

MA 45401-H01: Galois Theory Honors

Definitions and Results

Prof. Ilya Shkredov
Transcribed by Josh Park

Spring 2025

Contents

1	Introduction I	2
2	Introduction II	3
3	Field Extensions I	3
4	Field Extensions II	5
5	Algebraic Conjugates	6
6	Ruler and Compass Constructions	6
7	Cyclotomic Polynomials	6
8	Splitting Fields, Abel-Ruffini	6
9	Algebraic Closure I	7
10	Algebraic Closure II	8
11	Galois Groups I	9
12	Galois Groups II	9
13	Galois Groups III	9
14	Separability	10
15	The Primitive Element Theorem	10
16	Galois Fields I	11
17	Galois Fields II	12

1 Introduction I

Definition 1 (Symmetric function). A function $\varphi(x_1, \dots, x_n)$ is called symmetric if

$$\varphi(x_1, \dots, x_n) = \varphi(x_{\omega(1)}, \dots, x_{\omega(n)})$$

for all $\omega \in S_n$.

Definition 2 (Elementary symmetric polynomial).

$$\begin{aligned}\sigma_1 &= \sigma_1(x_1, \dots, x_n) = x_1 + \dots + x_n \\ \sigma_2 &= \sigma_2(x_1, \dots, x_n) = x_1x_2 + \dots + x_1x_n + x_2x_3 + \dots + x_{n-1}x_n \\ &\dots \\ \sigma_k &= \sigma_k(x_1, \dots, x_n) = \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} x_{i_1} \dots x_{i_k} \\ &\dots \\ \sigma_n &= \sigma_n(x_1, \dots, x_n) = \prod_{i=1}^n x_i\end{aligned}$$

Theorem 1.1. For any symmetric function $\psi(x_1, \dots, x_n)$, there exists a unique polynomial $P(t_1, \dots, t_n)$ such that $\psi(x_1, \dots, x_n) = P(\sigma_1, \dots, \sigma_n)$.

Vieta formulae:

$$\begin{aligned}x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n &= (x - x_1)(x - x_2) \dots (x - x_n) \\ &= x^n - \sigma_1x^{n-1} + \sigma_2x^{n-2} + \dots + (-1)^n\sigma_n\end{aligned}$$

Corollary 1. The discriminant D of $f \in R[x]$, where R is a ring and $f = x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$, is a polynomial in a_1, \dots, a_n and coefficients from R (i.e. $D \in R[a_1, \dots, a_n]$).

Note: Any cubic equation can be converted to a depressed cubic by

$$x^3 + Ax^2 + Bx + c = \left(x + \frac{A}{3}\right)^3 + p\left(x + \frac{A}{3}\right) + q.$$

Vieta's method: Using the trigonometric formula $\cos 3\varphi = 4\cos^3\varphi - 3\cos\varphi$, we can solve certain cubic equations. For example, consider $4x^3 - 3x = -\frac{1}{2}$. Let $x = \cos\varphi$. Then

$$\begin{aligned}\cos 3\varphi = -\frac{1}{2} &\iff 3\varphi = \pm\frac{2\pi}{3} + 2\pi k \quad \text{for } k \in \mathbb{Z} \\ &\iff \varphi = \pm\frac{2\pi}{9} + 2\pi k \\ &\iff x \in \left\{\cos\frac{2\pi}{9}, \cos\frac{4\pi}{9}, \cos\frac{8\pi}{9}\right\}.\end{aligned}$$

In general, we can use this method to solve $4x^3 - 3x = a \implies x = \cos\varphi$, $\cos 3\varphi$ and $\cos : \mathbb{C} \rightarrow \mathbb{C}$ is now a complex function. For $x^3 + px + q = 0$, set $x = ky$ such that $\frac{k^3}{pk} = \frac{-4}{3} \implies k = \pm\frac{\sqrt{-4p}}{3}$.

Definition 3 (Ferrari resolvent). Let $f(x) = x^4 + ax^3 + bx^2 + cx + d \in K[x]$ be a quartic polynomial over a field K of characteristic not 2. We define the Ferrari resolvent of f to be the associated cubic resolvent polynomial $R(z) \in K[z]$ given by

$$R(z) = z^3 - 2bz^2 + (b^2 - 4d + ac)z - c^2 - a^2d + 4bd.$$

Solving the resolvent allows one to reduce solving f to solving a system of quadratics.

Lagrange's method: Suppose $f(x) = x^3 + px + q$ is a depressed cubic with roots x_1, x_2, x_3 . Lagrange's method finds expressions involving the roots that take only a few values under permutation, then uses symmetry to connect them to the coefficients.

For instance, define

$$y_1 = x_1 + \zeta x_2 + \zeta^2 x_3,$$

where $\zeta = e^{2\pi i/3}$ is a primitive cube root of unity. Then define

$$y_2 = x_1 + \zeta^2 x_2 + \zeta x_3.$$

These expressions are not symmetric, but they only take a few values when the x_i 's are permuted. In particular, y_1^3 and y_2^3 are symmetric functions of the roots and thus can be written as polynomials in p and q .

Since the roots x_i are related to y_1 and y_2 , we can use symmetric combinations such as

$$x = \frac{1}{3}(y_1 + y_2)$$

to recover the original roots of $f(x)$.

