Galois Theory

Kevin

October 2024

1 Field extensions

A field k contains a smallest subfield (prime subfield) isomorphic to $\mathbb{F}_p$ if k as characteristic p or $\mathbb{Q}$ if k has characteristic 0.

Lemma 1.1. *Let K be a field, $0 \neq f \in k[X]$, then f has $\leq \deg f$ roots in k*

Definition. Let L be a field and $K \subseteq L$ a subfield. We say that L is an extension of K, written L/K.

Note that L, K necessarily have the same characteristic.

Example 1.2.

- $\mathbb{C}/\mathbb{R}$, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, $\mathbb{R}/\mathbb{Q}$
- (Adjoining a root of an irreducible polynomial) Let K be a field and $f \in k[X]$ irreducible. Recall that $k[X]$ is a PID, so (f) is a maximal ideal. Then $L = k[X]/(f)$ is a field extension of K and $\alpha = X + (f)$ is a root of f in L.

Let L/K be a field extension. Then L can be regarded as a K-vector space.

Definition. Let L/K be a field extension. Say L/K is finite if L is a finite dimensional K-vector space. We write $[L : K] = \dim_K L$ for its dimension which is called the degree of L/K. If note, then L/K is an infinite extension and write $[L : K] = \infty$.

We say that L/K is a quadratic (cubic, quartic, etc.) extension if $[L : K] = 2$ $(3, 4, ...)$. When $K = \mathbb{Q}$, we simply say L/K is quadratic, cubic, etc.

Example 1.3. $[\mathbb{C} : \mathbb{R}] = 2$, $[\mathbb{R} : \mathbb{Q}] = \infty$ If $L = K[X]/(f)$, f irred. over K, then $[L : K] = \deg f$.

Remark 1. Let K, L be field and $\phi : K \to L$ ring hom. $\ker \phi = \{0\}$ is forced as a field only has two ideals, so ϕ is an embedding, meaning that we can identify K as a subfield of L, i.e., we get a field extension.

Proposition 1.4. *Let K be a finite field of characteristic p, then $|K| = p^n$, where $n = [K : \mathbb{F}_p]$.*

Proof. $K \cong \mathbb{F}_p^n$ as an $\mathbb{F}_p$-vector space. □

Later will show that up to iso, there exists a unique fiel of order p^n for each prime p.

Proposition 1.5. *If K is a field then any finite subgroup $G \leq K^*$ is cyclic.*

Proof. By structure theorem, $G \cong C_{d_1} \times ... \times C_{d_t}$ where $1 < d_1 \mid ... \mid d_t$. If not cyclic then pick a prime $p \mid d_1$ and G contains a subgroup isomorphic to $C_p \times C_p$. Count the elements of order p (roots of $x^p - 1$), we get a contradiction. □

Proposition 1.6. *Let R be a ring of char p prime, Then the Frobenius map $\phi : R \to R$, $x \mapsto x^p$ is a ring hom.*

Proof. Expand $(x + y)^p$ and use characteristic. We get $(x + y)^p = x^p + y^p$ which proves additivity. The rest is trivial. □

Remark 2. Have $\phi(a) = a$ for all $a \in \mathbb{F}_p \subseteq R$. So Fermat's little theorem is a trivial consequence of the proposition above.

Theorem 1.7 (Tower law)**.** *Let M/L and L/K be field extensions. M/K is finite $\Leftrightarrow$ M/L and L/K are both finite. In this situation, $[M : K] = [M : L][L : K]$*

Proof. "⇒": As an L-vector sapce, M is finite dim, and L is a K-subspace of M so also finite dim over K.

"⇐": Let $v_1, ..., v_n$ be a K-basis of L and $w_1, ..., w_m$ an L-basis for M. We claim that $\{v_i w_j\}$ is a K-basis of M.

- (Spanning) If $x \in M$, then $x = \sum \lambda_j w_j = \sum \mu_{ij} v_i w_j$ by spanning properties of the given basis.
- (Independence) If $\sum \mu_{ij} v_i w_j = 0$, then $\sum_j \left(\sum_i \mu_{ij} v_i\right) w_j = 0$, so $\sum_i \mu_{ij} v_i = 0$ for all j, so $\mu_{ij} = 0$ for all i, j.

□

Definition. Let L/K be a field extension. Let $\alpha_1, ..., \alpha_n \in L$, then $K[\alpha_1, ..., \alpha_n]$ is the samllest subring of L containint K and $\alpha_1, ..., \alpha_n$. $K(\alpha_1, ..., \alpha_n) = \{\frac{f(\alpha_1,...,\alpha_n)}{g(\alpha_1,...,\alpha_n)} : f, g \in K[x_1, ..., x_n]\}$ is the smallest subfield of L containing K and α_i.

Observe that $K(\alpha_1, ..., \alpha_n)$ is the field of fractions of $K[\alpha_1, ..., \alpha_n]$.

Definition. A field extension L/K is said to be simple if $L = K(\alpha)$ for some $\alpha \in L$.

Observe that the evaluation map $\phi : K[X] \to L$ is a ring hom and is the unique ring hom such that $\phi(c) = c$ for all $c \in K$, and $\phi(X) = \alpha$.

Definition. Let $(f) = \ker \phi$. α is algebraic if $f \neq 0$. Otherwise α is said to be transcendental.

If α is algebraic, then f is irreducible and unique up to units. We scale f to make it monic.

Definition. This monic f is called the minimal polynomial of α over K.

By 1st isomorphism theorem, $K[X]/(f) = K[\alpha]$, so in this case $K(\alpha) = K[\alpha]$. Moreover, $[K(\alpha); K] = \deg f$.

Remark 3. If we want to compute the inverse of $\alpha \in L$ which is algebraic over K with min polynomial f over K, then choose $0 \neq \beta \in K(\alpha)$ and we have $\beta = g(\alpha)$ for some $g \in K[X]$. Since f is irreducible and $\beta \neq 0$, f, g are coprime, then can run Euclidean algorithm.

Definition. A field extension L/K is algebraic if for all $\alpha \in L$, α is algebraic over K.

Remark 4. $[K(\alpha) : K] < \infty$ iff α is algebraic over K. If $[L : K] < \infty$, then L/K is algebraic.

Example 1.8. $K = \mathbb{Q}$, $L = \bigcup_n \mathbb{Q}(\sqrt[2^n]{2})$ is an infinite algebraic extension.

Lemma 1.9. *Let L/K be a field extension and $\alpha_1, ..., \alpha_n \in L$, then $\alpha_1, ..., \alpha_n$ are algebraic over K iff $[K(\alpha_1, ..., \alpha_n) : K] < \infty$.*

Proof. "only if": Adjoin a single α_i at a time and observe that each step gives a finite extension. □

Corollary 1.10. *Let L/K be a field extension. $\{\alpha \in L : \alpha$ algebraic over $K\}$ is a subfield of L*

Proof. If α, β are algebraic, then $\alpha \pm \beta, \alpha\beta, 1/\alpha$ $(\alpha \neq 0)$ are elements of $K(\alpha, \beta)$ which is an algebraic extension by the preceding lemma. □

Proposition 1.11. *M/L, L/K are field extensions. Then M/K is algebraic iff M/L and L/K are both algebraic*

Proof. "only if": Clear (by definition).

"if": If $\alpha \in M$, then there exists $f = c_0 + c_1 X + ... + c_n X^n \in L[X]$ s.t. $f(\alpha) = 0$. Let $L_0 = K(c_0, ..., c_n)$. Since each c_i is algebraic over K, $[L_0 : K] < \infty$. Also, $[L_0(\alpha) : L_0] \leq \deg f < \infty$. So $[L_0(\alpha) : K] < \infty$ by tower law, so α is algebraic over K. □

Example 1.12.

- Let $f(x) = x^d - n$, where $n, d \in \mathbb{Z}, d \geq 2, n \neq 0$. Suppose there exists p prime s.t. $n = p^e m$, $p \nmid m$ and $(d, e) = 1$, then we claim that f is irreducible over $\mathbb{Q}$ and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = d$, where $\alpha = \sqrt[d]{n}$.

  By Bezout's lemma, can find $r, s \in \mathbb{Z}$ s.t. $rd + se = 1$. We may arrange so that $s > 0$. Then $p^{dr} n^s = p^{dr}(p^e m)^s = pm^s$. We put $\beta = p^r \alpha^s$ so that $\beta^d = pm^s$, then β is a root of $g(x) = x^d - pm^s$, which is irreducible over $\mathbb{Z}$ by Eisenstein's criterion and hence irreducible over $\mathbb{Q}$ by Gauss's lemma. So $[\mathbb{Q}(\beta) : \mathbb{Q}] = d$ and $[\mathbb{Q}(\alpha) : \mathbb{Q}] \leq d$, but $\mathbb{Q}(\beta) \subseteq \mathbb{Q}(\alpha)$, so in fact $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$ and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = d$.

- Let ζ_p be a primitive pth root of unity, where p is an odd prime. Let $\alpha = \zeta_p + \zeta_p^{-1}$. We want to compute the degree of $\mathbb{Q}(\alpha)/\mathbb{Q}$. ζ_p is a root of $(x^p - 1)/(x - 1)$ which is irreducible (GRM), so $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p-1$. Observe that over $\mathbb{Q}(\alpha)$, ζ_p is a root of $g(x) = x^2 - \alpha x + 1$. So $[\mathbb{Q}(\zeta_p) : \mathbb{Q}(\alpha)] = 1, 2$. It can't be one since one contains complex numbers and the other is real, so $[\mathbb{Q}(\alpha) : \mathbb{Q}] = (p-1)/2$ by tower law.
- $\mathbb{Q}(\alpha)$, $\alpha = \sqrt{m} + \sqrt{n}$, m, n, mn not squares. Clearly, $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{m}, \sqrt{n})$. Conversely, can write $m = \alpha^2 - 2\alpha\sqrt{n} + n$, so $\sqrt{n} = (\alpha^2 - m + n)/(2\alpha)$, so $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{m}, \sqrt{n})$. $[\mathbb{Q}(\sqrt{m}, \sqrt{n}) : \mathbb{Q}(\sqrt{n})] \leq 2$ as $\sqrt{m}$ is a root of $X^2 - m$. Can show by squaring and rationality that $\sqrt{m} \notin \mathbb{Q}(\sqrt{n})$, so $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ by tower law.

2 Ruler and Compass Construction

Given a finite set of points $S \subseteq \mathbb{R}^2$, the following operations are allowed.

1. Draw a straight line through two points in S.
2. Draw a circle with center $x \in S$ and radius the distance between two points in S.
3. Enlarge S by adjoining the intersection of two discint lines/circles.

Definition. $(x, y) \in \mathbb{R}^2$ is constructible from S if one can enlarge S to contain (x, y) by a finite sequence of operations above. We say that $x \in \mathbb{R}$ is constructible if $(x, 0)$ can be constructed from $\{(0, 0), (1, 0)\}$.

Definition. A subfield $K \subseteq \mathbb{R}$ is constructible if there exists $n \geq 0$ and a sequence of subfields of $\mathbb{R}$, $\mathbb{Q} = F_0 \subseteq F_1 \subseteq ... \subseteq F_n$ s.t. $K \subseteq F_n$.

