Note on Algebra

Contents

Chapter 1

Group theory

1.1 Group Homomorphisms

By G we always mean a group.

Definition. Let G, G' be two groups. A function $\psi : G \to G'$ is a **group homomorphism** if for each $x, y \in G$ we have $\psi(xy) = \psi(x)\psi(y)$.

Proposition 1.1.1. Let G, G' be groups and $\psi : G \to G'$ a homomorphism.

1. $\ker \psi \trianglelefteq G$
2. If $N \trianglelefteq G$, then N is the kernel of some homomorphism.
3. $a \ker \psi = \psi^{-1}(\psi(a))$.

Theorem 1.1.2 (Lagrange's)**.** $|G| < \infty \Rightarrow \forall H \leqslant G[|H| \,\big|\, |G|]$

Definition (Index)**.** Let H be a subgroup of G. The **index** of H in G is defined to be

$$[G : H] := \#\{\text{left cosets of } H \text{ in } G\}$$

Corollary 1.1.2.1. $|G| < \infty \Rightarrow \forall g \in G\,[|\langle g \rangle| \,\big|\, |G|]$. In particular, $\operatorname{ord} g \mid |G|$ for all $g \in G$.

Corollary 1.1.2.2 (Euler's)**.** $\forall n \in \mathbb{N}\, \forall a \in \mathbb{Z}\,[(n, a) = 1 \Rightarrow a^{\phi(n)} \equiv 1 \pmod{n}]$

Corollary 1.1.2.3. If $|G| = p$ is a prime, then $G \cong \mathbb{Z}/p\mathbb{Z}$.

Proposition 1.1.3. Let $K \leqslant H \leqslant G$. Then $[G : H][H : K] = [G : K]$.

Remark 1.1.4. The converse of the Lagrange theorem is not true in general. However, we do have some partial converse results:

1. If G is abelian and $n \mid |G|$, then there's a subgroup of order n.
2. (Cauchy's) If $p \mid |G|$ is a prime, then there's a subgroup of order p.
3. (Sylow's) If $|G| = p^n m$, where p is a prime and $p \nmid m$, then there's a subgroup of order p^j for $j = 1, \ldots, n$.

Proposition 1.1.5. $\forall H, K \leqslant G \left[|H||K| < \infty \Rightarrow |HK| = \dfrac{|H||K|}{|H \cap K|}\right]$

Proposition 1.1.6. $\forall H, K \leqslant G\,[HK \leqslant G \Leftrightarrow KH = HK]$

Corollary 1.1.6.1. $\forall H, K \leqslant G\,[H \leqslant N_G(K) \Rightarrow HK = KH \leqslant G]$. In particular, if $H \leqslant G$ and $N \trianglelefteq G$, then $KH \leqslant G$.

Corollary 1.1.6.2. If N is a normal subgroup of a finite group G with $(|N|, [G : N]) = 1$, then N is the unique normal subgroup of order $|N|$.

Theorem 1.1.7 (Isomorphism theorems)**.** Let G' be a group and $\psi : G \to G'$ a group homomorphism.

1. $G/\ker\psi \cong \operatorname{Im}\psi$
2. $\forall A, B \leqslant G \left[A \leqslant N_G(B) \Rightarrow \dfrac{AB}{B} \cong \dfrac{A}{A \cap B}\right]$
3. $\forall H, K \trianglelefteq B \left[H \leqslant K \Rightarrow \dfrac{G/H}{K/H} \cong \dfrac{G}{K}\right]$
4. Let $N \trianglelefteq G$ and $\pi : G \to G/N$ be the projection map. Then π induces a set-theoretic bijection between $\{H \leqslant G \mid N \leqslant H\}$ and $\{H \leqslant G/N\}$. In particular, π restricts to a bijection between $\{H \trianglelefteq G \mid N \leqslant H\}$ and $\{H \trianglelefteq G/N\}$.

Corollary 1.1.7.1 (universal property of quotient groups)**.** Let G' be a group and $\psi : G \to G'$ a group homomorphism. If $N \trianglelefteq \ker\psi$, then ψ induces a homomorphism $\psi' : G/N \to G'$. Moreover, $\psi = \psi' \circ \pi$, where $\pi : G \to G/N$ is the projection.

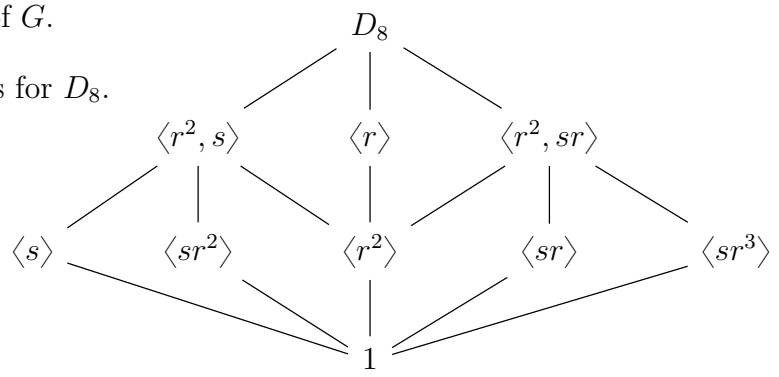
1.2 Composition Series

Definition. A group G is **simple** if $N \trianglelefteq G \Rightarrow N = 1 \vee N = G$.

Definition. A sequence of subgroup of G: $1 = N_0 \leqslant N_1 \leqslant \cdots \leqslant N_k = G$ is a **composition series** for G if $N_i \trianglelefteq N_{i+1}$ and N_{i+1}/N_i is simple for $i = 0, \ldots, k-1$.

- We call N_{i+1}/N_i a **composition factor** of G.

Example 1.2.1. There are 7 composition series for D_8.
All composition factors are C_2.



Lemma 1.2.2 (Zassenhaus')**.** Let H, K, H', K' be subgroups of a group G with $H' \trianglelefteq H$ and $K' \trianglelefteq K$. Then

(a) $(H \cap K')\, H' \trianglelefteq (H \cap K)\, H'$ and $(K \cap H')\, K' \trianglelefteq (K \cap H)\, K'$

(b) $((H \cap K)\, H') \,/\, ((H \cap K')\, H') \cong ((K \cap H)\, K') \,/\, ((K \cap H')\, K')$.

Proof.

1. Note that $H \cap K' \trianglelefteq H \cap K$ and $K \cap H' \trianglelefteq K \cap H$. Pick $g \in (H \cap K)\, H'$ and $a \in (H \cap K')\, H'$, then $g = kh$ and $a = bd$ for some $k \in H \cap K$, $c, h \in H'$ and $b \in H \cap K'$. Then

$$gag^{-1} = khbch^{-1}k^{-1} = kbh_1ch^{-1}k^{-1} = b_1\left(kh_1ch^{-1}k^{-1}\right) \in (H \cap K')\, H'$$

   for some $h_1 \in H'$ and $b_1 \in H \cap K'$ by the normality. Hence $(H \cap K')\, H' \trianglelefteq (H \cap K)\, H'$. Similarly, $(K \cap H')\, K' \trianglelefteq (K \cap H)\, K'$.

2. By the second isomorphism theorem, we have

$$\frac{(H \cap K)\, H'}{(H \cap K')\, H'} \cong \frac{H \cap K}{(H \cap K) \cap (H \cap K')\, H'}$$

   and

$$\frac{(H \cap K)\, K'}{(H' \cap K)\, K'} \cong \frac{H \cap K}{(H \cap K) \cap (H' \cap K)\, K'}$$

   Note that $(H \cap K) \cap (H \cap K')\, H' = (H \cap K')\, (H' \cap K) = (H \cap K) \cap (H' \cap K)\, K'$, so the result ensues.

□

Theorem 1.2.3 (Jordan-Hölder)**.** Let G be a nontrivial finite group. Then

1. G has a composition series.
2. Composition factors are unique in the sense that if

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_m = G \text{ and } 1 = K_0 \trianglelefteq K_1 \trianglelefteq \cdots \trianglelefteq K_n = G$$

are two composition series, then $k = m$ and $\{M_{i+1}/M_i\} = \{N_{i+1}/N_i\}$ up to isomorphisms as multisets.

Proof. 1. This follows from the induction on $n = |G|$.

2. Let

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_m = G \text{ and } 1 = K_0 \trianglelefteq K_1 \trianglelefteq \cdots \trianglelefteq K_n = G$$

be two composition series. Define $H_{ij} = (H_i \cap K_j)\, H_{i-1}$ and $K_{ij} = (K_j \cap H_i)\, K_{j-1}$ for $0 < i \leqslant m$ and $0 < j \leqslant n$ respectively. Then

$$\begin{aligned} &1 \subseteq H_{10} \subseteq \cdots \subseteq H_{1n} \subseteq H_{20} \subseteq \cdots \subseteq H_{2n} \subseteq \cdots \subseteq H_{m0} \subseteq \cdots \subseteq H_{mn} = G \text{ and} \\ &1 \subseteq K_{01} \subseteq \cdots \subseteq K_{m1} \subseteq K_{02} \subseteq \cdots \subseteq K_{m2} \subseteq \cdots \subseteq K_{0n} \subseteq \cdots \subseteq K_{mn} = G \end{aligned}$$

are two series of G. Clearly

$$H_{(i+1)0} = (H_{i+1} \cap K_0)\, H_i = H_i = H_i H_{i-1} = (H_i \cap K_n)\, H_{i-1} = H_{in}$$

Similarly, we have $K_{0(j+1)} = K_{mj}$. By Zassenhaus' lemma, we have

$$\begin{aligned} H_{ij}/H_{i(j-1)} &= ((H_i \cap K_j)\, H_{i-1}) \,/\, ((H_i \cap K_{j-1})\, H_{i-1}) \\ &\cong ((K_j \cap H_i)\, K_{j-1}) \,/\, ((K_j \cap H_{i-1})\, K_{j-1}) = K_{ij}/K_{(i-1)j}. \end{aligned}$$

Since

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_m = G \text{ and } 1 = K_0 \trianglelefteq K_1 \trianglelefteq \cdots \trianglelefteq K_n = G$$

are composition series, $m = |\{(i,j) \,|H_{ij}/H_{i(j-1)} \neq 1\}| = |\{(i,j) \,|K_{ij}/K_{(i-1)j} \neq 1\}| = n$. and there is a permutation $\sigma \in S_n$ such that

$$H_{i+1}/H_i = K_{\sigma(i)+1}/K_{\sigma(i)},\ 0 \leqslant i < n$$

since $H_{ij}/H_{i(j-1)} \cong K_{ij}/K_{(i-1)j}$ for $0 < i, j \leqslant n = m$.

□

Remark 1.2.4. In general, structure of N and G/N do not uniquely determine G. For instance,

$$G = D_8,\ N = \langle r^2 \rangle,\ G/N = V_4 \text{ and } G' = Q_8,\ N' = \langle -1 \rangle,\ G'/N' = V_4$$

Definition. Let G be a group with composition series

$$1 = N_0 \trianglelefteq \cdots \trianglelefteq N_s = G.$$

The **(composition) length** of G is defined by $\ell(G) := s$, which is well-defined by Jordan-Hölder theorem.

Lemma 1.2.5. If A is a simple group and φ is a group homomorphism from A, then $\varphi(A)$ is either trivial or isomorphic to A.

Proposition 1.2.6. Let

$$1 \longrightarrow G' \longrightarrow G \longrightarrow G'' \longrightarrow 1$$

be a exact sequence of groups. Then G admits a composition series if and only if G' and G'' admit composition series. In particular, $\ell(G) = \ell(G') + \ell(G'')$. (HW. 8)

Remark 1.2.7 (Hölder program)**.**

1. Classify all finite simple groups.
    - This was solved in 1980's: 18 infinite families of simple groups and 26 sporadic simple groups.
2. For any 2 groups A, B, determine all groups G such that $N \cong A$ and $G/N \cong B$ for some normal subgroup $N \trianglelefteq G$.
    - This is very difficult, as shown on the right.

n	# of groups of order 2^n
1	1
2	2 (C_4, V_4)
3	5 (C_2^3, $C_2 \times C_4$, C_8, D_8, Q_8)
4	14
$\vdots$	$\vdots$
10	49487365422

Definition. A group is **solvable** if all of its composition factors are abelian.

Lemma 1.2.8. Let G be finite and solvable.

1. Any subgroup H of G is solvable.

2. Let ϕ be any homomorphism from G. Then $\phi(G)$ is solvable. In particular, any quotient group of G is solvable.

Proposition 1.2.9. Let G be a finite group. (HW. 7)

1. G is solvable.
2. G has a chain of subgroups: $1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_s = G$ such that H_{i+1}/H_i is cyclic, $0 \leqslant i < s$.
3. All composition factors of G are cyclic of a prime order.
4. G has a chain of subgroups: $1 = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_t = G$ such that each N_i is a normal subgroup of G and N_{i+1}/N_i is abelian, $0 \leqslant i < t$.

Remark 1.2.10. A polynomial equation over a field F is solvable in radicals if and only if its Galois group is solvable.

1.3 Transpositions and Alternating Groups

Proposition 1.3.1. Let G be a cyclic group.

1. Every subgroup of H is cyclic.
2. If $|G| < \infty$, then there's a set-theoretic bijection between $\{d \in \mathbb{N} \mid d \,\big|\, |G|\}$ and $\{H \mid H \leqslant G\}$.
3. If $|G| = \infty$, then $H \cong \mathbb{Z}$.

Proposition 1.3.2 (disjoint cycle decomposition)**.** Every element in S_n can be written uniquely as a product of disjoint cycles.

Definition. The **orbit** for an element in S_n is the number of disjoint cycles, 1-cycles included, in its disjoint cycle decomposition.

Proposition 1.3.3. For each $\sigma \in S_n$, $\sigma(i_1 \cdots i_k)\sigma^{-1} = (\sigma(i_1) \cdots \sigma(i_k))$.

Corollary 1.3.3.1. Conjugation by an element in S_n sends a permutation to another permuation of the same cycle type.

Definition. $\sigma \in S_n$ is a **transposition** if it's a 2-cycle.

Proposition 1.3.4. Every element of S_n can be written as a product of transpositions.

Proposition 1.3.5. No permutation in S_n can be written both as a product of an even # of transposition and an odd # of transposition.

Proof.

Claim. If $\sigma \in S_n$ and τ is a transposition, then $\#\{\text{orbits for } \tau\sigma\} = \#\{\text{orbits for } \sigma\} \pm 1$

Let $\tau = (i\, j)$. We discuss the following two cases:

1° i, j lie in 2 different orbits for σ. Let $\sigma = (i\, a_1 \cdots a_r)(j\, b_1 \cdots b_s)\mu_1 \cdots \mu_m$ be the decomposition for σ (r, s could be 0). Then

$$(i\, j)(i\, a_1 \cdots a_r)(j\, b_1 \cdots b_s) = (i\, a_1 \cdots a_r\, j\, b_1 \cdots b_s)$$

2° i, j lie in the same orbit. Then

$$(i\, j)(i\, a_1 \cdots a_r\, j\, b_1 \cdots b_s) = (i\, a_1 \cdots a_r)(j\, b_1 \cdots b_s)$$

We return to the proof of the proposition. Assume $\sigma = \sigma_1 \cdots \sigma_k$, where σ_j's are transposition. For each $\tau \in S_n$, let $o(\tau)$ denote the number of its orbits. Then by Claim, we have

$$\begin{array}{rll} o(\mathrm{id}) & = n & \equiv n \pmod 2 \\ o(\sigma_k) & = n-1 & \equiv n-1 \pmod 2 \\ o(\sigma_{k-1}\sigma_k) & = n-2 \vee n & \equiv n-2 \pmod 2 \\ \vdots & & \\ o(\sigma_1 \cdots \sigma_k) & & \equiv n-k \pmod 2 \end{array}$$

Hence $k \equiv n + o(\sigma) \pmod 2$. □

Remark 1.3.6. There's an alternative proof of the proposition above: consider $S_n \curvearrowright \mathbb{Z}[x_1, \ldots, x_n]$ by $\sigma f(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$ and $P(x) := \prod_{1 \leqslant i \leqslant j \leqslant n} (x_i - x_j)$. Check that if τ is a transposition, then $\sigma_1(\sigma_2 f) = (\sigma_1\sigma_2)f$ and $\tau P = -P$.

Definition. An element in S_n is an **even/odd permutation** if it's a product of an even/odd number of transposition.

Definition. $A_n := \{\sigma \in S_n \mid \sigma \text{ is even}\}$ is called the **alternating group of degree** n.

Remark 1.3.7. A cycle of even/odd length is and odd/even permutation.

Proposition 1.3.8.
1. $A_n \leqslant S_n$
2. If $n \geqslant 2$, then $[S_n : A_n] = 2$, and hence $A_n \trianglelefteq S_n$.
3. A_n is generated by 3-cycles.

Proof.

2. Let $B_n := S_n \backslash A_n$. Then $\begin{array}{ccc} A_n & \longrightarrow & B_n \\ \sigma & \longmapsto & (1\,2)\sigma \end{array}$ is a set-theoretic bijection.
3. $(i\,j)(i\,j) = 1$, $(i\,j)(i\,k) = (i\,k\,j)$, $(i\,j)(k\,\ell) = (i\,k\,j)(i\,k\,\ell)$.

□

Example 1.3.9. $A_1 = 1$, $A_2 = 1$, $A_3 = \langle (1\,2\,3) \rangle \cong C_3$, $A_4 = \{1, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3), 8\text{ 3-cycles}\}$. Note that $\{1, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} \trianglelefteq A_4$, which implies that A_4 is not simple.

Remark 1.3.10. Note that A_4 provide a counterexample to the converse statement of the Lagrange's theorem: $6 \mid 12 = |A_4|$ but A_4 fails to have a subgroup of order 6.

Proof. Say $H \leqslant A_4$ such that $|H| = 6$. Then $H \trianglelefteq A_4$. Since $|H| > 4$, H contains a 3-cycle. By conjugating with $(1\,2)(3\,4)$, we find that H contains all 3-cycles, a contradiction. □

Notation 1.3.11. For $\sigma, \tau \in S_n$, let σ^τ denote the conjugation of σ by τ, i.e, $\sigma^\tau = \tau\sigma\tau^{-1}$.

Theorem 1.3.12. For $n \geqslant 5$ and $n = 3$, A_n is simple.

Proof.

1° A_n is generated by 3-cycles.
2° If $H \trianglelefteq A_n$ contains a 3-cycles, then $H = A_n$.
3° If H is a nontrivial normal subgroup of A_n, then it contains a 3-cycle.

2° WLOG, assume H contains $(1\,2\,3)$. Let $(i\,j\,k)$ be another 3-cycle. We construct $\sigma \in A_n$ such that $\sigma(1) = i$, $\sigma(2) = j$ and $\sigma(3) = k$ so that $(1\,2\,3)^\sigma \in H \trianglelefteq A_n$.

- $\{i, j, k\} \cap \{1, 2, 3\} = \varnothing$. Take $\sigma = (1\,i\,2\,j)(3\,k)$.
- $\#\{i, j, k\} \cap \{1, 2, 3\} = 1$, say $i = 1$. Take $\sigma = (2\,j)(3\,k)$.
- $\#\{i, j, k\} \cap \{1, 2, 3\} = 1$. If $i = 1, j = 2$, take $\sigma = (3\,k\,4)$. If $i = 2, j = 1$, take $\sigma = (3\,k)(1\,2)$

3° Say $\sigma \in H$ is a nontrivial element. Consider the following possible cases for the cycle decomposition of σ.

- It contains a cycle of length $\geqslant 4$. Say $\sigma = (1 \cdots m)\tau$, $m \leqslant 4$. Then

$$\sigma^{-1}\sigma^{(1\,2\,3)} = \tau^{-1}(1\,2 \cdots m)^{-1}(2\,3\,1\,4 \cdots m)\tau = (1\,3\,m)$$

- It contains more than one 3-cycles. Say $\sigma = (1\,2\,3)(4\,5\,6)\tau$. Then

$$\sigma^{-1}\sigma^{(1\,2\,4)} = (1\,4\,2\,6\,3)$$

  It reduces to the first case.

- It contains one 3-cycle and several transposition. Then σ^2 is a 3-cycle.
- It contains only transpositions. Say $\sigma = (1\,2)(3\,4)\tau$. Put $\theta := \sigma^{-1}\sigma^{(1\,2\,3)} = (1\,3)(2\,4)$. Then

$$\theta^{-1}\theta^{(1\,3\,5)} = (1\,3\,5)$$

□

1.4 Group Actions

Definition. A **(left) group action** of a group G on a set A is a map $\begin{array}{c} G \times A \longrightarrow A \\ (g,a) \longmapsto ga \end{array}$ such that

1. $(g_1g_2)a = g_1(g_2a)$ for all $g_1, g_2 \in G$ and $a \in A$
2. $1a = a$ for all $a \in A$

Proposition 1.4.1. Let G be a group and A a set. Assume that G acts on A.

1. Define $\phi_g : A \to A$ by $\phi_g(a) := ga$. Then $\phi_g \in S_A$
2. Define $\Phi : G \to S_A$ by $\Phi(g) := \phi_g$. Then Φ is a group homomorphism.

Definition. Φ in the preceding proposition is called the **permutation representation of** G associated to the given group action.

Example 1.4.2.

1. Define $G \times A \to A$ by $(g,a) \mapsto a$ for all $g \in G$ and $a \in A$. This is called the trivial action.
2. F acts on F^n by $r(a_1, \ldots, a_n) := (ra_1, \ldots, ra_n)$.
3. S_n acts on $\{1, \ldots, n\}$ by $\sigma i = \sigma(i)$.
4. $\mathrm{SL}_2(\mathbb{R})$ acts on $\mathbb{H} := \{z \in \mathbb{C} \mid \operatorname{Im} z > 0\}$ by $\begin{pmatrix} a & b \\ c & d \end{pmatrix} z := \dfrac{az+b}{cz+d}$.
5. G acts on itself by left multiplication.
6. G acts on itself by conjugation.

Proposition 1.4.3. Assume that G acts on A. Define $\sim$ on A by $a \sim b \Leftrightarrow a = gb$ for some $g \in G$. Then $\sim$ is an equivalence relation.

Definition. The equivalence class in the preceding proposition in called an **orbit**. The orbit containing $a \in A$ is denoted by Ga.

Proposition 1.4.4. Assume that G acts on A. For $a \in A$, let $G_a := \{g \in G \mid ga = a\}$. Then $G_a \leqslant G$.

Definition. G_a is the preceding proposition is called the **stabilizer subgroup of** a.

Proposition 1.4.5 (Orbit-stabilizer formula)**.** Assume that G acts on A. Then

$$Ga \longrightarrow \{ \text{ all left cosets of } G_a \}$$

$$ga \longmapsto gG_a$$

is a set-theoretic bijection. In particular, if $\#G < \infty$, $|Ga| = [G : G_a]$ and $|G| = |G_a||Ga|$

Theorem 1.4.6 (Cauchy's)**.** Let G be a finite group and p be a prime dividing $|G|$. Then there's an element $x \in G$ of order p.

Proof. Consider the set

$$\mathcal{S} = \{(x_1, x_2, \ldots, x_p) \in G^p \mid x_1 x_2 \cdots x_p = 1\}.$$

Define the relation $\sim$ on $\mathcal{S}$ by letting

$$\alpha \sim \beta \Leftrightarrow \beta = (1\,2\,\cdots\,p)^k \alpha \text{ for some } k$$

It's clear that $\sim$ is an equivalence relation. Viewing the equivalence relation as a action of C_p on $\mathcal{S}$. then by the orbit-stabilizer formula, the size of an orbit, an equivalence class, is either p or 1 since p is a prime. Since the size of the orbit of $(1, \ldots, 1)$ is 1 and p divides $|G|^{p-1}$, there must be at least $p-1$ orbits whose sizes are 1, and they must be of the form $(x, \ldots, x)$ with $x^p = 1$. Such x is the desired element. □

Definition. Assume that G acts on A.