2 Introduction II

Theorem 2.1 (Lagrange). Let $\varphi = \varphi(x_1, \dots, x_n)$ and

$$\text{orb}(\varphi) = \{\varphi^\omega = \varphi(x_{\omega(1)}, \dots, x_{\omega(n)}) \mid \omega \in S_n\}.$$

Then y_1, \dots, y_k are roots of some polynomial with degree $\leq k$ whose coefficients depend on elementary symmetric polynomials $\sigma_1, \dots, \sigma_n$ in a polynomial way.

Theorem 2.2 (Lagrange). Let $\varphi, \psi \in K[x_1, \dots, x_n]$ and $G_\varphi = \{\omega \in S_n \mid \varphi^\omega = \varphi\} \leq G_\psi$. Then $\psi = R(\varphi)$ where R is a rational function whose coefficients are symmetric functions on x_1, \dots, x_n .

Definition 4 (Group action). Let G be a group and X be a set. The (left) group action of G on X is the map $\cdot : G \times X \rightarrow X$ such that

1. $e_G \cdot x = x, \quad \forall x \in X$
2. $g \cdot (h \cdot x) = (g \cdot h) \cdot x, \quad \forall x \in X, \forall g, h \in G$

Definition 5 (Orbit). Let G be a group, X be a set, and $x \in X$. Then we define the orbit of x , $G \cdot x = \text{orb}(x)$, as $\{g \cdot x \mid g \in G\}$. Moreover, $\text{orb}(x) \subseteq X$.

Definition 6 (Stabilizer). Let G be a group, X be a set, and $x \in X$. Then we define the stabilizer of x , $\text{stab}(x)$, as $\{g \in G \mid g \cdot x = x\}$. Moreover, $\text{stab}(x) \leq G$.

Theorem 2.3. Let G be a finite group that acts on X . Then for all $x \in X$, $|\text{orb}(x)| \cdot |\text{stab}(x)| = |G|$.

Definition 7 (Polynomial ring). Let R be a commutative ring. Then the ring of polynomials with coefficients in R is

$$R[t] = \left\{ \sum_{i=0}^n c_i t^i : n \in \mathbb{Z}_+, c_i \in R \right\}$$

3 Field Extensions I

Definition 8 (Integral domain). Let R be a commutative ring. Then R is an integral domain if $ab = 0$ implies that $a = 0$ or $b = 0$ for all $a, b \in R$.

Definition 9 (Euclidean domain). Let R be an integral domain. Then R is a Euclidean domain if there exists some function $f : R \setminus \{0\} \rightarrow \mathbb{Z}_{\geq 0}$ such that for all $a, b \neq 0 \in R$, there exist elements $q, r \in R$ such that $a = qb + r$ where $r = 0$ or $f(r) < f(b)$.

Theorem 3.1 (Bézout's Identity). Let R be a Euclidean domain. For $a, b \in R$, there exists $\alpha, \beta \in R$ such that $\gcd(a, b) = \alpha a + \beta b$.

Definition 10 (Irreducible). Let F be a field, and $f \in F[t] \setminus F$. Then f is irreducible if $\nexists g, h \in F[t] \setminus F$ of strictly smaller degree such that $f = gh$.

Definition 11 (Unique factorization domain). Let R be an integral domain. Then R is a unique factorization domain (UFD) if for irreducible $p_i \in R$, any nonzero $x \in R$ can be written uniquely (up to ordering) as $x = p_1 p_2 \cdots p_k$, $k \geq 1$.

Fact: If R is an Euclidean domain, then R is a UFD (and PID)

Corollary 2. Let $f \in \mathbb{F}[t]$ be a monic polynomial with $\deg f \geq 1$. Then we can write $f = f_1 f_2 \cdots f_k$ uniquely (up to ordering) for irreducible monic polynomials f_j .

Definition 12. Let R be a UFD. When $a_0, \dots, a_n \in R$ are not all 0, we can generalize the greatest common divisor of a_0, \dots, a_n (written $\gcd(a_0, \dots, a_n)$) any element $c \in R$ satisfying

- (i) $c \mid a_i$ ($0 \leq i \leq n$), and
- (ii) if $d \mid a_i$ ($0 \leq i \leq n$), then $d \mid c$.

When $f = \sum_{j=0}^d a_j x^j \in R[x]$ is a non-zero polynomial, we define a content of f to be any $\gcd(a_0, \dots, a_d)$ and $\gcd(f) = \gcd(a_0, \dots, a_d)$. We say that $f \in R[x]$ is primitive if $f \neq 0$ and the content of f is divisible only by units of R .

Lemma 1 (Gauss). $\gcd(fg) = \gcd f \cdot \gcd g$

Corollary 3. $f \in \mathbb{Z}[t]$ is irreducible $\iff f$ is irreducible over $\mathbb{Q}[t]$

Corollary 4. If R is a UFD with field of fractions Q and $f \in R[X]$ with $\deg f > 0$, then f is irreducible in $R[X] \iff f$ is irreducible in Q .

Theorem 3.2 (Eisenstein's Criterion). Let R be a UFD with field of fractions Q and let $f = a_0 + a_1 X + \dots + a_n X^n \in R[X]$ with $\gcd(f) = 1$. Suppose there exists an irreducible element $p \in R$ such that

- (i) $p \mid a_i$ for $0 \leq i < n$,
- (ii) $p^2 \nmid a_0$, and
- (iii) $p \nmid a_n$,

then f is irreducible in $R[X]$ (and hence also in $Q[X]$).