Remark 5. By tower law, $[K : \mathbb{Q}]$ is a power of 2.

Theorem 2.1. *If $x \in \mathbb{R}$ is contructible then $\mathbb{Q}(x)$ is a constructible subfield of $\mathbb{R}$.*

Proof. Suppose $S \subseteq \mathbb{R}^2$ is a finite set of points all of whose coordinates belong to a constructible subfield K. It suffices to show that if we adjoin $(x, y) \in \mathbb{R}^2$ to S by using allowed operations, then $K(x, y)$ is also constructible.

Note that (x, y) is a point of intersection of two lines/circles, so $x = r + s\sqrt{v}, y = t + u\sqrt{v}$ (all coeff are in K). Then, $(x, y) \in K(\sqrt{v}) \subseteq F_n(\sqrt{v})$, where F_n is the last subfield in the increasing sequence ($K \subseteq F_n$). So $F_n(\sqrt{v})$ is a degree 1 or 2 extension of F_n, so $K(x, y)$ is constructible. □

Remark 6. It can be shown that $(x \pm y, 0)$, $(x/y, 0)$, and $(\sqrt{x}, 0)$ are constructible from $(0, 0), (1, 0), (x, 0), (y, 0)$. Also, the converse of the theorem holds, i.e., $\mathbb{Q}(x)$ constructible $\implies$ x constructible. (why?)

Corollary 2.2. *If $x \in \mathbb{R}$ is constructible then x is algebraic over $\mathbb{Q}$ and $[\mathbb{Q}(x) : \mathbb{Q}]$ is a power of 2.*

Example 2.3. Some classical problems:

- Constructing a square with equal area as a circle with random radius is impossible since this amounts to constructing $\sqrt{\pi}$
- Construdcting a cube whose volume is twice that of a give cube is impossible as this amounts to constructing $\sqrt[3]{2}$, which has degree 3 over $\mathbb{Q}$.
- There is no general method of trisecting an angle. For instance when the angle is $2\pi/3$. If $2\pi/9$ is constructible then $\cos(2\pi/9)$ is constructible, but we see that $2\cos(2\pi/9)$ has minimal polynomial $X^3 - 3X + 1$ (Use $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$). Degree 3, not a power of 2. This also shows that regular 9-gon can't be constructed by ruler & compass.

3 Splitting Fields

Definition. Let K be a field, and let $0 \neq f \in K[X]$. An extension L/K is called a splitting field of f over K if

1. f splits into linear factors over L.

2. $L = K(\alpha_1, ..., \alpha_n)$ where α_i are the roots of f.

Remark 7. The 2nd condition is equivalent to saying f doesn't split into linear factors over any subfield of L. The 2nd condition implies $[L : K] < \infty$.

Theorem 3.1 (Existence of splitting field)**.** *If $f \in K[X]$ is a non-zero polynomial, then there exists a splitting field of f over K.*

Proof. Perform induction on $\deg f$. If f is linear then we are done by setting $L = K$. Assume that every poly of degree $< \deg f$ has a splitting field, and let g be an irreducible factor fo f and let $K_1 = K[X]/(g)$ and $\alpha_1 = X + (g)$. Then $f(X) = (X - \alpha_1)f_1(X)$ for some $f_1 \in K_1[X]$ with strictly smaller degree. By induction, there exists a splitting field for f_1 over K_1, say $L = K_1(\alpha_2, ..., \alpha_n)$. We claim that L is a splitting field of f over K. Obviously f splits as linear factors, and $L \cong K(\alpha_1, ..., \alpha_n)$. □

Definition. L/K, M/K field extensions. A K-homomorphism (or equivalently, K-embedding) of L into M is a ring hom, $L \to M$ which is the identity on K.

Theorem 3.2. *Let $L = K(\alpha)$ for some algebraic α with min poly f. Let M/K be any field extension. Then there is a bijection*

$$\{K\text{-}hom\ L \to M\} \leftrightarrow \{\alpha \in M : f(\alpha) = 0\}$$

given by $\tau \mapsto \tau(\alpha)$.

Proof. The correspondence is well-defined by direct computation, i.e., $\tau(\alpha)$ is indeed a root. To see injectivity, note that any K-hom is uniquely determined by $\tau(\alpha)$ since $L = K[X]/(f)$ which has basis $\{1, \alpha, ..., \alpha^n\}$. To see surjectivity, note that evalutation at α gives an iso $K[X]/(f) \to L$ by $X + (f) \mapsto \alpha$. Let $\beta \in M$ be a root of f. Since f is irred, it's the min poly for $\beta \in K$. Evaluation at β and 1st iso gives another iso of the same form. Since both are K-embeddings composing one with the inverse of the other gives a K-hom such that $\tau(\alpha) = \beta$. □

Example 3.3. There are exactly 2 $\mathbb{Q}$-homs $\mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$.

Definition. Let L/K, M/K be field extensions and let $\sigma : K \to K'$ be afield embedding. A σ-embedding (or σ-hom) $\tau : L \to M$ is an embedding s.t. $\tau(x) = \sigma(y)$ for all $x \in K$.

Note that taking $\sigma = \mathrm{id}_K$ recovers the defn of K-hom.

Theorem 3.4. *Let $L = K(\alpha)$, where α is algebraic over K with min poly f. $\sigma : K \to K'$ embedding and M/K' field extn. Then there is a bijection*

$$\{\sigma\text{-}hom\ L \to M\} \leftrightarrow \{\alpha \in M : \sigma f(\alpha) = 0\}$$

So in particular, the number of σ-homs $L \to M$ is $\leq [L : K]$.

Note: If $f = \sum_i c_i X^i$ with $c_i \in K$, then $\sigma f = \sum_i \sigma(c_i) X^i$.

Example 3.5. $K = \mathbb{Q}(\sqrt{2})$. $L = K(\sqrt{1 + \sqrt{2}})$. (Exercise: $1 + \sqrt{2}$ is not a square in K) There are 2 K-embeddings $L \to \mathbb{R}$ from theorem 3.5. However, if $\sigma : K \to K$ is the non-trivial map $a + b\sqrt{2} \mapsto a - b\sqrt{2}$, then there is no σ-beddings $L \to \mathbb{R}$.

Theorem 3.6. *$0 \neq f \in K[X]$, L splitting field of f over K and $\sigma : K \to M$ any field embedding s.t. $\sigma f \in M[X]$ splits into linear factors. Then*

1. *$\exists$ a σ-embedding $\tau : L \to M$*
2. *If M is a splitting field of f over K then τ is an isomorphism*

Proof. To prove 1, we proceed by induction on $n = [L : K]$. The base case $n = 1$ is trivial. Suppose $n > 1$ and g is a irreducible factor of f of degree > 1. Let $\alpha \in L$ be a root of g and $\beta \in M$ a root of σg. By Thm 3.7, σ extends to an embedding $\sigma_1 : K(\alpha) \to M$ s.t. $\alpha \mapsto \beta$ and $[L : K(\alpha)] < n$. Now, $[L : K(\alpha)] < n$, so by induction hypothesis can further extend σ_1 to a $\tau : L \to M$.

To prove 2, pick $\tau : L \to M$ (by(i)) and $\alpha_1, ..., \alpha_n$ roots of f in L, $\tau(\alpha_1), ..., \tau(\alpha_n)$ roots of σf in M. Then M is a splitting field of σf over σK, so $M = \sigma K(\tau(\alpha_1), ..., \tau(\alpha_n)) = \tau(K(\alpha_1, ..., \alpha_n)) = \tau(L)$. If L/K, M/K are splitting field over of f over K and $\sigma : K \to M$ inclusion, then (i) and (ii) gives a K-iso $L \cong M$. □

Example 3.7. $X^3 - 2$ over $\mathbb{F}_7$. Splitting field $\mathbb{F}_7(\alpha)$, $\alpha^3 = 2$ as $X^3 = (X - \alpha)(X - 2\alpha)(X - 4\alpha)$.

Definition. A field K is algebraically closed if every non-constant poly over $K[X]$ has a root in K.

Lemma 3.8. *A field K field. TFAE*

1. *K alg-closed*
2. *If L/K extn and $\alpha \in L$ is alg over K then $\alpha \in K$*
3. *L/K algebraic implies that $L = K$*
4. *L/K finite implies $L = K$.*

Definition. If L/K is algebraic and L is algebraically closed, then we say that L is an algebraic closure of K.

Lemma 3.9. *If L/K is algebraic extn s.t. every poly $f \in K[X]$ splits over L. Then L is algebraically closed.*

Proof. If not, then there eixsts an extension M/L algebraic with $[M : L] > 1$, so M/K is algebraic. Pick any $\alpha \in M$. f its min poly over K, then f splits in L, which implies that $\alpha \in L$, so $M = L$. □

Theorem 3.10. *If (i) $K \subseteq \mathbb{C}$ OR (ii) K is contructible, then K has an algebraic closure.*

Proof. (i) If $K \subseteq \mathbb{C}$, then $L = \{\alpha \in \mathbb{C} : \alpha \text{ algebraic over } K\}$ works.

(ii) If K is constructible, then so is $K[X]$. Enumerate monic irreducible polynomials $f_1, f_2, \ldots$ and construct a chain $K = L_0 \subset L_1 \subset L_2 \subset \ldots$ where L_i is the splitting field of f_i over L_{i-1}. Define $L = \bigcup_n L_n$. □

Remark 8. If $K = \mathbb{Q}$, then the proof of (i) implies that $\bar{\mathbb{Q}}$ (the set of algebraic numbers) is algebraically closed.

4 Symmetric Polynomials

Motivation: $f(X) = X^3 + aX^2 + bX + c$. Sub $X - a/3$ in place of X so can wlog assume $a = 0$. Get a system of of roots α, β, γ. We have

$$\alpha = \frac{1}{3}[(\alpha + \beta + \gamma) + (\alpha + \omega\beta + \omega^2\gamma) + (\alpha + \omega^2\beta + \omega\gamma)]$$

Write $\alpha + \omega\beta + \omega^2\gamma = u$ and $\alpha + \omega^2\beta + \omega\gamma = v$ can show that $u^3 + v^3 = -27c$ and $uv = -3b$. Then can solve for u^3 and v^3 using the quadratic $X^2 + 27cX - 27b^3$ and get the cubic formula.

Definition. R ring, $f \in R[X_1, \ldots, X_n]$ is symmetric if $f(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = f(X_1, \ldots, X_n)$ for all $\sigma \in S_n$.

Clearly, the set of symmetric polynomials is a subring of $R[X_1, \ldots, X_n]$.

Definition. Elementary symmetric functions are the polynomials $s_1, \ldots, s_n$ in $\mathbb{Z}[X_1, \ldots, X_n]$ s.t.

$$\prod_{i=1}^{n}(T + X_i) = T^n + s_1 T^{n-1} + \ldots + s_{n-1}T + s_n$$

i.e.,

$$s_r = \sum_{i_1 < \ldots < i_r} X_{i_1} \ldots X_{i_r}$$

Theorem 4.1 (Symmetric function theorem).