1. The subgroup $\{g \in G \mid ga = a \,\forall\, a \in A\} = \ker \Phi$ is called the **kernel of the group action**.
2. The group action is called **faithful** if the kernel is trivial.
3. The group action is called **transitive** if $\forall\, a, b \in A\, \exists\, g \in G\, [a = gb]$, i.e, $\#\{Ga \mid a \in A\} = 1$.

1.4.1 Burnside's lemma

Theorem 1.4.7 (Burnside's) (Frobenius')**.** Assume that G acts on X and $|G|, |X| < \infty$. For $g \in G$, let $X_g := \{x \in X \mid gx = x\}$. Then

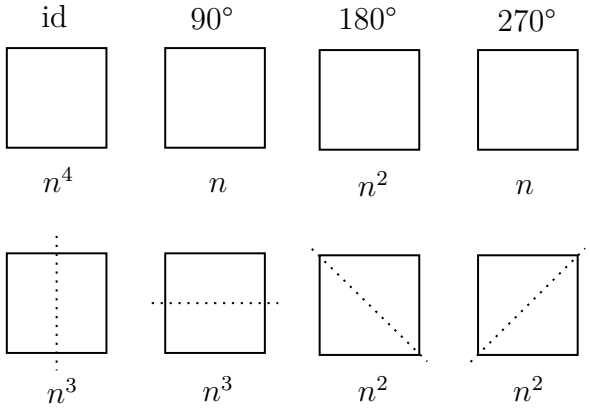
$$\#\{Gx \mid x \in X\} = \frac{1}{|G|} \sum_{g \in G} |X_g|$$

Proof. Consider $\mathcal{S} := \{(g, x) \in G \times X \mid gx = x\}$. Then $\mathcal{S} := \bigsqcup_{g \in G} \{(g, x) \mid gx = x\}$, and thus $|\mathcal{S}| = \sum_{g \in G} |X_g|$. On the other hand, $\mathcal{S} := \bigsqcup_{x \in X} \{(g, x) \mid gx = x\}$, and thus

$$\begin{aligned} |\mathcal{S}| &= \sum_{x \in X} |G_x| = \sum_{\mathcal{O}\text{: orbit}} \sum_{x \in \mathcal{O}} |G_x| = \sum_{\mathcal{O}\text{: orbit}} \sum_{x \in \mathcal{O}} \frac{|G|}{|G_x|} \\ &= \sum_{\mathcal{O}\text{: orbit}} \sum_{x \in \mathcal{O}} \frac{|G|}{|\mathcal{O}|} = |G| \sum_{\mathcal{O}\text{: orbit}} \frac{1}{|\mathcal{O}|} \sum_{x \in \mathcal{O}} 1 = |G| \cdot \#\{Gx \mid x \in X\} \end{aligned}$$

□

Example 1.4.8. Given n distinct colors, we count the number of ways to paint the frame of a square with Burside's lemma. Let X the set that collects all possible coloring, assuming the frame is fixed. Consider D_8-action on X as usual. Hence # of orbits $= \frac{1}{8}(n^4 + 2n^3 + 3n^2 + 2n)$, as shown in the following picture.



1.4.2 Primitive actions

Definition. Subgroups of symmetric groups are called **permutation groups**.

From now on, we let A be a nonempty finite set and G be a permutation group on A.

Definition. A G-action on A ($|A| \geqslant 2$) is **doubly transitive** if G acts transitively on $(A \times A) \backslash \Delta$, where Δ is the diagonal of $A \times A$.

Example 1.4.9. S_n is doubly transitive on $\{1, 2, \ldots, n\}$ for $n \geqslant 2$.

Definition. Let G transitive. A **block** is a nonempty subset B of A such that $\forall \sigma \in G\, [\sigma(B) \cap B \neq \varnothing \Rightarrow \sigma(B) = B]$.

Definition. G is said to be **primitive** if it's transitive and the only blocks in A are A and $\{a\}, a \in A$.

Proposition 1.4.10. Let G be transitive. (HW. 9)

1. If B is a block containing $a \in A$, then

$$G_B := \{\sigma \in G \mid \sigma(B) = B\}$$

is a subgroup of G containing G_a. In particular,

$$A = \bigsqcup_{i=1}^{n} \sigma_i(B)$$

for some $\sigma_i \in G$.

2. G is primitive if and only if G_a is maximal in G for each $a \in A$

3. If G is doubly transitive, then G is primitive.

Proposition 1.4.11. Let the action G on A be transitive and faithful. Suppose G acts on A primitively, then for any $1 \neq H \trianglelefteq G$, the induced action H on A is transitive.

1.4.3 Actions by left multiplication

Definition. The permutation representation of G associated to the left multiplication is called the **left regular representation**.

Proposition 1.4.12. G acts on itself by left multiplication is faithful and transitive.

Theorem 1.4.13 (Cayley's)**.** Any group G can be embedded in to its symmetric group S_G.

Theorem 1.4.14. Let $H \leqslant G$ and $X := \{\text{all left cosets of } H \text{ in } G\}$. Consider the G-action on X be left multiplication.

1. The action is transitive and $G_{1H} = H$.

2. The kernel is $\bigcap_{g \in G} gHg^{-1}$, which is the largest normal subgroup of G contained in H.

Corollary 1.4.14.1. Assume that $|G| < \infty$ and p is the smallest prime factor of $|G|$. Then any subgroup of index p in G is normal in G.

Proof. Let $K := \bigcap_{g \in G} gHg^{-1}$. Then $G/K \cong$ a subgroup in S_p. Thus

$$p[H : K] = [G : H][H : K] = [G : K] \mid |S_p| = p!$$

i.e, $[H : K] \mid (p-1)!$. Since $[H : K] \mid |G|$ p is the smallest prime factor, we deduce $[H : K] = 1$, i.e, $H = K \trianglelefteq G$. □

Example 1.4.15.

1. Let $G = D_8$ and $H = \langle s \rangle$. We have $\bigcap_{g \in D_8} gHg^{-1} = 1$, i.e, G acts on $\{\text{left cosets of } H\}$ faithfully. Hence $D_8 \cong$ a subgroup of S_4.

2. Any nontrivial subgroup of Q_8 contains $\{\pm 1\}$. If $|H| \neq 1$, then the action on the left cosets of H isn't faithful. Hence, Q_8 cannot embedded into S_7.

Lemma 1.4.16. If $H \trianglelefteq G$ has prime index p, then for all $K \leqslant G$, either $K \leqslant H$ or $G = HK$ with $[K : K \cap H] = p$.

Proposition 1.4.17. Let G be a finite group and $\Phi : G \to S_G$ be the left regular representation.

1. For each $g \in G$, $\Phi(g)$ is an odd permutation if and only if $|g|$ is even and $|G|/\operatorname{ord} g$ is odd.

2. If $\operatorname{Im} \Phi \nsubseteq A_G$, then G has a subgroup of index 2.

Proof.

1. Put $\Phi(g) = \phi_g$ and $n := |G|$. For each $g \in G$, identify ϕ_g with its image in S_n via the canonical isomorphism $S_G \to S_n$. Fix a $g \in G$, and let $\sim$ be the equivalence relation generated by

$$a \sim b \Leftrightarrow ab^{-1} = g^k \text{ for some } k \in \mathbb{N}$$

   Clearly, each equivalence class has the same cardinality $\operatorname{ord} g$, and each corresponds to a cycle in the cycle decomposition of ϕ_g. Hence each cycle has length $\operatorname{ord} g$ and the number of cycles is $\dfrac{|G|}{\operatorname{ord} g}$. Hence

$$\phi_x \text{ is odd } \Leftrightarrow (\operatorname{ord} g - 1)\frac{|G|}{\operatorname{ord} g} \text{ is odd} \Leftrightarrow \frac{|G|}{\operatorname{ord} g} \text{ is odd and } \operatorname{ord} g \text{ is even}$$

2. Since $A_G \trianglelefteq S_G$ has index 2 and $\operatorname{Im} G \notin A_G$, we have $[\operatorname{Im} G : \operatorname{Im} G \cap A_G]$ by Lemma 1.4.16. Then $\Phi^{-1}(\operatorname{Im} G \cap A_G)$ is a subgroup of G of index 2.

□

Corollary 1.4.17.1. If G is a finite group with $\nu_2(|G|) = 1$, then G has a subgroup of index 2.

1.4.4 Actions by conjugation

Definition. Let G be a group.

1. The orbit of $a \in G$ under the action of conjugation is called the **conjugacy class** of a, and is denoted by $\mathrm{Cl}(a)$.
2. The stabilizer G_a ($a \in G$) under conjugation is denoted by $C_G(a)$, called the **centralizer of** a.
3. $a, b \in G$ are said to be **conjugates** if $b = gag^{-1}$ for some $g \in G$.

- By the orbit-stabilizer formula, we have $\#\,\mathrm{Cl}(a) = [G : C_G(a)]$.

Definition. The **center** of a group G is the subgroup

$$Z(G) := \{a \in G \mid ag = ga \; \forall g \in G\}$$

- $Z(G)$ is the kernel of the action by conjugation. Hence the action is not faithful in general.
- $g \in Z(G)$ if and only if $\mathrm{Cl}(g) = \{g\}$.

Proposition 1.4.18. Let G be a group. If $G/Z(G)$ is cyclic, then G is abelian.

Theorem 1.4.19 (Class equation)**.** Let G be finite, and $g_1, \ldots, g_n$ the representatives of conjugacy classes of G having more than 1 elements. Then

$$|G| = |Z(G)| + \sum_{i=1}^{n} [G : C_G(g_i)]$$

Definition. Let p be a prime. A finite group is called a **p-group** if $|G| = p^n$ for some $n \in \mathbb{N}$.

Corollary 1.4.19.1. If G is a p-group, then $Z(G) \neq 1$.

Corollary 1.4.19.2. If G is a p-group of order p^2, then G is abelian, and $G \cong C_p^2$ or $G \cong C_{p^2}$.

Corollary 1.4.19.3. Any finite p-group is solvable.

Corollary 1.4.19.4. Let p be a prime and G a group of order p^n. Then G has a subgroup of order p^i for $i = 0, \ldots, n$.

1.4.5 Conjugacy classes in S_n

Definition. Let $\sigma \in S_n$. If the cycle decomposition of σ is a product of cycles of lengths

$$n_1 \leqslant n_2 \leqslant \cdots \leqslant n_k$$

(including 1-cycles so that $\sum_{i=1}^{k} n_i = n$), then the sequence of integers $n_1, \ldots, n_k$ is called the **cycle types of** σ.

Definition. A nondecreasing sequence of positive integers $n_1 \leqslant n_2 \leqslant \cdots \leqslant n_k$ such that $\sum_{i=1}^{k} n_i = n$ is called a **partition of** n.

Proposition 1.4.20. Two elements in S_n are conjugates if and only if they have the same cycle type.

Corollary 1.4.20.1. There's a set-theoretic bijection between {conjugacy classed of S_n} and {partitions of n}.

Example 1.4.21. We demonstrate the correspondence with S_6.

partition	$\lvert$conjugacy class$\rvert$	$\lvert C_{S_6}(\cdot)\rvert = \dfrac{\lvert S_6\rvert}{\lvert\text{conjugacy class}\rvert}$
6	$6!/6$	$6 = \#\langle(1\,2\,\cdots\,6)\rangle$
$3+3$	$6!/(3\cdot 3\cdot 2) = 40$	$18 = \#\langle(i\,j\,k), (\ell\,m\,n), (i\,\ell)(j\,m)(k\,n)\rangle$
$2+2+2$	$6!/(2\cdot 2\cdot 2\cdot 3!) = 15$	48
$2+1+1+1$	$6!/(2\cdot 4!) = 15$	48

1.4.6 Conjugacy classes in A_n

Lemma 1.4.22. Let G be a group, $\mathcal{K}$ a conjugacy class of G and $N \trianglelefteq G$. Then either $K \cap N = \varnothing$ or $K \subseteq N$. Hence a normal subgroup of G is a disjoint union of some conjugacy classes.

Lemma 1.4.23. Let $\sigma \in A_n$ and σ^{S_n} and σ^{A_n} denote the conjugacy classes of σ in S_n and A_n, respectively. If σ commutes with some odd permutation, then $\sigma^{A_n} = \sigma^{S_n}$. Otherwise, $\sigma^{S_n} = \sigma^{A_n} \sqcup (1\,2)\sigma^{A_n}(1\,2)$.

Proof. If σ commutes with an odd permutation, say τ, then for any $\rho \in S_n \backslash A_n$,

$$\rho\sigma\rho^{-1} = \rho\tau\sigma(\rho\tau)^{-1} \in \sigma^{A_n}$$

and thus $\sigma^{S_n} = \sigma^{A_n}$. Now suppose σ does not commute with any odd permutation.

Claim. $\sigma^{A_n} \cap (1\,2)\sigma^{A_n}(1\,2) = \varnothing$.

Suppose otherwise there are $g, g' \in A_n$ such that $g\sigma g^{-1} = (1\,2)g'\sigma g'^{-1}(1\,2)$, then σ commutes with $g'^{-1}(1\,2)g$, a contradiction since $g'^{-1}(1\,2)g$ is odd. $\square$

Lemma 1.4.24. Let $\sigma \in S_n$ whose cycle type consists of distinct integers. Then σ only commutes with the subgroup generated by the cycles in its cycle decomposition.

Proof. Let $\sigma = \sigma_1 \cdots \sigma_k$ be its cycle decomposition, counting 1-cycles. Suppose otherwise that there's a permutation $\tau \notin \langle \sigma_i \mid i = 1, \ldots, k \rangle$ such that $\sigma\tau = \tau\sigma$. WLOG, let $\{i \mid \sigma_i \text{ and } \tau \text{ are not disjoint}\} = \{1, \ldots, r\}$ for some $r \leqslant k$. Since $\sigma\tau = \tau\sigma$, $\tau\sigma_1 \cdots \sigma_r\tau^{-1} = \sigma_1 \cdots \sigma_r$. τ cannot send elements in σ_i to σ_j since $|\sigma_i| \neq |\sigma_j|$ for all $i \neq j$. Also, orders of the elements in σ_i must be preserved under τ for otherwise $\tau\sigma_i\tau^{-1} \neq \sigma_i$ for all i. Hence, τ must be a product of $\sigma_i^{m_i}$ for some integer m_i for all $i \leqslant r$, a contradiction. □

Theorem 1.4.25. $\sigma \in S_n$ does not commute with odd permutation if and only if its cycle type consists of distinct odd integers.

Proof. ($\Rightarrow$) Note that σ commutes with cycles in its cycle decomposition, so the cycle type of σ consists of odd integers. Were two cycle to have the same length, say $\alpha = (1 \cdots k)$ and $\beta = (k+1 \cdots 2k)$ for some odd integer k, then $\tau := (1\ k+1) \cdots (k\ 2k) \in S_n \backslash A_n$ satisfies $\tau\alpha\tau^{-1} = \beta$ and $\tau\beta\tau^{-1} = \alpha$, implying $\tau\alpha\beta = \alpha\beta\tau$. Thus, $\tau\sigma = \sigma\tau$, a contradiction. Hence its cycle type must consist of distinct odd integers.
($\Leftarrow$) This follows directly from Lemma 1.4.24. □

Corollary 1.4.25.1. Let $\mathcal{K}$ be a conjugacy class of S_n and assume $\mathcal{K} \subseteq A_n$. Then $\mathcal{K}$ consists of two conjugacy classes in A_n if and only if the cycle type of an element of $\mathcal{K}$ consists of distinct odd integers.

Example 1.4.26. Even permutation in A_5 are

cycle types	S_n	A_n
5-cycles	$\lvert\sigma^{S_5}\rvert = 24$	$12 + 12$
3-cycles	$\lvert\sigma^{S^5}\rvert = 20$	20
$(i\,j)(k\,\ell)$	$\lvert\sigma^{S^5}\rvert = 15$	15
1	1	1

Now, no proper partial sums of $\{1, 15, 20, 12, 12\}$ is a divisor of 60. Hence A_5 is simple.

Proposition 1.4.27. Consider the G-action on $\{H \mid H \leqslant G\}$ by conjugation.

1. The stabilizer subgroup of $H \leqslant G$ is $N_G(H)$.
2. The number of subgroup conjugate to H is $[G : N_G(H)]$.

Proposition 1.4.28. A_n $(n \geqslant 5)$ does not have a proper subgroup of index $< n$.

Proof. Let $H \lneq A_n$ be of index $m < n$ and consider the A_n-action on the set of all left cosets of H by left translation. □

1.4.7 Automorphisms

Definition. Let G be a group and A a nonempty subset of G.

1. The **centralizer** of A in G is the subgroup $C_G(A) := \{g \in G \mid ag = ga \,\forall a \in A\}$
2. The **normalizer** of A in G is the subgroup $N_G(A) := \{g \in G \mid gAg^{-1} = A\}$
3. The **normal closure of** A in G, or the **normal subgroup generated by** A, is the subgroup generated by $\bigcup_{a \in A} \mathrm{Cl}(a)$.

Definition. Let G be a group.

1. The **automorphism group** of G is $\mathrm{Aut}(G) := \{f : G \to G \mid f \text{ is a group isomorphism}\}$.
2. The **inner automorphism group** of G is $\mathrm{Inn}(G) := \{f : G \to G \mid \exists g \in G \,\forall x \in G\, [f(x) = gxg^{-1}]\}$.

Proposition 1.4.29. Let G be a group and H a subgroup of G.

1. $G/Z(G) \cong \mathrm{Inn}\, G$
2. $N_G(H)/C_G(H) \leqslant \mathrm{Aut}\, H$.
3. $\mathrm{Inn}\, G \trianglelefteq \mathrm{Aut}\, G$

Example 1.4.30.

1. $\begin{aligned} (\mathbb{Z}/n\mathbb{Z})^\times &\longrightarrow \mathrm{Aut}(C_n) \\ a &\longmapsto [x \mapsto x^a] \end{aligned}$ is an isomorphism, and thus $\mathrm{Aut}(C_n) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. Furthermore, if $n = p^k$, then
$$(\mathbb{Z}/n\mathbb{Z})^\times = \begin{cases} C_{p^{k-1}(p-1)} & \text{if } p \neq 2 \\ C_2 \times C_{2^{k-2}} & \text{if } p = 2 \wedge k \geqslant 2 \\ 1 & \text{if } p = 2 \wedge k = 1 \end{cases}$$

   Proof. For brevity, put $G := (\mathbb{Z}/n\mathbb{Z})^\times$. If $p = 2$, we see that $5 = 1 + 2^2$ has order 2^{k-2} in G, and thus $\pm 5^{2^{k-3}}$ have order 2. This shows G is not cyclic, and one of $\pm 5^{2^{k-3}}$ does not lie in $\langle 5 \rangle$. Hence $G = \langle 5 \rangle \times \langle s \rangle$, where $s = \pm 5^{2^{k-3}}$. For odd primes p, note that $1 + p$ has order p^{n-1} in G. Consider the reduction homomorphism
$$\psi : G \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times$$
$$a \,(\mathrm{mod}\, p^k) \longmapsto a \,(\mathrm{mod}\, p)$$
   Note that $\langle 1 + p \rangle \leqslant \ker \psi \lneq G$, so $\ker \psi = \langle 1 + p \rangle$, i.e, $\ker \psi = C_{p^{k-1}}$. Note also that $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order $p - 1$, and since $(p - 1, p^{k-1}) = 1$, we obtain $G = C_{p^{k-1}} \times C_{p-1} = C_{p^{k-1}(p-1)}$. □

2. $\operatorname{Aut} D_8 = D_8$ and $\operatorname{Aut} Q_8 = S_4$.

3. Let p be a prime. Then $\operatorname{Aut}(C_p^n) \cong \mathrm{GL}_n(\mathbb{F}_p)$. Also, $\#\,\mathrm{GL}_n(\mathbb{F}_p) = (p^n - 1)(p^n - p)\cdots(p^n - p^{n-1})$.

Proposition 1.4.31. $S_n = \operatorname{Inn} S_n = \operatorname{Aut} S_n$ for $n \geqslant 3, n \neq 6$. (HW. 8)

Proof. For $1 \leqslant k \leqslant n/2$, let

$$C_k : \{\sigma \in S_n \mid \sigma \text{ is a product of } k \text{ disjoint 2-cycles}\}$$

There are some facts:

- If $\tau \in \operatorname{Aut} S_n$, then $\tau(C_1) = C_k$ for some k.
- $\#C_k = \dbinom{n}{2k} \dfrac{(2k)!}{2^k k!}$.
- $\#C_k \neq \#C_1$ unless $k = 1$ or $n = 6$.

Also, one can show if $\psi \in \operatorname{Aut} S_n$ such that $\psi(C_1) = C_1$, then $\psi \in \operatorname{Inn} S_n$. With these facts we may deduce the second equality. For the first equality, note that $Z(S_n) = 1$ for $n \geqslant 3$, so $S_n = \operatorname{Inn} S_n$. □

Proposition 1.4.32. $[\operatorname{Aut} S_6 : \operatorname{Inn} S_6] = 2$.

Definition. $H \leqslant G$ is a **characteristic subgroup** of G if $\sigma(H) = H$ for each $\sigma \in \operatorname{Aut} G$, and we denote this as H char G.

Proposition 1.4.33. 1. H char $G \Rightarrow H \trianglelefteq G$

2. $(K$ char $H \wedge H \trianglelefteq G) \Rightarrow K \trianglelefteq G$

3. $(k$ char $H \wedge H$ char $G) \Rightarrow K$ char G

Example 1.4.34. 1. $Z(G)$ char G and $[G, G]$ char G.

2. Every subgroup of cyclic groups is characteristic. Thus every subgroup contained in a cyclic subgroup of G is normal in G.

1.5 Sylow's Theorem

In this section by p we mean a prime number, and G always denote a group.

Definition. Assume that $p \mid |G|$.

1. If $H \leqslant G$ with $|H| = p^a$ for some $a \in \mathbb{N}$, then we say that H is a **p-subgroup** of G.
2. If $|G| = p^a m$ with $a \in \mathbb{N}$ and $p \nmid m$ and $H \leqslant G$ with $|H| = p^a$, then we say H is a **Sylow p-subgroup** of G.

- We denote the set of all Sylow p-subgroup of G by $\mathrm{Syl}_p(G)$.

Lemma 1.5.1. Let G be a finite p-group and X a finite set. Assume that G acts on X. Let

$$X_G := \{x \in X \mid gx = x \ \forall g \in G\}$$

Then $|X| \equiv |X_G| \pmod{p}$.

Proof. Let $\mathcal{O}_1, \ldots, \mathcal{O}_n$ be the orbits under the action with $|\mathcal{O}_1| = \cdots = |\mathcal{O}_r| = 1$ and $|\mathcal{O}_{r+1}|, \ldots, |\mathcal{O}_n| > 1$ for some $r \in \mathbb{N}$. Note that $|\mathcal{O}_i| = 1$, say $\mathcal{O}_i = \{x\}$, means $x \in X_G$. Thus

$$|X| = |X_G| + \sum_{i=r+1}^{n} |\mathcal{O}_i| \equiv |X_G| \pmod{p}$$

since $|\mathcal{O}_i| \Big| |G|$ by the orbit-stabilizer formula. □

Theorem 1.5.2 (Sylow's)**.** Assume that $|G| = p^a m$ with $a \in \mathbb{N}$ and $p \nmid m$. Put $n_p = n_p(G) := \#\,\mathrm{Syl}_p(G)$.