Definition 13 (Field extension). Let L and K be fields. Then L is an extension of K if there exists a homomorphism $\varphi : K \rightarrow L$. Then we write $L : K$ or L/K , $\varphi(K) \cong K$ and identify $\varphi(K)$ with K .

Fact: Suppose that L is a field extension of K with associated embedding $\varphi : K \rightarrow L$. Then L forms a vector space over K , under the operations

$$\begin{aligned} \text{(vector addition)} \quad \psi : L \times L &\rightarrow L \quad \text{given by} \quad (v_1, v_2) \mapsto v_1 + v_2 \\ \text{(scalar multiplication)} \quad \tau : K \times L &\rightarrow L \quad \text{given by} \quad (k, v) \mapsto \varphi(k)v. \end{aligned}$$

Definition 14 (Degree, finite extension). Let $L : K$. Then the degree of $L : K$ is $[L : K] = \dim L$ over K as a vector space. We say that $L : K$ is a finite extension if $[L : K] < \infty$.

Definition 15 (Tower, intermediate field). We say that $M : L : K$ is a tower of field extensions if $M : L$ and $L : K$ are field extensions, and in this case we say that L is an intermediate field (relative to the extension $M : K$)

Theorem 3.3 (The Tower Law). *Suppose that $M : L : K$ is a tower of field extensions. Then $M : K$ is a field extension, and $[M : K] = [M : L][L : K]$.*

Corollary 5. *Suppose that $L : K$ is a field extension for which $[L : K]$ is a prime number. Then whenever $L : M : K$ is a tower of field extensions with $K \subseteq M \subseteq L$, one has either $M = L$ or $M = K$.*

4 Field Extensions II

Definition 16 (Smallest subring/subfield). Let $L : K$ with $K \subseteq L$.

- (i) When $\alpha \in L$, we denote by $K[\alpha]$ the smallest subring of L containing K and α , and by $K(\alpha)$ the smallest subfield of L containing K and α ;
- (ii) More generally, when $A \subseteq L$, we denote by $K[A]$ the smallest subring of L containing K and A , and by $K(A)$ the smallest subfield of L containing K and A .

Then

$$K[\alpha] = \left\{ \sum_{i=0}^d c_i \alpha^i : d \in \mathbb{Z}_{\leq 0}, c_0, \dots, c_d \in K \right\}$$

$$K(\alpha) = \{f/g : f, g \in K[\alpha], g \neq 0\}.$$

Definition 17 (Algebraic/transcendental element). Suppose that $L : K$ is a field extension with $K \subseteq L$ and $\alpha \in L$.

- (i) We say α is algebraic over K if $\exists f \neq 0 \in K[t]$ such that $f(\alpha) = 0$.
- (ii) If α is not algebraic over K , then we say α is transcendental over K .
- (iii) When every element of L is algebraic over K , we say that L is algebraic over K .

Definition 18 (Evaluation map). Suppose that $L : K$ is a field extension with $K \subseteq L$, and that $\alpha \in L$. We define the evaluation map $E_\alpha : K[t] \rightarrow L$ by putting $E_\alpha(f) = f(\alpha)$ for each $f \in K[t]$.

Definition 19 (Minimal polynomial). Suppose that $L : K$ is a field extension with $K \subseteq L$, and suppose that $\alpha \in L$ is algebraic over K . Then the minimal polynomial of α over K is the unique monic polynomial μ_α^K having the property that $\ker(E_\alpha) = (\mu_\alpha^K)$.

Lemma 2. 1. μ_α^K is irreducible over K ;

2. If $f \in K[t]$ such that $f(\alpha) = 0$, then $\mu_\alpha^K \mid f$;

3. If $f \in K[t]$ such that $f(\alpha) = 0$ and f is irreducible over K , then $\exists k \in K$ such that $f = k\mu_\alpha^K$.

Theorem 4.1. Let $L : K$ with $K \subseteq L$, and suppose that $\alpha \in L$ is algebraic over K .

- (i) $K[\alpha]$ is a field, and $K[\alpha] = K(\alpha)$;
- (ii) If $n = \deg \mu_\alpha^K$, then $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ is a basis for $K(\alpha)$ over K ($\implies [K(\alpha) : K] = \deg \mu_\alpha^K$).

Theorem 4.2 (Rational Root Theorem). Let $\frac{p}{q}$ be a root of $f = a_0 t^n + \dots + a_{n-1} t^{n-1} + a_n$, for $a_j \in \mathbb{Z}$, where p and q are coprime. Then $p \mid a_n$ and $q \mid a_0$.

Note: If α is transcendental over K , then $K(\alpha) \cong K(x)$ (where x is a formal variable).

Corollary 6. Let $L : K$ with $K \subseteq L$, and suppose that $\alpha \in L$ is algebraic over K . Then every element of $K(\alpha)$ is algebraic over K .

Corollary 7. Let $L : K$ with $K \subseteq L$. Then $[L : K] < \infty \iff L = K(\alpha_1, \dots, \alpha_n)$ for $\alpha_j \in L$.

