Algebraic Closure of Finite Fields

Stephen Liu February 21, 2025

Notes

Let fg denote the function composition $f \circ g$.

Main reference: Tomas W. Hungerford, *Algebra*.

1 Useful Results

If $|K| = q$ and $f \in K[x]$ is irreducible, then f divides $x^{q^n} - x$ if and only if $\deg f$ divides n.

Proof. Suppose $q = p^r$ for some prime $p > 0$ and positive integer r. Suppose f divides $x^{q^n} - x$. Let F be a splitting field of $x^{q^n} - x$ over K. By Corollary V.5.8 we have $[F : K] = n$. Since f is irreducible, for u a root of f in F, we have $[K(u) : K] = \deg f$. Since f divides $x^{q^n} - x$, its root u is contained in F. So we have $K \subseteq K(u) \subseteq F$, whence we have $\deg f = [K(u) : K]$ divides $[F : K] = n$.

Conversely, suppose $d = \deg f | n$. Let $E = K(u)$ for some $u \in F$ a root of f. Then we have $[E : K] = \deg g = d$, so E is finite and $|E| = |K|^{[E:K]} = q^d$. By Proposition V.5.10 E is Galois over K, hence normal. Since f has a root u in E, E contains all the roots of f, and hence is a splitting field of f. Now since $d|n$, by Corollary V.5.8 there exists a simple extension $F = E(v)$ such that $[F : E] = m := n/d$. So we have $|F| = |E|^{[F:E]} = q^{dm} = p^{rn}$. By Proposition V.5.6 F is a splitting field of the polynomial $x^{p^{rn}} - x$ over $\mathbb{F}_p$, thus consists of the p^{rn} roots of $x^{p^{rn}} - x$. In particular, every element in E is such a root. Since E contains all roots of f, we conclude that all roots of f are roots of $x^{p^{rn}} - x$, hence f divides $x^{p^{rn}} - x = x^{q^n} - x$. □

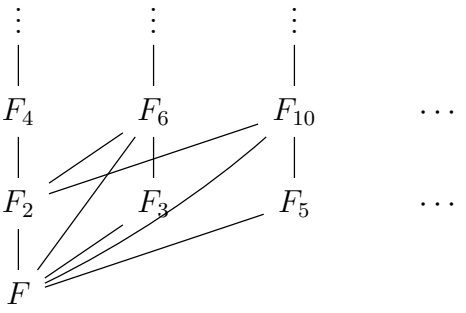
2 Galois Group of the Algebraic Closure

Let F be a finite field and $\overline{F}$ an algebraic closure of F. Show that

$$\mathrm{Gal}(\overline{F}/F) \cong \hat{\mathbb{Z}} := \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/n\mathbb{Z}.$$

Here is an explanation of the inverse system that is being used in the above notation: endow the positive integers with the partial order of divisibility: $m \leq n$ iff $m|n$. (Note, this is NOT the usual total order on the integers.) Thus whenever $m \leq n$, there is a natural projection map $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ that sends x mod n to x mod m, so we have a natural inverse system. We use $\hat{\mathbb{Z}}$ to denote the inverse limit of this system.

Proof. Suppose $|F| = q = p^r$ for some prime p and positive integer r. We begin with a construction of an inverse system. Fix an algebraic closure $\overline{F}$ of F. For every $n \geq 1$, by Corollary V.5.8 there is a unique (up to isomorphism) simple extension $F_n = K(u_n)$ of F in the algebraic closure $\overline{F}$ such that F_n is the splitting field of $x^{q^n} - x$ and is finite, with $[F_n : F] = n$. Then $F_1 = F$. For every $d|n$, $u_d \in F_d$ has a minimal polynomial f_d of degree d. Hence by V.5.7 f_d divides $x^{q^n} - x$, whose roots are in F_n. So $u_d \in F_n$ and therefore $F_d \subseteq F_n$. By Proposition V.5.10 every F_n is Galois over F. Hence we have the system of Galois extensions as the following.



Claim 1. The system $\{\mathrm{Aut}_F F_n : n \in \mathbb{N}\}$ is an inverse system isomorphic to $\{\mathbb{Z}/n\mathbb{Z} : n \in \mathbb{N}\}$.