1. $\mathrm{Syl}_p(G) \neq \varnothing$. More precisely, $|H| = p^i$ for some $H \leqslant G$ for each $i \in \{1, \ldots, a\}$, and each subgroup of order p^i $(1 \leqslant i \leqslant a-1)$ is normal in some subgroup of order p^{i+1}.
2. $P, Q \in \mathrm{Syl}_p(G) \Rightarrow \exists g \in G\,[Q = gPg^{-1}]$.
3. $n_p \equiv 1 \pmod{p}$ and $n_p \mid m$. More precisely, $n_p = [G : N_G(P)]$ for each $P \in \mathrm{Syl}_P(G)$.

Proof.

1. By Cauchy's theorem, G has a subgroup of order p. Assume inductively that there's $H_i \leqslant G$ such that $|H_i| = p^i$. Consider H_i-action on $X := \{\text{all left cosets of } H_i \text{ in } G\}$ by left multiplication. By Lemma 1.5.1, $|X_{H_i}| \equiv |X| \pmod{p}$. Note that

$$\begin{aligned} gH_i \in X_{H_i} &\Leftrightarrow hgH_i = gH_i \ \forall h \in H_i \\ &\Leftrightarrow g^{-1}hg \in H_i \ \forall h \in H_i \Leftrightarrow g \in N_G(H_i) \end{aligned}$$

Thus, $|X_{H_i}| = [N_G(H_i) : H_i]$. Also, $|X| = |G|/|H_i| = mp^{a-i} \mid p$, so $[N_G(H_i) : H_i] \equiv 0 \pmod{p}$. Hence there's a subgroup $\overline{H_{i+1}}$ of order p in $N_G(H_i)/H_i$ by Cauchy's theorem. Let $H_{i+1} := \pi^{-1}(\overline{H_{i+1}})$, where $\pi : N_G(H_i) \to N_G(H_i)/H_i$ is the natural projection. Then $|H_{i+1}| = p^{i+1}$ and $H_i \trianglelefteq H_{i+1}$.

2. Let $P, Q \in \mathrm{Syl}_p(G)$. Consider Q-action on $X := \{\text{all left cosets of } P \text{ in } G\}$ by left multiplication. By Lemma 1.5.1, $|X_Q| \equiv |X| \pmod{p}$. Note that

$$\begin{aligned} gP \in X_Q &\Leftrightarrow hgP = gP \ \forall h \in Q \\ &\Leftrightarrow g^{-1}hg \in P \ \forall h \in Q \\ &\Leftrightarrow g^{-1}Qg = P \Leftrightarrow gPg^{-1} = Q \end{aligned}$$

Since $|X_Q| \equiv |X| \pmod{p}$, there exists $g \in G$ such that $gPg^{-1} = Q$.

3. By 2. and Proposition 1.4.27, $n_p = \#\,\mathrm{Syl}_p(G) = [G : N_G(P)]$ for all $P \in \mathrm{Syl}_p(G)$. Since $P \leqslant N_G(P) \leqslant G$, $n_p \mid [G : P] = m$. Let $P \in \mathrm{Syl}_p(G)$ and consider P-action on $X = \mathrm{Syl}_p(G)$ by conjugation. By Lemma 1.5.1, $n_p = |x| \equiv |X_P| \pmod{p}$. Note that

$$Q \in X_P \Leftrightarrow gQg^{-1} = Q \ \forall g \in P \Leftrightarrow P \leqslant N_G(Q)$$

By 2., since $Q \trianglelefteq N_G(Q)$, Q is the unique Sylow p-group in $N_G(Q)$, and thus $P = Q$, implying that $n_p = |X| = |\{P\}| = 1$.

□

Corollary 1.5.2.1. Assume that $|G| = p^a m$ with $a \in \mathbb{N}$ and $p \nmid m$. Put $n_p = n_p(G) := \#\,\mathrm{Syl}_p(G)$. TFAE:

1. $n_p = 1$
2. All Sylow p-subgroups of G are normal in G.
3. All Sylow p-subgroups of G are characteristic.
4. All subgroups generated by elements of p-power order are p-groups.

Proof. $1 \Leftrightarrow 2, 3$ follows from the second part of Sylow's theorem. That $1 \Rightarrow 4$ is clear. For the reverse implication, let

$$X = \bigcup_{P \in \mathrm{Syl}_p(G)} P$$

which is a p-group by our assumption. Hence $P \leqslant \langle X \rangle$ for each $P \in \mathrm{Syl}_p(G)$, and thus $P = \langle X \rangle$. □

Corollary 1.5.2.2. For $P \in \mathrm{Syl}_p(G)$, we have $N_G(N_G(P)) = N_G(P)$.

Proof. That $N_G(N_G(P)) \supseteq N_G(P)$ is clear. For the reverse inclusion, note that $P \trianglelefteq N_G(P)$, and thus it's characteristic by the preceding corollary. Since, $N_G(P) \trianglelefteq N_G(N_G(P))$, by Proposition 1.4.33, we obtain $P \trianglelefteq N_G(N_G(P))$, implying $N_G(N_G(P)) \subseteq N_G(P)$. □

Proposition 1.5.3. Let $H \leqslant G$ and $P \in \mathrm{Syl}_p(G)$. Then $H \cap gPg^{-1} \in \mathrm{Syl}_p(H)$ for some $g \in G$.

Proof. Consider the H-action on X, the set of all left cosets of P in G, by left multiplication. The H-stabilizer of the points of X are of the form $H \cap gPg^{-1}$, with $g \in G$. Since $P \in \mathrm{Syl}_p(H)$, $p \nmid |X|$, and thus at least one orbit Hx whose order is not divisible by p. Then H_x is a p-group of the form $H \cap gPg^{-1}$ for some g. That $[H : H_x]$ is coprime to p indicates that $H_x \in \mathrm{Syl}_p(H)$. □

Corollary 1.5.3.1. Let $H \leqslant G$ and $P \in \mathrm{Syl}_p(H)$. Then $P = S \cap H$ for some $S \in \mathrm{Syl}_p(G)$.

Proposition 1.5.4 (Frattini argument)**.** Let $H \trianglelefteq G$. If $Q \in \mathrm{Syl}_p(H)$, then $HN_G(Q) = G$.

Proof. Let $g \in G$. Then $gQg^{-1} \subseteq gHg^{-1} = H$. Since $gQg^{-1} \in \mathrm{Syl}_p(H)$, $gQg^{-1} = hQh^{-1}$ for some $h \in H$, i.e, $h^{-1}g \in N_G(Q)$, i.e, $g \in HN_G(Q)$. □

Example 1.5.5. In S_3, $(1\,2), (1\,3), (2\,3)$ are elements of order 2 but the subgroup generated by them is not a 2-group.

1.5.1 Applications

Lemma 1.5.6. If $N, K \trianglelefteq G$ with $N \cap K = 1$, then $N \subseteq C_G(K)$.

Example 1.5.7. $|G| = pq$, where $p < q$ are distinct primes. We have $n_q = 1$, i.e, the Sylow q-subgroup Q is normal. Then

$$n_p = \begin{cases} 1 & \text{if } q \not\equiv 1 \pmod{p} \\ 1 \vee q & \text{if } q \equiv 1 \pmod{p} \end{cases}$$

- ($n_p = 1$) Then the Sylow p-subgroup P is normal in G. Since $P \cap Q = 1$, P and Q commute. Hence $G \cong C_p \times C_q \cong C_{pq}$.
- ($n_p = q$) Say $P = \langle x \rangle$ and $Q = \langle y \rangle$. Since $Q \trianglelefteq G$, $xyx^{-1} = y^j$ for some $j \in \mathbb{N}$. Note that

  $$y = x^p y x^{-p} = x^{p-1}(xyx^{-1})x^{-(p-1)} = x^{p-1}y^j x^{-(p-1)} = \cdots = y^{j^p}$$

  and thus $j^p \equiv 1 \pmod{q}$. Recall that $(\mathbb{Z}/q\mathbb{Z})^\times \cong C_{q-1}$, i.e, $(\mathbb{Z}/q\mathbb{Z})^\times = \langle a \Rightarrow$ for some $a \in \mathbb{Z}$. Write $j \equiv a^k \pmod{q}$ for some k. Then k satisfies

  $$a^{kp} \equiv 1 \pmod{q} \Rightarrow (q-1) \mid kp \Rightarrow \frac{q-1}{p} \,\Big|\, k$$

1° If $k = 0$, then $j = 1$, i.e, $xyx^{-1} = y$, implying that $G \cong C_p \times C_q \cong C_{pq}$.

2° If $l = \dfrac{q-1}{p}, 2\dfrac{q-1}{p}, \ldots, (p-1)\dfrac{q-1}{p}$, then G is nonabelian; however, all choices yield isomorphic groups.

Example 1.5.8. $|G| = 45 = 3^2 \times 5$. Then $n_3 = n_5 = 1$. Put $P_i \in \mathrm{Syl}_i(G)\,(i = 3, 5)$. Then $P_3, P_5 \trianglelefteq G$, so P_3 and P_5 commute. Thus

$$G \cong \begin{cases} C_9 \times C_5 \\ C_3 \times C_3 \times C_5 \cong C_3 \times C_{15} \end{cases}$$

- Alternative approach: since $P_3 \trianglelefteq G$, the P_5-action on P_3 by conjugation is well-defined, and it induces a group homomorphism $P_5 \xrightarrow{\Phi} \mathrm{Aut}\, P_3$. Since $|\mathrm{Aut}\, C_9| = |(\mathbb{Z}/9\mathbb{Z})^\times| = 6$, $|\mathrm{Aut}(C_3^2)| = (9-1)(9-3) = 48$ and $(5, 6) = 1 = (5, 48)$, $P_5/\ker\Phi = 1$, i.e, $\ker\Phi = P_5$. Hence $xgx^{-1} = g$ for each $x \in P_5, y \in P_3$, i.e, P_5 and P_3 commute.

Lemma 1.5.9. If $G \leqslant S_n$ is transitive, then $n \mid |G|$.

Example 1.5.10. $|G| = 12$ with $n_3 = 4 \Rightarrow G \cong A_4$. Consider G-action on $\mathrm{Syl}_3(G)$ by conjugation, which induces a homomorphism $G \xrightarrow{\Phi} S_4$. Then $G/\ker\Phi \cong T \leqslant S_4$. By Sylow's theorem, T is a transitive subgroup of S_4. Thus $|T| = 4 \vee 12$. 4 is not possible since this implies $\ker\Phi$ is a normal subgroup of order 3, a contradiction to the assumption $n_3 = 4$. Hence $G \cong$ a subgroup of order 12 in $S_4 \cong A_4$.

Definition. If G is abelian ($\Rightarrow$ every subgroup is normal), then for each $p \mid |G|$, there's a unique Sylow p-subgroup, called the **p-primary subgroup**.

Example 1.5.11. $|G| = 30$. Then $n_3 = 1 \vee 10$ and $n_5 = 1 \vee 6$. Note that $n_3 = 10$ and $n_5 = 6$ cannot happen at the same time since

$$\begin{cases} n_3 = 10 & \Rightarrow \exists\, 20 \text{ elements of order } 3 \\ n_5 = 6 & \Rightarrow \exists\, 24 \text{ elements of order } 5 \end{cases}$$

but $20 + 24 > 30$, a contradiction. Put $P_i \in \mathrm{Syl}_i(G)\,(i = 3, 5)$. Then we have

$$\text{either } P_3 \trianglelefteq G \text{ or } P_5 \trianglelefteq G$$

so $P_3P_5 \leqslant G$ has order 15. Since $[G : P_3P_5] = 2$, P_3P_5 is normal, and since it's cyclic, each subgroup of P_3P_5 is cyclic; in particular, $P_5, P_3 \trianglelefteq G$, i.e, $n_3 = n_5 = 1$. Put $P_3P_5 = \langle y\rangle$ and $P_2 = \langle x\rangle$. Then $xyx^{-1} = y^j$ for some j. Thus $j^2 \equiv 1 \pmod{15}$, as in Example 1.5.7. Hence $j \equiv 1, 4, 11, 14 \pmod{15}$. The four groups

$$G_j = \langle x, y \mid x^2 = y^{15} = 1, xyx^{-1} = y^j\rangle\,(j = 1, 4, 11, 15)$$

give 4 non-isomorphic groups of order 30. In fact, $G_1 \cong C_{30}$, $G_4 \cong D_6 \times C_5$, $G_{11} \cong D_{10} \times C_3$ and $G_{14} \cong D_{30}$.

Example 1.5.12. $|G| = 60$ with $n_5 = 6 \Rightarrow G$ is simple.

Proof. Suppose otherwise there's a normal subgroup H with $1 \neq H \neq G$. If $5 \mid |H|$, then H contains a Sylow 5-subgroup of G and since H is normal, H contains all of them. Hence $|H| \geqslant 1 + 4 \cdot 6 = 25$, and thus $|H| = 30$. Since a group of order 30 contains a normal 5-subgroup, H has a normal 5-subgroup, then so does G, which leads to a contradiction since $n_5 = 6$. Hence $|H|$ is not a multiple of 5. Then $|H| = 2, 3, 4, 6, 12$. If $|H| = 6, 12$, then H has a normal, and hence characteristic, Sylow subgroup, which is therefore normal in G. We then assume WLOG that $|H| = 2, 3, 4$. Put $G' = G/H$, then $|G'| = 30, 20, 15$. In each case G' contains a normal 5-subgroup, and hence G has a normal subgroup of order $10, 15, 20$, a contradiction since a nontrivial proper normal subgroup of G cannot be of order of a multiple of 5. Hence, G is simple. □

Remark 1.5.13. In fact, one can show any simple group of order 60 is isomorphic to A_5.

Lemma 1.5.14. Q_8 cannot be embedded into any symmetric group S_n with $n \leqslant 7$. (HW. 3)

Example 1.5.15. $G = S_4$. We have $4! = 2^3 \times 3$. Then

$$n_3 = \frac{4 \times 3 \times 2}{3} \times \frac{1}{2} = 4$$

Note that the Sylow 2-subgroups of S_4 are isomorphic to D_8. (One may verify this by considering actions on $\{1, 2, 3, 4\}$ of all possible groups of order 8.) Also, a Sylow 2-subgroup of S_4 depends only on the choice of 4-cycles contained in it. Thus

$$n_2 = \frac{4 \times 3 \times 2 \times 1}{4} \times \frac{1}{2}$$

Example 1.5.16. $G = S_5$. We have $5! = 2^3 \times 3 \times 5$. Likewise,

$$\begin{aligned} n_5 &= \frac{5 \times 4 \times 3 \times 2 \times 1}{5} \times \frac{1}{4} = 6 \\ n_3 &= \frac{5 \times 4 \times 3}{2} \times \frac{1}{2} = 10 \\ n_2 &= \frac{5 \times 4 \times 3 \times 2 \times 1}{4} \times \frac{1}{2} = 15 \end{aligned}$$

These imply $\#N_G(P_5) = \dfrac{120}{6} = 20$ and $\#N_G(P_3) = \dfrac{120}{10} = 12$. Concretely, we have, for instance, $N_G(P_3) = \langle (1\,2\,3), (4\,5), (2\,3) \rangle$

Exercise. 1. Find n_2, n_3, n_5 for S_6.

2. Find n_3 for S_9. (Note that a Sylow 3-subgroup is $\langle (1\,2\,3), (4\,5\,6), (7\,8\,9), \underbrace{(1\,4\,7)(2\,5\,8)(3\,6\,9)}_{\text{which normalizes } \langle (1\,2\,3), (4\,5\,6), (7\,8\,9) \rangle} \rangle$.)

1.6 Semi-direct Product

1.6.1 Fundamental Theorem of Finitely Generated Abelian Groups

Definition. A group G is **finitely generated** if $G = \langle A \rangle$ for some finite subset A of G.

Theorem 1.6.1. If G is a finitely generated abelian group, then

$$G \cong \mathbb{Z}^n \times C_{n_1} \times \cdots \times C_{n_t}$$

where $r \in \mathbb{Z}_{\geqslant 0}$ and $n_1, \ldots, n_t \in \mathbb{Z}_{geq0}$ such that $n_{i+1} \mid n_i$ for $i = 1, \ldots, t-1$. Moreover, they're uniquely determined.

- r is called the **(free) rank**, or **Betti number**, of G, and the n_i are called the **invariant factors** of G. Such a decomposition is called the **invariant factor decomposition** of G.

Theorem 1.6.2. If G is a finite abelian group of order $n = p_1^{e_1} \cdots p_k^{e_k}$, where the p_i are primes, then

$$G \cong A_1 \times \cdots \times A_k$$

where $A_i \cong C_{p_i^{f_1}} \times \cdots \times C_{p_i^{f_{t_i}}}$, $f_1 \geqslant \cdots \geqslant f_{t_1} \geqslant 1$ and $f_1 + \cdots + f_{t_i} = e_i$ for each i.

- The $p_i^{f_j}$ are called the **elementary divisors** of G, and such a decomposition is called the **elementary decomposition** of G. This decomposition is unique.

Example 1.6.3. Groups G of order 20. Then by Sylow's theorem, $n_5 = 1$. Let $P = \langle x \rangle \in \mathrm{Syl}_5(G)$ and let $Q \in \mathrm{Syl}_2(G)$.

1. $Q \cong V_4 = \langle y, z \rangle$: Since $P \trianglelefteq G$, $yxy^{-1} = x^i$ and $zxz^{-1} = x^j$ for some $i, j = 1, 4$.
   - $i = j = 1$: y, z commute with x, so $G \cong C_{10} \times C_2$.
   - $i = j = 4$: set $y' = yz$. Then $y'xy'^{-1}x$, thus $G \cong D_{20}$.
   - $i = 1, j = 4$: y commutes with x, so $\langle xy \rangle \cong C_{10}$ and $z(xy)z^{-1} = (xy)^{-1}$, thus $G \cong D_{20}$
   - $i = 4, j = 1$: the same as above.
2. $Q \cong C_4 = \langle y \rangle$: then $yxy^{-1} = x^j$ for some $j = 1, 2, 3, 4$.
   - $j = 1$: $G \cong C_{20}$.
   - $j = 4$: $G \cong \langle x, y \mid x^5 = y^4 = 1,\ yxy^{-1} = x^4 \rangle \cong C_5 \rtimes C_4$

- $j = 2, 3$ give the same structure, denoted as F_{20} and called the **Frobenius group** of order 20, which can be realized as the normalizer of $P = \langle (1\,2\,3\,4\,5) \rangle$ in S_5.

  Since $\#\operatorname{Syl}_5(S_5) = \frac{5!}{5} \cdot \frac{1}{4} = 6 = [S_5 : N_G(P)]$, we have $\#N_G(P) = 20$. Pick $y = (2\,3\,5\,4)$. One can see $y(1\,2\,3\,4\,5)y^{-1} = (1\,3\,5\,2\,4)$. Hence

$$N_G(P) = \langle (1\,2\,3\,4\,5), (2\,3\,5\,4) \rangle$$

1.6.2 Direct products

Theorem 1.6.4. If $H, K \trianglelefteq G$ and $H \cap K = 1$, then $HK \cong H \times K$.

Definition. Under the assumption of the theorem above, we say $G = HK$ is the **internal product** of H and K.

Example 1.6.5. Groups of order 30. As shown in Example 1.5.11, G admits a cyclic subgroup $\langle x \rangle$ of order 15. Let $\langle y \rangle \in \operatorname{Syl}_2(G)$. We have $yxy^{-1} = x^j$, $j = 1, 4, 11, 14$.

- $j = 1$: $G \cong C_{30}$.
- $j = 14$: $G \cong D_{30}$.
- $j = 4$: $yxy^{-1} = x^4$, then $yx^5y^{-1} = x^{20} = x^5$, thus $K := \langle x^5 \rangle \leqslant Z_G$. Also, we have $yx^3y^{-1} = x^{-3}$, so $H := \langle x^3, y \rangle \cong D_{10}$. One can check $H, K \trianglelefteq G$ and $H \cap K$, and hence $G = HK \cong H \times K = D_{10} \times C_3$.
- $j = 11$: similar as the case above, we have $G \cong D_6 \times C_5$.

Example 1.6.6. $D_{4n} = \langle r, s \rangle$ with n odd. Then $D_{4n} \cong D_{2n} \times C_2$, here $C_2 = \langle r^2 \rangle \leqslant Z_G$ and $D_{2n} = \langle r^2, s \rangle$.

Definition. Let G be a group. The **exponent** of G is the smallest positive integer m such that $g^m = 1$ for all $g \in G$. If no such integer exists, the exponent is ∞.

Proposition 1.6.7. Let G be an abelian group of exponent mn, where m, n are relatively prime. Then G is a direct sum of a subgroup of exponent m and a subgroup of exponent n. Moreover, such decomposition is unique.

Proof. Let $G^m := \{g^m \mid g \in G\}$ and $G^n := \{g^n \mid g \in G\}$. Since m, n are relatively prime, the Bézout identity indicates that $1 = am + bn$ for some integers m, n. Then $g = g^{am}g^{bn}$ for all $g \in G$; this shows $G = G^mG^n$. Since $(m, n) = 1$, $G^m \cap G^n = 1$, and since G is abelian, they're normal in G; hence $G = G^m \times G^n$. The uniqueness is guaranteed by the fact $(m, n) = 1$. □

1.6.3 Semi-direct products

Let G be a group, and set $H \trianglelefteq G$, $K \leqslant G$ with $H \cap K = 1$. We wish to define a group structure on the set

$$S = \{(h, k) \mid h \in H, k \in K\}$$

such that $HK \cong S$ under this group structure.

Observe that if $h_1, h_2 \in H$, $k_1, k_2 \in K$,

$$h_1k_1h_2k_2 = h_1(k_1h_2k_1^{-1})k_1k_2$$

Thus if $\phi : HK \to S$ is a homomorphism that $\phi(hk) = (h, k)$, then

$$(h_1, k_1)(h_2, k_2) = \phi(h_1k_1h_2k_2) = \phi(h_1(k_1h_2k_1^{-1})k_1k_2) = (h_1(k_1h_2k_1^{-1}), k_1k_2)$$

This suggests us to define the group structure on S to be

$$(h_1, k_1)(h_2, k_2) := (h_1(k_1h_2k_1^{-1}), k_1k_2)$$

which is called a **semi-direct product** of H and K. Note that $\phi : K \ni k \mapsto \eta_k \in \mathrm{Aut}(H)$ is a group homomorphism, where $\eta_k : H \ni h \mapsto khk^{-1} \in H$.

In general, if we are given two groups H, K, and a homomorphism $\phi : K \to \mathrm{Aut}(H)$, we may define a group structure on $\{(h, k) \mid h \in H, k \in K\}$, denoted as $H \rtimes_\phi K$, by

$$(h_1, k_1)(h_2, k_2) := (h_1\phi(k_1)(h_2), k_1k_2)$$

which is called the semi-direct product of H and K with respect to ϕ.

Theorem 1.6.8. $H \rtimes_\phi K$ is a group. Identifying H with $\{(h, 1) \mid h \in H\}$ and K with $\{(1, k) \mid k \in K\}$, we have $H \trianglelefteq H \rtimes_\phi K$, $K \leqslant H \rtimes_\phi K$, $H \cap K = 1$ and $HK = H \rtimes_\phi K$.