1. *Every symmetric polynomial over R can be written as a polynomial (coeff in R) in the elementary symmetric function.*
2. *There are no non-trivial relations between S_r. (Hence the expression obtained in (i) is unique)*

Proof. Let $f \in R[X_1,...,X_n]$, $f \in \sum_d f_d$ for f_d homogeneous of degree d. Then f being symmetric implies all f_d being symmetric. So WLOG assume f is homogeneous. Impose a lexicographic ordering by insisting that $X_1^{i_1}...X_n^{i_n} > X_1^{j_1}...X_n^{j_n}$ if $i_k = j_k$ for all $k \leq r-1$ and $i_r > j_r$. This is a total ordering. Pick the largest monomial $X_1^{i_1}...X_n^{i_n}$ that appear in f with non-zero coefficient $c \neq 0$. Then $X_{\sigma(1)}^{i_1}...X_{\sigma(n)}^{i_n}$ is in f for all $\sigma \in S_n$ by symmetry. Up to permutation of indices, we may assume that $i_1 \geq i_2 \geq ... \geq i_n$. So

$$X_1^{i_1-i_2}(X_1X_2)^{i_2-i_3}...(X_1X_2...X_n)^{i_n}$$

Let $g = s_1^{i_1-i_2}s_2^{i_2-i_3}...s_n^{i_n}$. Then f, g have the same largest monomial of degree d, so $f - cg$ is either zero or a sym homogeneous poly of degree d with strictly smaller leading monomial. Now we simply note that there are only finitely many monomials of degree d in $R[X_1,...,X_n]$, so the result follows from induction on degrees. ☐

We can rephrase the preceding theorem.

Theorem (Symmetric function theorem (*))**.** *There is a ring hom $\theta : R[Y_1,...,Y_n] \to R[X_1,...,X_n]$ given by $Y_i \mapsto s_i$.*

1. $\operatorname{im}\theta = \{$*sym polys on* $R[X_1,...,X_n]\}$*;*
2. *θ is injective.*

Proof. We only need to prove the second part. Let $s_{r,n} = s_r$, where n denotes the number of variables. Suppose $G \in R[Y_1,...,Y_n]$ with $G(s_{1,n},...,s_{n,n}) = 0$. Perform induction on n. The case $n = 1$ is clear. We write $G = Y_n^k H$ where $Y_n \nmid H$ and $k \geq 0$. Since $s_{n,n}$ is not a zero divisor in the poly ring, we have $H(s_{1,n},...,s_{n,n}) = 0$, so wlog assume $Y_n \nmid G$ if G is non-zero. Replacing $X_n = 0$ reduces the number of variables, and we observe that

$$s_{r,n}(X_1,...,X_{n-1},0) = \begin{cases} s_{r,n-1} & r < n \\ 0 & r = n \end{cases}$$

So this implies that $G(s_{1,n-1},...,s_{n-1,n-1},0) = 0$. By induction hypothesis, we have $G(Y_1,...,Y_{n-1},0) = 0$, so $Y_n \mid G$. So $G = 0$ is forced, proving injectivity. ☐

Example 4.2. Can use the algorithm to show that $\sum_{i \neq j} X_i^2 X_j = s_1s_2 - s_3$. Note that the leading term is $X_1^2X_2$.

Example 4.3. The discriminant of a poly can be written as a poly on the coefficients of the poly by symmetric function theorem.

5 Normal and Separable Extensions

Definition. An extension L/K is normal if it's algebraic and the minimal poly of every $\alpha \in L$ splits into linear factors over L. (i.e., if $f \in K[X]$ is irred over K and has a root in L, then it splits into linear factors over L.)

Theorem 5.1. *Let $[L : K] < \infty$. Then L/K is normal iff L is the splitting field for some $f \in K[X]$.*

Proof. "⇒": Write $L = K(\alpha_1,...,\alpha_n)$. Let f_i be the min poly of α_i over K. Being normal implies that f_i splits, so L is the splitting field of $f_1f_2...f_n$ by definition of splitting fields.

"⇐": Suppose L is the splitting field of $f \in K[X]$. Let $\alpha \in L$ with min poly g over K. Let M/L be a splitting field of g. WTS that $\beta \in M$ is a root of g implies $\beta \in L$.

$L(\alpha)$ is a splitting field of f over $K(\alpha)$; $L(\beta)$ is a splitting field of f over $K(\beta)$. Since α, β have the same min poly, $K(\alpha)$ and $K(\beta)$ are K-isomorphic. By uniqueness of splitting field, $L(\alpha) = L$ and $L(\beta)$ are K-isomorphic. So $[L(\beta) : L] = 1$, so $\beta \in L$. ☐

Define the formal derivative for poly over arbitrary fields.

Lemma 5.2. *$f \in K[X]$, $\alpha \in K$ root of f. Then α is a simple root iff $f'(\alpha) \neq 0$.*

Proof. Just compute ☐

Lemma 5.3. *Let $f, g \in K[X]$, and let L/K be any field extension. Then $\gcd(f, g)$ is the same when computed in $K[X]$ and in $L[X]$.*

Proof. Over K, the gcd is given by Eulicd's algorithm. The result is clearly identical over L as L/K is a field extension. □

Definition. A poly $f \in K[X]$ is separable if it splits into distinct linear factors in its splitting field. (inseparable = not separable)

Lemma 5.4. $0 \neq f \in K[X]$ *is separable iff* $\gcd(f, f') = 1$.

Proof. Work in the splitting field of f. (Lemma 5.3 says this is fine.) □

Theorem 5.5. *Let $f \in K[X]$ be irreducible. Then f is either separable or $f(X) = g(X^p)$ for some $g \in K[X]$. The second possibility may occur if* $\mathrm{char}(K) = p > 0$.

Proof. WLOG assume that f is monic. If f is irred. then $\gcd(f, f') = 1$ or f. If $f' \neq 0$, then $\gcd(f, f') = 1$, so separable. If $f' = 0$, then Write $f = \sum c_i x_i$, $f' = \sum i c_i x_i$. We see that $ic_i = 0$ for $i \geq 1$. So $p \mid ic_i$ for all i. If $p \nmid i$, then $p \mid c_i$, i.e., $c_i = 0$ in field of char p. If $c_i \neq 0$ in K, then $p \mid i$, so $f(X) = g(X^p)$ for some $g \in K[X]$. □

Definition. Let L/K be a field extension. Then

1. $\alpha \in L$ is separable over K if it's algebraic and its min poly over K is separable.
2. L/K separable if for all $\alpha \in L$, α is separable over K. (In particular, the definition implies that L/K is algebraic.)

Theorem 5.6 (Theorem of the primitive elements)**.** *If L/K is finite and separable, then $L = K(\theta)$ for some $\theta \in L$.*

Proof. Write $L = K(\alpha_1, ..., \alpha_n)$ smoe $\alpha_i \in L$. It is sufficient to deal with the case $L = K(\alpha, \beta)$, where f, g are minpolys of α, β over K. Work in splitting fields of fg, say M over L. Over M, write $f(X) = \prod_{i=1}^{r}(X - \alpha_i), g(X) = \prod_{i=1}^{s}(X - \beta_i)$, where $\alpha = \alpha_1$, $\beta = \beta_1$. L/K separable $\implies$ β separable $\implies$ $\beta_1, ..., \beta_s$ distinct. Pick $c \in K$ and let $\theta = \alpha + c\beta$. Define $F(X) = f(\theta - cX) \in K(\theta)[X]$. Then $F(\beta) = 0$. Consider $\gcd(F, g)$.

- If $\beta_2, ..., \beta_s$ are not roots of F, then $\gcd(F, g) = (X - \beta)$ over M, so $\gcd(F, g) = X - \beta$ over $K(\theta)$ by Lemma 5.3, so $\beta \in K(\theta)$. Then $\alpha = \theta - c\beta \in K(\theta)$, so $K(\alpha, \beta) = K(\theta)$.
- If $F(\beta_j) = 0$ for some $2 \leq j \leq s$, then $f(\theta - c\beta_j) = 0$ implies that $\alpha_i + c\beta_j = \alpha + c\beta$. We can solve for c, so if $|K| = \infty$, then we can always make another choice to avoid this. If $|K| < \infty$, then $|L| < \infty$, and Proposition 1.4 implies that $L^\times$ is cyclic, generated by some θ, then $L = K(\theta)$.

□

Remark 9. Thm 5.5, 5.6 $\implies$ If $[K : \mathbb{Q}] < \infty$ then $K = \mathbb{Q}(\alpha)$ for some $\alpha \in K$.

We introduce some notation. Let $\mathrm{Hom}_K(L, M)$ be the set of all K-embeddings $L \hookrightarrow M$, where $L/K, M/K$ are field extensions.

Lemma 5.7. *Let $[L : K] < \infty$, $L = K(\alpha)$, f min poly of α over K. M/K any field extension. Then $|\mathrm{Hom}_K(L, M)| \leq [L : K]$ with equality iff f splits into distinct linear factors over M.*

Proof. Thm 3.4 implies that $\mathrm{Hom}_k(L, M) \leftrightarrow \{\text{roots of } f \text{ in } M\} \leq [L : K]$ with equality iff f splits as distinct linear factors over M. □

Theorem 5.8. *Let $[L : K] < \infty$, $L = K(\alpha_1, ..., \alpha_n)$ and f_i min poly over α_i over K. M/K any field extension. Then, $|\mathrm{Hom}_K(L, M)| \leq [L : K]$ with equality iff each f_i splits into distinct linear factors.*

We can generalize this theorem to σ-embeddings.

Theorem. *With the same hypothesis, $\#\sigma$-embeddings $L \hookrightarrow M \leq [L : K]$ with equality iff each $\sigma(f_i)$ splits into distinct linear factors over M.*

Proof. Induction on n.

- If $n > 1$, then let $K_1 = K(\alpha_1)$. Then Thm 5.7 implies that $|\mathrm{Hom}_K(K_1, K)| \le [K_1 : K]$.
- The induction hypothesis implies $|\{\sigma\text{-embeddings } K(\alpha_2, ..., \alpha_n) \hookrightarrow M\}| \le [L : K_1]$.

The tower law implies that $\mathrm{Hom}_K(L, M) \le [L : K]$ with equality iff equality holds in both places. Now use Lemma 5.7. However, there is a slight little wrinkle for the second point. If each f_i splits into distinct linear factors over M, then for $2 \le i \le n$ min poly α_i over K_1 may change but still divide f_i, so still splits into distinct linear factors so equality holds in the second point. □

Corollary 5.9. *Let $[L : K] < \infty$. Let $L = K(\alpha_1, ..., \alpha_n)$, f_i min poly of α_i over K. Let M/K be any field extension in which $\prod_i f_i$ splits into linear factors. The TFAE,*

1. *L/K separable*
2. *Each α_i separable over K*
3. *Each f_i separable over K*
4. *$|\mathrm{Hom}_K(L, M)| = [L : K]$.*

Proof. 1) $\implies$ 2) $\implies$ 3) $\overset{5.8}{\implies}$ 4). Assume 4) is true. Let $\beta \in L$, then Thm 5.8 applied to $L = K(\alpha_1, ..., \alpha_n, \beta)$ implies that β is separable over K. Since β is arbitrary, we get 1). □

Remark 10. 1) $\Leftrightarrow$ 4) is a useful characterization of separable extensions.

