Course Review: Group Theory and Galois Theory

MAT205 Abstract Algebra II

Ma, Jia-Jun

Xiamen University Malaysia

Part I: Group Theory

Group Actions

Definition. An *action* of G on a set X is a map

$$G \times X \to X, \qquad (g, x) \mapsto g \cdot x,$$

satisfying $e \cdot x = x$ and $(gh) \cdot x = g \cdot (h \cdot x)$.

Equivalently, a group homomorphism

$$G \to \mathrm{Sym}(X).$$

Orbit-Stabilizer Theorem

Orbit and stabilizer.

$$\mathrm{Orb}(x) = \{g \cdot x : g \in G\}, \qquad \mathrm{Stab}(x) = \{g \in G : g \cdot x = x\} \leq G.$$

Orbit-Stabilizer Theorem.

$$|\,\mathrm{Orb}(x)| = [G : \mathrm{Stab}(x)].$$

Consequence. Orbit sizes divide $|G|$; distinct orbits partition X.

Conjugation Action and Conjugacy Classes

Definition. The *conjugation action* of G on itself is

$$g \cdot x = gxg^{-1}.$$

Its orbits are the *conjugacy classes*:

$$\mathrm{cl}(x) = \{gxg^{-1} : g \in G\}.$$

The stabilizer of x is the *centralizer*

$$Z_G(x) = \{g \in G : gx = xg\}.$$

The Class Equation

Applying Orbit-Stabilizer to the conjugation action,

$$|\operatorname{cl}(x)| = [G : Z_G(x)] \text{ divides } |G|.$$

Class equation. Taking one representative x_i from each non-central class,

$$|G| = |Z(G)| + \sum_i [G : Z_G(x_i)],$$

where each $[G : Z_G(x_i)] > 1$.

Main use: p-group arguments —each non-central term is divisible by p, so $p \mid |Z(G)|$.

Cauchy's Theorem and Sylow I, II

Definition. A *Sylow p-subgroup* of G is a maximal p-subgroup. For $|G| = p^a m$ with $\gcd(p, m) = 1$: P is Sylow iff $|P| = p^a$. Write $n_p = |\mathrm{Syl}_p(G)|$.

Cauchy's Theorem. If $p \mid |G|$, then G has an element of order p.

Sylow I. For each $1 \leq i \leq a$, G has a subgroup of order p^i. In particular, Sylow p-subgroups exist.

Sylow II. All Sylow p-subgroups of G are conjugate.

Sylow III and Its Corollary

Sylow III.

$$n_p \mid m \qquad \text{and} \qquad n_p \equiv 1 \pmod{p}.$$

Corollary.

$$P \trianglelefteq G \iff n_p = 1.$$

So to show G is *not* simple, it suffices to force $n_p = 1$ for some prime p.

Hints: Forcing $n_p = 1$ (I)

(A) Sylow III alone. List divisors of m that are $\equiv 1 \pmod{p}$. If only 1 satisfies both, $n_p = 1$.

Example. $|G| = 15$: $n_5 \mid 3$ and $n_5 \equiv 1 \pmod{5}$ force $n_5 = 1$.

(B) Element counting. If Sylow p-subgroups have prime order, distinct ones intersect trivially and contribute $n_p(p-1)$ elements of order p. Combine several such counts; if the total exceeds $|G|$, some n_p must equal 1.

Cue. $|G|$ is a product of distinct primes.

Hints: Forcing $n_p = 1$ (II)

(C) Small index / coset action. If $[G : P] = k$ is small, the action of G on G/P gives $G \to S_k$. When $|G| \nmid k!$, the kernel is nontrivial and forces P normal.

Cue. $[G : P]$ smaller than the smallest prime dividing $|G|$.

(D) Residual p-subgroup. After counting elements of other orders, the leftover p^a elements are exactly one Sylow p-subgroup, hence unique.

p-Groups: Center and Order p^2

Theorem. If $|G| = p^k > 1$ (p prime), then $Z(G) \neq \{e\}$.

Corollaries.

- Every group of order p^2 is abelian.
- Every finite p-group is nilpotent.