Remark 1.6.9. If $\phi : K \to \mathrm{Aut}(H)$ is trivial, then $H \rtimes_\phi K$ is simply the direct product $H \times K$.

Example 1.6.10.

1. $D_{2n} = \langle r, s\rangle$. $H = \langle r\rangle \trianglelefteq D_{2n}$, $K = \langle s\rangle$. Then $D_{2n} = H \rtimes_\phi K \cong H \rtimes_\phi C_2$, where $\phi(s) : h \mapsto shs^{-1} = h^{-1}$.

2. In general, if H is abelian and $K = \langle y\rangle$ is a cyclic group of order 2, define $\phi : K \to \mathrm{Aut}(H)$ by $\phi(y) : x \mapsto x^{-1}$; this gives $H \rtimes_\phi C_2$.

   In the case $H = \mathbb{Z}$, $Z \rtimes_\phi C_2$ is called the **infinite dihedral group**, denoted as D_∞.

3. More generally, if H is abelian, $K = C_{2n} = \langle y\rangle$ and $\phi : K \to \mathrm{Aut}(H)$ as above. Then we obtain $H \rtimes_\phi C_{2n}$.

4. $A_4 \cong (C_2 \times C_2) \rtimes C_3$.

Example 1.6.11. Groups of order p^3 for p odd primes.

Fact. If $|G| = p^3$ and G is nonabelian, then $Z(G) = [G, G] \cong C_p := \langle x \rangle$.

Lemma 1.6.12. The map $G \ni x \mapsto x^p$ is a homomorphism.

We have 2 cases:

1. All elements have order p. Let $y \notin \langle x \rangle$. Then $H := \langle x, y \rangle \cong C_p \times C_p$ and since $[G : H] = p$, $H \trianglelefteq G$. Let $z \notin H$. Since $x \in Z(G)$, $zxz^{-1} = x$; let $zyz^{-1} = x^a y^b$. Since $zyz^{-1}y^{-1} \in [G, G] = \langle x \rangle$, we have $b = 1$, i.e, $zyz^{-1} = x^a y$. a can be any integer between 1 and -1. But one can show each choice yields the same group structure. Hence

$$G = \langle x, y, z \mid x^p = y^p = z^p = 1,\ xy = yx,\ xz = zx,\ zy = xyz \rangle$$

2. G has an element y of order p^2. Then we have $y^p \in Z(G) \Rightarrow y^p = x^j$ for some $j = 1, \ldots, p-1$.

   Claim. $G \backslash \langle y \rangle$ has an element of order p.
   Let $z \in G \backslash \langle y \rangle$; again, $z^p = x^i$ for some $i = 1, \ldots, p-1$. Since $g \mapsto g^p$ is a homomorphism, we have $z' = y^i z^{-j}$ has order p, and it's not in $\langle y \rangle$.

   Thus $G = \langle y \rangle \rtimes \langle z' \rangle$, here $z' y z'^{-1} = y^k$ for some k such that $y^{k^p} = y$, i.e, $k^p \equiv 1 \pmod{p}^2$. Hence $k = 1 + k'p$ for some $p \nmid k'$. We may check each choice of k' gives the isomorphic group, hence

$$G = \langle y, z' \mid y^{p^2} = z^p = 1,\ zyz^{-1} = y^{1+p} \rangle$$

Example 1.6.13. Nonabelian groups G of order 8. As the fact above, $Z(G) = [G, G] := \langle x \rangle$ is cyclic of order p. Now assume $p = 2$.

1. $\exists\, y \notin \{1, x\}$ such that $y^2 = 1$: Then $H := \langle y$ is not normal in G. Consider the G-action on G/H by left translation. Then its kernel is $\bigcap_{g \in G} gHg^{-1} = 1$ since H is not normal and has order 2. Thus $G \cong T \leqslant S_{[G:H]} = S_4$, and hence $G \cong D_8$.

2. G does not have another element of order 2. Then $G \cong Q_8$. $(G/Z(G) \cong V_4)$

1.7 Special Genres of Groups

1.7.1 p-groups

Theorem 1.7.1. Let P be a group of order p^a. Then

1. $Z(P)$ is nontrivial.
2. $1 \neq H \trianglelefteq P \Rightarrow H \cap Z(P) \neq 1$
3. If $H \trianglelefteq P$, then for any p^b dividing $|H|$, there's a normal subgroup of P of order p^b in H. In particular, P has a normal subgroup of order p^b $(b = 1, \ldots, a)$
4. $H \lneq P \Rightarrow H \lneq N_G(H)$
5. Every maximal subgroup of P is of index p and is normal in P.

1.7.2 Nilpotent groups

Definition. Let G be a group. A **central series** for G is a sequence of (normal) subgroups $1 = H_0 \leqslant H_1 \leqslant \cdots \leqslant H_n = G$ such that $[G, H_i] \leqslant H_{i-1}$.

Remark 1.7.2. Note that $H \trianglelefteq G \Leftrightarrow [G, H] \leqslant H$. Thus $[G, H_i] \leqslant H_{i-1} \Rightarrow H_i \trianglelefteq G$. Also,

$$\begin{aligned} [G, H_i] \leqslant H_{i-1} &\Leftrightarrow 1 = [G/H_{i-1}, H_i/H_{i-1}] \leqslant G/H_{i-1} \\ &\Leftrightarrow H_i/H_{i-1} \leqslant Z(G/H_{i-1}) \end{aligned}$$

which is why such a sequence is called a *central* series.

There are 2 ways to construct central series for G, if such a sequence of subgroups exists:

- From the bottom: If $1 = H_0 \leqslant H_1 \leqslant \cdots \leqslant H_n = G$ is a central series, then $H_1 \leqslant Z(G)$. That is, the largest possible H_1 is $Z(G)$. Put $Z_0(G) = 1$ and $Z_1(G) = Z(G)$. Likewise, the largest possible choice for H_2/H_1 is $Z(G/H_1)$; thus, we choose $Z_2(G)$ be to the subgroup such that $Z_2(G)/Z_1(G) = Z(G/Z_1(G))$. Continuing in this way, we may define $Z_i(G)$ to be the subgroup such that $Z_i(G)/Z_{i-1}(G) = Z(G/Z_{i-1}(G))$.

Definition. The sequence of subgroups $1 = Z_0(G) \leqslant Z_1(G) \leqslant Z_2(G) \leqslant \cdots$ is called the **upper central series**, or **ascending central series** for G.

- From the top: The smallest normal subgroup N such that G/N is abelian is $[G,G]$. Let $G^0 = G$ and $G^1 = [G,G]$. Next, if N is a normal subgroup contained in G^1 and $G^1/N \leqslant Z(G/N)$, then we have for all $g \in G, h \in G^1$

$$ghN = hgN \Leftrightarrow g^{-1}h^{-1}gh \in N$$

so the smallest such N is $[G,G^1]$. Let $G^2 = [G,G^1]$. Continuing in this way, define $G^{i+1} = [G,G^i]$.

Definition. The sequence of the normal subgroups $G = G^0 \trianglerighteq G^1 \trianglerighteq G^2 \trianglerighteq \cdots$ is called the **lower central series**, or **descending central series** for G.

Theorem 1.7.3. Let G be a group. TFAE:

1. G has a central series.
2. $Z_n(G) = G$ for some n.
3. $G^m = 1$ for some m.

Moreover, if 2. or 3. holds, then the smallest n with $Z_n(G)$ and the smallest m with $G^m = 1$ coincide.

Definition. If G is a group satisfying one of the 3 statements above, then G is said to be **nilpotent**, and thus smallest n in 2. is called the **nilpotent class** of G.

Remark 1.7.4.
1. Nilpotent implies solvable. The converse may not hold in general. For instance, S_3 is solvable but not nilpotent since $Z(S_3) = 1$.
2. $Z_i(G), G^i$ are all characteristic subgroups of G.

Example 1.7.5.
1. Abelian groups are all nilpotent of class 1.
2. Q_8 and D_8 are nilpotent of class 2. In general, a nonabelian group of order p^3 is nilpotent of class 2.
3. All finite p-groups are nilpotent, since their centers are nontrivial.

Theorem 1.7.6. Let G be a finite group, $p_1, \ldots, p_n$ be all distinct prime divisors of $|G|$ and $P_i \in \mathrm{Syl}_{p_i}(G)\,(i = 1, \ldots, n)$. Then, TFAE:

1. G is nilpotent.
2. If $H \lneq G$, then $H \lneq N_G(H)$.
3. $P_i \trianglelefteq G$ for all i.
4. $G \cong P_1 \times \cdots \times P_n$.

1.7.3 Solvable groups

Definition. Let G be a group. Define $G^0 := G$, $G^{i+1} := [G^i, G^i]$. The sequence $G^0 \trianglerighteq G^1 \trianglerighteq \cdots$ is called the **derived series**, or **commutator series** for G.

Theorem 1.7.7. G is solvable $\Leftrightarrow G^n = 1$ for some $n \geqslant 0$.

Definition. If G is solvable, the smallest nonnegative n for which $G^n = 1$ is called the **solvable length** of G, denoted by $dl(G)$.

Example 1.7.8.

1. S_n is solvable if and only if $n \leqslant 4$.

   Proof. Note that $[S_n, S_n] \leqslant A_n$. By simplicity of A_n for $n \geqslant 5$ and $n = 3$, we see $[S_n, S_n] = A_n$; trivially, $[S_2 : S_2] = A_2 = 1$. For $n = 4$, normal subgroups of S_4 contained in A_4 are

   $$1,\ H = \{1, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} \text{ and } A_4$$

   Since $S_4/H \cong S_3$ is not abelian, thus $[S_4, S_4] = A_4$. (Recall that groups of order 6 are isomorphic to either C_6 or S_3.) The result follows again by the fact that A_n is simple for $n \geqslant 5$. □

2. Let $G = D_{2n} = \langle r, s \mid r^n = s^2 = 1, sr = r^{-1}s \rangle$. Then $[G, G] = \langle r^2 \rangle$.

   Proof. Since $s^{-1}r^{-1}sr = r^2$, $\langle r^2 \rangle \leqslant [G, G]$.

   - (n is odd) Then $\langle r^2 \rangle = \langle r \rangle$, implying that $G/\langle r^2 \rangle$ has order 2, thus $[G, G] \leqslant \langle r^2 \rangle$.
   - (n is even) That $[G : \langle r^2 \rangle] = 4$ implies $G/\langle r^2 \rangle$ has order 4, and thus $[G, G] \leqslant \langle r^2 \rangle$.

   In conclusion, we have $[G, G] = \langle r^2 \rangle$, which is cyclic, and thus G is solvable. □

Remark 1.7.9. In the definition of the solvable groups, the sequence $1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_s = G$ only require that $H_i \trianglelefteq H_{i+1}$, but H_i need not be normal in G. However, in the definition of the derived series, $G^i \trianglelefteq G$ for each i. (Recall that $[G, G]$ char G.)

Theorem 1.7.10 (Burnside's)**.** Groups of order $p^a q^b$, p, q being primes, are solvable.

Theorem 1.7.11 (Feit-Thompson)**.** Groups of odd order are solvable.

Chapter 2

Ring theory

2.1 Concept of Rings

Definition. A **ring** R is a set with two binary operations, $+$ and $\times$, such that

1. $(R, +)$ is an abelian group.
2. $\times$ is associative.
3. $a \times (b + c) = a \times b + a \times c$ and $(b + c) \times a = b \times a + c \times a$ for all $a, b, c \in R$.

We usually omit $\times$ if no ambiguity occurs.

- If $\times$ is commutative, then R is called a **commutative** ring.
- If R has an element, denoted by 1, such that $1 \times a = a = a \times 1$ for all $a \in R$, then R is called a **ring with identity** (or unity).

Let R be a ring with identity.

1. If for all $a \in R$ and $a \neq 0$, there's $b \in R$ such that $ab = ba = 1$, then R is called a **division ring**, and such a b is denoted by a^{-1}, called the **multiplicative inverse** of a.
2. If R is a noncommutative division ring, then R is a **skew field**.
3. If R is a commutative division ring with $0 \neq 1$, then R is a **field**.

Remark. If French, corps means field. But in mathematics, corps means division ring while corps commutatif means field.

Example 2.1.1.

1. Let R be any abelian group and define $\times$ on R by setting $a \times b = 0$ for all $a, b \in R$. Then R becomes a ring, called a trivial ring.
2. $R = \{0\}$ is the only ring such that $1 = 0$.
3. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are commutative rings; $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields.
4. $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring; it's a field $\Leftrightarrow$ n is a prime.
5. Let $\mathbb{H} := \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$, where $\mathbb{H}$ stands for Hamilton. Define $+$ on $\mathbb{H}$ componentwise and $\times$ by expanding directly via distributive law such that
   - $i^2 = j^2 = k^2 = -1$; $(-1)^2 = 1$

- $ij = k = -ji;\ \ jk = i = -kj;\ \ ki = j = -ik$

Then $\mathbb{H}$ is a noncommutative ring, called the **ring of real Hamilton Quaternions**.

Proof. If $\alpha = a + bi + cj + dk$, let $\overline{\alpha} := a - bi - cj - dk$, the **quaternionic conjugate**. Then $\alpha\overline{\alpha} = a^2 + b^2 + c^2 + d^2 \in \mathbb{R}_{\geqslant 0}$ and $\alpha\overline{\alpha} = 0 \Leftrightarrow \alpha = 0$, and hence $\alpha^{-1} = \dfrac{1}{\alpha\overline{\alpha}}\overline{\alpha}$. □

6. $M_n(\mathbb{Z}), M_n(\mathbb{Q}), M_n(\mathbb{R}), M_n(\mathbb{C})$ are rings with identity.
7. $2\mathbb{Z}$ is a commutative ring without identity.
8. $\left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$ is a field, isomorphic to $\mathbb{C}$.
9. The set of real-valued continuous functions defined on $[0, 1]$ is a commutative ring with identity. The set of real-valued continuous functions with compact support defined on $[0, 1]$ is a commutative ring without identity.

Proposition 2.1.2. Let R be a ring and $a, b \in R$.

1. $0a = a0 = 0$.
2. $(-a)b = a(-b) = -(ab)$, where $-a$ denotes the additive inverse of a.
3. $(-a)(-b) = ab$.
4. The multiplicative identity, if exists one, is unique.

Definition. Let R be a ring.

1. A nonzero element $a \in R$ is a **zero divisor** if there's $0 \neq b \in R$ such that $ab = 0$ or $ba = 0$.
2. Let R be a ring with identity $1 \neq 0$. An element $u \in R$ is an **unit** if there's $v \in R$ such that $uv = 1 = vu$. The set of all units in R is denoted by $R^\times$.

Remark 2.1.3.

1. $R^\times$ is automatically a multiplicative group, and is called the group of units of R.
2. A zero divisor is not a unit.
3. The definition of a division ring can be rephrased as a ring with identity such that all nonzero elements are units.

Example 2.1.4.

1. $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{Q})$ is a zero divisor. In fact, a matrix $A \in M_2(\mathbb{Q})$ is a zero divisor $\Leftrightarrow \det A = 0$, and is a unit $\Leftrightarrow \det A \neq 0$.
2. In $\mathbb{Z}/n\mathbb{Z}$, $\bar{a} \neq 0$ is a zero divisor $\Leftrightarrow \gcd(a, n) \neq 1$, and is a unit $\Leftrightarrow \gcd(a, n) = 1$.
3. Let $D \neq 1$ be a square-free integer. $\mathbb{Q}\left(\sqrt{D}\right) := \left\{a + b\sqrt{D} \mid a, b \in \mathbb{Q}\right\}$ is a field, and $\left(a + b\sqrt{D}\right)^{-1} = \dfrac{a - b\sqrt{D}}{a^2 - b^2 D}$.

Definition. A *commutative* ring with identity is said to be an **integral domain** if it possesses no zero divisor.

Proposition 2.1.5 (Cancellation laws)**.** Let R be a ring. If $0 \neq a \in R$ is not a zero divisor, then $ab = ac \Rightarrow b = c$ and $ba = ca \Rightarrow b = c$. In particular, if R is an integral domain, then the cancellation laws holds.

Corollary 2.1.5.1. A finite integral domain is a field.

Remark 2.1.6. If R is a finite ring with identity having no zero divisor, then R is a division ring. Also, a theorem of Wedderburn shows that a finite division ring is commutative, and hence a field.

Definition. A subset S of R is said to be a **subring** if S is an additive subgroup of R that is closed under multiplication. We denote the subring relation by $S \leqslant R$.

Example 2.1.7.

1. $\mathbb{Z} \leqslant \mathbb{Q} \leqslant \mathbb{R} \leqslant \mathbb{C}$.
2. $n\mathbb{Z} \leqslant \mathbb{Z}$.
3. $\mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k \leqslant \mathbb{H}$.
4. $\mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}\dfrac{1 + i + j + k}{2} \leqslant \mathbb{H}$.

Example 2.1.8. [The ring of quadratic integers] Let $D \neq 1$ be a square-free integer. Let

$$\mathcal{O} := \left\{a + b\sqrt{D} \in \mathbb{Q}\left(\sqrt{D}\right) \mid a + b\sqrt{D} \text{ is a root of some monic polynomial in } \mathbb{Z}[x]\right\}.$$

Exercise. $\mathcal{O} = \begin{cases} \mathbb{Z} + \mathbb{Z}\sqrt{D} & \text{if } D \equiv_4 2, 3 \\ \mathbb{Z} + \mathbb{Z}\dfrac{1 + \sqrt{D}}{2} & \text{if } D \equiv_4 1 \end{cases}$

Solution. Let $a+b\sqrt{D} \in \mathcal{O}$. Then $x^2-2ax+(a^2-b^2D) \in \mathbb{Z}[x]$. Let $a=\dfrac{m}{2},\ m \in \mathbb{Z}$. Then

$$a^2-b^2D \in \mathbb{Z} \Leftrightarrow m^2-(2b)^2D \in 4\mathbb{Z}$$

Let $b=\dfrac{n}{2},\ n \in \mathbb{N}$. Then it's equivalent to $m^2-n^2D \in 4\mathbb{Z}$. Assume that $D \equiv 2,3 \bmod 4$. Then m,n must be even since an odd square equal 1 modulo 4. This proves the first case. Now assume $D \equiv 1 \bmod 4$. Then m,n share the same parity and m,n can be even or odd. This proves the second case. □

$\mathcal{O}$ is called the **ring of integers in** $\mathbb{Q}\left(\sqrt{D}\right)$.

- In the case $D=-1$, the ring $\mathcal{O}=\mathbb{Z}[i]$ is called the **ring of Gaussian integers**.
- Define the **norm** function N on $\mathcal{O}$ by $N\left(a+b\sqrt{D}\right)=\left(a+b\sqrt{D}\right)\left(a-b\sqrt{D}\right)=a^2-b^2D$.
  - $N(\alpha\beta)=N(\alpha)N(\beta)$
  - $\alpha \in \mathcal{O}$ is a unit $\Leftrightarrow N(\alpha)=\pm 1$.

    Proof. ($\Leftarrow$) $N\left(a+b\sqrt{D}\right)=\pm 1 \Rightarrow \left(a+b\sqrt{D}\right)^{-1}=\pm\left(a-b\sqrt{D}\right) \in \mathcal{O}$. (check if $D \equiv_4 1$)
    ($\Rightarrow$) If $a+b\sqrt{D}$ is a unit, so is $a-b\sqrt{D}$ (check !), and thus $\left(a+b\sqrt{D}\right)\left(a-b\sqrt{D}\right) \in \mathbb{Z}$ is a unit.
    Hence $N\left(a+b\sqrt{D}\right)=\pm 1$. □
- When $D<0$, $\mathcal{O}^\times$ is finite.
  1. $(D=-2)\ N(a+b\sqrt{-2})=a^2+2b^2=1 \Leftrightarrow b=0, a=\pm 1$.
  2. $(D=-1)\ \mathcal{O}^\times=\{\pm 1,\pm i\}\ (a^2+b^2=1)$.
  3. $(D=-3)\ \mathcal{O}^\times=\{\exp\dfrac{k\pi i}{3} \mid k=0,\ldots,5\}\ (a^2+ab+b^2=1)$.
- When $D>0$, $\mathcal{O}^\times=\{\pm 1\}\times\langle\varepsilon\rangle$ for some $0<\varepsilon \in \mathcal{O}$, called the **fundamental unit**.
  - $D=2 \rightsquigarrow \varepsilon=1+\sqrt{2}$.
  - $D=3 \rightsquigarrow \varepsilon=2+\sqrt{3}$.
  - $D=5 \rightsquigarrow \varepsilon=\dfrac{1+\sqrt{5}}{2}$.
  - $D=6 \rightsquigarrow \varepsilon=5+2\sqrt{6}$.
  - $D=31 \rightsquigarrow \varepsilon=1520+271\sqrt{31}$.
  - $D=46 \rightsquigarrow \varepsilon=24335+3588\sqrt{46}$.
  - $D=65 \rightsquigarrow \varepsilon=8+\sqrt{65}$.
  - $D=67 \rightsquigarrow \varepsilon=48842+5967\sqrt{67}$.

$\diamond$ $D = 94 \rightsquigarrow \varepsilon = 2143295 + 221064\sqrt{94}$.

Remark 2.1.9. The determination of ε is closely related to **Pell's equation** $x^2 - Dy^2 = 1$. It was studied extensively in the 7-th century in India by Brahmagupta, who also studied Pythagorean triples. Finding ε can be done using continued fraction.

2.1.1 Polynomial rings

Let R be a ring and x an *indeterminate*. A **formal** sum

$$p(x) = a_n x^n + \cdots + a_1 x + a_0,\ a_j \in R$$

is called a **polynomial** in X with coefficients in R.

- If $a_n \neq 0$, n is called the **degree** of the polynomial p, denoted by $\deg p$, and a_n is called the **leading coefficient**.
- If $a_n = 1$, p is said to be **monic**.
- If $a_j = 0\ \forall j > 0$, then p is called a **constant polynomial**; if $a_0 \neq 0$, $\deg p = 0$, and if $a_0 = 0$, a **zero polynomial** 0, we define $\deg 0 := -\infty$.
- The set of all polynomials in x with coefficients in R is denoted by $R[x]$.
- Define $+$ and $\times$ on $R[x]$ by

$$\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} b_i x^i := \sum_{i=0}^{n} (a_i + b_i) x^i$$
$$\left(\sum_{i=0}^{n} a_i x^i\right)\left(\sum_{i=0}^{n} b_i x^i\right) := \sum_{k=0}^{2n} \left(\sum_{i=0}^{k} a_i b_{k-i}\right) x^k$$

  Under such $+$ and $\times$, $R[x]$ becomes a ring, called the **polynomial ring**.

Proposition 2.1.10. Let R be a ring.

1. If R is commutative, then so is $R[x]$.
2. If R has an identity, then so does $R[x]$.
3. Assume R is a integral domain and $p, q \in R[x]$. Then
   (a) $\deg pq = \deg p + \deg q$.

(b) $(R[x])^\times = R^\times$.

(c) $R[x]$ is an integral domain.

Example 2.1.11. In the case $R = \mathbb{Z}/4\mathbb{Z}$, $2(2x+2) = 0$ and $(2x+1)^2 = 1$.