Suppose $m|n$ for $n, m \in \mathbb{N}$. Since F_n is finite Galois over F_m (as $F \subseteq F_m \subseteq F_n$ and F_n is Galois over F), the restriction homomorphism

$$f_{mn} : \mathrm{Aut}_F F_n \to \mathrm{Aut}_F F_m, \sigma \mapsto \sigma|_{F_m}$$

is well defined and surjective by the fundamental theorem. Thus f_{nn} is the identity homomorphism and $f_{km} \circ f_{mn} = f_{kn}$ whenever $k|m|n$ by properties of restriction.

1.1 (V.5.8). The group $\mathrm{Aut}_F F_n$ is generated by $u \mapsto u^{p^r}$ for any $n \in \mathbb{N}$.

By Proposition V.5.10, $\mathrm{Aut}_F F_n$ is a cyclic subgroup of $\mathrm{Aut}_{\mathbb{F}_p} F_n$, which is generated by the $\mathbb{F}_p$-automorphism (Frobenious map) $\varphi : u \mapsto u^p$. Now since F_n is Galois over $\mathbb{F}_p$ we have

$$|\mathrm{Aut}_{\mathbb{F}_p} F_n| = [F_n : \mathbb{F}_p] = [F_n : F][F : \mathbb{F}_p] = nr$$

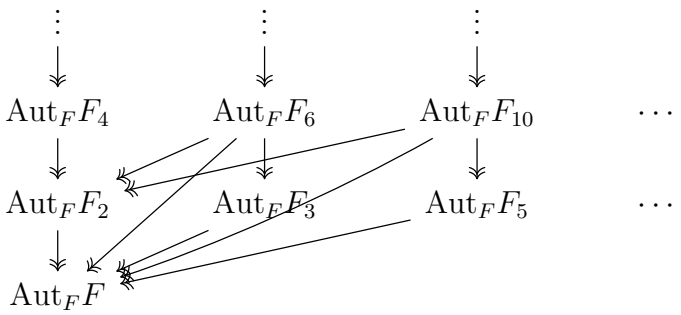
while $|\mathrm{Aut}_F F_n| = [F_n : F] = n$. So the subgroup $\mathrm{Aut}_F F_n$ has index r, and is hence generated by the order n element $\sigma_n := \varphi^r : u \mapsto u^{p^r} = u^q$ for $u \in F_n$.

For $m|n$ and $\sigma \in \mathrm{Aut}_F F_n$, we have $\sigma = \sigma_n^j$ for some $j \in \mathbb{Z}/n\mathbb{Z}$ such that $\sigma(u) = u^{q^j}$ for all $u \in F_n$. Thus in particular $\sigma|_{F_m}(u) = u^{q^j}$ for all $u \in F_m$. So $\sigma|_{F_m} = \sigma_m^j$. Since $\mathrm{Aut}_F F_m$ has order $m|n$, we have $\sigma|_{F_m} = \sigma_m^l$ for $l \equiv j \bmod m$, where $0 \le l < m$ is unique.

Note that we have isomorphisms $\mathrm{Aut}_F F_n \xrightarrow{\cong} \mathbb{Z}/n\mathbb{Z},\ \sigma_n^j \mapsto j$ for all $n \in \mathbb{N}, j \in \mathbb{Z}/n\mathbb{Z}$. The induced map by this isomorphism of the restriction f_{mn} is precisely the natural projection $\mathbb{Z}/n\mathbb{Z} \twoheadrightarrow \mathbb{Z}/m\mathbb{Z},\ j \mapsto j \bmod m$. Thus the diagrams of the following form

$$\begin{array}{ccc} \mathrm{Aut}_F F_n & \xrightarrow{f_{mn}} & \mathrm{Aut}_F F_m \\ \uparrow\downarrow\cong & & \uparrow\downarrow\cong \\ \mathbb{Z}/n\mathbb{Z} & \twoheadrightarrow & \mathbb{Z}/m\mathbb{Z} \end{array}$$

commute for all $m|n$. So we have an isomorphism between the inverse systems $\{\mathrm{Aut}_F F_n : n \in \mathbb{N}\}$ with restrictions f_{mn} and $\{\mathbb{Z}/n\mathbb{Z} : n \in \mathbb{N}\}$ with the natural projections, both defined under the same partial order of divisibility on $\mathbb{N}$.



