A Glossary of Galois Theory

Phil Hazelden

2012-02-04 Sat

1 Notation

Φ_n The n'th cyclotomic polynomial.

$\mathbb{F}_p$ The finite field $\mathbb{Z}/(p)$, where p is prime.

$\mathbb{F}_q$ A finite field of order $q = p^n$. Exists and is unique, but is not $\mathbb{Z}/(p)$ unless $n = 1$.

f_α^K The *minimal polynomial* of α over K; the unique monic polynomial in $K[X]$ of minimal degree such that $f_\alpha^K(\alpha) = 0$. Usually $\alpha \in L \backslash K$ where L/K is some field extension.

K A field.

$K(\alpha_1, \ldots, \alpha_n)$ The minimal field containing the subfield K and the elements α_i.

L A field; usually containing K.

L/K A field extension.

L^H See *fixed field*.

p A prime.

R A unique factorisation domain.

2 Definitions

Abelian An extension L/K is abelian if it is Galois, and $\mathrm{Gal}(L/K)$ is abelian.

Algebraic $\alpha \in L$ is algebraic over K if there is $f \in K[X]$ such that $f(\alpha) = 0$.

L/K is algebraic if every $\alpha \in L$ is algebraic over K.

Algebraically closed K is algebraic if all algebraic extensions of K are equal to K; equivalently if all finite extensions of K are equal to K; equivalently if every polynomial $f \in K[X]$ splits in K; equivalently if every nonconstant $f \in K[X]$ has a root in K.

Automorphism A K-automorphism $L \to L$ is an automorphism on L which restricts to the identity on K.

Automorphism group $\mathrm{Aut}(L/K)$ is the group of all K-automorphisms $L \to L$.

If $L^{\mathrm{Aut}(L/K)} = K$, then $\mathrm{Aut}(L/K)$ is also written $\mathrm{Gal}(L/K)$.

Constructible L/K is constructible if there is a sequence of extensions $K_1/K, K_2/K_1, \ldots, K_n/K_{n-1}$ with $L \subset K_n$ and each $[K_{i+1} : K_i] \in \{1, 2\}$.

Cyclotomic polynomial $\Phi_n = \prod_\zeta (X - \zeta) \in \mathbb{Z}[X]$ where ζ are the primitive n'th roots of unity. $X^n - 1 = \prod_{d|n} \Phi_d$.

Fixed field For $H \leq \mathrm{Aut}(L/K)$, L^H is the intermediate field ($K \leq L^H \leq L$) containing those elements of L which are fixed by every element of H. Also written $\mathrm{Fix}(H)$ if L is clear from the context. $L^H = \{\alpha \in L : g \in H \Rightarrow g(\alpha) = \alpha\}$.

Frobenius automorphism when K is a finite field of characteristic p, this is the map $F : K \to K : x \mapsto x^p$.

Galois extension L/K is *Galois* if $L^{\mathrm{Aut}(L/K)} = K$. That is, no $\alpha \in L$ is preserved by every K-automorphism $L \to L$.

Galois group $\mathrm{Gal}(L/K)$ is $\mathrm{Aut}(L/K)$, when L/K is Galois.

Normal L/K is normal if for each $\alpha \in L$, f_α^K splits in L.

All Galois extensions are normal, and L/K is normal iff L is the splitting field for some polynomial $f \in K[X]$.

Normal closure A normal closure of a finite extension L/K is a minimal M/L such that M/K is normal. A normal closure always exists, is finite, and any two normal closures are L-isomorphic.

Perfect A field is called perfect if all of its algebraic extensions are separable. All extensions of $\mathbb{Q}$, algebraically closed fields, and finite fields are perfect.

Primitive A polynomial $f \in R[X]$ is primitive if there is no irreducible $p \in R$ such that $p|f$.

If $g, h \in R[X]$ are primitive then so is gh.

If $g', h' \in \mathrm{Frac}(R)[X]$ and $f = g'h'$ is nonconstant primitive, then $\exists a, b \in \mathrm{Frac}(R)$: $ag', bh' \in R[X]$ are primitive and $f = abg'h'$.