2.1.2 Matrix rings

Let R be a ring and $M_n(R)$ the set of all $n \times n$ matrices with entries all from R. Defined $+$ and $\times$ by

$$(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij})$$
$$(a_{ij}) \times (b_{ij}) = (\sum_{k=1}^{n} a_{ik} b_{kj})$$

Then $M_n(R)$ is a ring under such $+$ and $\times$, called the **matrix ring**.

- In general $M_n(R)$ is not commutative, even R is commutative.
- In general $M_n(R)$ has zero divisors.
- A matrix of the form $\begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & a & \cdots & 0 \\ \vdots & & & \vdots \\ 0 & 0 & \cdots & a \end{pmatrix}$ is called a **scalar matrix**.
- If R is commutative, then scalar matrices commute with every element in $M_n(R)$. Moreover, if R has identity, the center of $M_n(R)$ is exactly the set of all scalar matrices. (HW. 13)
- If R has an identity, then $\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & & & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$ is the identity of $M_n(R)$.
- Assume that R has an identity. The group of units of $M_n(R)$ are denoted as $\mathrm{GL}_n(R)$, called the **general linear group** of degree n over R.
- If $S \leqslant R$, then $M_n(S) \leqslant M_n(R)$.
- $\{$upper (lower) triangular matrices$\} \leqslant M_n(R)$.

Remark. If R is commutative, we may define **determinant** as usual. Then $A \in \mathrm{GL}_n(R) \Leftrightarrow \det A \in R^\times$.

2.1.3 Group rings

Let R be a ring and G a group. Let

$$RG := \Big\{ \sum_{g\in G} a_g g \mid a_g = 0 \text{ for all but finitely many } g \in G \Big\}$$

with $+$ and $\times$ defined by

$$\sum_{g\in G} a_g g + \sum_{g\in G} b_g g := \sum_{g\in G} (a_g + b_g) g$$
$$\left(\sum_{g\in G} a_g g\right)\left(\sum_{g\in G} b_g g\right) := \sum_{g\in G}\left(\sum_{hh'=g} a_h b_{h'}\right) g$$

Then RG is a ring under $+$ and $\times$, called a **group ring**.

Remark. Some people also call it a group algebra, especially when R is a field. The notion of group rings appears naturally in the group representation theory.

- If R has an identity, then RG has an identity $1_R 1_G$.
- If R is commutative, then $r1_G$ commutes with every element in RG. More generally, let $\mathcal{C}$ be a conjugacy class of G with finite elements. Then $\sum_{g\in\mathcal{C}} rg$ is in the center of RG. In fact, under some *suitable* condition like, for instance, R is a commutative ring with identity 1 and G is a finite group, every element in the center of the RG is a linear combination of such sums. (HW. 13)
- If R is commutative and G is abelian, then RG is commutative.
- If $|G| > 1$, then RG in general has zero divisors. For instance, if g has order $m \geqslant 2$, then

$$(1_G - g)(1_G g + \cdots + 1_G g^{m-1}) = 1_G - g^m = 0$$

- Be careful with confusion arising from notation. For example, in $\mathbb{Q}Q_8$, the element $1\cdot 1 + 1\cdot(-1) \neq 0$, while in $\mathbb{H}$, $1 \cdot 1 + 1 \cdot (-1) = 0$.

2.2 Ring Homomorphisms and Quotient Rings

Definition. Let R and S be rings.

1. A **ring homomorphism** from R to S is a function $\varphi : R \to S$ such that $\varphi(a+b) = \varphi(a) + \varphi(b)$ and $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in R$.
2. The **kernel** of φ is defined to be the set $\ker \varphi := \{r \in R \mid \varphi(r) = 0\}$.
3. If φ is bijective, then φ is called an **isomorphism**. In such a case, we write $R \cong S$.

Example 2.2.1.

1. $\begin{array}{c} \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \\ x \longmapsto \overline{x} \end{array}$ is a ring homomorphism with kernel $n\mathbb{Z}$.
2. $\begin{array}{c} \mathbb{Z} \longrightarrow n\mathbb{Z} \\ x \longmapsto nx \end{array}$ is not a ring homomorphism unless $n = 0$ or 1.
3. Let R be a commutative ring and $a \in R$. Then $\begin{array}{c} R[x] \longrightarrow R \\ f(x) \longmapsto f(a) \end{array}$ is a ring homomorphism, called an **evaluation homomorphism at** a.

Proposition 2.2.2. Let $\varphi : R \to S$ be a ring homomorphism.

1. $\varphi(R) \leqslant S$.
2. $\ker \varphi \leqslant R$. Moreover, $a \ker \varphi$, $(\ker \varphi)a \subseteq \ker \varphi \ \ \forall a \in R$.

Discussion 2.2.3. Let $I \leqslant R$ be a subring and R/I be the set of all (left) cosets of I in R. We know that

$$(r + I) + (s + I) := (r + s) + I$$

is well-defined on R/I. Then when will

$$(r + I)(s + I) := rs + I$$

be well-defined? We first find its necessary condition. Suppose that it's well-defined. In particular, we must have for all $s \in I$ and $r \in R$

$$rs + I = (r + I)(s + I) = (r + I)(0 + I) = 0 + I$$

implying $rs \in I$ for all $s \in I$ and $r \in R$, i.e, $rI \subseteq I$ for all $r \in R$. Likewise, $Ir \subseteq I$ for all $r \in R$.
We'll show that this turns out to be sufficient as well. Suppose $rI, Ir \subseteq I$ for all $r \in R$. Now if $r_1+I = r_2+I$ and $s_1 + I = s_2 + I$, i.e, $r_1 = r_2 + a$ and $s_1 = s_2 + b$ for some $a, b \in I$, then

$$(r_1 + I)(s_1 + I) = ((r_2 + a) + I)((s_2 + b) + I) = (r_2 + a)(s_2 + b) + I = r_2s_2 + I$$

where the last equality results from the assumption that $rI, Ir \subseteq I$. We conclude our discussion as the following proposition.

Proposition 2.2.4. Let $I \leqslant R$. $(r + I, s + I) \mapsto rs + I$ is well-defined if and only if $rI, Ir \subseteq I$ for all $r \in R$. If at least one of them holds, then R/I is a ring under $+$ and $\times$ defined before.

Definition. Let $I \leqslant R$ be a subring.

1. If $rI \subseteq I$ (resp. $Ir \subseteq I$) for all $r \in R$, then I is called a **left** (resp. **right**) **ideal** of R.
2. If I is both a left ideal and right ideal, then I is called an **ideal** of R. We denote this relation as $I \trianglelefteq R$.
3. If I is an ideal of R, then R/I is called the **quotient ring** of R by I.

Example 2.2.5.

1. $\{0\}, R \trianglelefteq R$.
2. $n\mathbb{Z} \trianglelefteq \mathbb{Z}$.
3. If φ is a ring homomorphism from R, then $\ker \varphi \trianglelefteq R$. Conversely, any ideal is the kernel of some ring homomorphism.
4. In $R = M_2(\mathbb{Q})$, $\left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in \mathbb{Q} \right\}$ is a right ideal but not a left ideal, while $\left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \mid a, b \in \mathbb{Q} \right\}$ is a left ideal but not a right ideal.
5. $R = \mathbb{Q}[x]$. For $a \in \mathbb{Q}$, define $\begin{array}{ccc} \varphi_a : R[x] & \longrightarrow & R \\ f(x) & \longmapsto & f(a) \end{array}$. Then

$$\ker \varphi_a = \{f \in \mathbb{Q}[x] \mid f(a) = 0\} = \{(x - a)g(x) \in \mathbb{Q}[x] \mid g \in \mathbb{Q}[x]\}$$

In general, if R is a commutative ring, then for all $a \in R$, $(a) := \{ra \mid r \in R\}$ is an ideal, called the **principal ideal generated by** a.

6. $R = \mathbb{Q}[x]$. Following the notation above, we have

$$\ker \varphi_{\sqrt{-1}} = \left\{(x^2+1)g(x) \in \mathbb{Q}[x] \mid g \in \mathbb{Q}[x]\right\}.$$

   By the first isomorphism theorem, we have

$$\mathbb{Q}[x]\Big/(x^2+1) \cong \mathbb{Q}[\sqrt{-1}] = \left\{a + b\sqrt{-1} \mid a, b \in \mathbb{Q}\right\}.$$

   Likewise, the kernel of $\varphi_{-\sqrt{-1}}$ is also (x^2+1), and hence again $\mathbb{Q}[x]\Big/(x^2+1) \cong \mathbb{Q}[\sqrt{-1}]$. Combining these two isomorphisms, we obtain an **automorphism** $a + b\sqrt{-1} \mapsto a - b\sqrt{-1}$ of $\mathbb{Q}[\sqrt{-1}]$. This is the starting point of the *Galois theory*.

7. $\mathbb{Q}[x]/(x^2)$ has zero divisors, even though $\mathbb{Q}[x]$ is an integral domain.

8. If $I \trianglelefteq R$ is an ideal, then $M_n(I) \trianglelefteq M_n(R)$. Moreover, $M_n(I)$ is the kernel of the canonical projection $M_n(R) \to M_n(R/I)$. In fact, all ideals of $M_n(R)$ are of this form. (HW. 14)

9. Let R be a ring and G a group. We have the ring homomorphism $\sum r_g g \mapsto \sum r_g$. The kernel of this homomorphism is called the **augmentation ideal**.

Theorem 2.2.6 (Isomorphism theorems)**.** Let R, S be two rings.

1. If $\varphi : R \to S$ is a ring homomorphism, then $R\big/\ker\varphi \cong \operatorname{Im}\phi$.
2. If $A \leqslant R$ and $B \trianglelefteq R$, then $\dfrac{A+B}{B} \cong \dfrac{A}{A \cap B}$.
3. If $I, J \trianglelefteq R$ and $I \leqslant J$, then $\dfrac{R/I}{J/I} \cong \dfrac{R}{J}$.
4. If $I \trianglelefteq J$, then there's a natural bijection between $\{S \leqslant R \mid I \leqslant S\}$ and $\{S \leqslant R/I\}$. Moreover, there's a natural bijection between $\{S \trianglelefteq R \mid I \leqslant S\}$ and $\{S \trianglelefteq R/I\}$ as well.

Definition. Let $I, J \trianglelefteq R$. Define

$$I + J := \{a + b \mid a \in I, b \in J\} \text{ and } IJ := \left\{\sum_{i=1}^{n} a_i b_i \mid a_i \in I, b_j \in J, n \in \mathbb{N}\right\}$$

Remark 2.2.7. The set $\{ab \mid a \in I, b \in J\}$ may not be closed under $+$.

- $I = \{2p(x) + xq(x) \mid p, q \in \mathbb{Z}[x]\}$. We have $4, x^2 \in \{pq \mid p, q \in I\}$ but $4 + x^2 \notin \{pq \mid p, q \in I\}$.
- $R = \mathbb{Z}[\sqrt{-6}]$, $I = (5, 2+\sqrt{-6})$ and $J = (2, \sqrt{-6})$. We have

$$2 + \sqrt{-6} = 5\sqrt{-6} - (2+\sqrt{-6}) \cdot 2 - (2+\sqrt{-6})\sqrt{-6} \in IJ$$

  but $2 + \sqrt{-6}$ fails to be of the form ab, $a \in I,\ b \in J$.

2.2.1 Ideals

Definition. Let $A \subseteq R$.

1. $(A) := \bigcap\{I \trianglelefteq R \mid A \subseteq I\}$ is the **smallest ideal containing** A, also called the **ideal generated by** A. Likewise, the left and right ideals generated by A are similarly defined.
2. An ideal generated by a singleton is called a **principal ideal**.
3. An ideal is said to be **finitely generated** if it's generated by a finite set.

Proposition 2.2.8. Let R be a ring with identity $1 \neq 0$. Then

$$\begin{aligned} \text{the left ideal generated by } A \text{ is} \quad & RA := \left\{ \sum_{i=1}^{n} r_i a_i \mid r_i \in R, a_i \in I, n \in \mathbb{N} \right\} \\ \text{the right ideal generated by } A \text{ is} \quad & RA := \left\{ \sum_{i=1}^{n} a_i s_i \mid s_i \in R, a_i \in I, n \in \mathbb{N} \right\} \\ \text{the ideal generated by } A \text{ is} \quad & RAR := \left\{ \sum_{i=1}^{n} r_i a_i s_i \mid r_i, s_i \in R, a_i \in I, n \in \mathbb{N} \right\} \end{aligned}$$

Remark 2.2.9. Note that the proposition doesn't hold in general if R has no identity. For example, when $R = 2\mathbb{Z}$ and $A = \{2\}$, $(A) = R$ but $RAR = 8\mathbb{Z}$.

- In general, in the case of *commutative* rings, when people speak of the ideal generated by A, they usually refer to RA, rather than the smallest ideal containing A.
- If R is commutative with identity, then the principal ideal generated by $\{a\}$ is $Ra = \{ra \mid r \in R\}$. However, if R is noncommutative, it's $\left\{ \sum_{i=1}^{n} r_i a s_i \mid r_i, s_i \in R, i \in \mathbb{N} \right\}$.

Example 2.2.10.

1. $\{0\} = (0)$ and $R = (1)$ are principal if R has identity $1 \neq 0$.
2. If $R = \mathbb{Z}$, then every ideal is principal since all subgroups of $\mathbb{Z}$ is of the form $n\mathbb{Z}$.
3. If G is a finite group and R is a commutative ring with 1, then the augmentation ideal is generated by the set $\{g - 1 \mid g \in G\}$. This may not be the minimal set of generators; for example, if $G = \langle\sigma\rangle$, then the augmentation ideal is a principal ideal with generator $\sigma - 1$.
4. $R = \mathbb{Z}[\sqrt{-6}]$. $I = (2, \sqrt{-6})$ is not principal.

Proof. Suppose otherwise $I = (a)$. Then $2 = ab, \sqrt{-6} = ac$ for some b, c, and thus

$$4 = N(2) = N(a)N(b),\ 6 = N(\sqrt{-6}) = N(a)N(c)$$

where $N(a + b\sqrt{-6}) = a^2 + 6b^2$ is the norm function. Then $N(a) = 1, 2$ since they're integers.

- $N(a) = 1 \Rightarrow a = \pm 1$, a contradiction since $1 \notin (2, \sqrt{-6})$.
- $N(a) = 2$. No such a exists in $\mathbb{Z}[\sqrt{-6}]$.

□

5. $R = \mathbb{Z}[x]$. $I = (2, x) = \{2p(x) + xq(x) \mid p, q \in \mathbb{Z}[x]\}$ is not principal.

   Proof. If $I = (a)$, then a must be a constant polynomial, a contradiction. □

Remark 2.2.11. In Chapter 9, we'll see that if $\mathbb{F}$ is a field, then every ideal in $\mathbb{F}[x]$ is principal.

Proposition 2.2.12. Let R be a ring with identity and $I \trianglelefteq R$.

1. $I = R \Leftrightarrow I$ contains a unit.
2. Assume that R is commutative. Then R is a field $\Leftrightarrow$ the only ideals of R are $\{0\}$ and R.
3. Assume that R is an integral domain and $a, b \in R$. Then Then $(a) = (b) \Leftrightarrow a = ub$ for some unit u.

Corollary 2.2.12.1. If $\mathbb{F}$ is a field, then any nontrivial ring homomorphism from $\mathbb{F}$ must be injective.

Remark 2.2.13. For noncommutative ring R, we still have that if R is a division ring, then R has only two ideals $\{0\}$ and R. However, the converse may not hold in general. For example, if $\mathbb{F}$ is a field and $n \geqslant 2$, then $M_n(\mathbb{F})$ has only two ideals since an ideal must be of the form $M_n(I),\ I \trianglelefteq \mathbb{F}$ but $M_n(\mathbb{F})$ is not a division ring.

Definition. An ideal I of a ring R is said to be a **maximal ideal** if the only ideal containing I are I and S.

Corollary 2.2.13.1. Let R be a commutative ring with identity and $I \trianglelefteq R$. Then R/I is a field $\Leftrightarrow I$ is a maximal ideal.

Proof. This follows from Proposition 2.2.12 and the fourth isomorphism theorem. □

Remark 2.2.14. If R has no identity, R/I may not be a field for a maximal ideal I. For example, $R = 2\mathbb{Z}$ and $I = 4\mathbb{Z}$ but R/I is a trivial ring, i.e, $ab = 0$ for all $a, b \in R/I$.

Proposition 2.2.15. Let R be a ring with identity. Then every proper ideal I is contained in some maximal ideal.

Proof. The proof is based on the Zorn's lemma. Let $\mathcal{A} := \{\text{all proper ideals of } R \text{ containing } I\}$. If suffices to check if $\mathcal{C}$ is a chain in $\mathcal{A}$, then $\mathcal{C}$ has an upper bound in $\mathcal{A}$. Let $J = \bigcup_{S \in \mathcal{C}} S$. We claim $J \in \mathcal{A}$ and $S \leqslant J$ for all $S \in \mathcal{C}$. The latter is triviality. For the former, $1 \notin J$ since each $S \in \mathcal{C}$ is proper, and that it's an ideal is obvious. □

Remark 2.2.16. If R does not have identity, then R may not have a maximal ideal. For example $R = \mathbb{Q}$ with $\times$ defined by $ab = 0$ for all $a, b \in \mathbb{Q}$. Then $\mathbb{Q}$ has no identity and every additive group is an ideal. However, every proper additive subgroup is contained in another proper subgroup.

Example 2.2.17.

1. $n\mathbb{Z}$ is a maximal ideal $\Leftrightarrow \mathbb{Z}/n\mathbb{Z}$ is a field $\Leftrightarrow n$ is a prime.

2. $(2, x)$ is a maximal ideal of $\mathbb{Z}[x]$ since $\mathbb{Z}\big/(2, x) \cong \mathbb{Z}/2\mathbb{Z}$.
   (x) is not a maximal ideal since $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$ is not a field.

3. Let $\mathbb{F}$ be a field and G a group. Let I denote the augmentation ideal of $\mathbb{F}G$. Then I is maximal since $\mathbb{F}G/I \cong \mathbb{F}$ is a field, where the isomorphism comes from the fact that $I = \ker\left(\sum a_g g \mapsto \sum a_g\right)$ is the kernel of a surjective homomorphism from $\mathbb{F}G$ to $\mathbb{F}$. Notice that in this example G can be even non-abelian, $\mathbb{F}G$ is not commutative and has zero divisors.

Definition. A commutative ring with identity $1 \neq 0$ is called a **local ring** if it has a unique maximal ideal I, and R/I is called the **residue field** of R.

Proposition 2.2.18. Let R be a commutative ring with identity.

1. $I \neq (1)$ is an ideal of R such that every element of $R - I$ is a unit in R if and only if R is a local ring and I is the maximal ideal.

2. If I is a maximal ideal such that every element of $1 + I$ is a unit in R, then R is a local ring.

Proposition 2.2.19. (HW. 15) Let R be a commutative ring with identity. TFAE:

1. R is a local ring

2. $R - R^\times$ is an ideal of R

3. for any $x \in R$, either x or $1 - x$ is a unit

Question 2.2.20. When is R/I an integral domain?

Definition. Let R be a commutative ring. We say $I \trianglelefteq R$ is a **prime ideal** if it's a proper ideal such that $\forall a, b \in R\,[ab \in I \Rightarrow a \in I \vee b \in I]$.

Proposition 2.2.21. Let R be a commutative ring with identity $1 \neq 0$ and $I \trianglelefteq R$. Then R/I is an integral domain $\Leftrightarrow$ I is a prime ideal.

Proof.

$$\begin{aligned}\text{Integral domain} &\Leftrightarrow \forall a, b \in R\,[(a+I)(b+I) = 0 \Rightarrow a + I = 0 \vee b + I = 0] \\ &\Leftrightarrow \forall a, b \in R\,[ab \in I \Rightarrow a \in I \vee b \in I]\end{aligned}$$

□

Example 2.2.22.

1. $R = \mathbb{Z}$. $n\mathbb{Z}$ is a prime ideal $\Leftrightarrow$ $n = 0$ or n is a prime.

2. A **principal ideal domain** is an integral domain in which every ideal is principal. Then in such a ring every non-zero prime ideal is maximal.

   Proof. Let $(x) \neq 0$ be a prime ideal and $(y) \supsetneq (x)$. Then $x \in (y)$, i.e, $x = yz$ for some z. Thus $yz \in (x)$. Since $y \notin (x)$, $z \in (x)$, say $z = tx$. Hence $x = yz = ytx$, implying $yt = 1$, i.e, $(y) = (1)$. □

3. Note that $\{0\} \lneq p\mathbb{Z}$ are both prime ideals. In general, unlike maximal ideals, a prime ideal can by *properly* contained in another prime ideal.For example, $R = \mathbb{Q}[x_1, \ldots, x_n]$. Then

   $$(0) < (x_1) < (x_1, x_2) < \cdots < (x_1, \ldots, x_n)$$

   Each of ideals in the sequence is a prime ideal since $\mathbb{Q}[x_1, \ldots, x_n]/(x_1, \ldots, x_j) \cong \mathbb{Q}[x_{j+1}, \ldots, x_n]$ is an integral domain.

Remark 2.2.23. In general, if R is an integral domain, we define the **Krull dimension** to be the largest number of inclusions in a chain of prime ideals. This gives us a way to define the dimension of an algebraic variety.

Definition. An element x in a ring is **nilpotent** if $x^n = 0$ for some $n \in \mathbb{N}$.

Proposition 2.2.24. Let R be a commutative ring with $1 \neq 0$. The set, denoted by $\sqrt{0}$, of all nilpotent elements in R is an ideal (HW. 13), and $R/\sqrt{0}$ contains no nonzero nilpotent elements.

Definition. The ideal $\sqrt{0}$ is called the **nilradical** of R.

Proposition 2.2.25. The nilradical of a commutative ring R with $1 \neq 0$ in the intersection of all the prime ideals of R.

Proof. Let x be nilpotent and I any prime ideal. Since $x^n = 0 \in I$ for some $n \in \mathbb{N}$, $x \in I$ since I is prime. We next prove the reverse inclusion. Suppose x is not nilpotent. Let Σ denote the set of ideals with the property

$$n \in \mathbb{N} \Rightarrow x^n \notin I$$

Σ is not empty since $0 \in \Sigma$. By the Zorn's lemma to the set Σ, ordered by inclusion, Σ has a maximal element, denoted by J. We will show J is a prime ideal. Let $a, b \notin J$. Then $(a) + J, (b) + J \supsetneq J$ so they're not in Σ. Hence

$$x^n \in (a) + J, \quad x^m \in (b) + J$$

for some $n, m \in \mathbb{N}$, and thus $x^{m+n} \in (ab) + J$. This means $(ab) + J \notin \Sigma$, i.e, $ab \notin J$. Hence J is a prime ideal such that $x \notin J$. □

Definition. Let R be a commutative ring with $1 \neq 0$. The **Jacobson radical** $\mathrm{Jac}(R)$ is the intersection of all maximal ideals of R.

Proposition 2.2.26. Let R be a commutative ring with $1 \neq 0$. $x \in \mathrm{Jac}(R) \Leftrightarrow 1 - xy$ is a unit in R for all $y \in R$.

Proof. ($\Rightarrow$) Suppose $1 - xy$ is not a unit, then it's contained in a maximal ideal, say I. Since $x \in I$, $xy \in I$, and thus $1 \in I$, a contradiction.
($\Leftarrow$) Suppose $x \notin I$ for some maximal ideal I. Then $(x, I) = (1)$, and thus $xy + t = 1$ for some $y \in R$, $t \in I$, implying that $t = 1 - xy \in I$ is not a unit. □

Theorem 2.2.27 (Nakayama's lemma)**.** Let R be a commutative ring with $1 \neq 0$ and M a finitely generated R-module. Put $J = \mathrm{Jac}(R)$. If $M = IM$ for some $I \trianglelefteq J$, then $M = 0$.