Example 5.10. Let K be a field, $n \ge 2$. Then $[K(X) : K(X^n)] = n$. It suffices to show that $[K(X) : K(X^n)] \ge n$. We observe that $1, X, X^2, ..., X^{n-1}$ are linearly independent, so if there exists rational functions $g_0, ..., g_{n-1} \in K(X^n)$ s.t. $\sum g_j X^j = 0$, then clearing denominators, we get $g_j = 0$ for all j. Alternatively, we show that $T^n - Y$ is irreducible in $K[Y, T]$. Gauss's lemma implies that $T^n - Y$ is irreducible in $K(Y)[T]$, so $T^n - X^n$ is irreducible over $K(X^n)[T]$ as X^n is transcendental over K (c.f. ES1 Q8).

Example 5.11. We produce an example of inseparable extension. Let p be a prime, and $K = \mathbb{F}_p$ and $n = p$ int he previous example. Then $\mathbb{F}_p(X)/\mathbb{F}_p(X^p)$ is inseparable. The min poly f X over $\mathbb{F}_p(X^p)$ is $T^p - X^p = (T - X)^p$.

6 Galois Extensions

Definition. A K-automorphism of L/K is an element $\sigma \in \mathrm{Aut}(L)$ s.t. $\sigma|_K = \mathrm{id}_K$. We write this group as $\mathrm{Aut}(L/K)$.

Remark 11.
- $\mathrm{Aut}(L/K) = \mathrm{Aut}(L)$ if K is the prime subfield of L.
- If $[L : K] < \infty$, then any K-embedding $L \to L$ is surjective, so rank-nullity implies that $\mathrm{Hom}_K(L, L) = \mathrm{Aut}(L/K)$.

Lemma 6.1. *Let L/K be a finite extension. Then $|\mathrm{Aut}(L/K)| \le [L : K]$*

Proof. By Thm 5.8 □

Definition. If $S \subseteq \mathrm{Aut}(L)$, then define the fixed field of S to be $L^S = \{x \in L : \forall \sigma \in S, \sigma(x) = x\}$.

Definition. A field extension L/K is Galois if it's algebraic and $L^{\mathrm{Aut}(L/K)} = K$.

Example 6.2. $\mathbb{C}/\mathbb{R}$, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. Any finite extension $K/\mathbb{F}_p$ is Galois since the elements fixed by the Frobenius map are precisely roots of $X^p - X$, i.e., $\mathbb{F}_p$.

However, $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not Galois.

Theorem 6.3 (Classification of finite Galois extension)**.** *L/K field extension and $G = \mathrm{Aut}(L/K)$. TFAE,*

1. *L/K Galois*
2. *L/K normal and separable*
3. *L is the splitting field of a separable poly over K*

4. $|G| = [L : K]$ (c.f. Lemma 6.1).

Proof. 1) $\implies$ 2): Let $\alpha \in L$. Suppose $\{\sigma(\alpha) : \sigma \in G\} = \{\alpha_1, ..., \alpha_m\}$ and $f(X) = \prod_{i=1}^m (X - \alpha_i)$. Note that σ acts on $L[X]$ (on coeff of each poly) and $\sigma(f) = f$ for all σ. Since L/K is Galois, we must have $f \in K[X]$. Let g be the min poly of α over K, then $g \mid f$ since $g(\sigma(\alpha)) = \sigma(g(\alpha))$, so every root of f is a root of g. By construction, f is separable, so $f = g$, so g splits into distinct linear factors over L, so L/K is normal and separable.

2) $\implies$ 3): Thm 5.1 says L is the splitting field of some $f \in K[X]$. Wlog, suppose f is monic and write $f = \prod_{i=1}^m f_i^{e_i}$ (factorize into distinct irreducible factors in $K[X]$). L/K seprable implies that each f_i is separable. Moreover, if $i \neq j$, then $\gcd(f_i, f_j) = 1$ over K, so Lemma 5.3 implies that they are coprime over L. Replace $e_i = 1$, then we see that L is the splitting field of a separable poly.

3) $\implies$ 4): Let L be the splitting field of a separable poly $f \in K[X]$. Then $L = K(\alpha_1, ..., \alpha_n)$, where α_i are roots of f. Then the min poly f_i of each α_i divides f, so also splits into linear factors over L. Apply Thm 5.8.

4) $\implies$ 1): Note that $G \subseteq \mathrm{Aut}(L/L^G) \subseteq \mathrm{Aut}(L/K) = G$, so $G = \mathrm{Aut}(L/L^G)$, and $|G| = |\mathrm{Aut}(L/L^G)| \leq [L : L^G]$. Apply tower law to the tower $K \subseteq L^G \subseteq L$. □

Definition. If L/K is Galois, we write $\mathrm{Gal}(L/K)$ for $\mathrm{Aut}(L/K)$.

Remark 12. In the proof of 1) $\implies$ 2), we see that if L/K is Galois and $\alpha \in L$, then α has min poly $\prod_{i=1}^m (X - \alpha_i)$ where α_i are the distinct Galois conjugates of α.

Theorem 6.4 (Fundamental Theorem of Galois Theory)**.** *Let L/K be a finite Galois extension. $G = \mathrm{Gal}(L/K)$.*

1. *Let F be an intermediate field, i.e., $K \subseteq F \subseteq L$. Then L/F is Galois and* $\mathrm{Gal}(L/F) \leq G$.

2. *(Galois Correspondence) There is a bijection*

$$\begin{aligned} \{\textit{intermediate subfield } K \subseteq F \subseteq L\} &\longleftrightarrow \{\textit{subgroups } H \leq G\} \\ F &\longmapsto \mathrm{Gal}(L/F) \\ L^H &\longleftarrow H \leq G \end{aligned}$$

3. *If $K \subseteq L \subseteq L$, then F/K is Galois $\Leftrightarrow$ $\sigma F = F$ for all $\sigma \in G$ $\Leftrightarrow$* $\mathrm{Gal}(L/F) \trianglelefteq G$. *And In this situation, the restriction $G \to$* $\mathrm{Gal}(F/K), \sigma \mapsto \sigma|_F$ *is surjective with kernel H, so* $\mathrm{Gal}(F/K) = G/H$.

Proof. 1): Thm 6.2 $\implies$ L is a splitting field of some separable poly $f \in K[X]$. Then L is a splitting field of f over F, so L/F is Galois, and it is clear that $\mathrm{Gal}(L/F) \leq G$.

2): It is clear that $F = L^{\mathrm{Gal}(L/F)}$. To prove that the other composition is the identity, we first note that $H \subseteq \mathrm{Gal}(L/L^H)$. Conversely, Let $F = L^H$. As L/F is finite and separable, the thm of primitive elements implies that $L = F(\alpha)$ for some $\alpha \in L$. Then α is a root of $f(X) = \prod_{\sigma \in H}(X - \sigma(\alpha))$ which has coefficients in F, so $|\mathrm{Gal}(L/F)| = [L : L^H] = [F(\alpha) : F] \leq \deg(f) = |H|$, so $\mathrm{Gal}(L/L^H) \subseteq H$. So $H = \mathrm{Gal}(L/L^H)$.

3): **We claim that F/K is Galois $\Leftrightarrow$ $\sigma F = F$ for all $\sigma \in G$.** Supppose F/K is Galois. Let $\alpha \in F$ with min poly f over K. Then $\sigma(\alpha)$ is a root of f for every $\sigma \in G$. F/K is normal, so $\sigma(\alpha) \in F \implies \sigma F \subseteq F$. Done by rank-nullity. Conversely, let $\alpha \in F$. Remark 12 implies that the min poly of α over K is $\prod_{i=1}^n (X - \alpha_i)$, where $\alpha_i = \sigma(\alpha)$ for some $\sigma \in G$. [Note that we are really using the fact that L/K is Galois to deduce the min poly of α.] Since $\sigma(F) = F$, all α_i are elements of F, so F/K is normal and separable. [α_i's are distinct Galois conjugates of α.] So F/K is Galois.

To prove the second equivalence, we use Galois correspondence, i.e., $H \leq G \leftrightarrow F = L^H$. Then for each $\sigma \in G$, we compute

$$\begin{aligned} L^{\sigma H \sigma^{-1}} &= \{x \in L : \forall \tau \in H, \sigma\tau\sigma^{-1}(x) = x\} \\ &= \{x \in L : \forall \tau \in H, \tau\sigma^{-1} = \sigma(x)\} \\ &= \{x \in L : \sigma^{-1}(x) \in L^H = F\} \\ &= \sigma(F) \end{aligned}$$

so that $\sigma(F) = F \Leftrightarrow (\forall \sigma \in G,\ L^{\sigma H \sigma^{-1}} = L^H) \Leftrightarrow (\forall \sigma \in G,\ \sigma H \sigma^{-1} = G) \Leftrightarrow H \trianglelefteq G$.

In this situation, we clearly have $\ker(\mathrm{Gal}(L/K) \xrightarrow{\text{res}} \mathrm{Gal}(F/K)) = \mathrm{Gal}(L/F) = H$. The desired isomorphism $\mathrm{Gal}(F/K) \cong G/H$ then follows from 1st iso. □

Example 6.5. $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}) \cong C_2 \times C_2$. The automorphisms are uniquely determined by the images of $\sqrt{2}$ and $\sqrt{3}$.

Definition. Let L_1, L_2 be subfields of a field M. The composite L_1L_2 is the smallest subfield of M containing L_1 and L_2.

Theorem 6.6. *Let $[M:K] < \infty$, L_1, L_2 intermediate subfields*

(i) If L_1/K is Galois, then L_1L_2/L_2 is Galois, and have injective group homomorphism $\mathrm{Gal}(L_1L_2/L_2) \hookrightarrow \mathrm{Gal}(L_1/K)$. This is surjective if $L_1 \cap L_2 = K$.

(ii) If L_1/K, L_2/K are Galois, then L_1L_2/K is Galois and there is an injective group hom $\mathrm{Gal}(L_1L_2/K) \hookrightarrow \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$

Proof. (i): L_1/K is the splitting field of a separable poly f, so L_1L_2 is the splitting field of f over L_2, so L_1L_2/K is Galois. The restriction map is well-defined. Note that L_1/K is normal, so $\alpha \in L_1$ implies that $\sigma(\alpha) \in L_1$ for all $\sigma \in \mathrm{Gal}(L_1L_2/L_2)$, so $\sigma(L_1) = L_1$. To see injectivity, note that if $\sigma|_{L_1}$ is the identity, then by definition σ acts trivially on both L_1 and L_2, so σ is the identity. Suppose $L_1 \cap L_2 = K$. Since L_1/K is finite separable, we have $L_1 = K(\alpha)$ for some $\alpha \in L_1$ with min poly f over K. Suppose $f = gh$ over L_2 is a non-trivial factorization. Since f factorizes as into linear factors over L_1, we must have $g, h \in (L_1 \cap L_2)[X]$, but $L_1 \cap L_2 = K$, so this contradicts the fact that f is irreducible over K. Note that $L_1L_2 = L_2(\alpha)$, so $[L_1L_2 : L_2] = \deg(f) = [L_1 : K]$, so we have surjectivity. Conversely, since $\mathrm{im}(\mathrm{res}) \subseteq \mathrm{Gal}(L_1/(L_1 \cap L_2)) \subseteq \mathrm{Gal}(L_1/K)$. If the restriction map is surjective, then by Galois correspondence, we must have $L_1 \cap L_2 = K$.