FT of Finite Abelian Groups: Invariant Factors

Theorem (invariant factor form). Every finite abelian group G is isomorphic to a unique

$$\mathbb{Z}/d_1 \oplus \mathbb{Z}/d_2 \oplus \cdots \oplus \mathbb{Z}/d_k, \qquad d_1 \mid d_2 \mid \cdots \mid d_k.$$

The integers $d_1, \ldots, d_k$ are the *invariant factors*.

d_k is the exponent of G (smallest n with $nG = 0$).

FT of Finite Abelian Groups: Primary Decomposition

Theorem (elementary divisor form).

$$G \cong \bigoplus_{p \mid\mid |G|} G_p, \qquad G_p = \bigoplus_{i=1}^{r_p} \mathbb{Z}/p^{e_{p,i}}, \quad e_{p,1} \geq \cdots \geq e_{p,r_p} \geq 1.$$

G_p is the (unique, characteristic) Sylow p-subgroup of G; the prime powers $p^{e_{p,i}}$ are the *elementary divisors*.

Passage. G_p is the p-primary part of every invariant factor; invariant factors are assembled by aligning primary partitions column-by-column.

Worked Example: Invariant Factors vs. Elementary Divisors

Problem. Rewrite $G = \mathbb{Z}_{12} \oplus \mathbb{Z}_{18} \oplus \mathbb{Z}_{20}$ in both canonical forms.

Primary form. Split each summand by prime and collect:

$$G \cong \underbrace{\mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2}_{G_2} \oplus \underbrace{\mathbb{Z}_9 \oplus \mathbb{Z}_3}_{G_3} \oplus \underbrace{\mathbb{Z}_5}_{G_5}.$$

Invariant factors. Align columns of primary parts (largest with largest), fill missing entries with 1, multiply down:

p	d_3	d_2	d_1
2	4	4	2
3	9	3	1
5	5	1	1
col	180	12	2

$$\Longrightarrow \qquad G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_{180}.$$

Worked Example: Classifying Abelian Groups of Order 200

Problem. List all abelian groups of order 200, up to isomorphism.

Solution. $200 = 2^3 \cdot 5^2$.

- 2-part: one of $\mathbb{Z}_8,\ \mathbb{Z}_4 \times \mathbb{Z}_2,\ \mathbb{Z}_2^3$ (the 3 partitions of 3).
- 5-part: one of $\mathbb{Z}_{25},\ \mathbb{Z}_5 \times \mathbb{Z}_5$ (the 2 partitions of 2).

The six groups are

$$\mathbb{Z}_8 \times \mathbb{Z}_{25},\quad \mathbb{Z}_8 \times \mathbb{Z}_5^2,\quad \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_{25},$$
$$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_5^2,\quad \mathbb{Z}_2^3 \times \mathbb{Z}_{25},\quad \mathbb{Z}_2^3 \times \mathbb{Z}_5^2.$$

Simple Groups and Composition Series

Definition. A nontrivial group S is *simple* if its only normal subgroups are 1 and S.

Definition. A *composition series* of G is a subnormal series

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = 1$$

with every factor G_i/G_{i+1} simple; n is the *composition length*.

Every finite group has a composition series.

Jordan–Hölder Theorem

Theorem. Any two composition series of G have the same length, and after reordering, isomorphic factors.

Invariant. The multiset of composition factors $\{G_i/G_{i+1}\}$ is an invariant of G.

These composition factors are the "simple building blocks" of G.

Worked Example: Composition Factors of an Abelian Group

Problem. Determine the composition factors of $A = \mathbb{Z}_{20} \times \mathbb{Z}_{45}$.

Solution. A is finite abelian, so its composition factors are cyclic of prime order, one for each prime factor of $|A|$ (with multiplicity). Since

$$|A| = 20 \cdot 45 = 900 = 2^2 \cdot 3^2 \cdot 5^2,$$

the composition factors are

$$\mathbb{Z}_2,\ \mathbb{Z}_2,\ \mathbb{Z}_3,\ \mathbb{Z}_3,\ \mathbb{Z}_5,\ \mathbb{Z}_5.$$

Solvable Groups

Definition. G is *solvable* if it has a subnormal series

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_n = 1$$

with every G_i/G_{i+1} *abelian*.

Equivalent (finite G).

- Every composition factor is cyclic of prime order.
- No composition factor is non-abelian simple.