Theorem 4.3. Let $L : K$ be a field extension, and define

$$L^{\text{alg}} = \{\alpha \in L : \alpha \text{ is algebraic over } K\}.$$

Then L^{alg} is a subfield of L .

5 Algebraic Conjugates

Lemma 3. Let \mathbb{F} be a field with $f \in \mathbb{F}[t]$ irreducible. Then $\mathbb{F}[t]/(f)$ is a field.

Corollary 8. If $L : K$ with $\alpha \in L$ algebraic over K , then $K[t]/(\mu_\alpha^K)$ is a field.

Theorem 5.1. Let K be a field, and suppose that $f \in K[t]$ is irreducible. Then there exists a field extension $L : K$, with associated embedding $\varphi : K[t] \rightarrow L[y]$, having the property that L contains a root of $\varphi(f)$.

Definition 20 (Algebraic conjugate). Suppose α algebraic over K and μ_α^K factors as a product of linear polynomials over a field $L \supseteq K$:

$$\mu_\alpha^K(x) = (x - \alpha_1) \cdots (x - \alpha_n), \quad \alpha_1, \dots, \alpha_n \in L.$$

Then $\alpha_1, \dots, \alpha_n$ are algebraic conjugates of α .

Lemma 4. Let $(x - \alpha_1) \cdots (x - \alpha_n) \in K[x]$ and $f(\bar{y}, x_1, \dots, x_n) \in K[\bar{y}, x_1, \dots, x_n]$ be symmetric polynomial in x_1, \dots, x_n . Then $f(\bar{y}, x_1, \dots, x_n) \in K[\bar{y}]$.

Theorem 5.2. Let α be algebraic over K with algebraic conjugates $\alpha = \alpha_1, \dots, \alpha_n$. Then for all $f \in K[x]$, the conjugates of $f(\alpha)$ are exactly $f(\alpha_1), \dots, f(\alpha_n)$.

6 Ruler and Compass Constructions

7 Cyclotomic Polynomials

Theorem 7.1. For prime p , we have $x^p - 1 = (x - 1)(x^{p-1} + \cdots + 1)$ and $\mu_{\varepsilon_p}^{\mathbb{Q}} = x^{p-1} + \cdots + 1$.

Definition 21 (n^{th} cyclotomic polynomial).

$$\Phi_n(x) = \prod_{\substack{\varepsilon \in \sqrt[n]{1} \\ |\varepsilon|=n}} (x - \varepsilon) = \frac{x^n - 1}{\prod_{d|n, d < n} \Phi_d(x)}$$

Theorem 7.2. Φ_n is irreducible over \mathbb{Q} .

Corollary 9. (a) $[\mathbb{Q}(\exp(\frac{2\pi i}{n})) : \mathbb{Q}] = \varphi(n)$ (where φ is Euler's totient function);

(b) $[\mathbb{Q}(\cos(\frac{2\pi}{n})) : \mathbb{Q}] = \frac{1}{2}\varphi(n)$. Furthermore, all algebraic conjugates of $\cos \frac{2\pi}{n}$ are $\cos \frac{2\pi k}{n}$ for $\gcd(k, n) = 1$.

(c) Let $c = \frac{a+bi}{a-bi} \in \sqrt[n]{1}$, where $a, b \in \mathbb{Z}$. Then $c \in \{\pm i, \pm 1\}$

Lemma 5. Let \mathbb{F} be a finite field. Then $\mathbb{F}^\times = \mathbb{F} \setminus \{0\}$ is a cyclic group.

8 Splitting Fields, Abel-Ruffini

Definition 22 (Splitting field). Let $L : K$ with embedding $\varphi : K \rightarrow L$ and $f \in K[t] \setminus K$. We say f splits over L if $\varphi(f) = c \prod_{j=1}^n (x - \alpha_j)$ for $\alpha_j \in L$ and $c \in \varphi(K)$. We say that $M : K$ is a splitting field extension for f if f splits over L , $\varphi(K) \subseteq M \subseteq L$, and M is the smallest subfield of L containing $\varphi(K)$ over which f splits.

Lemma 6. Let $L : K$ be a splitting field extension for $f \in K[t]$ relative to the embedding $\varphi : K \rightarrow L$, and let $\alpha_j \in L$ be roots of $\varphi(f)$. Then $L = \varphi(K)(\alpha_1, \dots, \alpha_n)$.

Lemma 7. Let $L : K$ be a splitting field extension for $f \in K[t] \setminus K$. Then $[L : K] \leq (\deg f)!$.

Lemma 8. Let $L : K$ and $M : K$ be splitting field extensions for $f \in K[t] \setminus K$. Then $L \cong M$ (in particular, $[L : K] = [M : K]$).

Definition 23 (Radical, radical extension, solvability by radicals). Let $L : K$ and $\beta \in L$. We say that β is radical over K when $\beta^n \in K$ for some $n \in \mathbb{N}$ (so $\beta = \alpha^{1/n}$ for some $\alpha \in K$ and some $n \in \mathbb{N}$). We say that $L : K$ is an extension by radicals when there is a tower of field extensions $L = L_r : L_{r-1} : \dots : L_0 = K$ such that $L_i = L_{i-1}(\beta_i)$ with β_i radical over L_{i-1} (for $1 \leq i \leq r$). We say $f \in K[t]$ is solvable by radicals if there is a radical extension of K over which f splits.