A field extension L/K is primitive if $L = K(\alpha)$ for some α.

A primitive n'th root of unity is one which has order n.

Radical A finite extension L/K is radical if we can write $L = K(\alpha_1, \ldots, \alpha_r)$ with integers $n_1, \ldots n_r$ such that for each i, $\alpha_i^{n_i} \in K(\alpha_1, \ldots, \alpha_{i-1})$.

Separable polynomial An irreducible polynomial $f \in K[X]$ is seperable if its derivative is nonzero; equivalently if f has no repeated root in any larger field L/K; equivalently if f splits into distinct linear factors over its splitting field.

Every polynomial is separable over a field of characteristic 0 (an extension of $\mathbb{Q}$).

Separable extension L/K is separable if for each $\alpha \in L$, f_α^K is separable.

An extension is Galois iff it is normal and separable. (i.e. iff for each $\alpha \in L$, $f_\alpha^K = c(X - \alpha_1) \cdots (X - \alpha_n)$ where the α_i are distinct elements of L.)

Solvable Finite L/K is solvable if it is contained in some radical extension. $f \in K[X]$ is solvable if its splitting field is solvable. A group G is solvable if there is a chain $G = G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_n = \{1\}$, such that each G_i/G_{i+1} is abelian.

Split $f \in K[X]$ splits in $L \subset K$ if $f = c(X - \alpha_1) \cdots (X - \alpha_n)$ where $\alpha_i \in L$. (i.e. all roots of f are in L.)

Splitting field L/K is a splitting field for $f \in K[X]$ if

- f splits in L
- $L = K(\alpha_1, \ldots, \alpha_n)$ where α_i are roots of f in L (i.e. L is not "too big").

3 Theorems

3.1 Irrecuducibility of polynomials

Remainder theorem If $f \in K[X]$ and $\alpha \in K$, then $(X - \alpha)|f$ iff $f(\alpha) = 0$.

Gauss' lemma If $f \in R[X]$ is nonconstant primitive and irreducible over R, then it is irreducible over $\mathrm{Frac}(R)$.

Reduction Suppose $f \in R[X]$ is primitive, $p \in R$ is irreducible and $(f \mod p)$ is irreducible in $(R/(p))[X]$. Then f is irreducible in $R[X]$.

Eisenstein's criterion Suppose $f \in R[X]$ primitive and $\exists p \in R$ irreducible such that: $p \nmid a_n$; $p \mid a_i$ for $0 \leq i < n$; $p \mid a_0^2$. Then f is irreducible over R and $\mathrm{Frac}(R)$.

3.2 Field extensions

- If α is algebraic then $K(\alpha) \cong K[X]/(f_\alpha^K)$, $\alpha \mapsto X$. If $n = \deg_K(\alpha)$ then $[K(\alpha) : K] = n$ and $1, \alpha, \ldots, \alpha^{n-1}$ is a basis of the K-vector space $K(\alpha)$.

- If α is transcendental then $K(\alpha) \cong K(X)$, $\alpha \mapsto X$.

- Finite field extensions are algebraic.

- If $K(\alpha)$ is an algebraic extension and L/K is any extension, there is a bijection

$$\{K\text{-homomorphisms } K(\alpha) \to L\} \to \{\text{roots of } f_\alpha^K \text{ in } L\}$$

  mapping $\varphi \mapsto \varphi(\alpha)$. (Note, α need not be in L.)

- **Tower law** $[M : K] = [M : L][L : K]$

- If L/K is a finite field extension, then every K-homomorphism $L \to L$ is a K-automorphism.