Nilpotent Groups

Definition. G is *nilpotent* if its lower central series reaches 1:

$$G = \gamma_1(G) \trianglerighteq \gamma_2(G) = [G, G] \trianglerighteq \gamma_3(G) = [G, \gamma_2(G)] \trianglerighteq \cdots = 1,$$

equivalently, its upper central series $1 \trianglelefteq Z(G) \trianglelefteq Z_2 \trianglelefteq \cdots$ reaches G.

Equivalent (finite G). G is the direct product of its Sylow subgroups (equivalently, every Sylow subgroup is normal).

Hierarchy. abelian $\Rightarrow$ nilpotent $\Rightarrow$ solvable; both strict (D_4 nilpotent non-abelian, S_3 solvable non-nilpotent).

A_n Is Simple for $n \geq 5$

Theorem. A_n is simple and non-abelian for every $n \geq 5$.

Below $n = 5$: $A_3 \cong \mathbb{Z}_3$ is abelian simple, and A_4 has a normal Klein-four subgroup

$$V_4 = \{e,\ (12)(34),\ (13)(24),\ (14)(23)\}.$$

Corollary. S_n is solvable $\iff$ $n \leq 4$. For $n \geq 5$, S_n has A_n as a non-abelian simple composition factor.

Worked Example: A_4 Is Solvable

Setup. Inside A_4 (order 12), the *Klein four-group* is

$$V_4 = \{e,\ (12)(34),\ (13)(24),\ (14)(23)\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Conjugation permutes the three non-identity elements $(\sigma(ab)(cd)\sigma^{-1} = (\sigma a\,\sigma b)(\sigma c\,\sigma d))$, so $V_4 \trianglelefteq A_4$.

Composition series.

$$A_4 \triangleright V_4 \triangleright \langle (12)(34) \rangle \triangleright 1,$$

with successive quotients $\mathbb{Z}_3,\ \mathbb{Z}_2,\ \mathbb{Z}_2$. All are cyclic of prime order, so A_4 is solvable.

Characteristic Subgroups

Definition. $H \leq G$ is *characteristic* in G ($H \operatorname{char} G$) if $\alpha(H) = H$ for every $\alpha \in \operatorname{Aut}(G)$.

Standard examples. $Z(G)$; $[G, G]$; each pA and $A[p]$ in a finite abelian group; each $p^k G$ in a finite abelian p-group.

Theorem. If $K \operatorname{char} H$ and $H \trianglelefteq G$, then $K \trianglelefteq G$. In particular, characteristic subgroups of G are normal.

The Normalizer–Centralizer Theorem

Definitions.

$$N_G(H) = \{g \in G : gHg^{-1} = H\},$$
$$Z_G(H) = \{g \in G : ghg^{-1} = h \ \forall h \in H\}.$$

Theorem. $Z_G(H) \trianglelefteq N_G(H)$, and

$$N_G(H)/Z_G(H) \hookrightarrow \mathrm{Aut}(H).$$

Special case. For $H = \{x\}$: $N_G(\{x\}) = G$ and $Z_G(\{x\}) = Z_G(x)$; recovers $[G : Z_G(x)] = |\,\mathrm{cl}(x)|$.

Part II: Fields and Galois Theory

Irreducibility Toolbox (I): Eisenstein

Almost every Part-II problem hinges on an irreducibility check.

Eisenstein's criterion. For $f = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$, if some prime p satisfies

$$p \mid a_0, a_1, \ldots, a_{n-1}, \qquad p \nmid a_n, \qquad p^2 \nmid a_0,$$

then f is irreducible over $\mathbb{Q}$.

Substitution trick. If $f(x+a)$ (some $a \in \mathbb{Z}$) is Eisenstein, so is f. E.g. $\Phi_p(x+1)$ is Eisenstein at p.

Irreducibility Toolbox (II): Roots, mod p, Gauss

Rational Root Theorem. If $f \in \mathbb{Z}[x]$ has rational root p/q in lowest terms, then $p \mid a_0$ and $q \mid a_n$.

Useful for degree 2 or 3: f is irreducible over $\mathbb{Q}$ iff it has no rational root.