Proof. Let $M = \langle a_1, \ldots, a_n \rangle_R$. Since $a_i \in IM$, $a_i = \sum_{j=1}^{n} r_{ij} a_j$ for some $r_{ij} \in I$. Put $A := (r_{ij}) \in M_n(I)$ and $\mathbf{a} := (a_1\, a_2\, \cdot\, a_n)^t$. Then we have $A\mathbf{a} = \mathbf{a}$, i.e, $(A - I)\mathbf{a} = 0$. Put $B = A - I$. Then

$$\det B \cdot I\mathbf{a} = \mathrm{adj}\, B \cdot B\mathbf{a} = 0$$

i.e, $(\det B)a_i = 0$ for each i. Note that $\det B = \chi_A(1) = \pm 1 + r$ for some $r \in I \subseteq J$, so $\det B \in R^\times$ by Proposition 2.2.26. Hence $a_i = 0$ for each i. □

2.2.2 Rings of Fractions

Goal 2.2.28. Let R be a commutative ring. Construct a larger ring $Q \geqslant R$ such that every nonzero non-zero divisor element in R has an inverse of Q ($R = \mathbb{Z}$, $Q = \mathbb{Q}$, for instance).

Observation 2.2.29. Let $S = \{b \in R \mid b \neq 0 \text{ and is not a zero divisor}\}$ and $b \in S$. If Q contains b^{-1}, then it also contains ab^{-1} for all $a \in R$ to be a ring. Thus a natural setting for defining Q is

$$\mathcal{A} := \{(a, b) \in R \times S\}$$

Now bb^{-1} should be the identity of Q as we imagine. Thus we should identify (b, b) with (d, d). More general, if $ab^{-1} = cd^{-1}$, i.e, $ad = bc$, we should identity (a, b) with (c, d). Accordingly, we define $\sim$ on $\mathcal{A}$ by

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc$$

This is an equivalence relation. Let $Q := \mathcal{A} / \sim$ and denote the equivalence class of (a, b) as $\dfrac{a}{b}$. Define $+$ and $\times$ on Q by

$$\frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd}$$
$$\frac{a}{b} \times \frac{c}{d} := \frac{ac}{bd}$$

Then Q is made into a ring and $\begin{array}{ccc} R & \hookrightarrow & Q \\ a & \longmapsto & \dfrac{ae}{e} \end{array}$ is an canonical injective ring homomorphism for each $e \in S$.

Thus R can be regarded as a subring of Q and every nonzero non-zero divisor element $\dfrac{be}{e}$ of R has an inverse $\dfrac{e}{be}$.

Definition. The ring Q constructed is called the **ring of fractions** of R. In the case when R is an integral domain, then Q is a field, called the **field of fractions**.

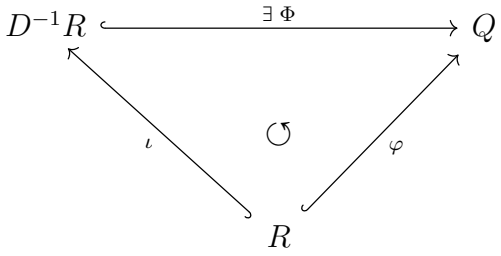
Example 2.2.30. The following are some examples of rings and their rings of fractions.

R	Q
$\mathbb{Z}$	$\mathbb{Q}$
$\mathbb{Z}[\sqrt{D}]$	$\mathbb{Q}[\sqrt{D}]$
$2\mathbb{Z}$	$\mathbb{Q}$
$\mathbb{F}[x]$	$\mathbb{F}(x)$

More generally, we may construct $Q \geqslant R$ such that a particular subset of R has an inverse in Q. Namely, let $D \subseteq R$ such that *a)* it does not contain 0 nor zero divisor of R and *b)* is closed under multiplication. Then we can construct a ring, denoted by $D^{-1}R := (R \times D)/\sim$, in which every element of D has an inverse.

Theorem 2.2.31. $D^{-1}R$ is the *smallest* commutative ring with identity containing R as a subring such that every element in D is a unit, in the sense of the following universal property:

- Let S be any commutative ring with identity and $\varphi : R \to S$ any injective ring homomorphism such that $\varphi(d)$ is a unit in S for all $d \in D$. Then there's an injective ring homomorphism $\Phi : D^{-1}R \to S$ extending φ.



Proof. The injection from R to $D^{-1}R$ is given by

$$\begin{aligned} \iota : R &\longrightarrow D^{-1}R \\ a &\longmapsto \frac{ae}{e} \end{aligned}$$

where e is any element of D. Since $\dfrac{ae}{e} = \dfrac{ad}{d}$ for all $d, e \in D$, ι does not depend on the choice of e.

- ι is a ring homomorphism since D is multiplicative closed.
- ι is injective since D does not contain 0 nor zero divisor.

Via ι, we may view R as a subring of Q. We are ready perfectly to show the universal property. Let $\varphi : R \to S$ be an injective homomorphism such that $\varphi(d)$ is a unit $\in S$ for all $d \in D$. Define $\Phi : D^{-1}R \to Q$ by sending rd^{-1} to $\varphi(r)\varphi(d)^{-1}$ for all $r \in R$, $d \in D$.

- Φ is well-defined and is an extension of φ.
- Φ is a ring homomorphism.
- Φ is injective.

- $\varphi = \Phi \circ \iota$.

□

Definition. Let $\mathbb{F}$ be a field and $A \subseteq \mathbb{F}$. The **subfield generated by** A is the intersection of all subfields of F containing A, i.e, the smallest subfield containing A.

Corollary 2.2.31.1. Let R be an integral domain and Q the field of fractions of R. If a field $\mathbb{F}$ contains a subring R' isomorphic to R, then the subfield generated by R' is isomorphic to Q.

Proof. Let $\varphi : R \cong R' \subseteq \mathbb{F}$ be a ring isomorphism from R to R'. Then φ is an injective homomorphism from R into $\mathbb{F}$. Then by Theorem 2.2.31, there's an injective ring homomorphism $\Phi : Q \to \mathbb{F}$ extending φ. Note that every subfield containing $R' = \varphi(R)$ contains the elements of the form $\varphi(rs^{-1})$ for all $r, s \in R$ and every element of $\Phi(Q) \cong Q$ is of the same form as R'. Hence $\Phi(Q)$ is exactly the subfield of $\mathbb{F}$ generated by R'. □

Example 2.2.32.

1. $R = \mathbb{Z}, D = \{1, 2, 2^2, \ldots\}$. $D^{-1}R = \mathbb{Z}[\frac{1}{2}]$.
2. $R = \mathbb{Z}, D = \{\text{all odd integers}\}$. $D^{-1}R = \left\{\frac{a}{b} \in \mathbb{Q} \mid b \text{ is odd}\right\}$. It has a unique maximal ideal (2).

Example 2.2.33. More generally, if R is an integral domain and P is a prime ideal, then $D := R - P$ has no 0 and zero divisor and is closed under multiplicative. Then $D^{-1}R$ is a local ring with the unique maximal ideal generated by P. This process is called the **localization of** R **at** P.

2.2.3 Chinese Remainder Theorem

Recall the Chinese remainder theorem:

- If $\gcd(m, n) = 1$, the congruence equations

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned}$$

  is solvable in $\mathbb{Z}$ for all $a, b \in \mathbb{Z}$.

Observe that the condition $\gcd(m, n) = 1$ is equivalent to $m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$. Now we give a generalized version.

Theorem 2.2.34 (Chinese remainder theorem)**.** Let R be a commutative ring with identity $1 \neq 0$ and $I_1, I_2, \ldots, I_n$ be ideals in R.

1. The map
$$\phi : R \longrightarrow R/I_1 \times \cdots \times R/I_n$$
$$r \longmapsto (r + I_1, \ldots, r + I_n)$$
is a ring homomorphism with $\ker \phi = \bigcap_{i=1}^{n} I_i$.

2. If $I_i + I_j = R$ for all $i \neq j$, then ϕ is surjective and $\bigcap_{i=1}^{n} I_i = I_1 I_2 \cdots I_n$.

Proof.

1. A straightforward computation.

2. We prove this for $n = 2$. Assume that $I_1 + I_2 = R$. Since $1 \in R$, $1 = x + y$ for some $x \in I_1$, $y \in I_2$. Observe that $\phi(x) = (x+I_1, x+I_2) = (0+I_1, x+I_2) = (0, 1)$ and $\phi(y) = (1, 0)$. Thus for all $r_1, r_2 \in R$, we have $\phi(r_1 y + r_2 x) = (r_1 + I_1, r_2 + I_2)$, demonstrating the surjectivity of ϕ. We next show the second statement. It's clear that $I_1 I_2 \subseteq I_1 \cap I_2$. Let $a \in I_1 \cap I_2$. Then $a = a \cdot 1 = ax + ay \in I_1 I_2$. Hence $I_1 I_2 = I_1 \cap I_2$. The general case follows once $I_1 + I_2 \cdots I_n = R$ is established.

□

Corollary 2.2.34.1. If $n = p_1^{e_1} \cdots p_k^{e_k}$, then
$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{e_k}\mathbb{Z}$$
as rings. In particular,
$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{e_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k^{e_k}\mathbb{Z})^\times$$
as groups.

2.3 Special Domains

2.3.1 Euclidean Domains

Recall the **Euclidean algorithm** for $\mathbb{Z}$: to find $\gcd(a, b)$, $b > 0$, we compute

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ &\vdots \\ r_{n-2} &= q_{n-1} r_{n-1} + r_n \\ r_{n-1} &= q_n r_n + 0 \end{aligned}$$

with $0 < r_n < r_{n-1} < \cdots < r_2 < r_1 < b$ and $q_i \in \mathbb{Z}_{\geqslant 0}$. Then $r_n = \gcd(a, b)$.

Discussion 2.3.1. Why does this work? It's down to three properties:

1. On $\mathbb{Z}$, there's a function, namely the absolute value, taking values in $\mathbb{Z}$ that *measures* the size of an element in $\mathbb{Z}$.
2. (Division algorithm) $\forall a, b_{\neq 0} \in \mathbb{Z}\ \exists\, q, r \in \mathbb{Z}\, [a = qb + r \wedge 0 \leqslant r < b]$.
3. $\mathbb{Z}_{\geqslant 0}$ has a property that any strictly decreasing sequence in $\mathbb{Z}_{\geqslant 0}$ must terminate in a finite stage.

Definition. Let R be integral domain.

1. A function $N : R\backslash\{0\} \to \mathbb{Z}_{\geqslant 0}$ is called a **norm**.
2. R is called an **Euclidean domain** if there is a norm N on R such that for all $a, b_{\neq 0} \in R$, there are $q, r \in R$ with
   - $a = bq + r$
   - $r = 0$ or $N(b) > N(r)$.

Example 2.3.2.
1. $\mathbb{Z}$ with $N(a) = |a|$.
2. $\mathbb{F}[x]$ ($\mathbb{F}$: a field) with $N(f) = \deg f$ (Note that $N(0) := -\infty$).
3. $\mathbb{Z}[\sqrt{-1}]$ with $N(a + b\sqrt{-1}) = a^2 + b^2$.

   Proof. Let $\alpha, \beta_{\neq 0} \in \mathbb{Z}[\sqrt{-1}]$ be given. To find $q, r \in \mathbb{Z}[\sqrt{-1}]$ such that $\alpha = q\beta + r$, we let q be a lattice point closest to $\dfrac{\alpha}{\beta}$ and let $r := \alpha - q\beta$. Then $|q - \dfrac{\alpha}{\beta}|^2 \leqslant \dfrac{1}{2}$, i.e, $|r|^2 = |\alpha - q\beta|^2 \leqslant \dfrac{1}{2}|\beta|^2$. $\square$

4. $\mathbb{Z}[\frac{-1+\sqrt{-11}}{2}]$, $\mathbb{Z}[\frac{-1+\sqrt{-7}}{2}]$, $\mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$, $\mathbb{Z}[\sqrt{-2}]$ are Euclidean domains with N being $|\cdot|^2$. (HW. 16)

5. Any discrete valuation ring R is a Euclidean domain with $N(a) := \nu(a)$.

   Proof. Given $a, b_{\neq 0} \in R$, if $\nu(b) > \nu(a)$, then $a = 0 \cdot b + a$; if $\nu(b) \leqslant \nu(a)$, then take $q = ab^{-1} \in R$, i.e, $a = qb$. □

6. Any field is a Euclidean domain with $N(a) = 0$ for all a.

Proposition 2.3.3. Any ideal in an Euclidean domain R is principal.

Proof. Let N be the norm function associated with R. Let $I \trianglelefteq R$. If $I = (0)$, there's nothing to prove. Suppose $I \neq (0)$. Let $b_{\neq 0} \in I$ such that $N(b) = \min\{N(r) \mid r \in I\}$. For any $a \in I$, we have $a = qb + r$ for some $q, r \in R$ with $r = 0$ or $N(b) > N(r)$. Since $r = a - qb \in I$, it forces that $r = 0$ since b has smallest norm in I. Hence $a = qb$. □

Example 2.3.4.

1. $\mathbb{Z}[x]$ is not an Euclidean domain since $(2, x)$ is not principal.
2. $\mathbb{Z}[\sqrt{-6}]$ is not an Euclidean domain since $(2, \sqrt{-6})$ is not principal.
3. $\mathbb{Z}[\sqrt{-5}]$ is not an Euclidean domain since $(3, 1+\sqrt{-5})$ is not principal.

Definition. Let R be a commutative ring and $a, b \in R$ with $b \neq 0$.

1. If there's a $c \in R$ such that $a = bc$, then we say b **divides** a, or a is a **multiple** of b, and write $b \mid a$.
2. A **G.C.D.** of a, b, if exists, is an element $d \in R$ such that $d \mid a, b$ and $d' \mid d$ for all d' such that $d' \mid a, b$. If it is the case, we write $d = \gcd(a, b)$, or simply $d = (a, b)$.

Remark 2.3.5. Note that a G.C.D. may not exist in general. For example, $R = \mathbb{Z}[\sqrt{-5}]$, $a = 6$ and $b = 3(1+\sqrt{-5})$.

Proof. If $d \mid a, b$, then $N(d) \mid N(a) = 36$ and $N(d) \mid N(b) = 54$ by the multiplicativity of N, and thus $N(d) \mid 18$. On the other hand, $3 \mid a, b$ and $1 + \sqrt{-5} \mid a, b$. If d is a G.C.D. of a, b, $9 = N(3) \mid N(d)$ and $6 = N(1+\sqrt{-5}) \mid N(d)$, and thus $18 \mid N(d)$. Therefore, $N(d) = 18$; however, in $\mathbb{Z}[\sqrt{-5}]$, there's no element of norm 18. □

Remark 2.3.6. Let R be a Euclidean domain. Then $(\gcd(a, b)) = (a, b)$ given that a G.C.D. of a, b exists.

Proof. Note $b \mid a \Leftrightarrow a \in (b) \Leftrightarrow (a) \leqslant (b)$, so a G.C.D d of a, b satisfies $(a), (b) \leqslant (d)$, and thus $(a, b) \leqslant (d)$. Also, if $(a, b) \leqslant (d')$, then $(d) \leqslant (d')$. Hence if d exists, (d) is the smallest principal ideal containing (a, b). Since any ideal in a Euclidean domain is principal, the smallest principal ideal containing (a, b) is simply (a, b) itself, and thus $(d) = (a, b)$. □

This somewhat shows that it'll not cause confusion to denote $\gcd(a, b)$ by (a, b).

Remark 2.3.7. $\gcd(a, b)$, if exists, is unique up to a unit.

Remark 2.3.8. The Euclidean algorithm for $\mathbb{Z}$ is very fast, in the sense that the divisions required to compute (a, b) is $\leqslant 5 \cdot (\#$ of digits of the smaller one between $a, b)$. Precisely, it's less than

$$\min\left\{\frac{\log a}{\log \frac{1+\sqrt{5}}{2}}, \frac{\log b}{\log \frac{1+\sqrt{5}}{2}}\right\} + 1$$

Some books on continued fractions may mention this.

Proposition 2.3.9 (A *criterion* for showing a ring is not a Euclidean domain)**.** Let R be an integral domain and $S \subseteq R \backslash \{0\}$. If R is an Euclidean domain, then there's a $b \in R \backslash S$ such that $\forall\, a \in R \,\exists\, q, r \in R$ with *1)* $a = qb + r$ and *2)* $r = 0$ or $r \in S$.

Proof. Let N be the associated norm. Let $b \in R \backslash S$ such that $b \neq 0$ and $N(b) = \min\{N(a) \mid a \in R \backslash (S \cup \{0\})\}$. Since R is an Euclidean domain, $a = qb + r$ with $r = 0$ or $N(b) > N(r)$, which implies $r \in S$. □

Example 2.3.10. $R = \mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ is not a Euclidean domain (in fact R is PID).

Proof. Suppose otherwise R is a Euclidean domain. Choose $S = \{\pm 1\}$ and let b be an element satisfying the property in Proposition 2.3.9. Consider $a = 2$. Then $b \mid 2 - r$ for $r \in \{0, \pm 1\}$, i.e, $b \mid 1, 2, 3$, i.e, $N(b) \mid 1, 4, 9$, where N is the usual norm on R. Since

$$N(x + y\frac{1+\sqrt{-19}}{2}) = x^2 + xy + 5y^2$$

that $N(b) = 1, 4, 9$ implies $b = \pm 1, \pm 2, \pm 3$, where ± 1 are impossible since $\pm 1 \in S$.
Consider $a = \dfrac{1+\sqrt{-19}}{2}$. However, none of a, $a \pm 1$ can be divisible by any of $\pm 2, \pm 3$, and thus R is not a Euclidean domain. □

2.3.2 Principal Ideal Domains

Definition. A **principal ideal domain**, or **PID** for short, is an integral domain in which every ideal is principal.

Example 2.3.11.

1. Proposition 2.3.3 shows that a Euclidean domain is PID.
2. $\mathbb{Z}[x], \mathbb{Z}[\sqrt{-5}], \mathbb{Z}[\sqrt{-5}]$ are NOT PIDs.
3. $\mathbb{Z}[\frac{1+\sqrt{D}}{2}]$ for $D = -3, -7, -11, -19, -43, -67, -163$ and $\mathbb{Z}[\sqrt{D}]$ for $D = -1, -2$ are PIDs.

Remark. $N(x + y\frac{1+\sqrt{-163}}{2}) = x^2 + xy + 41y^2$. Consider $f(n) = n^2 + n + 41$. Note $f(n)$ is a prime for $n = 0, 1, \ldots, 39$. Some theorems in the algebraic number theory with the fact $\mathbb{Z}[\frac{1+\sqrt{-163}}{2}]$ is a PID imply that if $p \mid n^2 + n + 41$, then there's an $\alpha \in \mathbb{Z}[\frac{1+\sqrt{-163}}{2}]$ such that $N(\alpha) = p$. We may check that the smallest prime that N represents is 41. Thus, if $f(n) < 41^2 - 1$, $f(n)$ must be a prime.

Proposition 2.3.12. Let R be a PID, $a, b_{\neq 0} \in R$ and $d \in R$ such that $(d) = (a, b)$. Then

1. $d = \gcd(a, b)$.
2. $d = ax + by$ for some $x, y \in R$.
3. d is unique up to units.

Proof. See Remark 2.3.6. □

Proposition 2.3.13. Every nonzero prime ideal in a PID is maximal.

Proof. Let (p) be a prime ideal and suppose $(p) \leqslant (a) \trianglelefteq (1)$. Since $p \in (a)$, $p = ab$ for some b, and thus $a \in (p)$ or $b \in (p)$. If $a \in (p)$, $(a) = (p)$. If $b \in (p)$, $(b) = (p)$, implying a is a unit, and thus $(a) = (1)$. □

Corollary 2.3.13.1. If R is a commutative ring such that $R[x]$ is a PID, then R is a field.

Proof. Since (x) is a prime ideal in $R[x]$, (x) is maximal, i.e, $R \cong R[x]/(x)$ is a field. □

Proposition 2.3.14. Let R be a integral domain. If every prime ideal of R is principle, then R is a PID. (HW. 16)

Proof.

1° Let $\mathcal{S} := \{I \trianglelefteq R \mid I \text{ is not principal}\}$. Suppose otherwise $\mathcal{S} \neq \varnothing$. Show $\mathcal{S}$ admits a maximal element.

2° Let $I \in \mathcal{S}$ be maximal. Let $ab \in I$ but $a, b \notin I$. Let $I_a = (I, a)$, $I_b = (I, b)$ and

$$J := \{r \in R \mid rI_a \subseteq I\}$$

Show that $I_a = (\alpha)$ and $J = (\beta)$ with $I \subsetneq I_b \subseteq J$ and $I_a J = (\alpha\beta) \subseteq I$.

3° If $x \in I$, show $x = s\alpha$ for some $s \in J$. Show $I = I_a J$ is principal, which is a contradiction.

□

Proposition 2.3.15. Let R be a PID and D a multiplicative closed subset of R. Then $D^{-1}R$ is a PID. (HW. 16)

Definition. A positive norm N on an integral domain is called a **Dedekind-Hasse norm** if $N(0) = 0$ and for all $a, b_{\neq 0} \in R$, either $a \in (b)$ or there's a $c \in (a, b)$ such that $0 < N(c) < N(b)$.

Proposition 2.3.16. R is a PID if and only if R has a Dedekind-Hasse norm N.

Proof. ($\Leftarrow$) Let $(0) \neq I \trianglelefteq R$ and let $0 \neq b \in I$ such that $N(b) = \min\{N(a) \mid a \in I - \{0\}\}$. Then $I = (b)$. ($\Rightarrow$) Since R is a PID, R is a UFD. Define $N : R \to \mathbb{Z}_{\geqslant 0}$ by $N(0) = 0$ and $N(a) = 2^n$ if $a = up_1 \cdots p_n$, where $p_i s$ are irreducibles and u is a unit. Clearly, we have $N(ab) = N(a)N(b)$ and N is positive. Let $a, b_{\neq 0} \in R$. Since R is PID, $(a, b) = (r)$ for some $r \in R$. If $a = qb$ for some q, then $(r) = (a, b) = (b)$. Otherwise, $(b) \neq (r)$. Since $b \in (r)$, $b = xr$ for some non-unit t, and thus $N(b) > N(r)$. □

Remark 2.3.17. The norm N constructed in the proof possesses more properties:

1. $N(ab) = N(a)N(b)$
2. $N(a) = 0 \Leftrightarrow a = 0$
3. $N(a) = 1 \Leftrightarrow a$ is a unit.

2.3.3 Unique Factorization Domains

Recall the **fundamental theorem of arithmetic**: every positive integer has a unique prime factorization. The notion of **unique factorization domain**, or **UFD** for short, generalizes this property of $\mathbb{Z}$. Note that there are two properties of primes that we use very often

1. $p = ab \Rightarrow a$ or b is a unit ± 1.

2. $p \mid ab \Rightarrow p \mid a$ or $p \mid b$.

Definition. Let R be an integral domain and $p \in R \backslash (R^\times \cup \{0\})$.

1. p is called a **irreducible** if $p = ab$ implies a or b is a unit, i.e, $(p) = (a)$ or (b).
2. p is called a **prime** if $p \mid ab$ implies $p \mid a$ or $p \mid b$, i.e, (p) is a prime ideal.
3. If $a, b \in R$ satisfies $a = ub$ for some unit u, then a, b are said to be **associates**.