3.3 Automorphism groups and intermediate fields

- There is a map {intermediate fields of L/K} $\to$ {subgroups of $\mathrm{Aut}(L/K)$}, given by $L' \to \mathrm{Aut}(L/L')$.
- $L/N/M/K$ field extensions with N/M finite. Then $[\mathrm{Aut}(L/M) : \mathrm{Aut}(L/N)] \leq [N : M]$.
- Corollary: L/K finite $\Rightarrow |\mathrm{Aut}(L/K)| \leq [L : K]$.
- If $H \leq G \leq \mathrm{Aut}(L/K)$ then $[L^H : L^G] \leq [G : H]$.
- Special case: if H is trivial we have $[L : L^G \leq |G|$.
- Corollary: $[L : L^{\mathrm{Aut}(L/K)}] \leq |\mathrm{Aut}(L/K)| \leq [L : K]$.
- If L/K is finite then it is Galois iff $|\mathrm{Aut}(L/K)| = [L : K]$.
- Special case: if $L = K(\alpha)$ with $[L : K] = n$, then L/K is Galois iff f_α^K has precisely n distinct roots in L.
- **Fundamental theorem of Galois theory** Let L/K be a finite Galois extension. There is an inclusion-reversing bijection

$$\{M : L/M/K\} \leftrightarrow \{H : H \leq \mathrm{Aut}(L/K)\}$$

  mapping $M \mapsto \mathrm{Aut}(L/M)$ and $L^H \leftarrow\!\shortmid H$. Moreover, L/M is Galois; $[L : M] = |H|$ and $[M : K] = [\mathrm{Gal}(L/K) : H]$; M/K is Galois iff $H \trianglelefteq \mathrm{Gal}(L/K)$ and these imply $\mathrm{Gal}(M/K) = \mathrm{Gal}(L/K)/H$.
- For $L/M/K$ with L/K Galois, TFAE:
  - $\mathrm{Gal}(L/M) \trianglelefteq \mathrm{Gal}(L/K)$
  - For each $\sigma \in \mathrm{Gal}(L/K)$, $\sigma(M) = M$
  - M/K is Galois
  - M/K is normal

3.4 Splitting fields

- Given nonzero $f \in K[X]$ of degree n, there is a splitting field L with $[L : K] \leq n!$.
- **Isomorphism extension theorem** If $\sigma : K \to K'$ is an isomorphism, $f \in K[X]$, L is a splitting field of f and L' is a splitting field of $\sigma(f)$, then there is an isomorphism $L \to L'$ extending σ.
- Corollary: $f \in K[X]$ has a unique splitting field up to K-isomorphism.
- For a finite extension L/K, TFAE:
  - L/K is normal
  - L/K is a splitting field for some $f \in K[X]$

- For any extension M/L and K-homomorphism $\sigma : L \to M$, $\sigma(L) = L$.

- Any finite extension L/K has a normal closure N/L which is finite and unique up to L-isomorphism.

- Every field K has an algebraic closure, unique up to K-isomorphism.

3.5 Separability

- $f \in K[X]$ has a repeated root a iff $X - a$ divides both f and f'.

- **Separable polynomials** If $f \in K[X]$ is irreducible, TFAE:
  - f has no repeated roots in any extension L/K
  - f splits into distinct linear factors over its splitting field
  - $f' \neq 0$.

- If $\operatorname{char} K = 0$, every irreducible polynomial is separable.

- If $\operatorname{char} K = p > 0$, f irreducible, then f is separable iff there is $g \in K[X]$ such that $f = g(X^p)$.

- A finite extension L/K is Galois iff it is normal and separable; iff it is the splitting field of some $f \in K[X]$ such that all irreducible factors of f are separable.

- **Primitive extension theorem** finite L/K is primitive iff there exist only finitely many intermediate fields.

- Corollary: Finite degree separable extensions are primitive.

3.6 Finite fields

- A finite subgroup of K^* is cyclic.

- If L/K are both finite fields, the extension is primitive.

- $|K| = p^n$ iff K is a splitting field of $X^n - X \in \mathbb{F}_p[X]$.

- Corollary: there is a unique finite field of order p^n.

- If $|K| = p^n$ then $K/\mathbb{F}_p$ is Galois, and $\operatorname{Gal}(K/\mathbb{F}_p)$ is cyclic of order n, generated by the Frobenius automorphism F.

- Corollary: the subfields of $\mathbb{F}_{p^n}$ are $\mathbb{F}_{p^m}$ for each $m|n$.

- Corollary: if L is finite then any L/K is Galois, with $\operatorname{Gal}(L/K)$ generated by a power of F.