Claim 2. There exists a homomorphism $p_n : \mathrm{Gal}(\overline{F}/F) \to \mathrm{Aut}_F F_n$ for each $n \in \mathbb{N}$ such that $f_{mn} p_n = p_m$ whenever $m|n$.

2.1 (V.5.11(a)). $\overline{F}$ is Galois over F.

The algebraic closure $\overline{F}$ contains the union $\cup_{n\in\mathbb{N}} F_n$. Now for all $0 \neq u \in \overline{F}$, since u is algebraic over F, it has a minimal polynomial f of degree some $n \in \mathbb{N}$ and hence divides

$x^{q^n} - x$ by V.5.7 as above. So we have $u \in F_n$, and in fact $\overline{F} = \cup_{n\in\mathbb{N}} F_n$. Also since f divides $x^{q^n} - x \in F[x]$, which has q^n distinct roots, f has distinct roots and hence is separable. Thus every element $u \in \overline{F}$ is separable. By definition $\overline{F}$ is a splitting field of all polynomials in $F[x]$. So by Theorem V.3.11 we conclude that $\overline{F}$ is algebraic Galois over F.

Then since F_n are intermediate fields of $\overline{F}$ over F, $\overline{F}$ is Galois over F_n for all n. Therefore, the restrictions

$$p_n : \mathrm{Gal}(\overline{F}/F) \to \mathrm{Aut}_F F_n,\ \sigma \mapsto \sigma|_{F_n}$$

are well-defined homomorphisms by Lemma V.2.13. Furthermore, for $m|n$ we have $f_{mn}p_n = p_m$ as f_{mn} is also a restriction.

Claim 3. Together with $\{p_n : n \in \mathbb{N}\}$, the group $G = \mathrm{Gal}(\overline{F}/F)$ is the inverse limit of the inverse system $\{\mathrm{Aut}_F F_n : n \in \mathbb{N}\}$, which is isomorphic to $\{\mathbb{Z}/n\mathbb{Z} : n \in \mathbb{N}\}$. Therefore $\mathrm{Gal}(\overline{F}/F) \cong \hat{\mathbb{Z}}$ by the universal property of the inverse limit.

Denote $G = \mathrm{Gal}(\overline{F}/F)$. Let B be a group together with homomorphisms $\varphi_n : B \to \mathrm{Aut}_F F_n$ for all n such that $f_{mn}\varphi_n = \varphi_m$ whenever $m|n$. [1] We have shown that $\overline{F} = \cup_{n\in\mathbb{N}} F_n$. So for every $0 \neq u \in \overline{F}$, we have $u \in F_{k_u}$ for some $k_u \in \mathbb{N}$ such that u has degree k_u over F. We define a map $\varphi : B \to G$ by $\varphi(b) = \beta$ where $\beta(u) = \varphi_{k_u}(b)(u)$ for each $0 \neq u \in \overline{F}$ and $\beta(0) = 0$.

3.1. The map φ is well-defined, that is, β is in fact an F-automorphism of $\overline{F}$.

3.1.1. β is a well-defined map. For every $0 \neq u \in \overline{F}$, since u has degree k_u over F, we have $u^{q^k} - u \neq 0$ for all $k < k_u$. Because otherwise we would have $u \in F_k$ and u has degree $\leq k < k_u$. Hence u has multiplicative order $q^{k_u} - 1$ in the group $(F_{k_u})^\times$, and hence we have $F_{k_u} = F(u)$. If we also have $u \in F_n$ for some $n \in \mathbb{N}$ then $F_{k_u} \subseteq F_n$ holds and therefore the restriction $f_{k_u m}$ is defined. In this case

$$\varphi_{k_u}(b)(u) = [f_{k_u n}\varphi_n](b)(u) = \varphi_n(b)(u)$$

holds. So $\beta(u) = \varphi_{k_u}(b)(u)$ is well-defined.

