, n + 1$ with

$$\sum_{i=1}^{n+1} y_i g(x_i) = 0, \ \ \forall g \in G.$$

Say r is minimal so that $y_1, \ldots, y_r$ are all different from 0, $y_i = 0$ for $i > r$.

Now let $\gamma, h \in G$:

$$0 = \gamma(\sum_{i=1}^{r} y_i h(x_i)) = \sum_{i=1}^{r} \gamma(y_i)\gamma \cdot h(x_i) = \sum_{i=1}^{r} \gamma(y_i) g(x_i)$$

where $g = \gamma h \in G$ is arbitrary.

Thus for all $\gamma \in G$, the $\gamma(y_i)$ define a relation among the $g(x_i)$. Since r was chosen minimal, these relations are all proportional to each other, hence to the relation with $\gamma = 1$. There are thus elements $\alpha_\gamma \in L^\times$ such that

$$\sum_{i=1}^{r} \gamma(y_i) g(x_i) = \alpha_\gamma (\sum_{i=1}^{r} y_i g(x_i))$$

Comparing coefficients, we find

$$\frac{\gamma(y_i)}{y_i} = \alpha_\gamma, i = 1, \ldots, r.$$

This in turn implies that $\gamma(\frac{y_i}{y_1}) = \frac{y_i}{y_1}$ for all i and all γ. Thus

$$z_i = \frac{y_i}{y_1} \in K.$$

Now return to the relation $\sum_i x_i y_i = 0$ (with $g = 1$); divide through by y_1 to get

$$\sum_i z_i x_i = 0.$$

This is a linear relation over K, thus the x_i are not linearly independent, which is a contradiction.