3.7 Cyclotomic fields

- Let L/K be any field extension and $\zeta \in L$ a primitive n'th root of 1. Then $K(\zeta)/K$ is Galois, and there is an injective homomorphism $\mathrm{Gal}(K(\zeta)/K) \to (\mathbb{Z}/n\mathbb{Z})^* : \sigma \mapsto (k \text{ such that } \sigma(\zeta) = \zeta^k)$.
- If $K = \mathbb{Q}$ above, then the homomorphism is an isomorphism, and Φ_n is irreducible.
- Corollary: any subfield of $\mathbb{Q}(\zeta)$, where ζ is any root of unity, is abelian over $\mathbb{Q}$.
- Any abelian extension of $\mathbb{Q}$ is a subfield of some $\mathbb{Q}(\zeta)$. (Proof nonexaminable.)
- The regular n-gon can be constructed from two points in the plane iff n is of the form $n = 2^m \prod_{i=1}^{k} p_i$, where the p_i are distinct Fermat primes (primes of the form $2^j + 1$).

3.8 Solvability in radicals

- If x can be written in terms of $\times$, $\div$, $+$, $-$ and $\sqrt[n]{\ }$ ($n \in \mathbb{N}$) applied to elements of K, then $K(x)/K$ is solvable.
- If L/K is radical and N is the normal closure, then N/K is radical.
- A finite extension L/K is radical iff its normal closure N/K is radical.
- Irreducible $f \in K[X]$ is solvable iff there is a solvable extension L/K with some $x \in L$ such that $f(x) = 0$.
- If $\zeta \in K$ is a primitive n'th root of unity, and $\alpha^n \in K$, then $K(\alpha)/K$ is Galois with $\mathrm{Gal}(K(\alpha)/K)$ cyclic of order dividing n.
- If G is a solvable group and $H \leq G$, then H is solvable; if $H \trianglelefteq G$ then G/H is solvable also.
- Let $\mathrm{char}\, K = 0$, $f \in K[X]$ be solvable, and L be the splitting field of f. Then $\mathrm{Gal}(L/K)$ is solvable.
- If $H \trianglelefteq G$ and G/H is abelian, then $[G, G] \leq H$.
- $[A_5, A_5] = A_5$; as a corollary, A_5 is not solvable.
- If p is prime, $H \leq S_p$, and H conains a p-cycle and a 2-cycle, then $H = S_p$.
- If $f \in \mathbb{Q}[X]$ is an irreducible quintic with three real and two complex roots, then f is not solvable.
- Corollary: there is no general formula for solving quintic polynomials in radicals.

3.9 Calculating Galois groups

In this section we let $f \in K[X]$ of degree n, and L be it's splitting field, with f having no repeated roots in L. We write $\mathrm{Gal}(f)$ for $\mathrm{Gal}(L/K)$, which can be thought of as a subgroup of S_n, as each $\sigma \in \mathrm{Gal}(f)$ is defined by a permutation of the roots of f.

We write $f = \sum_{i=0}^{n} a_i X^i = \prod_{i=1}^{n} (X - \alpha_i)$. We also let $\Delta = \prod_{i<j} (\alpha_i - \alpha_j)$ and $D = \Delta^2 = \prod_{i \neq j} |a_i - a_j|$, the discriminant of f.

- f is irreducible iff $\mathrm{Gal}(f)$ is transitive (i.e. for every pair α_1, α_2 of roots of f, there is $\sigma \in \mathrm{Gal}(f) : \sigma(\alpha_1) = \alpha_2$).
- Any polynomial expression in α_i which is symmetric (invariant under permutation of the α_i) is a polynomial in the a_i (so e.g. D is but Δ isn't).
- Let $\sigma \in \mathrm{Gal}(f)$. Then $\sigma(\Delta) = \pm\Delta$, $+$ if σ is an even permutation and $-$ if σ is an odd permutation of roots.
- Corollary: $\mathrm{Gal}(f) \leq A_n$ iff $\Delta \in K$.
- Corollary: If f is irreducible and $n = 3$, then $\mathrm{Gal}(f) = A_3$ if $\Delta \in K$, S_3 otherwise.