(ii): L_i/K is the splitting field of f_i over K, where f_i is separable. Then L_1L_2/K is the splitting field of $\mathrm{lcm}(f_1, f_2)$ over K, which is separable, so L_1L_2/K is Galois. We define a homomorphism $\mathrm{Gal}(L_1L_2/K) \to \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$ by $\sigma \mapsto (\sigma|_{L_1}, \sigma|_{L_2})$. Injectivity is clear. It's surjective iff $[L_1L_2 : K] = [L_1 : K][L_2 : K]$ iff $[L_1L_2 : L_2][L_2 : K] = [L_1 : K][L_2 : K]$ iff $[L_1L_2 : L_2] = [L_1 : K]$ iff $L_1 \cap L_2 = K$ by (i). □

Theorem 6.7. *L/K finite separable. Then $\exists M/L$ s.t.*

(i) M/K is Galois

(ii) If $L \subseteq M' \subseteq M$ and M'/K is Galois, then $M = M'$

Definition. We say that M/K is the Galois closure of L/K.

Proof. (i): The theorem of primitive element implies that $L = K(\alpha)$. Let f be the min poly of α over K and let M be the splitting field of f over L, then M/K is Galois.

(ii): If $L \subseteq M' \subseteq M$ and M'/K is Galois, then f splits into linear factors over M', but by uniqueness of splitting field we must have $M' = M$. □

Example 6.8. $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ has Galois closure $\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q}$.

7 Finite Field

Theorem 7.1. *If $q = p^n$ for p prime, then*

(i) There exists a field of order q

(ii) It is unique up to iso. (Any field with q elements is a splitting field of $X^q - X$ over $\mathbb{F}_p$. In particular, any two finite field of order q are isomorphic.)

Proof. (i) Let L be the splitting field of $X^q - X$ over $\mathbb{F}_p$. Let $K \subset L$ be the fixed field of $\phi : L \to L, x \mapsto x^q$. Then $K = \{\alpha \in L : \phi(\alpha) = \alpha\} = \{\alpha \in L : \alpha^q = \alpha\}$, so $|K| \le q$. By considering the derivative, we see that $x^q - x$ is separable over $\mathbb{F}_p$, so $|K| = q$.

(ii) If K is a field of order q, then Lagrange theorem implies that $\alpha^q = \alpha$ for all $\alpha \in K$. Then $X^q - X$ splits into linear factors, i.e. $\prod_{\alpha \in K}(X - \alpha)$. Clearly this polynomial doesn't split over any proper subfield, so K is the splitting field of $X^q - X$ over $\mathbb{F}_p$. Then follows from the uniqueness of splitting field. □

Remark 13. There is no canonical isomorphism.

Theorem 7.2. *$\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois, and $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong C_n$ generated by the Frobenius.*

Proof. Let $L = \mathbb{F}_{p^n}$. Let $G \subseteq \text{Aut}(L/\mathbb{F}_p)$ be the subgroup generated by the Frobenius map ϕ. Then $|L^G| = |L^\phi| = |\{\alpha \in L : \alpha^p = \alpha\}| \le p$. Also, $\mathbb{F}_p \subseteq L^G$, so $L^G = \mathbb{F}_p$. Note that $L^{\text{Aut}(L/\mathbb{F}_p)}$ is a subfield of $L^G = \mathbb{F}_p$, so $L^{\text{Aut}(L/\mathbb{F}_p)} = \mathbb{F}_p$, so $L/\mathbb{F}_p$ is Galois with Galois group $\langle \phi \rangle \cong C_n$. ☐

Hence, any finite extension of finite field is Galois.

Corollary 7.3. *$L = \mathbb{F}_{p^n}$ has a unique subfield of order p^m for each $m \mid n$ and no others.*

Proof. Essentially a consequence of Galois correspondence. ☐

8 Traces and Norms

L/K finite extension of degree n. For $\alpha \in L$, $m_\alpha : L \to L, x \mapsto \alpha x$ is K-linear.

Definition. $\text{Tr}_{L/K}(\alpha) = \text{tr}(m_\alpha)$ and $N_{L/K}(\alpha) = \det m_\alpha$.

Lemma 8.1. *(i) $\text{Tr}_{L/K} : L \to K$ is K-linear.*

(ii) $N_{L/K} : L \to K$ is multiplicative

(iii) If $\alpha \in K$, then $\text{Tr}_{L/K}(\alpha) = [L : K]\alpha$ and $N_{L/K}(\alpha) = \alpha^{[L:K]}$.

(iv) $N_{L/K}(\alpha) = 0$ iff $\alpha = 0$.

Proof. Trivial. ☐

Lemma 8.2. *Let $M/L/K$ be finite extensions and $\alpha \in L$. Then $\text{Tr}_{M/K}(\alpha) = [M : L]\,\text{Tr}_{L/K}$ and $N_{M/K} = N_{L/K}(\alpha)^{[M:L]}$.*

Proof. Write down the matrix in some basis of L, then pick a K-basis of M as in the proof of Tower law, then $[m_\alpha]_{M/K}$ will be in block diagonal form. ☐

Theorem 8.3. *Suppose $[L : K] < \infty$ and $\alpha \in L$ with min poly $f(X) = X^n + c_{n-1}X^{n-1} \cdots + c_0$ over K. Then $\text{Tr}_{L/K}(\alpha) = -[L : K(\alpha)]c_{n-1}$ and $N_{L/K}(\alpha) = ((-1)^n c_0)^{[L:K(\alpha)]}$.*

Proof. By lemma 8.2, suffices to prove the case $L = K(\alpha)$. Write m_α in the basis $1, \alpha, ..., \alpha^{n-1}$, i.e., the companion matrix of f, then can read off trace and det. ☐

Theorem 8.4 (Transitivity of traces and norms)**.** *$M/L/K$ finite extensions with $\alpha \in M$. Then $\text{Tr}_{M/K}(\alpha) = \text{Tr}_{L/K}(\text{Tr}_{M/L}(\alpha))$ and $N_{M/K}(\alpha) = N_{L/K}(N_{M/L}(\alpha))$.*

Proof. (Proof non-examinable) will write up this part later. ☐

Theorem 8.5. *L/K (finite) Galois extension with $G = \text{Gal}(L/K)$. Let $\alpha \in L$. Then $\text{Tr}_{L/K} = \sum_{\sigma \in G} \sigma(\alpha)$ and $N_{L/K} = \prod_{\sigma \in G} \sigma(\alpha)$.*

Proof. The min poly of α is given by $\prod_{i=1}^n (X - \alpha_i)$. Let $m = [L : K(\alpha)] = |\text{Gal}(L/K(\alpha))| = |\text{Stab}_G(\alpha)|$. Use theorem 8.3. ☐

The following is a variant for separable extension. Let $\bar{K}$ be the algebraic closure of K, then $|\text{Hom}_K(L, \bar{K})| = [L : K]$

Theorem 8.6. *L/K is separable of deg d. Let $\sigma_1, ..., \sigma_d$ be K-embeddings $L \hookrightarrow \bar{K}$. Let $\alpha \in L$. Then $\text{Tr}_{L/K}(\alpha) = \sum_{i=1}^d \sigma_i(\alpha)$ and $N_{L/K}(\alpha) = \prod_{i=1}^d \sigma_i(\alpha)$.*

Proof. f be min poly over K. Thm 3.4 implies that $\text{Hom}_K(K(\alpha), \bar{K}) \leftrightarrow \{\alpha_1, ..., \alpha_n\}$. By separability, each K-embedding $K(\alpha) \hookrightarrow\!\!\to \bar{K}$ extends to $L \hookrightarrow \bar{K}$ in exactly $m = [L : K(\alpha)]$ ways. Apply thm 8.3 and note that $|\{1 \le i \le d : \sigma_i(\alpha) = \alpha_j\}| = m$. ☐

9 The Galois Group of a Polynomial

$f \in K[X]$ separable of degree n. Let L be a splitting field of f over K. Then $\mathrm{Gal}(L/K)$ acts on the roots of f which determines an injectie group homomorphism $\mathrm{Gal}(L/K) \to S_n$.

Definition. The image of this hom $\mathrm{Gal}(L/K) \to S_n$ is the Galois group of f over K, denoted $\mathrm{Gal}(f)$ or $\mathrm{Gal}(f/K)$.

Note that this is only defined up to conjugation.

Lemma 9.1. *Let $f \in K[X]$ separable. f irred iff $\mathrm{Gal}(f/K)$ is transitive.*

Proof. "⇐:" If $f = gh$ for gh non-const. Then $\mathrm{Gal}(f/K)$ sends roots of g to roots of g and not roots of h, so the Galois group cannot be transitive.

"⇒" WLOG assume f monic with a root $\alpha \in L$. Then f is the min poly of α over K. We have $\{\sigma(\alpha) : \sigma \in \mathrm{Gal}(L/K)\} = \{\text{roots of } f \text{ in } L\}$, i.e., the action of $\mathrm{Gal}(L/K)$ on roots of f is transitive. □

Definition. Let $f \in K[X]$ be a monic separable poly with roots $\alpha_1, ..., \alpha_n$. Splitting field L. Define $\mathrm{disc}(f) = \prod_{i<j}(\alpha_i - \alpha_j)^2$.

Lemma 9.2. *Assume $\mathrm{char}(K) \neq 2$. Let $\Delta = \mathrm{disc}(f)$. The fixed field of $\mathrm{Gal}(f/K) \cap A_n$ is $K(\sqrt{\Delta})$. In particular, $\mathrm{Gal}(f/K) \subseteq A_n$ iff Δ is a square in K.*

Proof. Let $\delta = \prod_{i<j}(\alpha_i - \alpha_j)$. Separability and $\mathrm{char}(K) \neq 2$ implies that $\delta \neq -\delta$. If $\sigma \in G = \mathrm{Gal}(f/K)$, then $\sigma(\delta) = \epsilon(\sigma)\delta$. Note that $G \cap A_n = \{\sigma \in G, \epsilon(\sigma) = 1\} = \mathrm{Gal}(L/K(\delta))$ which corresponds to $K(\delta)$ be Galois correspondence. □

9.1 Roots of quartic polys

Note that S_4 acts on the set of double transpositions by conjugation, which gives a homomomorphism $\pi : S_4 \to S_3$. One can check that $\ker \pi = V_4$.

Transitive subgroup of S_4	Image under π
S_4	S_3
A_4	A_3
C_4, D_8	C_2
V_4	$\{e\}$

If $f = \prod_{i=1}^4 (X - \alpha_i)$ is a monic quartic, define

$$\beta_1 = (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4)$$
$$\beta_2 = (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4)$$
$$\beta_3 = (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3)$$

Definition (Resolvent cubic)**.** $\prod_{i=1}^3 (X - \beta_i)$

Theorem 9.3. *f, g as above.*

(i) $f \in K[X] \implies g \in K[X]$

(ii) f *separable* $\implies g$ *separable*

(iii) (i) and (ii) $\implies \pi(\mathrm{Gal}(f/K)) = \mathrm{Gal}(g/K)$.