Reduction mod p. If $p \nmid a_n$ and $\bar{f} \in \mathbb{F}_p[x]$ is irreducible, then f is irreducible over $\mathbb{Q}$.

Gauss's Lemma. A primitive $f \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Q}$ iff irreducible over $\mathbb{Z}$; the product of two primitive polynomials is primitive.

Simple Extensions

Definition. An extension of the form $F(\alpha)$.

When α is algebraic with minimal polynomial m_α of degree n,

$$F(\alpha) \cong F[x]/(m_\alpha),$$

with F-basis

$$\{1,\ \alpha,\ \alpha^2,\ \ldots,\ \alpha^{n-1}\}.$$

In particular, $[F(\alpha) : F] = \deg m_\alpha$.

Kronecker's Construction

Theorem. For any field F and any irreducible $f \in F[x]$, the quotient

$$K := F[x]/(f)$$

is a field; F embeds into K via constants; and $\bar{x} := x + (f) \in K$ is a root of f.

Consequences.

- Every $f \in F[x]$ has a splitting field: iterate Kronecker.
- Two roots of the same irreducible give F-isomorphic simple extensions (isomorphism extension).

Tower Law

Theorem (Tower Law). For a tower $F \subseteq K \subseteq E$,

$$[E : F] = [E : K] \cdot [K : F].$$

Multiplicative and always finite when both factors are.

Immediate consequence. If $[K : F]$ divides $[E : F]$; and if $[E : F] < \infty$, then every intermediate field K has $[K : F] \mid [E : F]$.

Worked Example: A Degree Computation

Problem. Compute $[\mathbb{Q}(\sqrt{6}, \sqrt[3]{10}) : \mathbb{Q}]$.

$[\mathbb{Q}(\sqrt{6}) : \mathbb{Q}] = 2$ and $[\mathbb{Q}(\sqrt[3]{10}) : \mathbb{Q}] = 3$ (Eisenstein at $p = 2$ or $p = 5$).

Let $d = [\mathbb{Q}(\sqrt{6}, \sqrt[3]{10}) : \mathbb{Q}]$. Tower Law through each subfield gives $2 \mid d$ and $3 \mid d$, so $6 \mid d$; Tower Law also gives $d \leq 2 \cdot 3 = 6$. Hence $d = 6$.

The Index $\{E : F\}$

Definition. $\{E : F\}$ is the number of F-embeddings

$$E \to \overline{F}$$

(Fraleigh's notation). Multiplicative in towers, like $[E : F]$.

Chain of inequalities.

$$|\mathrm{Aut}(E/F)| \;\leq\; \{E : F\} \;\leq\; [E : F].$$

- $|\mathrm{Aut}(E/F)| = \{E : F\} \iff E/F$ is *normal*.
- $\{E : F\} = [E : F] \iff E/F$ is *separable*.

Minimal Polynomial

Definition. For α algebraic over F, the *minimal polynomial* $m_\alpha \in F[x]$ is the monic generator of the ideal

$$\{f \in F[x] : f(\alpha) = 0\} \trianglelefteq F[x].$$

Properties.

- m_α is irreducible over F.
- $[F(\alpha) : F] = \deg m_\alpha$.
- $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is an F-basis of $F(\alpha)$, where $n = \deg m_\alpha$.

Conjugates and the Isomorphism Extension

Definition. α, β are *conjugate over* F if $m_\alpha = m_\beta$; equivalently, roots of the same monic irreducible.

Isomorphism Extension. If α, β are conjugate, there is a unique F-isomorphism

$$F(\alpha) \xrightarrow{\sim} F(\beta), \qquad \alpha \mapsto \beta,$$

and it extends to an automorphism of any normal closure containing both.

Consequence. The conjugates of α are the roots of m_α in $\overline{F}$.

Worked Example: Listing Conjugates

Problem. List the conjugates of $\sqrt[5]{11}$ over $\mathbb{Q}$.

Solution. $x^5 - 11$ is irreducible over $\mathbb{Q}$ (Eisenstein at $p = 11$), so it is the minimal polynomial of $\sqrt[5]{11}$.