Theorem 8.1 (Abel-Ruffini). Let $K = \mathbb{C}(a_1, \dots, a_n)$ where a_1, \dots, a_n are formal variables. Let $f(x) = x^n + a_1x^{n-1} + \dots + a_n \in K[x]$ be the generic polynomial of degree $n \geq 5$ over K . Then $f(x)$ is not solvable by radicals.

9 Algebraic Closure I

Definition 24 (Algebraically closed field, algebraic closure). Let M be a field.

- (i) We say that M is algebraically closed if every non-constant polynomial $f \in M[t]$ has a root in M .
- (ii) We say that M is an algebraic closure of K if $M : K$ is an algebraic field extension having the property that M is algebraically closed.

Lemma 9. Let M be a field. The following are equivalent:

- (i) The field M is algebraically closed;
- (ii) every non-constant polynomial $f \in M[t]$ factors in $M[t]$ as a product of linear factors;
- (iii) every irreducible polynomial in $M[t]$ has degree 1;
- (iv) the only algebraic extension of M containing M is itself.

Definition 25 (Chain). Suppose that X is a nonempty, partially ordered set with \leq denoting the partial ordering. A chain C in X is a collection of elements $\{a_i\}_{i \in I}$ of X having the property that for every $i, j \in I$, either $a_i \leq a_j$ or $a_j \leq a_i$.

Zorn's Lemma: Suppose that X is a nonempty, partially ordered set with \leq the partial ordering. If every non-empty chain C in X has an upper bound in X , then X has at least one maximal element m (i.e. $b \in X$ with $m \leq b \implies b = m$).

Corollary 10. Any proper ideal A of a commutative ring R is contained in a maximal ideal.

Lemma 10. Let K be a field. Then there exists an algebraic extension $E : K$, with $K \subseteq E$, having the property that E contains a root of every irreducible $f \in K[t]$, and hence also every $g \in K[t] \setminus K$.

Theorem 9.1 (Existence of Algebraic Closures). Suppose that K is a field. Then there exists an algebraic extension \overline{K} of K having the property that \overline{K} is algebraically closed.

Definition 26 (Extension of field homomorphism, isomorphic field extensions). For $i = 1$ and 2 , let $L_i : K_i$ be a field extension relative to the embedding $\varphi_i : K_i \rightarrow L_i$. Suppose that $\sigma : K_1 \rightarrow K_2$ and $\tau : L_1 \rightarrow L_2$ are isomorphisms. We say that τ extends σ if $\tau \circ \varphi_1 = \varphi_2 \circ \sigma$. In such circumstances, we say that $L_1 : K_1$ and $L_2 : K_2$ are isomorphic field extensions.

$$\begin{array}{ccc} L_1 & \xrightarrow{\tau} & L_2 \\ \uparrow \varphi_1 & \nearrow & \uparrow \varphi_2 \\ K_1 & \xrightarrow{\sigma} & K_2 \end{array}$$

When $\sigma : K_1 \rightarrow K_2$ and $\tau : L_1 \rightarrow L_2$ are homomorphisms (instead of isomorphisms), then τ extends σ as a homomorphism of fields when the isomorphism $\tau : L_1 \rightarrow L'_1 = \tau(L_1)$ extends the isomorphism $\sigma : K_1 \rightarrow K'_1 = \sigma(K_1)$.

Definition 27 (K -homomorphism). Let $L : K$ be a field extension relative to the embedding $\varphi : K \rightarrow L$, and let M be a subfield of L containing $\varphi(K)$. Then, when $\sigma : M \rightarrow L$ is a homomorphism, we say that σ is a K -homomorphism if σ leaves $\varphi(K)$ pointwise fixed, which is to say that for all $\alpha \in \varphi(K)$, one has $\sigma(\alpha) = \alpha$.

Lemma 11. Suppose that $L : K$ is a field extension with $K \subseteq L$, and that $\tau : L \rightarrow L$ is a K -homomorphism. Suppose that $f \in K[t]$ has the property that $\deg f \geq 1$, and additionally that $\alpha \in L$.

- (i) if $f(\alpha) = 0$, one has $f(\tau(\alpha)) = 0$;
- (ii) if τ is a K -automorphism of L , then $f(\alpha) = 0 \iff f(\tau(\alpha)) = 0$.

Theorem 9.2. Let $\sigma : K_1 \rightarrow K_2$ be a field isomorphism. Suppose that L_i is a field with $K_i \subseteq L_i$ ($i = 1, 2$). Suppose also that $\alpha \in L_1$ is algebraic over K_1 , and that $\beta \in L_2$ is algebraic over K_2 . Then we can extend σ to an isomorphism $\tau : K_1(\alpha) \rightarrow K_2(\beta)$ in such a manner that $\tau(\alpha) = \beta$ if and only if $m_\beta(K_2) = \sigma(m_\alpha(K_1))$.

$$\begin{array}{ccccc} K_2 & \xrightarrow{\varphi_2} & K_2(\beta) & \xhookrightarrow{\iota_2} & L_2 \\ \downarrow \sigma & & \downarrow \tau & & \\ K_1 & \xrightarrow{\varphi_1} & K_1(\alpha) & \xhookrightarrow{\iota_1} & L_1 \end{array}$$

Note: When $\tau : K_1(\alpha) \rightarrow K_2(\beta)$ is a homomorphism, and τ extends the homomorphism $\sigma : K_1 \rightarrow K_2$, then τ is completely determined by σ and the value of $\tau(\alpha)$.