In particular, if f is irreducible then $\mathrm{Gal}(g/K)$ determines $\mathrm{Gal}(f/K)$ up to conjugation in S_4.

Proof. (i) Each coeff of g is a sym poly in $\mathbb{Z}[\beta_1, \beta_2, \beta_3]$ hence symmetric in $\mathbb{Z}[\alpha_1, \alpha_2, \alpha_3, \alpha_4]$. By symmetric function theorem, g is a $\mathbb{Z}$-coefficient polynomial in the coefficients of f.

(ii) Compute $\beta_1 - \beta_2 = (\alpha_1 - \alpha_4)(\alpha_3 - \alpha_2)$. Repeat for all combination.

(iii) Let M be a splitting field of f over K. Let $L = K(\beta_1, \beta_2, \beta_3)$, which is a splitting field of g over K. Observe that under the restriction map $\mathrm{Gal}(M/K) \to \mathrm{Gal}(L/K)$, the action of σ on α_i restricts to the action of $\pi(\sigma)$ on β_i. This restriction map is surjective, so we have what we want. □

Proposition 9.4. *If f is monic quartic, g its resolvent cubic. Then*

(i) $\mathrm{disc}(f) = \mathrm{disc}(g)$

(ii) If $f = X^4 + pX^2 + qX + r$, *then* $g(X) = X^3 - 2pX^2 + (p^2 - 4r)X + q^2$.

Proof. Compute.... □

One can obtain a formula for the roots of quartic polys.

1. Make the quartic depressed.
2. Find $\beta_1, \beta_2, \beta_3$ using Cardano's formula.
3. Choose square roots such that $\sqrt{-\beta_1}\sqrt{-\beta_2}\sqrt{-\beta_3} = -q$, then $\alpha_1 = \frac{1}{2}(\sqrt{-\beta_1} + \sqrt{-\beta_2} + \sqrt{-\beta_3})$.

9.2 Further results

Lemma 9.5. *Let $f \in \mathbb{F}_p[X]$ be a separable poly whose irred. factors have degree $n_1, ..., n_r$. Then* $\mathrm{Gal}(f/\mathbb{F}_p)$ *is generated by a single element of cycle type $(n_1, ..., n_r)$.*

Proof. Let L be a splitting field of f over $\mathbb{F}_p$. Let $\alpha_1, ..., \alpha_n$ be roots of f in L. Thm8.2 implies that $G = \mathrm{Gal}(L/\mathbb{F}_p)$ is cyclic generated by the Frobenius $x \mapsto x^p$. Note that $\mathrm{Gal}(f/\mathbb{F}_p)$ acts transitively on the roots of each irred. factor, so the Frobenius acts by an element of cycle type $(n_1, ..., n_r)$. □

Theorem 9.6 (Reduction mod p)**.** *$f \in \mathbb{Z}[X]$ monic separable of degree $n \geq 1$. Let p be a prime such that $\bar{f}$ (reduction of f mod p) is spearable over $\mathbb{F}_p$. Then* $\mathrm{Gal}(\bar{f}/\mathbb{F}_p) \subseteq \mathrm{Gal}(f/\mathbb{Q})$.

Corollary 9.7. *Same assumption on f and p. Suppose $\bar{f} = g_1 \cdots g_r \in \mathbb{F}_p[X]$, where g_i is irred. of degree n_i. Then* $\mathrm{Gal}(f/\mathbb{Q}) \subseteq S_n$ *contains an element of cycle type $(n_1, ..., n_r)$.*

Proof. This is essentially a consequence of lemma 9.5 and 9.6. □

Let $f \in K[X]$ be a monic separable polynomial of degree n with splitting field L and roots $\alpha_1, ..., \alpha_n$. Let

$$F(T_1, ..., T_n, X) = \prod_{\sigma \in S_n} (X - \alpha_1 T_{\sigma(1)} + \cdots + \alpha_n T_{\sigma(n)})$$

This is a polynomial in $K[T_1, ..., T_n, X]$. Note that this polynomial ring admits an action of S_n by permuting the variables $T_1, ..., T_n$, and F is fixed by this action.

Lemma 9.8. *Let $F_1 \in K[T_1, ..., T_n, X]$ be an irreducible factor of F. Then* $\mathrm{Gal}(f/K)$ *is conjugate to* $\mathrm{Stab}_{S_n}(F_1)$.

Proof. WLOG, assume F_1 is monic in X. Replacing F_1 by $\tau \cdot F_1$ for some $\tau \in S_n$, we may assume that it has a factor $X - (\alpha_1 T_1 + \cdots + \alpha_n T_n)$. Then for each $\sigma \in G = \mathrm{Gal}(f/K)$, F_1 has a factor $X - (\alpha_{\sigma(1)} T_1 + \cdots + \alpha_{\sigma(n)} T_n)$. Hence, $\prod_{\sigma \in G}(X - (\alpha_{\sigma(1)} T_1 + \cdots + \alpha_{s\sigma(n)} T_n))$ has coefficients in K and divides F_1 and hence must be equal to F_1 by irreducibility. By direct computation, we have $\tau \cdot F_1 = F_1$ iff $G = G\tau^{-1}$ iff $\tau \in G$. □

We now try to prove Thm 9.6.

Proof of Thm 9.6 (Non-examinable). By symmetric function theorem, coefficients of F are $\mathbb{Z}$-coeff polys in the coeffs of f. So if $f \in \mathbb{Z}[X]$, then $F \in \mathbb{Z}[T_1, ..., T_n, X]$. Similarly, $\bar{f} \in \mathbb{F}_p[X]$ and $\bar{F} \in \mathbb{F}_p[T_1, ..., T_n, X]$. Write $F = F_1 \cdots F_s$, where F_i are distinct irreducibles and similarly $\bar{F} = \Phi_1 \cdots \Phi_t$. WLOG, $\Phi_1 \mid \bar{F}_1$. Then

$$\{\tau \in S_n : \tau \cdot \Phi_1 = \Phi_1\} \subseteq \{\tau \in S_n : \tau \cdot F_1 = F_1\}$$

□

10 Cyclotomic and Kummer Extension

K field, $n \geq 1$ integer, and $\text{char}(K) \nmid n$ (trivially true if $\text{char} K = 0$). Let L/K be the splitting field of $x^n - 1$ (so L/K is Galois since $x^n - 1$ is separable)

Let $\mu_n = \{x \in L : x^n = 1\} \leq L^\times$. This is cyclic of order n, called the group of nth root of unity.

Definition. $\zeta_n \in \mu_n$ is a primitive nth root of unity if ζ_n has order n in μ_n.

Definition. $K(\zeta_n)/K$ is a cyclotomic extension.

Theorem 10.1. *There is an injective group hom* $\chi : \text{Gal}(K(\zeta_n)/K) \hookrightarrow (\mathbb{Z}/n)^\times$. *In particular* $\text{Gal}(K(\zeta_n)/K)$ *is abelian and* $[K(\zeta_n) : K] \mid \phi(n)$, *where* ϕ *is Euler's totient function.*

Of course this still requires $\text{char} K \nmid n$.

Proof. Every automorphism σ fixing K is uniquely determined its value at ζ_n (it has to map ζ_n to ζ_n^a where a is unique mod n), which has to be another primitive nth root of unity (need to be a bijection). Can check that $\chi(\sigma) = a$ is well-defined and an injective group hom. □

Remark 14. Note that χ doesn't depend on the choice of ζ_n.

Corollary 10.2. *If* $K = \mathbb{F}_p$ *and* $p \nmid n$, *then* $[K(\zeta_n) : K] =$ *order of* p *in* $(\mathbb{Z}/n)^\times$.

Proof. The Galois group is generated by Frobenius, so the degree is the order of Frobenius, under the injective hom χ, this translates to the order of p in $(\mathbb{Z}/n)^\times$. □

Definition. The nth cyclotomic poly is $\Phi_n(x) = \prod_{(a,n)=1}(x - \zeta_n^a)$, where $\zeta_n = e^{i2\pi/n}$.

We note that $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ permutes primitive roots of unity, so $\Phi_n(x) \in \mathbb{Q}[x]$. Note that we also have $x^n - 1 = \prod_{d|n} \Phi_d(x)$. Now proceed by induction, the base case clearly holds. If also holds for Φ_k, $k < n$, then $\Phi_n(x) f(x) = x^n - 1$ for some $f \in \mathbb{Z}[X]$ by induction hypothesis, then Gauss's lemma implies that f divides $x^n - 1$ in $\mathbb{Z}[X]$. The quotient has to be $\Phi_n(x)$, so $\Phi_n(x) \in \mathbb{Z}[x]$.

Theorem 10.3. *If* $K = \mathbb{Q}$, *then* χ *in Thm 10.1 is an iso. [In particular,* Φ_n *is irred over* $\mathbb{Q}$ *and* $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$*]*

Proof. Suppose p prime $p \nmid n$. WTS $\text{im}\,\chi$ contains $p \mod n$ (Then $\text{im}\,\chi$ contains $a \mod n$ for all a s.t. $(a,n) = 1$, which would give us surjectivity) Let f, g be min polys of ζ_n and ζ_n^p over $\mathbb{Q}$.

(i) If $f = g$, then there exists $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ s.t. $\sigma(\zeta_n) = \zeta_n^p$. Done.

(ii) If $f \neq g$, then f, g are distinct irreducible monic factors of $x^n - 1$ and $f, g \in \mathbb{Z}[X]$. Have $fg \mid (x^n - 1)$. We see that ζ_n is a root of $g(X^p)$, so $f(X) \mid g(X^p)$. Reducing mod p, we have $\bar{f}(X) \mid \bar{g}(X)^p$, but this would imply that $x^n - 1$ is inseparable over $\mathbb{F}_p$. Contradiction.

□

Theorem 10.4 (Gauss)**.** $n \geq 3$, $\zeta_n = e^{i2\pi/n}$. *TFAE,*

(i) A regular n*-gon is contructible by ruler and compass*

(ii) $\alpha = 2\cos(2\pi/n)$ *is contructible*

(iii) $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^k$ *for some* k

(iv) $\phi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ *is a power of* 2.

Proof. To see (iii) implies (iv), We note that $\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset \mathbb{Q}(\zeta_n)$, where the last extension has degree ≤ 2 and the first extension is a power of 2, and $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$. Similar argument shows (iv) implies (iii).

Need to prove (iv) implies (ii). By the converse of Thm 2.1 (whose proof was omitted), it suffices to show that $\mathbb{Q}(\alpha)$ is constructible. By FTGT, this amounts to finding a suitable chain of subgroups, $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\alpha)) = H_1 \leq H_2 \leq \cdots \leq H_m = \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, but this is easy since $|H_m|$ is a power of 2. (If $H_1, ..., H_j$ have been chosen, then G/H_j has order $2^{\text{something}}$, then gH_j has order 2 for some g, then just let $H_{j+1} = \langle H_j, g \rangle$.) □

Corollary 10.5. *A regular* n*-gon is constructible iff* n *is a product of a power of* 2 *and distinct primes of the form* $F_n = 2^{2^k} + 1$.