Its five roots in $\mathbb{C}$:

$$\zeta_5^k \sqrt[5]{11}, \qquad k = 0, 1, 2, 3, 4, \qquad \zeta_5 = e^{2\pi i/5}.$$

These are the conjugates of $\sqrt[5]{11}$ over $\mathbb{Q}$.

Algebraic Closure

Definition. A field $\overline{F}$ is an *algebraic closure* of F if $\overline{F}/F$ is algebraic and every nonconstant $f \in \overline{F}[x]$ splits over $\overline{F}$.

Theorem (Steinitz).

- Every field F has an algebraic closure.
- Any two algebraic closures of F are F-isomorphic.

Working inside a fixed $\overline{F}$ makes "the" conjugates of α, "the" splitting field of f, and "the" normal closure of E/F well-defined.

Splitting Field

Definition. E/F is a *splitting field* for $f \in F[x]$ if

- f splits over E (factors into linear factors), and
- E is generated over F by the roots of f.

Existence and uniqueness. By iterating Kronecker's construction, every $f \in F[x]$ has a splitting field, unique up to F-isomorphism.

Normal Extensions

Definition. E/F finite is *normal* if every F-embedding $\sigma : E \to \overline{F}$ satisfies $\sigma(E) = E$.

Equivalences. TFAE:

1. Every irreducible $p \in F[x]$ with a root in E splits in E.
2. E is the splitting field over F of some $f \in F[x]$.
3. Every F-embedding $E \to \overline{F}$ has image E.

Checking Non-Normality: a Standard Pattern

Criterion. If some irreducible $f \in F[x]$ has *one* root in E but does not *split* in E, then E/F is not normal.

Prototype. $\mathbb{Q}(\sqrt[3]{a})/\mathbb{Q}$ is not normal for any non-cube $a > 0$: it contains the real root $\sqrt[3]{a}$ of the irreducible $x^3 - a$, but not the non-real roots $\omega\sqrt[3]{a},\ \omega^2\sqrt[3]{a}$.

Same pattern covers $\mathbb{Q}(\sqrt[3]{2}),\ \mathbb{Q}(\sqrt[3]{3}),\ \mathbb{Q}(\sqrt[3]{5}),\ \ldots$

Separability and Galois Extensions

Definition. α is *separable* over F if m_α has no repeated roots in $\overline{F}$. E/F is separable if every $\alpha \in E$ is separable over F.

Automatic separability. In characteristic 0, and for any finite field.

Definition. E/F finite is *Galois* if it is normal and separable, equivalently

$$|\operatorname{Aut}(E/F)| = [E : F].$$

Finite Fields: Existence and Uniqueness

Theorem. For each prime power $q = p^n$, there is a subfield $\mathbb{F}_q \subseteq \overline{\mathbb{F}_p}$ with exactly q elements; any two finite fields of order q are $\mathbb{F}_p$-isomorphic.

Construction.

$$\mathbb{F}_{p^n} = \{a \in \overline{\mathbb{F}_p} : a^{p^n} = a\},$$

the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$.

Multiplicative group. $\mathbb{F}_q^\times$ is cyclic of order $q - 1$ (every finite subgroup of a field's $F^\times$ is cyclic).

The Frobenius Automorphism

Frobenius. The map

$$\sigma : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}, \qquad \sigma(a) = a^p,$$

is a field automorphism.

Theorem.

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \sigma \rangle \cong \mathbb{Z}_n,$$

cyclic of order n.

Subfields of $\mathbb{F}_{p^n}$

Subfield criterion.

$$\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n} \quad \Longleftrightarrow \quad d \mid n.$$

Subfields are unique for each admissible order.

Root factorization.

$$x^{p^n} - x = \prod_{a \in \mathbb{F}_{p^n}} (x - a).$$

Consequence. $x^q - x + 1$ has no root in $\mathbb{F}_q$: no finite field is algebraically closed.

Worked Example: Smallest Field Where $x^{15} - 1$ Splits

Problem. Find the smallest n such that $x^{15} - 1 \in \mathbb{F}_2[x]$ splits over $\mathbb{F}_{2^n}$.

Solution. $x^{15} - 1$ splits over $\mathbb{F}_{2^n}$ iff $\mathbb{F}_{2^n}^{\times}$ (cyclic of order $2^n - 1$) contains all 15th roots of unity, iff $15 \mid 2^n - 1$.