3.1.2. β is an F-automorphism. For every $u, v \in \overline{F}$, we have $u \in F_{k_u}, v \in F_{k_v}$ for some $k_u, k_v \in \mathbb{N}$. Then in particular we have $u, v \in F_{k_u k_v}$. Thus

$$\beta(u - v) = \varphi_{k_u k_v}(b)(u - v) = \varphi_{k_u k_v}(b)(u) - \varphi_{k_u k_v}(b)(v) = \beta(u) - \beta(v);$$

$$\beta(uv^{-1}) = \varphi_{k_u k_v}(b)(uv^{-1}) = \varphi_{k_u k_v}(b)(u)(\varphi_{k_u k_v}(b)(v))^{-1} = \beta(u)(\beta(v))^{-1}$$

[1] We have shown that $u \mapsto u^q$ generates each $\mathrm{Aut}_F F_n$. So $\varphi_n(b) = \sigma_n^{j_n} : u \mapsto u^{q^{j_n}}$ for some $j_n \in \mathbb{Z}/n\mathbb{Z}$. And by $f_{mn}\varphi_n = \varphi_m$ we have $j_n \cong j_m \bmod m$ whenever $m|n$. So we can view $\varphi_n : B \to \mathbb{Z}/n\mathbb{Z}, b \mapsto j_n$.

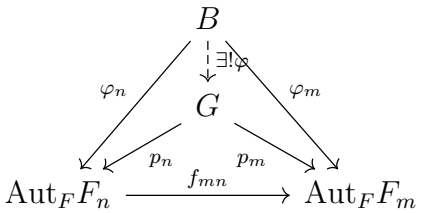
(given $v \neq 0$) since $\varphi_{k_uk_v}(b) \in \mathrm{Aut}_F F_{k_uk_v}$. So β is a field homomorphism. Similarly, if $\beta(u) = \beta(v)$ for some $u, v \in \overline{F}$ then $\varphi_{k_uk_v}(b)(u) = \varphi_{k_uk_v}(b)(v)$, which implies $u = v$. So β is injective. For every $u \in \overline{F}$, since $\varphi_{k_u}(b)$ is an F-automorphism, there exists $w \in F_{k_u}$ such that $u = \varphi_{k_u}(b)(v) = \beta(v)$. So β is surjective. Finally, since $F \subseteq F_n$ for all $n \in \mathbb{N}$, we have $\beta(x) = \varphi_n(b)(x) = x$ since $\varphi_n(b)$ fixes F. So β fixes F. Therefore, β is an F-automorphism of $\overline{F}$.

3.2. The map φ is a group homomorphism.

Let $b, b' \in B$. Then for all $u \in \overline{F}$, the map $\varphi_{k_u} : B \to \mathrm{Aut}_F F_{k_u}$ is a homomorphism. Thus we have

$$\varphi(bb')(u) = \varphi_{k_u}(bb')(u) = \varphi_{k_u}(b)[\varphi_{k_u}(b')(u)] = \varphi(b)[\varphi(b')(u)],$$

where $\varphi(b')(u) \in F_{k_u}$. Hence φ is a group homomorphism.



3.3. The map φ is the unique group homomorphism satisfying $p_n\varphi = \varphi_n$ for all n.

For every $n \in \mathbb{N}$, we have $p_n|_{F_n} = id_{F_n}$. So for all $b \in B$ we have $p_n\varphi(b)(u) = \varphi(b)(u) = \varphi_n(u)$ for all $u \in F_n$. Thus $p_n\varphi = \varphi_n$ holds.

Now suppose $\psi : B \to G$ is another group homomorphism such that $p_n\psi = \varphi_n$ for all n. Then necessarily we have $p_n\psi(b) = p_n\varphi(b)$ for all $b \in B$. For any $u \in \overline{F}$, since $u \in F_{k_u}$ we have

$$\psi(b)(u) = \psi(b)|_{F_{k_u}}(u) = p_{k_u}\psi(b)(u) = \varphi_{k_u}(b)(u) = \varphi(b)(u).$$

We conclude that $\psi = \varphi$ and hence φ is unique. Therefore we have $G \cong \hat{\mathbb{Z}}$. □