The Fundamental Theorem of Galois Theory (FTGT)

Pierre-Yves Gaillard

Abstract. We give a short and self-contained proof of the Fundamental Theorem of Galois Theory (FTGT) for finite degree extensions.

We derive the FTGT (for finite degree extensions) from two statements, denoted (a) and (b). These two statements, and the way they are proved here, go back at least to Emil Artin (precise references are given below). The derivation of the FTGT from (a) and (b) takes about four lines, but I haven't been able to find these four lines in the literature, and all the proofs of the FTGT I have seen so far are much more complicated. So, if you find either a mistake in these four lines, or a trace of them the literature, please let me know.

The argument is essentially taken from Chapter II of Emil Artin's Notre Dame Lectures [A]. More precisely, statement (a) below is implicitly contained in the proof Theorem 10 page 31 of [A], in which the uniqueness up to isomorphism of the splitting field of a polynomial is verified. Artin's proof shows in fact that, when the roots of the polynomial are distinct, the number of automorphisms of the splitting extension coincides with the degree of the extension. Statement (b) below is proved as Theorem 14 page 42 of [A]. The proof given here (using Artin's argument) was written with Keith Conrad's help.

Theorem

Let E/F be an extension of fields, let $a_1, \dots, a_n$ be distinct generators of E/F such that the product of the $X - a_i$ is in $F[X]$. Then

- the group G of automorphisms of E/F is finite,

- there is a bijective correspondence between the sub-extensions S/F of E/F and the subgroups H of G, and we have

$$S \leftrightarrow H \iff H = \mathrm{Aut}(E/S) \iff S = E^H \implies [E : S] = |H|,$$

where E^H is the fixed subfield of H, where $[E : S]$ is the degree (that is the dimension) of E over S, and where $|H|$ is the order of H.

Proof

We claim:

(a) If S/F is a sub-extension of E/F, then $[E : S] = |\mathrm{Aut}(E/S)|$.

(b) If H is a subgroup of G, then $|H| = [E : E^H]$.

Proof that (a) and (b) imply the theorem. Let S/F be a sub-extension of E/F and put $H := \mathrm{Aut}(E/S)$. Then we have trivially $S \subset E^H$, and (a) and (b) imply

$$[E : S] = [E : E^H].$$

Conversely let H be a subgroup of G and set $\overline{H} := \mathrm{Aut}(E/E^H)$. Then we have trivially $H \subset \overline{H}$, and (a) and (b) imply $|H| = |\overline{H}|$.

Proof of (a). Let $1 \leq i \leq n$. Put $K := S(a_1, \ldots, a_{i-1})$ and $L := K(a_i)$. It suffices to check that any F-embedding ϕ of K in E has exactly $[L : K]$ extensions to an F-embedding Φ of L in E; or, equivalently, that the polynomial $p \in \phi(K)[X]$ which is the image under ϕ of the minimal polynomial of a_i over K has $[L : K]$ distinct roots in E. But this is clear since p divides the product of the $X - a_j$.

Proof of (b). In view of (a) it is enough to check $|H| \geq [E : E^H]$. Let k be an integer larger than $|H|$, and pick a

$$b = (b_1, \ldots, b_k) \in E^k.$$

We must show that the b_i are linearly dependent over E^H, or equivalently that $b^\perp \cap (E^H)^k$ is nonzero, where $\bullet^\perp$ denotes the vectors orthogonal to $\bullet$ in E^k with respect to the dot product on E^k. Any element of $b^\perp \cap (E^H)^k$ is necessarily orthogonal to hb for any $h \in H$, so

$$b^\perp \cap (E^H)^k = (Hb)^\perp \cap (E^H)^k,$$

where Hb is the H-orbit of b. We will show $(Hb)^\perp \cap (E^H)^k$ is nonzero. Since the span of Hb in E^k has E-dimension at most $|H| < k$, $(Hb)^\perp$ is nonzero. Choose a nonzero vector x in $(Hb)^\perp$ such that $x_i = 0$ for the largest number of i as possible among all nonzero vectors in $(Hb)^\perp$. Some coordinate x_j is nonzero in E, so by scaling we can assume $x_j = 1$ for some j. Since the subspace $(Hb)^\perp$ in E^k is stable under the action of H, for any h in H we have $hx \in (Hb)^\perp$, so $hx - x \in (Hb)^\perp$. Since $x_j = 1$, the j-th coordinate of $hx - x$ is 0, so $hx - x = 0$ by the choice of x. Since this holds for all h in H, x is in $(E^H)^k$.

[A] Emil Artin, Galois Theory, Lectures Delivered at the University of Notre Dame, Chapter II: http://projecteuclid.org/euclid.ndml/1175197045.

This is version 1. Last version available at http://www.iecn.u-nancy.fr/∼gaillapy/DIVERS/Galois-short/.