Computing powers of 2 modulo 15:

$$2^1 = 2, \quad 2^2 = 4, \quad 2^3 = 8, \quad 2^4 = 16 \equiv 1 \pmod{15}.$$

The order of 2 mod 15 is 4, so the smallest such n is $\boxed{n = 4}$.

Cyclotomic Fields

Theorem. The minimal polynomial of $\zeta_n = e^{2\pi i/n}$ over $\mathbb{Q}$ is the cyclotomic polynomial Φ_n, irreducible of degree $\varphi(n)$.

Hence

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n), \qquad \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times,$$

via $\sigma_a : \zeta_n \mapsto \zeta_n^a$ for $a \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Structure of $(\mathbb{Z}/n\mathbb{Z})^\times$

Chinese Remainder Theorem.

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong \prod_p (\mathbb{Z}/p^{e_p}\mathbb{Z})^\times.$$

Each factor.

- Cyclic for odd p^{e_p}, and for $n = 2, 4$.
- $(\mathbb{Z}/2^k\mathbb{Z})^\times \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}}$ for $k \geq 3$ (not cyclic).

Worked Example: Cyclotomic Galois Groups, Cyclic and Not

(a) Prime modulus. Is $\mathrm{Gal}(\mathbb{Q}(\zeta_{11})/\mathbb{Q})$ cyclic?
Yes. $(\mathbb{Z}/11\mathbb{Z})^\times = \mathbb{F}_{11}^\times$ is the multiplicative group of a field, hence cyclic, of order 10.

(b) Composite modulus. Is $\mathrm{Gal}(\mathbb{Q}(\zeta_{12})/\mathbb{Q})$ cyclic?
No. $\mathrm{Gal}(\mathbb{Q}(\zeta_{12})/\mathbb{Q}) \cong (\mathbb{Z}/12\mathbb{Z})^\times = \{1, 5, 7, 11\}$; each non-identity squares to 1:

$$5^2 \equiv 1, \quad 7^2 \equiv 1, \quad 11^2 \equiv 1 \pmod{12}.$$

So the group is $\mathbb{Z}_2 \times \mathbb{Z}_2$, not cyclic.

Primitive Element Theorem

Theorem. Every finite separable extension E/F is simple: there exists $\gamma \in E$ with

$$E = F(\gamma).$$

In particular, every finite Galois extension is generated by a single element.

Practical form. For $E = F(\alpha_1, \ldots, \alpha_n)$ separable over an infinite F, almost every $\gamma = c_1\alpha_1 + \cdots + c_n\alpha_n$ works. Standard example: $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

Fundamental Theorem of Galois Theory

Let E/F be finite Galois, $G = \mathrm{Gal}(E/F)$.

Theorem. The map $K \mapsto \mathrm{Gal}(E/K)$ is a bijection from intermediate fields onto subgroups of G:

1. $K = E^{\mathrm{Gal}(E/K)}$ and $\mathrm{Gal}(E/E^H) = H$;
2. $[E : K] = |\mathrm{Gal}(E/K)|$, $[K : F] = [G : \mathrm{Gal}(E/K)]$;
3. K/F normal $\iff$ $\mathrm{Gal}(E/K) \trianglelefteq G$; then $\mathrm{Gal}(K/F) \cong G/\mathrm{Gal}(E/K)$;
4. the correspondence **reverses inclusions**.

Worked Example: Galois Group of a Cubic Splitting Field

Problem. Let E be the splitting field of $x^3 - 3$ over $\mathbb{Q}$. Find $\mathrm{Gal}(E/\mathbb{Q})$ with explicit generators.

Solution. $E = \mathbb{Q}(\sqrt[3]{3}, \omega)$ with $\omega = e^{2\pi i/3}$. Tower Law:

$$[E : \mathbb{Q}] = 3 \cdot 2 = 6.$$

E is normal (splitting field) and separable (char. 0), so Galois.