Proof. Look at the formula of Euler's totient function. see that $\phi(n)$ is a power of 2 iff n is a product of a power of 2 and distinct primes of the form 2^m, but if $2^m + 1$ is a prime then m is a power of 2 (put $x = 2^a$ in $x^b + 1 = (x+1)(......)$ which is a non-trivial factorization when $m = 2^a b$ for some odd b). ☐

Theorem 10.6 (Linear independence of field embeddings)**.** *L, K fields, $\sigma_1, ..., \sigma_n : K \hookrightarrow L$. distinct field embeddings. If $\lambda_1, ..., \lambda_n \in L$ satisfy $\lambda_1\sigma_1(x) + \cdots + \lambda_n\sigma_n(x) = 0$ for all $x \in K$, then $\lambda_1 = \cdots = \lambda_n = 0$.*

Proof. Induction on n. Trivial if $n = 1$. Now, if $n \geq 2$, and $\lambda_1\sigma_1(x) + \cdots + \lambda_n\sigma_n(x) = 0$ for all $x \in K$, then pick $y \in K$ s.t. $\sigma_1(y) \neq \sigma_2(y)$ and replace x by xy. We then get $\lambda_1\sigma_1(x)\sigma_1(y) + \cdots + \lambda_n\sigma_n(x)\sigma_n(y) = 0$ for all $x \in K$. Now subtract a suitable multiple of the first equation from this, we eliminate $\lambda_1\sigma_1(x)\sigma_1(y)$. Invoke the induction hypothesis. ☐

10.1 Kummer's theory

Assume $\operatorname{char} K \nmid n$. and $\mu_n \subseteq K$. Let $a \in K^\times$. Consider the splitting field L/K of $x^n - a$, which is separable by considering derivatives, so L/K is Galois. If α is a root, then $f(X) = \prod_{j=0}^{n-1}(X - \zeta_n^j\alpha)$ so that $L = K(\alpha)$.

Definition. $K(\sqrt[n]{a})/K$ is called a Kummer extension (require $\mu_n \subseteq K$)

Theorem 10.7. *If $\mu_n \subseteq K$ and $a \in K^\times$, then there exists an injective group hom $\theta : \operatorname{Gal}(K(\sqrt[n]{a})/K) \to \mu_n$. In particular, $\operatorname{Gal}(K(\sqrt[n]{a})/K)$ is cyclic and $[K(\sqrt[n]{a}) : K] \mid n$.*

Proof. Let G be the Galois group. If $\sigma \in G$, then $\sqrt[n]{a}$ and $\sigma(\sqrt[n]{a})$ are roots of $x^n - a$, so $\sigma(\sqrt[n]{a}) = \zeta_n^r\sqrt[n]{a}$ for some r which is unique. Define $\theta(\sigma) = \zeta_n^r$. Note that any $\sigma \in G$ is uniquely determined by $\sigma(\sqrt[n]{a})$. ☐

Remark 15. The defn of θ doesn't depend on the choice of ζ_n or the choice of $\sqrt[n]{a}$. To see this, suppose α, β are roots of $x^n - a$, then $\alpha^n/\beta^n = 1$, so $\alpha/\beta \in K$, so $\sigma(\alpha/\beta) = \alpha/\beta$, so $\sigma(\alpha)/\alpha = \sigma(\beta)/\beta$.

Definition. $(K^\times)^n = \{x^n : x \in K\}$.

Corollary 10.8. *$\mu \subseteq K$, $a \in K^\times$. Then*

(i) $[K(\sqrt[n]{a}) : K]$ = order of a in $K^\times/(K^\times)^n$.

(ii) $x^n - a$ is irreducible over K $\Leftrightarrow$ a is not a dth power in K for any $1 < d \mid n$.

Proof. (i) $\alpha = \sqrt[n]{a}$. G Galois group. $a^m \in (K^\times)^n$ iff $\alpha^m \in K^\times$ iff $\sigma(\alpha^m) = \alpha^m$ for all $\sigma \in G$ iff $\theta(\sigma)^m = 1$ iff $\operatorname{im}\theta \subseteq \mu_m$ iff $|\operatorname{im}\theta| \mid m$ iff $[K(\alpha) : K] \mid m$, so $[K(\alpha) : K]$ = least m s.t. $a^m \in (K^\times)^n$, i.e., the order of a in $K^\times/(K^\times)^n$.

(ii) $x^n - a$ is irred over K iff $[K(\alpha) : K] = n$ iff a has order n in $K^\times/(K^\times)^n$ iff $\nexists m \mid n, m < n$ s.t. $a^m \in (K^\times)^n$ iff $\nexists\, d \mid n$, $d > 1$ s.t. $a \in (K^\times)^d$, where d is the complementary divisor of m. [Note: in the last "iff", we used the fact that $\mu_n \subseteq K \Rightarrow \mu_m \subseteq (K^\times)^d$ where $n = md$.] ☐

Theorem 10.9 (Kummer)**.** *If $\operatorname{char} K \nmid n$ and $\mu_n \subseteq K$, then every degree n Galois extension L/K with cyclic Galois group is of the form $L = K(\sqrt[n]{a})$ for some $a \in K^\times$.*

Proof. Suppose $\operatorname{Gal}(L/K) = \langle\sigma\rangle \cong C_n$, Consider $\sum_{j=0}^{n-1}\zeta_n^j\sigma^j(x)$ (Lagrange resolvent). By linear independence of field embeddings, there exists x such that $0 \neq \alpha = \sum_{j=0}^{n-1}\zeta_n^j\sigma^j(x)$. By direct computation, $\sigma(\alpha) = \zeta_n^{-1}\alpha$. From this we know that the Galois conjugates of α are given by $\zeta_n^j\alpha$. Also by direct computation $\sigma(\alpha^n) = \alpha^n$, so $\alpha^n = a \in K$. Also, the min poly of α is $x^n - a$, so $K(\alpha)/K$ has degree n, so $K(\alpha) = L$. ☐

Now let $\operatorname{char} K = 0$ and $f \in K[X]$ irreducible.

Definition. f is soluble by radicals over K if there exists fields $K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_m$ s.t. f has a root in K_m and $K_i = K_{i-1}(\alpha_i)$ for all $1 \leq i \leq m$, where $\alpha_i^{d_i} \in K_{i-1}$, $d_i \geq 1$.

Definition. A finite group G is soluble if there exists subsgroups $\{e\} = H_0 \leq H_1 \leq \cdots \leq H_m = G$ s.t. $H_{i-1} \trianglelefteq H_i$ for all $1 \leq i \leq m$ and H_i/H_{i-1} is abelian.

Remark 16. The above definition is unchanged if replace abelian by cyclic or cyclic of prime order.

Lemma 10.10. *If G is soluble then every subgroup of G is soluble.*

Theorem 10.11. *$f \in K[X]$ irred. f soluble by radicals over K iff $\text{Gal}(f/K)$ is soluble as a group.*

Lemma 10.12. *Let L/K be a finite Galois extension with $\text{Gal}(L/K) = \{\sigma_1, ..., \sigma_m\}$, $\sigma_1 = \text{id}$. Let $\alpha \in L^\times$ and $n \geq 1$. Then $M = L(\mu_n, \sqrt[n]{\sigma_1(a)}, \dots, \sqrt[n]{\sigma_m(a)})$ is a Galois extension of K.*

Proof. Let $f = \prod_{j=1}^m (X^n - \sigma_j(a)) \in K[X]$. M is the composite of L and a splitting field of f over K, so M/K is Galois. (This is Thm 6.6 (ii)) ☐

Proof of Thm 10.11. ($\Rightarrow$) There exists a sequence of fields $K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_m$ s.t. f has a root in K_m and for each $1 \leq i \leq m$, $K_i = K_{i-1}(\alpha_i)$ with $\alpha_i^{d_i} \in K_{i-1}$. Repeatedly applying lemma 10.12, we may assume that K_m/K is Galois. By adjoinng suitable roots of unity, we may further assume that each extension K_i/K_{i-1} is either cyclotomic or Kummer. By Thm 10.1 and 10.7, $\text{Gal}(K_i/K_{i-1})$ is abelian. By FTGT, $\text{Gal}(K_m/K)$ is soluble. Since f has a root in K_m and K_m/K is normal, we know that f splits over K_m. This means that $\text{Gal}(f/K)$ is a quotient of $\text{Gal}(K_m/K)$, which must also be soluble.

($\Leftarrow$) By FTGT, there exists a sequence of fields $K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_m$ s.t. K_m is the splitting field of f over K and that each K_i/K_{i-1} is Galois with cyclic Galois group (refined definition). Let $n = \text{lcm}_{1 \leq i \leq m}[K_i : K_{i-1}]$ and consider $K = K_0 \subseteq K_0(\zeta_n) \subseteq K_1(\zeta_n) \subseteq \cdots \subseteq K_m(\zeta_n)$. Then $K_i(\zeta_n)/K_{i-1}(\zeta_n)$ is Galois and the group homomorphism $\text{Gal}(K_i(\zeta_n)/K_{i-1}(\zeta_n)) \to \text{Gal}(K_i/K_{i-1})$ is injective. Hence, each $\text{Gal}(K_i(\zeta_n)/K_{i-1}(\zeta_n))$ is cyclic of order dividing n. ☐

11 Algebraic Closure

Definition. A rel $\leq$ on a set S is a partial order of $\forall x, y, z \in S$,

(i) $x \leq x$

(ii) $x \leq y$ and $y \leq z$ implies $x \leq z$. (iii) $x \leq y$ and $y \leq x$ implies $x = y$.

$(S, \leq)$ is a poset. It's said to be totally ordered if moreover for all $x, y \in S$ have either $x \leq y$ or $y \leq x$.

Let $T \subseteq S$.

(i) T is a chain if it's totally ordered by $\leq$

(ii) $x \in S$ is an upper bound for T if $t \leq x$ for all $t \in T$.

(iii) $x \in S$ is maximal if $\nexists y \in S$ with $x \leq y$ and $x \neq y$

Theorem 11.1 (Zorn's lemma)**.** *Let S be a non-empty poset. Assume that every chain has an upper bound, then S has a maximal element.*

Theorem 11.2. *K field.*

(i) $\exists$ an algebraic extension L/K s.t. every non-constant $f \in K[X]$ has a root in L.

(ii) K has algebraic closure $\bar{K}$.

Proof. (i): Let $S = \{\text{monic non-constant polynomials over } K\}$. Let $R = K[X_f : f \in S]$. Let $I \subseteq R$ be the ideal generated by $\{f(X_f) : f \in S\}$. We claim that $I \neq R$.

proof of claim: If $1 \in I$, then

$$1 = \sum_{f \in T} g_f f(X_f) \qquad (*)$$

for some $T \subseteq S$ finite and $g_f \in R$. Let L/K be a splitting field of $\prod_{f \in T} f$ and for each $f \in T$ $\alpha_f \in L$ a root of f. Define a ring homomorphism $\phi : R \to L[X_f : f \in S \setminus T]$ as follows:

$$\phi(X_f) = \begin{cases} \alpha_f & f \in T \\ X_f & f \notin T \end{cases}$$

and ϕ fixes elements of K.