Corollary 11. Let $L : M$ be a field extension with $M \subseteq L$. Suppose that $\sigma : M \rightarrow L$ is a homomorphism, and $\alpha \in L$ is algebraic over M . Then the number of ways we can extend σ to a homomorphism $\tau : M(\alpha) \rightarrow L$ is equal to the number of distinct roots of $\sigma(m_\alpha(M))$ that lie in L .

10 Algebraic Closure II

Theorem 10.1. Let $L : K$ be an algebraic extension with $K \subseteq L$ and $\varphi : K \rightarrow \overline{K}$ be a homomorphism. Then there exists an extension of φ to a homomorphism $\psi : L \rightarrow \overline{K}$.

Theorem 10.2. If L and M are both algebraic closures of K , then $L \cong M$.

Corollary 12. Let $L : K$ be an extension with $K \subseteq L$. Suppose that $g \in L[t]$ is irreducible over L , and that $g \mid f$ in $L[t]$, where $f \in K[t] \setminus \{0\}$. The g divides a factor of f that is irreducible over K .

Thus, there exists an irreducible $h \in K[t]$ having the property that $h \mid f$ in $K[t]$, and $g \mid h$ in $L[t]$.

Definition 28 (Normal extension). The extension $L : K$ is normal if it is algebraic, and every irreducible polynomial $f \in K[t]$ either splits over L or has no root in L .

Theorem 10.3. $K(\alpha) : K$ is normal \iff all conjugates of α are contained in $K(\alpha)$.

Theorem 10.4. A finite extension $L : K$ is normal $\iff L$ is a splitting field extension for some $f \in K[t] \setminus K$.

11 Galois Groups I

Definition 29 (Galois group of polynomial). Let $L = K(\alpha_1, \dots, \alpha_n)$ and let $P(\alpha_1, \dots, \alpha_n)$ where $P \in K[\alpha_1, \dots, \alpha_n]$ is an element of L . Then we define

$$\text{Gal}_K(f) = \{\sigma \in S_n \mid \forall P \in K[\alpha_1, \dots, \alpha_n], \text{ if } P(\alpha_1, \dots, \alpha_n) = 0 \text{ then } P(\alpha_{\sigma(1)}, \dots, \alpha_{\sigma(n)}) = 0\}$$

Lemma 12. 1. $\text{Gal}_K(f) \leq S_n$;

2. If $K_1 : K$, then $\text{Gal}_{K_1}(f) \leq \text{Gal}_K(f)$.

Definition 30. Let $L : K$ be a field extension. Then

$$\text{Gal}_K(L) = \text{Gal}(L : K) = \{\varphi \in \text{Aut}(L) : \varphi \text{ is a } K\text{-homomorphism}\}$$

Definition 31 (Galois automorphism on splitting field). Let $\sigma \in \text{Gal}_K f$ where L is a splitting field for f over K , and define $\hat{\sigma} \in \text{Aut}_K(L)$ such that $\hat{\sigma}(P(\alpha_1, \dots, \alpha_n)) = P(\alpha_{\sigma(1)}, \dots, \alpha_{\sigma(n)})$.

Lemma 13. The map $\psi(\sigma) = \hat{\sigma}$ is a group isomorphism.

Theorem 11.1. If $L : K$ is an algebraic extension and $\sigma : L \rightarrow L$ is a K -homomorphism, then $\sigma \in \text{Aut}(L)$

Lemma 14. Suppose that $M : K$ is a normal extension. Then:

- (a) for any $\sigma \in \text{Gal}(M : K)$ and $\alpha \in M$, we have $\mu_{\sigma(\alpha)}^K = \mu_{\alpha}^K$;
- (b) for any $\alpha, \beta \in M$ with $\mu_{\alpha}^K = \mu_{\beta}^K$, there exists $\tau \in \text{Gal}(M : K)$ having the property that $\tau(\alpha) = \beta$.

12 Galois Groups II

Lemma 15. Suppose that $L : K$ is a normal extension with $K \subseteq L \subseteq \overline{K}$. Then for any K -homomorphism $\tau : L \rightarrow \overline{K}$, we have $\tau(L) = L$.

Lemma 16. For $n \geq 2$, S_n is generated by

- 1. transpositions (ij) ;
- 2. transpositions $(1i)$;
- 3. adjacent transpositions $(12), (23), \dots, (n-1, n)$;
- 4. (12) and $(12 \dots n)$;
- 5. (12) and $(23 \dots n)$;
- 6. (ij) and $(i \dots i_p)$ where p is prime.

Lemma 17. Let $(i_1 \dots i_k) \in S_n$. Then for all $\sigma \in S_n$, one has $\sigma(i_1 \dots i_k)\sigma^{-1} = (\sigma(i_1) \dots \sigma(i_k))$.

Note: $|\text{Gal}_K(f)| = [L : K]$ where $L : K$ is a splitting field extension for f .

13 Galois Groups III

Theorem 13.1 (Kronecker). Let $p \geq 3$ be a prime and $f \in \mathbb{Q}[x]$ be irreducible over \mathbb{Q} with $\deg f = p$. If the equation $f(x) = 0$ is solvable by radicals, then the number of real roots of f is 1 or p .