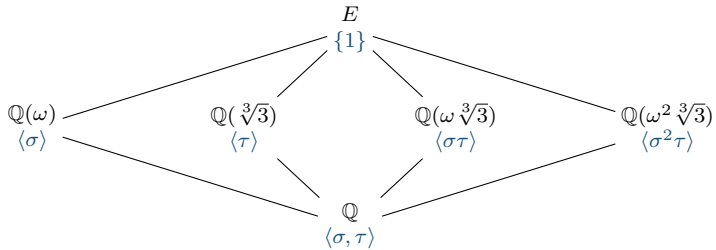
Let

$$\sigma : \sqrt[3]{3} \mapsto \omega\sqrt[3]{3},\ \omega \mapsto \omega \text{ (order 3)}, \quad \tau : \sqrt[3]{3} \mapsto \sqrt[3]{3},\ \omega \mapsto \omega^2 \text{ (order 2)}.$$

Then $\tau\sigma\tau^{-1} = \sigma^{-1}$, so $\mathrm{Gal}(E/\mathbb{Q}) = \langle \sigma, \tau \rangle \cong S_3$.

Worked Example: Explicit Galois Correspondence

Subgroup lattice of $\mathrm{Gal}(E/\mathbb{Q}) \cong S_3$ and its fixed fields (field lattice drawn upside-down):



Only $\langle\sigma\rangle$ (index 2) is normal, matching $\mathbb{Q}(\omega)/\mathbb{Q}$ as the unique normal proper subextension. The three order-2 subgroups are conjugate, matching the three non-normal cubic subfields.

Counting Irreducibles via Frobenius Orbits

Key idea. Monic irreducibles of degree d over $\mathbb{F}_q$ correspond to $\langle \mathrm{Fr} \rangle$-orbits of size d inside $\mathbb{F}_{q^d}$, where $\mathrm{Fr}(\alpha) = \alpha^q$.

d prime. Every $\alpha \in \mathbb{F}_{q^d} \setminus \mathbb{F}_q$ has degree exactly d, so its orbit has size d. Hence

$$\#\{\text{monic irreducibles of degree } d\} = \frac{q^d - q}{d}.$$

General formula (Gauss/Möbius).

$$\#\{\text{degree } n \text{ irreducibles over } \mathbb{F}_q\} = \frac{1}{n} \sum_{d \mid n} \mu(d)\, q^{n/d}.$$

Möbius function. $\mu : \mathbb{Z}_{\geq 1} \to \{-1, 0, 1\}$:

$$\mu(1) = 1, \quad \mu(p_1 p_2 \cdots p_k) = (-1)^k \text{ for distinct primes } p_i, \quad \mu(d) = 0 \text{ if } p^2 \mid d.$$

Constructions: The Wantzel Criterion

Setup. A point $z \in \mathbb{C}$ is *constructible* from $\{0, 1\}$ if it can be obtained by finitely many straightedge-and-compass steps.

Theorem (Wantzel). z is constructible iff z lies in a tower

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_r, \qquad [K_{i+1} : K_i] = 2.$$

In particular, $[\mathbb{Q}(z) : \mathbb{Q}]$ is a power of 2 —a *necessary* condition.

Classical Impossibilities and Regular n-gons

Classical impossibilities.

- Doubling the cube: $\sqrt[3]{2}$ has degree 3, not a power of 2.
- Trisecting a general angle: $\cos 20^\circ$ has degree 3.
- Squaring the circle: π is transcendental.

Gauss–Wantzel. The regular n-gon is constructible iff

$$n = 2^k p_1 \cdots p_s$$

with distinct Fermat primes $p_i = 2^{2^m} + 1$.

Solvability by Radicals

Definition. $f \in F[x]$ is *solvable by radicals* over F if its splitting field lies in a tower

$$F = K_0 \subset K_1 \subset \cdots \subset K_r, \qquad K_{i+1} = K_i(\sqrt[n_i]{a_i}).$$

Galois Criterion. Over a field of characteristic 0,

$$f \text{ solvable by radicals} \iff \mathrm{Gal}(E/F) \text{ solvable},$$

where E is the splitting field of f over F.

Abel–Ruffini: The Quintic Is Not Solvable

Generic degree n. The Galois group of the generic degree-n polynomial over the field of coefficients is S_n.

For $n \geq 5$, S_n is not solvable: A_n is a non-abelian simple composition factor.

Theorem (Abel–Ruffini). There is no general formula in radicals solving the quintic —or any generic polynomial of degree ≥ 5.