Proposition 2.3.18. In an integral domain, a prime is an irreducible.

Proof. Let p be a prime and $p = ab$. Then $a \in (p)$ or $b \in (p)$. If $a \in (p)$, b is a unit. If $b \in (p)$, a is a unit. □

Example 2.3.19. In $\mathbb{Z}[\sqrt{-5}]$, $2, 3, 1 \pm \sqrt{-5}$ are irreducibles but not primes.

Proof. If $a = bc$, then $N(a) = N(b)N(c)$. Also, $N(a) = 1 \Leftrightarrow a$ is a unit. Since $N(2) = 4, N(3) = 9, N(1 \pm \sqrt{-5}) = 6$ but no element has norm 2 or 3, they're all irreducibles. Since $2 \times 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ but $2, 3 \nmid 1 \pm \sqrt{-5}$, they're not primes. □

Proposition 2.3.20. In a PID, an irreducible is a prime.

Proof. Let p be an irreducible. We will show that (p) is maximal. Let $(p) \leqslant (a) \trianglelefteq (1)$. Then we have $p \in (a)$, i.e, $p = ab$ for some b. Since p is irreducible, a or b is a unit. If a is a unit, $(a) = (1)$. If b is a unit, $(a) = (p)$. □

Definition. A **UFD** is an integral domain R with the following properties: if $r \in R$ is not 0 nor a unit, then

1. r can be written as a finite product of irreducibles.
2. the factorization is unique up to units and order in the sense that if $r = p_1 \cdots p_m = q_1 \cdots q_n$ with p_i, q_i irreducibles, then $m = n$ and after renumbering, if necessary, $p_i = u_i q_i$ for some units u_i.

Example 2.3.21.
1. All fields are UFDs.
2. PIDs are UFDs. Thus $\mathbb{Z}, \mathbb{F}[x], \mathbb{Z}[\sqrt{-1}]$ are UFDs.
3. If R is UFD, so is $R[x]$. Thus $\mathbb{Z}[x_1, \ldots, x_n]$ and $\mathbb{F}[x_1, \ldots, x_n]$ are UFDs.
4. $\mathbb{Z}[2i]$ is not a UFD since $\pm 2, \pm 2i$ are irreducibles, we have $4 = 2 \cdots 2 = (2i)(-2i)$ but 2 is not an associates of $\pm 2i$ ($\pm i \notin \mathbb{Z}[2i]$). However, for elements with odd norm in $\mathbb{Z}[2i]$, the UF property still holds

5. $\mathbb{Z}[\sqrt{-5}]$ is not a UFD since $6 = 2\cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$. However, $\mathbb{Z}[\sqrt{-5}]$ still has a UF property at the level of ideals in the following sense: every non-zero ideal in $\mathbb{Z}\sqrt{-5}]$ can be written uniquely as a product of primes ideals.

$$(6) = \underbrace{(2, 1+\sqrt{-5})^2}_{P_2}\,\underbrace{(3, 1+\sqrt{-5})}_{P_3}\,\underbrace{(3, 1-\sqrt{-5})}_{P_{3'}}$$

One can check they're all maximal and $(2) = P_2^2, (3) = P_3P_3', (1+\sqrt{-5}) = P_3, (1-\sqrt{-5}) = P_3'$. This UF property at the level of ideals is a property or a definition of a **Dedekind domain**.

Proposition 2.3.22. In a UFD, primes $\Leftrightarrow$ irreducibles.

Proof. ($\Leftarrow$) Let p be an irreducible and $ab \in (p)$, i.e, $ab = pt$ for some t. Let $a = up_1 \cdots p_n$ and $b = vq_1 \cdots q_m$, where p_i, q_i are irreducibles and u, v are units. By the uniqueness of the factorization, p must divide at least one of p_i, q_i, and thus $a \in (p)$ or $b \in (p)$. □

Proposition 2.3.23. Let R be a UFD and $a, b_{\neq 0} \in R$. Suppose that $a = up_1^{e_1} \cdots p_n^{e_n}$ and $b = vp_1^{f_1} \cdots p_n^{f_n}$, where p_is are irreducibles and u, v are units. Then $\gcd(a, b) = p_1^{\min\{e_1, f_1\}} \cdots p_n^{\min\{e_n, f_n\}}$.

Lemma 2.3.24 (Ascending chain condition for PIDs, **ACC**)**.** Let R be PID. If $I_1 \leqslant I_2 \leqslant \cdots$ is an ascending chain of ideals in R, then there's an $N \in \mathbb{N}$ such that $I_n = I_N$ for all $n \geqslant N$.

Proof. Let $I = \bigcup_k I_k$. This is clearly an ideal. Since R is PID, $I = (a)$ for some $a \in R$. Since $a \in I$, $a \in I_N$ for some $N \in \mathbb{N}$, and thus $I \subseteq I_n$ for all $n \geqslant N$. The result follows. □

Theorem 2.3.25. Every PID is a UFD.

Proof. We break the proof into three steps. Let $r \in R\backslash(R^\times \cup \{0\})$.

1° Show that r is divisible by some irreducible.

2° Show that r is a finite product of irreducibles.

3° Show that the factorization is unique.

1° If r is reducible, we are done. Otherwise, $r = r_1s_1$ for some $r_1, s_1 \in R\backslash(R^\times \cup \{0\})$. If r_1 is irreducible, we are done. Otherwise, continuing this process we will obtain $r_1, r_2, \ldots$. Consider the chain

$$(r) \lneq (r_1) \lneq (r_2) \lneq \cdots$$

where inequalities are due to that s_i are not units. By Lemma 2.3.24, this chain cannot go on for good, and thus there's an $N \in \mathbb{N}$ such that r_N is irreducible by our construction with $r_N \mid r$.

2° If r is irreducible, we are done. Otherwise, by 1°, $r = r_1 s_1$ for some irreducible s_1. If r_1 is irreducible, we are done. Otherwise, continuing this process we obtain $r_1, r_2, \ldots$. Consider the chain

$$(r) \lneq (r_1) \lneq (r_2) \lneq \cdots$$

By Lemma 2.3.24, this chain cannot go on for good, and thus there's an $N \in \mathbb{N}$ such that r_N is irreducible by our construction. Thus $r = s_1 \cdots s_N r_N$.

3° Suppose $r = p_1 \cdots p_n = q_1 \cdots q_m$, where p_i, q_i are irreducibles, and hence primes by Proposition 2.3.20. Since $p_1 \mid q_1 \cdots q_m$, WLOG, say $p_1 \mid q_1$, i.e, $p_1 u_1 = q_1$. Since q_1 is irreducible, u_1 is a unit. Hence $p_2 \cdots p_n = u_1 q_2 \cdots q_m$. The proof will be completed by continuing this process.

□

Irreducibles/primes in $\mathbb{Z}[i]$

Observation 2.3.26. In the following, by p we always denote a prime in $\mathbb{Z}$.

1. If $\pi \in \mathbb{Z}[i]$ has norm p, then π is an irreducible.
2. If π is a prime in $\mathbb{Z}[i]$, then $(\pi) \cap \mathbb{Z} = p\mathbb{Z}$ for some p. In this case, we say π is a **prime of $\mathbb{Z}[i]$ lying above** p.

- Case $p = 2$: $2 = (1+i)(1-i)$ and $\pm 1 \pm i$ are associates of each other; $(2) = (1+i)^2$.
- Case $p \equiv_4 3$: $a^2 + b^2 = p$ has no solution in $\mathbb{Z}$, implying that p is an irreducible in $\mathbb{Z}[i]$; this also implies that $\mathbb{Z}[i]/(p)$ is a field of p^2 elements.
- Case $p \equiv_4 1$: recall that $(\mathbb{Z}/p\mathbb{Z})^\times$ is a cyclic group, i.e, $(\mathbb{Z}/p\mathbb{Z})^\times = \langle a \rangle$. for some a. Let $n := a^{(p-1)/4}$. Then $n^2 = a^{(p-1)/2}$. Since $\operatorname{ord} a = p - 1$, $a^{(p-1)/2} \equiv_p -1$, i.e, $(n+i)(n-i) = n^2 + 1 \equiv_p 0$. Now $p \mid (n+i)(n-i)$ but $p \nmid (n+i), (n-i)$, so p is not a prime in $\mathbb{Z}[i]$. Hence $p = (a+bi)(a-bi)$ for some $a, b \in \mathbb{Z}$ such that $a^2 + b^2 = p$; also note that $a + bi$ and $a - bi$ are not associates.

Proposition 2.3.27.
1. p is a sum of two squares $\Leftrightarrow p = 2$ or $p \equiv 1 \pmod 4$.
2. Irreducibles in $\mathbb{Z}[i]$ are $1 + i$, $p(\equiv_4 3)$, $a \pm bi$ with norm $p(\equiv_4 1)$ and their associates.

Corollary 2.3.27.1. Let $n = 2^a p_1^{e_1} \cdots p_k^{e_k} q_1^{f_1} \cdots q_m^{f_m}$, where $p_i \equiv_4 1$, $q_i \equiv_4 3$ are primes. Then n is a sum of two squares $\Leftrightarrow 2 \mid f_j$ for all j.

2.4 Polynomial Rings

Proposition 2.4.1. Let R be an integral domain.

1. $\deg fg = \deg f + \deg g$ for all $f, g \in R[x]$.
2. $R[x]^\times = R^\times$.
3. $R[x]$ is an integral domain.

Proposition 2.4.2. Let $I \trianglelefteq R$ and $(I) = I[x]$. Then $R[x]/(I) \cong (R/I)[x]$. In particular, if I is a prime ideal, (I) is a prime ideal of $R[x]$.

Proof. Consider the **reduction homomorphism** $R[x] \to (R/I)[x]$. □

Definition. Let $x_1, \ldots, x_n$ be indeterminates. The **polynomial ring in variables $x_1, \ldots, x_n$ with coefficients in** R is defined inductively to be

$$R[x_1, \ldots, x_n] := R[x_1, \ldots, x_{n-1}][x_n]$$

- A **monomial** is an element of $[x_1, \ldots, x_n]$ of the form $x_1^{d_1} \cdots x_n^{d_n}$.
- The **degree** of a nonzero polynomial is the largest degree of any of its monomial terms.
- A polynomial is said to be **homogeneous** if each of its monomial terms shares the same degree.

Theorem 2.4.3. Let F be a field. Then $\deg : F[x] \to \mathbb{Z}$ is a Euclidean norm on $F[x]$.

Corollary 2.4.3.1. If F is a field. Then $F[x]$ is an Euclidean domain, and hence PID and UFD.

Remark 2.4.4. According to the proof of ED ⇒ PID, an ideal of $F[x]$ is generated by a polynomial of smallest degree in it.

Proposition 2.4.5. Let R be a commutative ring. Then R is a field ⇔ $R[x]$ is a PID.

2.4.1 Gauss' lemma

Lemma 2.4.6 (Gauss')**.** Let R be a UFD and F be its field of fractions. If $f \in R[x]$ is reducible in $F[x]$, then it's reducible in $R[x]$. More precisely, if $f(x) = A(x)B(x)$ for some nonconstant $A, B \in F[x]$, then there are $r, s \in F^\times$ such that $f(x) = a(x)b(x)$, where $a = rA, b = sB \in R[x]$.

Proof. Let $f(x) = A(x)B(x)$ for some nonconstant polynomials $A, B \in F[x]$. Pick $d_1, d_2 \in R$ such that $a'(x) = d_1A(x), b' = d_2B(x) \in R[x]$; for instance, just take d_1 and d_2 to be LCMs of denominators of coefficients in A and B, respectively. Put $d = d_1d_2$. Then $df(x) = a'(x)b'(x)$. Since R is a UFD, we have $d = p_1 \cdots p_n$ for some irreducibles p_j in R, and hence in $R[x]$. Since $R[x]/p_jR[x] \cong (R/(p_j))[x]$ is an integral domain, (p_j) is a prime ideal in $R[x]$. Consider the reduction homomorphism modulo p_1. Then $0 \equiv df(x) = a'(x)b'(x) \pmod{p_1}$, and hence a' or b' belongs to (p_1). WLOG, say $a' \in (p_1)$. Then $a''(x) := \frac{1}{p_1}a'(x) \in R[x]$. Then $p_2 \cdots p_n f(x) = a''(x)b'(x)$. Continuing this way and we will obtain $a, b \in R[x]$ such that $f(x) = a(x)b(x)$. □

Corollary 2.4.6.1. Let R be a UFD and F be its field of fractions. Let $f \in R[x]$ such that 1 is a GCD of its coefficients. Then f is irreducible in $R[x] \Leftrightarrow f$ is irreducible in $F[x]$.

Proof. ($\Rightarrow$) follows from Lemma 2.4.6.
($\Leftarrow$) Suppose f is reducible in $R[x]$. Since 1 is a GCD of coefficients of f, $f(x) = a(x)b(x)$ for some nonconstant polynomials $a, b \in R[x]$, and hence f is reducible in $F[x]$ with the same factorization. □

Theorem 2.4.7. $R[x]$ is a UFD $\Leftrightarrow R$ is a UFD.

Proof. ($\Rightarrow$) is clear.
($\Leftarrow$) Let F denote the field of fractions of R and put $f(x) = p_1(x) \cdots p_n(x)$ a factorization of $f(x)$ into a product of irreducibles in $F[x]$. By Lemma 2.4.6, there are $r_j \in F^\times$ such that $P_j(x) := r_jp_j(x) \in R[x]$ and $f(x) = P_1(x) \cdots P_n(x)$. Let d_j denote a GCD of coefficients of $P_j(x)$ and put $Q_j(x) := \frac{1}{d_j}P_j$. Then

$$f(x) = d_1 \cdots d_n Q_1(x) \cdots Q_n(x)$$

Let $d_1 \cdots d_n = s_1 \cdots s_m$ be a factorization of $d_1 \cdots d_n$ into irreducibles in R, and hence in $R[x]$. Now

$$f(x) = s_1 \cdots s_m Q_1(x) \cdots Q_n(x)$$

Since 1 is a GCD of coefficients in Q_j and Q_j is irreducibles in $F[x]$, Q_j is irreducible in $R[x]$ by Corollary 2.4.6.1. The uniqueness of the factorization follows from the UF property of R and $F[x]$. □

Corollary 2.4.7.1. If R is a UFD, so is $R[x_1, \ldots, x_n]$.

2.4.2 Irreducibility criteria

Proposition 2.4.8. Let F be a field and $f \in F[x]$.

1. $f(x)$ has a factor $x - \alpha \in F[x] \Leftrightarrow \alpha$ is a root of f.

2. If $\deg f = 2, 3$, then f is reducible $\Leftrightarrow$ it has a root in F.

Proposition 2.4.9. Let R be a UFD and F its field of fractions. Let $f(x) = a_n x^n + \cdots + a_0 \in R[x]$ with $a_n \neq 0$. If $\frac{p}{q} \in F$ with $\gcd(p, q) = 1$ is a root of f, then $q \mid a_n$ and $p \mid a_0$.

Proof. By Lemma 2.4.6, since f is reducible in $F[x]$, it's reducible in $R[x]$, and $qx - p \mid f(x)$ in $R[x]$. □

Proposition 2.4.10. Let I be a proper ideal in an integral domain R and f a nonconstant monic polynomial in $R[x]$. If $f(x) \bmod I$ can not be factored into a product of two polynomials of smaller degree in $(R/I)[x]$, then f is irreducible in $R[x]$.

Example 2.4.11. There are examples where $f(x)$ factorizes in $(R/I)[x]$ for all prime ideals I in R but fails to factorize in $R[x]$. For example, $f(x) = x^4 + 1 \in \mathbb{Z}[x]$ is reducible modulo every prime number but irreducible in $\mathbb{Z}[x]$:

- If $p \equiv_8 1$, $a^4 \equiv_p -1$ for some $a \in \mathbb{Z}$, and thus $a^4 + 1 = 0$.
- If $p \equiv_8 5$, $a^2 \equiv_p -1$ for some $a \in \mathbb{Z}$, and thus $x^4 + 1 = (x^2 - a)(x^2 + a)$.
- If $p \equiv_8 3, 7$, $a^2 \equiv_p \mp 2$ for some $a \in \mathbb{Z}$, and thus $x^4 + 1 = (x^2 \pm 1)^2 \mp 2x^2 = (x^2 - ax \pm 1)(x^2 + ax \pm 1)$.

Example 2.4.12. $x^2 + xy + 1$ is irreducible in $\mathbb{Z}[x, y]$ since $\mathbb{Z}[x, y]/(y) \cong \mathbb{Z}[x]$ and $x^2 + 1$ is irreducible in $\mathbb{Z}[x]$.

Proposition 2.4.13 (Eisenstein's criterion)**.** Let P be a prime ideal in an integral domain R. Let $f(x) = a_n x^n + \cdots + a_0 \in R[x]$ $(n \geqslant 1)$ be such that $a_n \in R^\times$, $a_n \notin P$, $a_{n-1}, \ldots, a_0 \in P$ but $a_0 \notin P^2$. Then $f(x)$ is irreducible in $R[x]$.

Proof. Suppose $f(x) = a(x)b(x)$ for some $a, b \in R[x]$. Modulo P we have $f(x) \equiv a_n x^n \pmod{P}$. Note that for an integral domain D, the factorization of x^n in $D[x]$ can be only a product of some powers of x, up to units. Thus $a(x) \equiv ux^k$ and $b(x) \equiv vx^{n-k} \pmod{P}$ for some $u, v \notin P$. If $k \neq 0, n$, then the constant terms of a, b must be in P, leading to $a_0 \in P^2$, a contradiction. Hence $a(x)$ or $b(x)$ is a constant polynomial. Since a_n is a unit, the constant polynomial must be a unit in $R[x]$. □

Example 2.4.14.

1. $x^4 + 2x^3 + 4x^2 + 8x + 2$ is irreducible in $\mathbb{Z}[x]$.
2. $y^2 + x^3 - x$ is irreducible in $\mathbb{Z}[x, y]$.
3. Let p be a prime and $\Phi_p(x) = \dfrac{x^p - 1}{x - 1} = x^{p-1} + \cdots + 1$. We have $\Phi_p(x + 1) = \dfrac{(x + 1)^p - 1}{x} = x^{p-1} + px^{x-2} + \cdots + p$. Hence Φ_p is irreducible in $\mathbb{Z}[x]$.

Proposition 2.4.15. Let $f(x) = a_0 + a_1x + \cdots + a_kx^k + \cdots + a_nx^n \in \mathbb{Z}[x]$ and p a prime integer such that $p \mid a_i$ for $i = 0, \cdots, (k-1)$, $p \nmid a_k$, $p \nmid a_n$, and $p^2 \nmid a_0$. Then $f(x)$ has an irreducible factor in $\mathbb{Z}[x]$ of degree at least k.

Proposition 2.4.16 (Perron's)**.** Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_n \in \mathbb{Z}[x]$ such that $|a_{n-1}| > 1 + |a_{n-2}| + \cdots + |a_0|$ and $a_0 \neq 0$. Then f is irreducible over $\mathbb{Z}$.

Proof. Let $\alpha_1, \ldots, \alpha_n$ be roots of f. WLOG, assume $|\alpha_1| \geqslant \cdots \geqslant |\alpha_n|$.

- $|\alpha_1| \geqslant 1$ since $|a_0| \geqslant 1$.
- Put $A(z) = a_{n-1}z^{x-1}$. Then for $|z| = 1$, we have

  $$|f(z) - A(z)| \leqslant 1 + |a_{n-2}| + \cdots + |a_0| < |a_{n-1}| = |A(z)|$$

  By the Rouché's theorem, $\#Z_f \cap B_1(0) = \#Z_A \cap B_1(0) = n - 1$.
- Suppose otherwise $f = gh$, $\deg g, \deg h \geqslant n$. Then exactly one of $g(\alpha_1), h(\alpha_1)$ is 0, say $g(\alpha_1) = 0$. This forces $|h(0)| < 1$, so $h(0) = 0$, implying $a_0 = f(0) = 0$, a contradiction.

□

Proposition 2.4.17 (Cohn's)**.** Let $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_n \in \mathbb{Z}[x]$. If there's a $\mathbb{N} \ni b \geqslant 2$ such that $0 \leqslant a_i < b$ for each i and $f(b)$ is a prime p, then f is irreducible over $\mathbb{Z}$.

Proof. Suppose $f = gh$, $\deg g, \deg h \geqslant 1$. Then $p = f(b) = g(b)h(b)$. WLOG, say $|g(b)| = p$ and $h(b)| = 1$.

Claim. If $f(\alpha) = 0$, then $\operatorname{Re}\alpha \leqslant 0$ or $|\alpha| < \dfrac{1 + \sqrt{4b-3}}{2}$.

- If $b \geqslant 3$, $\dfrac{1 + \sqrt{4b-3}}{2} < b - 1$, so $|b - \alpha| > 1$. Hence $1 = |h(b)| > 1$, a contradiction.

Claim. If $f(\alpha) = 0$ then $\operatorname{Re}\alpha < \dfrac{3}{2}$ $(\Rightarrow |2 - \alpha| > |1 - \alpha|)$.

- Let $\alpha_1, \ldots, \alpha_s$ be roots of h. Then

  $$|h(1)| = |c||1 - \alpha_1| \cdots |1 - \alpha_s| < |c||2 - \alpha_1| \cdots |2 - \alpha_s| = |h(2)| = 1$$

  i.e, $|h(1)| < 1$, which forces that $h(1) = 0$, a contradiction.

□

2.4.3 Polynomial rings over fields

Let F denote a field.

Proposition 2.4.18. Maximal ideals in $F[x]$ are precisely $(p(x))$, where $p(x)$ are irreducibles. Hence, $F[x]/(p(x))$ is a field $\Leftrightarrow$ $p(x)$ is irreducible.

Proof. Let I be a maximal ideal in $F[x]$. Since $F[x]$ is a PID, $I = (p(x))$ for some $p \in F[x]$ and I is a prime ideal. Hence p is a prime, and thus an irreducible. □

Proposition 2.4.19. Let $g(x) = f_1(x)^{n_1} \cdots f_k(x)^{n_k} \in F[x]$ be a nonconstant polynomial, where f_i are irreducible and distinct. Then

$$F[x]/(g(x)) \cong (F[x]/(f_1(x)^{n_1})) \times \cdots \times (F[x]/(f_k(x)^{n_k}))$$

Proposition 2.4.20. If α is a root of $f \in F[x]$ in F, then $x - \alpha \mid f(x)$. Hence, a polynomial of degree n in $F[x]$ has at most n roots in F.

Proposition 2.4.21. Any finite subgroup of $F^\times$ is cyclic. In particular, if F is a finite field, then $F^\times$ is cyclic.

Proof. Say G is a finite subgroup of $F^\times$. By FTFGAG, $G \cong (\mathbb{Z}/a_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/a_k\mathbb{Z})$ with $a_i \mid a_{i-1}$. Observe that $x^{a_1} = 1$ for all $x \in G$. If $k \geqslant 2$, then there are more than a_1 roots for $x^{a_1} - 1$, a contradiction. Hence $k = 1$, i.e, G is cyclic. □

2.4.4 Hilbert's basis theorem

Definition. A commutative ring with 1 is called **Noetherian** if every ideal of R is finitely generated.

Proposition 2.4.22. Let R is a commutative ring. TFAE: (HW. 17)

1. R is Noetherian.
2. The Ascending chain condition for R holds.
3. Every nonempty collection of ideals of R has a maximal element.