Lemma 18. Let p be prime and $G \leq S_p$ such that G acts transitively on $\{1, \dots, p\}$. Then G contains a cycle of order p .

Theorem 13.2. If $L : K$ is a finite extension, then $|\text{Gal}_K(L)| \leq [L : K]$.

14 Separability

Definition 32 (Separable). Let K be a field.

- (i) An irreducible polynomial $f \in K[t]$ is separable over K if it has no multiple roots, meaning that $f = \lambda(t - \alpha_1)(t - \alpha_2) \cdots (t - \alpha_d)$, where $\alpha_1, \dots, \alpha_d \in \bar{K}$ are distinct.
- (ii) A non-zero polynomial $f \in K[t]$ is separable over K if its irreducible factors in $K[t]$ are separable over K .
- (iii) When $L : K$ is a field extension, we say that $\alpha \in L$ is separable over K when α is algebraic over K and μ_α^K is separable.
- (iv) An algebraic extension $L : K$ is a separable extension if every $\alpha \in L$ is separable over K .

Lemma 19. Suppose that $L : M : K$ is a tower of algebraic field extensions. Assume that $K \subseteq M \subseteq L \subseteq \bar{K}$, and suppose that $f \in K[t] \setminus K$ satisfies the property that f is separable over K . If $g \in M[t] \setminus M$ has the property that $g \mid f$, then g is separable over M . Thus, if $\alpha \in L$ is separable over K then α is separable over M , and if $L : K$ is separable then so is $L : M$.

Lemma 20. 1. If $L : M$ is an algebraic field extension, $\alpha \in L$ and $\sigma : M \rightarrow \bar{M}$ is a homomorphism, then $\sigma(\mu_\alpha^M)$ is separable over $\sigma(M) \iff \mu_\alpha^M$ is separable over M .

2. If $L : K$ is a splitting field extension for $f \in K[t]$ and f is separable over K , then $L : K$ is separable.

Theorem 14.1. Let $L : K$ be a finite extension with $K \subseteq L \subseteq \bar{K}$, whence $L = K(\alpha_1, \dots, \alpha_n)$ for some $\alpha_1, \dots, \alpha_n \in L$. Put $K_0 = K$, and for $1 \leq i \leq n$, set $K_i = K_{i-1}(\alpha_i)$. Finally, let $\sigma_0 : K \rightarrow \bar{K}$ be the inclusion map.

- (i) If α_i is separable over K_{i-1} for $1 \leq i \leq n$, then there are $[L : K]$ ways to extend σ_0 to a homomorphism $\tau : L \rightarrow \bar{K}$.
- (ii) If α_i is not separable over K_{i-1} for some i with $1 \leq i \leq n$, then there are fewer than $[L : K]$ ways to extend σ_0 to a homomorphism $\tau : L \rightarrow \bar{K}$.

Theorem 14.2. Let $L : K$ be a finite extension with $L = K(\alpha_1, \dots, \alpha_n)$. Set $K_0 = K$, and for $1 \leq i \leq n$, inductively define K_i by putting $K_i = K_{i-1}(\alpha_i)$. Then the following are equivalent:

- (i) the element α_i is separable over K_{i-1} for $1 \leq i \leq n$;
- (ii) the element α_i is separable over K for $1 \leq i \leq n$;
- (iii) the extension $L : K$ is separable.

Corollary 13. Suppose that $L : K$ is a finite extension. If $L : K$ is a separable extension, then the number of K -homomorphism $\sigma : L \rightarrow \bar{K}$ is $[L : K]$, and otherwise the number is smaller than $[L : K]$.

Corollary 14. Suppose that $f \in K[t] \setminus K$ and that $L : K$ is a splitting field extension for f . Then $L : K$ is a separable extension $\iff f$ is separable over K . More generally, suppose that $L : K$ is a splitting field extension for $S \subseteq K[t] \setminus K$. Then $L : K$ is a separable extension \iff each $f \in S$ is separable over K .

15 The Primitive Element Theorem

Definition 33 (Simple extension). Suppose $L : K$ is a field extension relative to the embedding $\varphi : K \rightarrow L$. We say that $L : K$ is a simple extension if there is some $\gamma \in L$ having the property that $L = \varphi(K)(\gamma)$.

Theorem 15.1 (The Primitive Element Theorem). If $L : K$ be a finite, separable extension with $K \subseteq L$, then $L : K$ is a simple extension.

Corollary 15. Suppose that $L : K$ is an algebraic, separable extension, and suppose that for every $\alpha \in L$, the polynomial μ_α^K has degree at most n over K . Then $[L : K] \leq n$.

Fact: Let $L : K$ be a normal extension and let $\deg(\mu_\alpha^K) \leq n$ for all $\alpha \in L$. Then $[L : K] \leq n$.

Corollary 16. If $f \in K[t]$ is irreducible over K , then $\text{Gal}_K(f)$ acts transitively on the roots of f .