Now applying ϕ to $(*)$ gives $1 = \sum_{f \in T} \phi(g_f) f(\alpha_f) = 0$, which is a massive contradiction. ☐

This means that R/I has a maximal ideal, so $\exists J \trianglelefteq R$ maximal s.t. $I \subseteq J$ (we have used Zorn's lemma). Let $L = R/J$ and let $\alpha_f = X_f + J$. Then $f(\alpha_f) = 0$. Observe that

$$L = \bigcup_{T\subseteq S, |T|<\infty} K(\alpha_f : f \in T)$$

so L/K is algebraic.

(ii): Repeating the construction from (i), we get a sequence $K = K_0 \subseteq K_1 = L \subseteq K_2 \subseteq \cdots$ with the property that each non-constant poly in $K_n[X]$ has a root in K_{n+1}. The field $\bigcup_{n\in\mathbb{N}} K_n$ is an algebraic closure of K. □

Proposition 11.3. *Let L/K be an algebraic extension, M/K a field extension with M algebraically closed. Then there exists K-embedding $L \hookrightarrow M$.*

Proof. Define $S = \{(F,\sigma) : K \subseteq F \subseteq L,\ \sigma : F \to M\ (K\text{-embedding})\}$ equipped with the partial order $(F_1,\sigma_1) \le (F_2,\sigma_2)$ if $F_1 \subseteq F_1$ and $\sigma_2|_{F_1} = \sigma_1$. Note that the poset $(S,\le)$ defined this way is non-empty as $(K, \mathrm{id}) \in S$. Suppose $T = \{(F_i,\sigma_i) : i \in I\}$ is a chain where I is some index set. Let $F = \bigcup_{i\in I} F_i$ and $\sigma : F \to M, x \mapsto \sigma_i(x)$ if $x \in F_i$. This is a well-defined element of S which is an upper bound of T. We are now in the situation of Zorn's lemma, so S has a maximal element, say (F,σ).

Let $\alpha \in L$. Since L/K is algebraic, α must be algebraic over F. Since M is algebraically closed, we can extend $\sigma : F \hookrightarrow M$ to $\tau : F(\alpha) \hookrightarrow M$. Then $(F,\sigma) \le (F(\alpha),\tau)$. By maximality we must have $\alpha \in F$, so $F = L$. □

Here is a variant: **Let L/K be algebraic extension and $\sigma : K \hookrightarrow M$ field embedding with M algebraically closed. Then there exists a σ-embedding $L \hookrightarrow M$.**

Corollary 11.4 (Uniqueness of algebraic closure)**.** *K field. L_1, L_2 algebraic closures of K. Then there exists a K-isomorphism $\phi : L_1 \to L_2$.*

Proof. Prop. 11.2 implies that there exists a K-embedding $\phi : L_1 \hookrightarrow L_2$. If $\alpha \in L_2$, then α is algebraic over K and hence algebraic over $\phi(L_1)$, but $\phi(L_1) \cong L_1$ which is algebraically closed. If we consider the sequence of inclusion $K \subseteq \phi(L_1) \subseteq L_2$, it must be the case that $\alpha \in \phi(L_1)$, i.e. $L_1 \cong L_2$. □

12 Artin's Theorem and Invariant Theory

Theorem 12.1 (Artin's Thm on invariants)**.** *Let L be a field and $G \subseteq \mathrm{Aut}(L)$ a finite subgroup. Then L/L^G is a finite Galois extension with Galois group G. In particular $[L : L^G] = |G|$.*

Proof. Let $K = L^G$ and $\alpha \in L$. Let $f = \prod_{i=1}^n (X - \alpha_i)$ where $\alpha_1, \dots, \alpha_n$ are the distinct elements of $\{\sigma(\alpha) : \sigma \in G\}$. Then $\sigma(f) = f$ for all $\sigma \in G$, so $f \in K[X]$. This shows that α is algebraic and separable over K, so L/K is algebraic and separable, and $[K(\alpha) : K] \le |G|$ for all $\alpha \in L$. Pick $\alpha \in L$ s.t. $[K(\alpha) : K]$ is maximal, then we claim that $L = K(\alpha)$.

proof of claim: Let $\beta \in L$. Then $K(\alpha,\beta)/K$ is finite and separable. By the theorem of primitive element, $K(\alpha,\beta) = K(\theta)$ for some $\theta \in L$, but now $[K(\theta) : K] \le [K(\alpha) : K]$. Since it is also true that $K(\alpha) \subseteq K(\theta)$, we must have $\beta \in K(\alpha)$. □

Now, $|\mathrm{Aut}(L/K)| \le [L : K] = [K(\alpha) : K] \le |G|$. Also, $G \subseteq \mathrm{Aut}(L/K)$, so $|\mathrm{Aut}(L/K)| = [L : K]$, so L/K is Galois, so $G = \mathrm{Aut}(L/K) = \mathrm{Gal}(L/K)$. □

Example 12.2. Let $L = \mathbb{C}(X_1, X_2)$. Define $\sigma, \tau \in \mathrm{Aut}(L)$ by $(\sigma f)(X_1, X_2) = f(iX_1, -iX_2)$ and $(\tau f)(X_2, X_2) = f(X_2, X_1)$. Let $G = \langle \sigma, \tau \rangle$. In fact, $G \cong D_8$. We observe that $X_1X_2, X_1^4 + X_2^4 \in L^G$ so that $\mathbb{C}(X_1X_2, X_1 + X_2^4) \subseteq L^G \subseteq L$. By Artin's theorem, L/L^G is Galois and $[L : L^G] = 8$. Observe that $f(T) = (T^4 - X_1^4)(T^4 - X_2^4)$ has coefficients in $\mathbb{C}(X_1X_2, X_1^4 + X_2^4)$, so $[L : \mathbb{C}(X_1X_2, X_1^4 + X_2^4)] \le 8$, so $L^G = \mathbb{C}(X_1X_2, X_1^4 + X_2^4)$.

Suppose R is a ring and $G \subseteq \mathrm{Aut}(R)$ is a subgroup. Invariant theory seeks to describe the subring $R^G = \{x \in R : \forall \sigma \in R,\ \sigma(x) = x\}$. This motivates Hilbert's basis theorem. It's also important in algebraic geometry (the quotient of an algebraic variety by a group action).

Example 12.3. $G = D^8$ acts on $\mathbb{C}[X_1, X_2]$ as in the previous example. Then $\mathbb{C}[X_1, X_2]^G = \mathbb{C}[X_1X_2, X_1^4 + X_2^4]$. Note that $\mathbb{C}[X_1, X_2]^G$ is spanned by $\{X_1^r X_2^s + X_1^s X_2^r : r \equiv s \pmod 4\}$ as a $\mathbb{C}$-vector space.

Example 12.4. Note that if k is a field, $L = k(X_1, ..., X_n)$. $G = S_n$ acts on L. L^G contains elementary symmetric polynomials. Symmetric functions implies that $R^G = k[s_1, ..., s_n]$, where $R = k[X_1, ..., X_n]$ and s_i elementary symmetric polynomials.

Theorem 12.5. *In the previous example, $L^G = k(s_1, ..., s_n)$.*

Proof one: Suppose $f/g \in L^G$ for some f, g coprime. Then $\sigma(f) = c_\sigma f$ and $\sigma(g) = c_\sigma g$ for some $c_\sigma \in k^\times$. Since G is finite of order $N = n!$, we have $f = \sigma^N(f) = c_\sigma^N f$, so $c_\sigma^N = 1$. Therefore fg^{N-1} and g^N are elements of R^G, so $f/g = \frac{fg^{N-1}}{g^N} \in k(s_1, ..., s_n)$. □

Proof two: Define $f(T) = \prod_{i=1}^n (T - X_i) = T - s_1 T^{n-1} + \cdots + (-1)^n s_n \in k(s_1, ..., s_n)[T]$ which has degree n in T. Then L is a splitting field of f over $k(s_1, ..., s_n)$. We have $[L : k(s_1, ..., s_n)] \leq n!$. By Artin's theorem, $[L : L^G] = n!$, so $L^G = k(s_1, ..., s_n)$. □

Remark 17. We've shown that the Galois group of a generic (monic) polynomial of degree n is S_n. Exercise: show that for all finite group G there exists a finite Galois extension whose Galois group is G. Note that it may not be possible to specify K in advance. For instance, the case $K = \mathbb{Q}$ (inverse Galois problem) is unsolved.

Corollary 12.6. *Let S_n act on $L = k(X_1, ..., X_n)$ by permuting variables. If $\mathrm{char}(k) \neq 2$, then $L^{A_n} = k(s_1, ..., s_n, \delta)$, where $\delta = \prod_{i<j}(X_i - X_j)$.*

Proof. Note that $[L^{A_n} : k(s_1, ..., s_n)] = 2$. Have $\sigma(\delta) = \mathrm{sgn}(\sigma)\delta$ for all $\sigma \in S_n$. Inparticular, $\delta \in L^{A_n}$ and $\delta \notin L^{S_n}$, so $L^{A_n} = k(s_1, ..., s_n, \delta)$. □

Remark 18. One can also show that $R^{A_n} = k[s_1, ..., s_n, \delta]$, where $R = k[X_1, ..., X_n]$. [Idea: If $f \in R^{A_n}$, pick $\sigma \in S_n \setminus A_n$. Write $f = \frac{1}{2}(f + \sigma(f) + f - \sigma(f))$. Then $f - \sigma(f)$ is divisible by δ.]

Theorem 12.7 (Fundamental Theorem of Algebra)**.** *We know what the statement is.*

Proof. We will make use of the following facts

(i) Every poly $f \in \mathbb{R}[X]$ of odd degree has a root in $\mathbb{R}$

(ii) Every quadratic polynomial in $\mathbb{C}[X]$ has a root.

(iii) Every group of order 2^n, $n \geq 1$, has a subgroup of index 2.

Suppose $L/\mathbb{C}$ is a non-trivial finite extension. Replacing L by its Galois closure over $\mathbb{R}$, we may assume $L/\mathbb{R}$ is Galois. Let $G = \mathrm{Gal}(L/\mathbb{R})$. Let $H \leq G$ be a Sylow 2-subgroup. Then $[L^H : \mathbb{R}] = [G : H]$ is odd. So if $\alpha \in L^H$, then $[\mathbb{R}(\alpha) : \mathbb{R}]$ is odd. Hence, $\alpha \in \mathbb{R}$ by (i). Therefore $L^H = \mathbb{R}$ and $G = H$, so G is a 2-group. Let $G_1 = \mathrm{Gal}(L/\mathbb{C}) \leq \mathrm{Gal}(L/\mathbb{R}) = G$, then G_1 is a (non-trivial) 2-group. Take a subgroup $G_2 \leq G_1$ of index 2, then $[L^{G_2} : \mathbb{C}] = 2$, which contradicts (ii). □