16 Galois Fields I

Definition 34 (Formal derivative). We define the derivative operator $\mathcal{D} : K[t] \rightarrow K[t]$ by

$$\mathcal{D} \left(\sum_{k=0}^n a_k t^k \right) = \sum_{k=1}^n k a_k t^{k-1}.$$

Theorem 16.1. Let $f \in K[t] \setminus K$, and let $L : K$ be a splitting field extension for f . Assume that $K \subseteq L$. Then the following are equivalent:

- (i) The polynomial f has a repeated root over L ;
- (ii) There is some $\alpha \in L$ for which $f(\alpha) = 0 = (\mathcal{D}f)(\alpha)$;
- (iii) There is some $g \in K[t]$ having the property that $\deg g \geq 1$ and g divides both f and $\mathcal{D}f$.

Definition 35 (Inseparable). A polynomial $f \in K[t]$ is inseparable over K if f is not separable over K , meaning that f has an irreducible factor $g \in K[t]$ having the property that g has fewer than $\deg g$ distinct roots in K .

Theorem 16.2. Suppose that $f \in K[t]$ is irreducible over K . Then f is inseparable over K if and only if $\text{char}(K) = p > 0$, and $f \in K[t^p]$, which is to say that $f = a_0 + a_1 t^p + \cdots + a_m t^{mp}$, for some $a_0, \dots, a_m \in K$.

Definition 36 (Frobenius map). Suppose that $\text{char}(K) = p > 0$. The Frobenius map $\phi : K \rightarrow K$ is defined by $\phi(\alpha) = \alpha^p$.

Theorem 16.3. Suppose that $\text{char}(K) = p > 0$, and put $F = \{c \cdot 1_K : c \in \mathbb{Z}\}$. Then F is a subfield (called the prime subfield) of K , and $F \cong \mathbb{Z}/p\mathbb{Z}$.

Definition 37 (Fixed field). Let $L : K$ be a field extension. When G is a subgroup of $\text{Aut}(L)$, we define the fixed field of G to be

$$\text{Fix}_L(G) = \{\alpha \in L : \sigma(\alpha) = \alpha \text{ for all } \sigma \in G\}.$$

Theorem 16.4. Suppose that $\text{char}(K) = p > 0$, and let F be the prime subfield of K . Let $\phi : K \rightarrow K$ denote the Frobenius map. Then ϕ is an injective homomorphism, and $\text{Fix}_\phi(K) = F$.

Corollary 17. Suppose that $\text{char}(K) = p > 0$ and K is algebraic over its prime subfield. Then the Frobenius map is an automorphism of K .

Corollary 18. Suppose that $\text{char}(K) = p > 0$ and K is algebraic over its prime subfield. Then all polynomials in $K[t]$ are separable over K .

Corollary 19 (**). Suppose that $\text{char}(K) = 0$. Then all polynomials in $K[t]$ are separable over K .

Theorem 16.5. Suppose that $\text{char}(K) = p > 0$. Let

$$f(t) = g(t^p) = a_0 + a_1 t^p + \cdots + a_{n-1} t^{(n-1)p} + t^{np}$$

be a non-constant monic polynomial over K . Then $f(t)$ is irreducible in $K[t]$ if and only if $g(t)$ is irreducible in $K[t]$ and not all the coefficients a_i are p -th powers in K .

17 Galois Fields II

Theorem 17.1. *Let p be a prime, and let $q = p^n$ for some $n \in \mathbb{N}$. Then:*

- (a) *There exists a field \mathbb{F}_q of order q , and this field is unique up to isomorphism.*
- (b) *All elements of \mathbb{F}_q satisfy the equation $t^q = t$, and hence $\mathbb{F}_q : \mathbb{F}_p$ is a splitting field extension for $t^q - t$.*
- (c) *There is a unique copy of \mathbb{F}_q inside any algebraically closed field containing \mathbb{F}_p .*

Theorem 17.2. *Let p be a prime, and suppose that $q = p^n$ for some $n \in \mathbb{N}$. Then:*

- (a) $\text{Gal}(\mathbb{F}_q : \mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$;
- (b) *The field \mathbb{F}_q contains a subfield of order p^d if and only if $d \mid n$. When $d \mid n$, moreover, there is a unique subfield of \mathbb{F}_q of order p^d .*

Definition 38 (Norm, Trace). Let p be a prime and let $\alpha \in \mathbb{F}_q$ where $q = p^n$ for some $n \in \mathbb{N}$. Then we define

$$\begin{aligned}\text{Tr}(\alpha) &= \alpha + \alpha^p + \cdots + \alpha^{p^{n-1}} \\ &= \alpha + \varphi(\alpha) + \cdots + \varphi^{n-1}(\alpha)\end{aligned}$$

and

$$\begin{aligned}\text{Norm}(\alpha) &= \alpha \cdot \alpha^p \cdots \alpha^{p^{n-1}} = \alpha^{\frac{p^n-1}{p-1}} \\ &= \alpha \cdot \varphi(\alpha) \cdots \varphi^{n-1}(\alpha)\end{aligned}$$

Lemma 21. *Let p be a prime and let $\alpha \in \mathbb{F}_q$ where $q = p^n$ for some $n \in \mathbb{N}$.*

- 1. *For all $\alpha \in \mathbb{F}_q$, one has $\text{Tr}(\alpha), \text{Norm}(\alpha) \in \mathbb{F}_p$;*
- 2. *If $p \neq 2$, then $\exists \alpha_1$ such that $\text{Tr}(\alpha_1) \neq 0$ and $\exists \alpha_2 (\neq 0)$ such that $\text{Norm}(\alpha_2) \neq 1$.*