Theorem 2.4.23 (Hilbert's basis theorem)**.** If R is Noetherian, then so is $R[x]$

Proof. Let $I \trianglelefteq R[x]$. For $f(x) \in R[x]$, let $LC(f)$ denote the leading coefficient in $f(x)$.

1° Let $L := \{LC(f) \mid f(x) \in I\}$.

Claim. $L \trianglelefteq R$.

2° Since R is Noetherian, we have $L = (a_1, \ldots, a_n)$ for some $a_j \in R$. Let $f_1, \ldots, f_n \in I$ be such that $LC(f_j) = a_j$.

3° Let $N = \max\{\deg f_j \mid j = 1, \ldots, n\}$. For each $d = 0, \ldots, N-1$, let $L_d := \{LC(f) \mid f \in I \wedge \deg f = d\}$.

Claim. $L_d \trianglelefteq R$.

4° Since R is Noetherian, $L_d = (b_{d,1}, \ldots, b_{d,k_d})$ for some $b_{d,j} \in R$. Let $f_{d,j} \in I$ be a polynomial such that $LC(f_{d,j}) = b_{d,j}$.

Claim. $I = (f_1, \ldots, f_n, f_{d,j} \mid d = 0, \ldots, N-1, j = 1, \ldots, k_d)$ Let $f \in I$.

(i) Assume $\deg f \geqslant N$. Since $L = (a_1, \ldots, a_n)$, we have $LC(f) = r_1 a_1 + \cdots + r_n a_n$ for some $r_j \in R$. Then

$$f - \left(r_1 x^{\deg f - \deg f_1} f_1 + \cdots + r_n x^{\deg f - \deg f_n} f_n\right)$$

has degree $\leqslant \deg f - 1$. Continuing this way, we reduce the proof of this case to $\deg f \leqslant N - 1$.

(ii) Assume $\deg f \leqslant N-1$. Since $L_d = (b_{d,1}, \ldots, b_{d,k_d})$, $L(f) = s_1 b_{d,1} + \cdots + s_{k_d} b_{d,k_d}$ for some $s_j \in R$. Then

$$f - (s_1 f_{d,1} + \cdots + s_{k_d} f_{d,k_d})$$

has degree $\leqslant \deg f - 1$. Continuing this way, the proof is completed.

□

2.4.5 Resultants

Notation 2.4.24. Let R be a ring with 1 and $n \in \mathbb{N}$. We put $Z := (\delta_{i,n+1-j}) \in M_n(R)$, the **reverse identity**, and $N := (\delta_{i,j-1}) \in M_n(R)$.

In the following context, we let F denote a field, $f, g \in F[x]$, $n := \max\{\deg f, \deg g\}$ and $f(x) = f_0 + f_1 x + \cdots + f_n x^n$. Note that f may not has degree n.

Definition. We define the **Hankel matrix**

$$H_f := \begin{pmatrix} f_1 & f_2 & \cdots & f_n \\ f_2 & f_3 & & \\ \vdots & & \iddots & \\ f_n & & & \end{pmatrix}$$

and the **Toeplitz matrix**

$$T_f := \begin{pmatrix} f_0 & f_1 & \cdots & f_{n-1} \\ & & & \vdots \\ & \ddots & & f_1 \\ & & & f_0 \end{pmatrix}$$

of the polynomial f.

From the definition, we have

$$ZH_f = \begin{pmatrix} f_n & & & \\ \vdots & \ddots & & \\ \vdots & & \ddots & \\ f_1 & \cdots & \cdots & f_n \end{pmatrix}, \qquad ZT_f = \begin{pmatrix} & & & f_0 \\ & & \iddots & \vdots \\ & \iddots & & \vdots \\ f_0 & \cdots & \cdots & f_{n-1} \end{pmatrix}$$

We list some properties of H_f and T_f:

- $ZT_f = (ZT_f)^t = T_f^t Z$, and thus $ZT_f Z = T_f^t ZZ = T_f^t$, i.e, $T_f = ZT_f^t Z$.
- $T_f T_g = T_g T_f$, since $T_f = f_0 I + f_1 N + \cdots + f_{n-1} N^{n-1}$.
- $ZH_f ZH_g = ZH_g ZH_f$, and thus $H_f ZH_g = H_g ZH_f$.

Notation 2.4.25. 1. $v_n(x) := \begin{pmatrix} 1 & x & \cdots & x^{n-1} \end{pmatrix}^t$.

2. For $A = (a_j k) \in M_n(F)$, we put $a(x,y) := \sum_{j,k=0}^{n-1} a_{jk} x^j y^k = v_n(x)^t A v_n(y) \in F[x,y]$.

Definition (Resultant matrix)**.** The **resultant matrix**, denoted by R, of two polynomials f, g is defined to be the $2n \times 2n$ matrix

$$R := \begin{pmatrix} T_f & ZH_f \\ T_g & ZH_g \end{pmatrix}$$

Explicitly,

$$R := \begin{pmatrix} f_0 & \cdots & f_{n-1} & f_n & & \\ & & \vdots & \vdots & \ddots & \\ & \ddots & \vdots & \vdots & & \\ & & f_0 & f_1 & \cdots & f_n \\ g_0 & \cdots & g_{n-1} & g_n & & \\ & & \vdots & \vdots & \ddots & \\ & \ddots & \vdots & \vdots & & \\ & & g_0 & g_1 & \cdots & g_n \end{pmatrix} \in M_{2n}(F)$$

Note that $Rv_{2n}(x) = \Big(f(x)\ f(x)x\ \cdots\ f(x)x^{n-1}\ g(x)\ \cdots\ g(x)x^{n-1}\Big)^t = \begin{pmatrix} f(x)v_n(x) \\ g(x)v_n(x) \end{pmatrix}$

Definition (Bézoutian)**.** The **Bézoutian**, denoted by B, of two polynomials f, g is defined implicitly by

$$F[x,y] \ni f(x)g(y) - g(x)f(y) := (x-y)b(x,y) = (x-y)\Big(v_n(x)^t B v_n(y)\Big)$$

Lemma 2.4.26. $B = H_f T_g - H_g T_f = (H_f T_g - H_g T_f)^t$. In particular, B is symmetric.

Proof. Since $x^n - y^n = (x-y)\sum_{j=0}^{n-1} x^{n-1-j}y^j = (x-y)\Big(v_n(x)^t Z v_n(y)\Big)$, we have

$$\begin{aligned}
(x^n - y^n)b(x,y) &= (x-y)b(x,y)\Big(v_n(x)^t Z v_n(y)\Big) \\
&= (f(x)g(y) - g(x)f(y))\Big(v_n(x)^t Z v_n(y)\Big) \\
&= \begin{pmatrix} f(x)v_n(x) \\ g(x)v_n(x) \end{pmatrix}^t \begin{pmatrix} O & Z \\ -Z & O \end{pmatrix} \begin{pmatrix} f(y)v_n(y) \\ g(y)v_n(y) \end{pmatrix} \\
&= Rv_{2n}(x)^t \begin{pmatrix} O & Z \\ -Z & O \end{pmatrix} Rv_{2n}(y) = v_{2n}(x)^t \cdot R^t \begin{pmatrix} O & Z \\ -Z & O \end{pmatrix} R \cdot v_{2n}(y)
\end{aligned}$$

On the other hand,

$$\begin{aligned}
(x^n - y^n)b(x,y) &= (x^n - y^n)\Big(v_n(x)^t B v_n(y)\Big) \\
&= (z^n v_n(x))^t B v_n(y) - v_n(x)^t B (y^n v_n(y)) \\
&= v_{2n}(x)^t \begin{pmatrix} O & -B \\ B & O \end{pmatrix} v_{2n}(y)
\end{aligned}$$

Hence

$$\begin{aligned}
\begin{pmatrix} O & -B \\ B & O \end{pmatrix} &= R^t \begin{pmatrix} O & Z \\ -Z & O \end{pmatrix} R \\
&= \begin{pmatrix} T_f & ZH_f \\ T_g & ZH_g \end{pmatrix}^t \begin{pmatrix} O & Z \\ -Z & O \end{pmatrix} \begin{pmatrix} T_f & ZH_f \\ T_g & ZH_g \end{pmatrix} \\
&= \begin{pmatrix} T_f^t & T_g^t \\ (ZH_f)^t & (ZH_g)^t \end{pmatrix} \begin{pmatrix} ZT_g & ZZH_g \\ -ZT_f & -ZZH_f \end{pmatrix} \\
&= \begin{pmatrix} ZT_fZ & ZT_gZ \\ ZH_f & ZH_g \end{pmatrix} \begin{pmatrix} ZT_g & H_g \\ -ZT_f & -H_f \end{pmatrix} \\
&= \begin{pmatrix} O & ZT_fZH_g - ZT_gZH_f \\ H_fT_g - H_gT_f & O \end{pmatrix} \\
&= \begin{pmatrix} O & -(H_fT_g - H_gT_f)^t \\ H_fT_g - H_gT_f & O \end{pmatrix}
\end{aligned}$$

□

Lemma 2.4.27.

$$\begin{pmatrix} I & O \\ T_f & ZH_f \end{pmatrix} R = \begin{pmatrix} O & I \\ Z & T_f + ZH_g \end{pmatrix} \begin{pmatrix} B & O \\ O & I \end{pmatrix} \begin{pmatrix} I & O \\ T_f & ZH_f \end{pmatrix}$$

Proof.

$$\begin{aligned}
\begin{pmatrix} I & O \\ T_f & ZH_f \end{pmatrix} R &= \begin{pmatrix} I & O \\ T_f & ZH_f \end{pmatrix} \begin{pmatrix} T_f & ZH_f \\ T_g & ZH_g \end{pmatrix} \\
&= \begin{pmatrix} T_f & ZH_f \\ T_f^2 + ZH_fT_f & T_fZH_f + \underbrace{ZH_fZH_g}_{\text{commutes}} \end{pmatrix} \\
\text{(Lemma 2.4.26)} &= \begin{pmatrix} T_f & ZH_f \\ ZB + (T_f + ZH_f)T_f & (T_f + ZH_g)ZH_f \end{pmatrix} \\
&= \begin{pmatrix} O & I \\ ZB & T_f + ZH_g \end{pmatrix} \begin{pmatrix} I & O \\ T_f & ZH_f \end{pmatrix} \\
&= \begin{pmatrix} O & I \\ Z & T_f + ZH_g \end{pmatrix} \begin{pmatrix} B & O \\ O & I \end{pmatrix} \begin{pmatrix} I & O \\ T_f & ZH_f \end{pmatrix}
\end{aligned}$$

□

Theorem 2.4.28. $\dim\ker R = \dim\ker B = \deg\gcd(f,g)$.

Proof. Suppose $\deg f = n$. Then $\operatorname{rank} H_f = \operatorname{rank}\begin{pmatrix} f_1 & f_2 & \cdots & f_n \\ f_2 & f_3 & & \\ \vdots & & \iddots & \\ f_n & & & \end{pmatrix} = n$. By Lemma 2.4.27,

$$\underbrace{\begin{pmatrix} I & O \\ T_f & ZH_f \end{pmatrix}}_{\text{rank}=2n} R = \underbrace{\begin{pmatrix} O & I \\ Z & T_f + ZH_g \end{pmatrix}}_{\text{rank}=2n} \begin{pmatrix} B & O \\ O & I \end{pmatrix} \underbrace{\begin{pmatrix} I & O \\ T_f & ZH_f \end{pmatrix}}_{\text{rank}=2n}$$

and thus $\operatorname{rank} R = \operatorname{rank}\begin{pmatrix} B & O \\ O & I \end{pmatrix}$. Therefore, $\dim\ker R = \dim\ker B$.
For the last equality, we introduce the linear transformation

$$\begin{aligned} M : F[x]_{<n} \times F[x]_{<n} &\longrightarrow F[x]_{<2n} \\ (u,v) &\longmapsto uf + vg \end{aligned}$$

and put $h = \gcd(f,g)$ and $k = \deg h$. Then $f = h\hat{f}, g = h\hat{g}$ with $\gcd(\hat{f},\hat{g}) = 1$. Consider the set

$$S := \left\{ (u,v) \in F[x]_{<n} \times F[x]_{<n} \mid u = -\hat{g}q, v = \hat{f}q, q \in F[x]_{<k} \right\}$$

Claim. $\ker M = S$, and thus $\dim\ker M = k$.

Clearly, $S \subseteq \ker M$. Now suppose $u, v \in F[x]_{<n}$ and $fu + gv = 0$. Then $\hat{f}u = -\hat{g}v$. Since $\gcd(\hat{f},\hat{g}) = 1$, $u = \hat{g}p$ and $v = \hat{f}q$ for some $p, q \in F[x]$. Then $p = -q$, implying $(u,v) \in S$. Therefore, $S \supseteq \ker M$.

Let

$$\beta = \{(1,0), \ldots, (x^{n-1}, 0), (0,1), \ldots, (0, x^{n-1})\}$$

be an ordered basis for $F[x]_{<n} \times F[x]_{<n}$ and

$$\beta' = \{1, \ldots, x^{2n-1}\}$$

an ordered basis of $F[x]_{<2n}$. Then

$$[M]_{\beta}^{\beta'} = \begin{pmatrix} f_0 & & & & g_0 & & & \\ \vdots & f_0 & & & \vdots & g_0 & & \\ \vdots & \vdots & \ddots & & \vdots & \vdots & \ddots & \\ f_n & \vdots & & f_0 & g_n & \vdots & & g_0 \\ & f_n & & \vdots & & g_n & & \vdots \\ & & \ddots & \vdots & & & \ddots & \vdots \\ & & & f_n & & & & g_n \end{pmatrix} = R^t$$

Hence,

$$\dim\ker B = \dim\ker R = \dim\ker R^t = \dim\ker M = k = \deg\gcd(f,g)$$

□

Corollary 2.4.28.1. Suppose that f, g are nonconstant. Then $\deg\gcd(f,g) \geqslant 1 \Leftrightarrow hf + kg = 0$ for some $k, h \in F[x]\backslash\{0\}$ with $\deg h < \deg g$ and $\deg k < \deg f$.

Definition (Resultant)**.** Let $\deg f = n$ and $\deg g = m$. The **resultant**, denoted by $R_{f,g}$, is defined to be

$$R_{f,g} = \det \begin{pmatrix} f_0 & \cdots & f_{n-1} & f_n & & \\ & & \vdots & \vdots & \ddots & \\ & \ddots & \vdots & \vdots & & \\ & & f_0 & f_1 & \cdots & f_n \\ g_0 & \cdots & g_{m-1} & g_m & & \\ & & \vdots & \vdots & \ddots & \\ & \ddots & \vdots & \vdots & & \\ & & g_0 & g_1 & \cdots & g_m \end{pmatrix}_{(n+m)\times(n+m)}$$

Corollary 2.4.28.2. $\deg\gcd(f,g) \geqslant 1 \Leftrightarrow R_{f,g} = 0$. (HW. 18)

Proof. Let $\deg f = n$ and $\deg g = m$. Consider the linear transformation

$$\begin{aligned} M : F[x]_{<n} \times F[x]_{<m} &\longrightarrow F[x]_{<n+m} \\ (u, v) &\longmapsto uf + vg \end{aligned}$$

and Let

$$\beta = \{(1,0), \ldots, (x^{n-1}, 0), (0,1), \ldots, (0, x^{m-1})\}$$

be an ordered basis for $F[x]_{<n} \times F[x]_{<m}$ and

$$\gamma = \{1, \ldots, x^{n+m-1}\}$$

an ordered basis of $F[x]_{<n+m}$. Then we have $[M]_\beta^\gamma = (\text{resultant matrix})^t$. □

Proposition 2.4.29. Let F be a field and let $f(x) = \prod_{i=1}^{n}(x - \alpha_i) \in F[x]$ and $g(x) = \prod_{i=1}^{m}(x - \beta_i) \in F[x]$ be two polynomials. Then

$$R_{f,g} = \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j)$$

Proof. Suppose all the x_i are distinct and all the y_j are distinct. Consider $R_{f,g}$ as a polynomial of the x_i and the y_j. By Corollary 2.4.28.2, $x_i = y_j \Leftrightarrow R_{f,g} = 0$; this shows $x_i - y_j \mid R_{f,g}$ for all i, j. Since F is a UFD and each $x_i - y_j$ is relatively prime, $\prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j) \,\big|\, R_{f,g}$. Also, $\deg_{x_i} R_{f,g} = n$ and $\deg_{y_j} R_{f,g} = m$, so $R_{f,g} = c\prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j)$ for some $c \in F$. Letting $\beta_j = 0$ for all j, we see $R_{f,g} = f_0^m = \prod_{i=1}^{n}\alpha_i^m$, and thus $c = 1$. □

Corollary 2.4.29.1. Under the same notation above, we have

$$R_{f,g} = \prod_{i=1}^{n} g(\alpha_i) = \prod_{j=1}^{m} f(\beta_j)$$

2.5 Artinian Rings

- In this section, all ring are assumed to be commutative with $1 \neq 0$.

Definition. R is called an **Artinian ring** if it satisfies any of the two equivalent conditions:

1. R satisfies the **descending chain condition (D.C.C.)**.
2. Any nonempty collection of ideals of R has a minimal element.

Example 2.5.1. $\mathbb{Z}$ is Noetherian (since it's PID) but not Artinian; for instance $\mathbb{Z} \supseteq 2\mathbb{Z} \supseteq 4\mathbb{Z} \supseteq \cdots$.

Definition. The **Krull dimension**, or simply dimension, of R is the maximum length, the number of $\subsetneq$, of a chain of prime ideals $P_1 \subsetneq P_2 \subseteq \cdots$.

Example 2.5.2. The Krull dimension of $\mathbb{Z}$ is 1; $0 \subsetneq p\mathbb{Z}$.

Lemma 2.5.3. Let I, J be ideals.

1. If $I + J = (1)$, then $I^k + J^\ell = (1)$ for any $k, \ell \in \mathbb{N}$.
2. If $IJ \subseteq P$ for some prime ideal P, then $I \subseteq P$ or $J \subseteq P$.

Lemma 2.5.4. Let R be an Artinian ring and I an ideal of R. Then R/I is Artinian.

Lemma 2.5.5. Let R, S be Noetherian rings. Then $R \times S$ is Noetherian.

Theorem 2.5.6. Let R be an Artinian ring. Put $J = \operatorname{Jac} R$.

1. the number of maximal ideals in R is finite
2. $R/J \cong$ a product of a finite number of fields
3. Every prime ideal is maximal. In particular, the Krull dimension is 0.
4. J is nilpotent, i.e, $J^n = 0$ for some $n \in \mathbb{N}$. Moreover, $J = \sqrt{0}$
5. $R \cong$ a product of finitely may Artinian local rings
6. R is Noetherian.

Proof.

1. Let $\mathcal{S} := \{M_1 \cap \cdots \cap M_k \mid M_i \text{ is maximal ideals of } R\}$. Since R is Artinian, $\mathcal{S}$ contains a minimal element $I = M_1 \cap \cdots \cap M_n$, where each M_i is maximal.

Claim. $M_1, \dots, M_n$ are the only maximal ideals of R.

Let M be a maximal ideal and consider $M \cap I \in \mathcal{S}$. By the minimality, we have $M \cap I = I$. Then $I \subseteq M$, i.e,

$$M_1 \cap \cdots \cap M_n \subseteq M$$

By Lemma 2.5.3.1, $M = M_j$ for some j.

2. Let $M_1, \dots, M_n$ be the maximal ideals of R. Clearly, $M_i + M_j = (1)$ if $i \neq j$. Then by the Chinese Remainder theorem,

$$R/J \cong R/M_1 \times \cdots \times R/M_n$$

Each term on the right is a field since M_i is maximal.

3. Let P be a prime ideal. It suffices to check if $x \notin P$, then $(x, P) = R$. Consider the chain

$$(x, P) \supseteq (x^2, P) \supseteq (x^3, P) \supseteq \cdots$$

Since R is Artinian, $(x^n, P) = (x^{n+1}, P)$ for some $n \in \mathbb{N}$. In particular, $x^n = rx^{n+1} + a$ for some $r \in R, a \in P$, i.e, $x^n(1 - xr) = a$. Since $x \notin P$, so is x^n, which implies that $1 - xr \in P$, i.e, $1 \in (x, P)$.

4. Consider the chain

$$J \supseteq J^2 \supseteq J^3 \supseteq \cdots$$

Since R is Artinian, $J^n = J^{n+1}$ for some $n \in \mathbb{N}$. We claim $J^n = 0$. Suppose otherwise that $J^n \neq 0$. Let $\mathcal{S} := \{I \trianglelefteq R \mid IJ^n \neq 0\} (\neq \varnothing)$. Since R is Artinian, $\mathcal{S}$ has a minimal element, say I_0. Let $x \in I_0$ such that $xJ^n \neq 0$. Then by the minimality, $I_0 = (x)$. But now $((x)J)J^n = (x)J^{n+1} = (x)J^n$, so by the minimality we have $(x)J = (x)$. By the Nakayama's lemma, $(x) = 0$, a contradiction. Hence $J^n = 0$.

5. Since $J^n = 0$, we have $M_1^n \cdots M_m^n = 0$, where $M_1, \dots, M_m$ are the maximal ideals of R. Then

$$R \cong R/J^n \cong R/M_1^n \times \cdots \times R/M_m^n$$

by Lemma 2.5.3.2 and the Chinese Remainder theorem. Note that the only maximal ideal in R/M_i^n is M_i/M_i^n, and thus R/M_i^n is local. By Lemma 2.5.4, R/M_i^n is Artinian.

6. By 5. and Lemma 2.5.5, it suffices to prove the case when R is an Artinian local ring. Now assume that R is an Artinian local ring with the maximal ideal $M = \operatorname{Jac} R$. By 4., $M^n = 0$ for some $n \in \mathbb{N}$. Then $M^{k-1}/M^k \, (k \leqslant n)$ is a R/M-vector space. Check

   - Artinian implies $\dim_{R/M} M^{k-1}/M^k < \infty$, implying M^{k-1}/M^k is Noetherian as R-modules.

- $I \trianglelefteq S$ as rings $\Rightarrow$ (S is Noetherian $\Leftrightarrow$ I and S/I are Noetherian as S-modules)

□

Corollary 2.5.6.1. R is an Artinian ring if and only if R is Noetherian and of Krull dimension 0.

2.6 Discrete Valuation Rings

Definition. (HW. 13)

1. A **discrete valuation** on a field K is a function $\nu : K^\times \to \mathbb{Z}$ such that

   (a) ν is surjective

   (b) $\nu(xy) = \nu(x) + \nu(y)$ for all $x, y \in K^\times$

   (c) $\nu(x+y) \geqslant \min\{\nu(x), \nu(y)\}$ if $x + y \neq 0$ for all $x, y \in K^\times$

   The subring $\{a \in K^\times \mid \nu(a) \geqslant 0\} \cup \{0\}$ is called the **valuation ring** of ν.

2. An integral domain R is called a **discrete valuation ring (D.V.R.)** if it's the valuation ring of a discrete valuation on its fraction of rings.

Example 2.6.1.

1. $K = \mathbb{Q}$, p : a prime. Define $\nu_p(p^k \frac{a}{b}) = k$. Then the DVR is

$$\left\{p^k \frac{a}{b} \mid k \geqslant 0\right\} \cup \{0\} = \mathbb{Z}_p$$

2. F : a field, $K = F(x)$, $R = F[x]$. For each irreducible polynomial $f \in F[x]$ and for each $r \in F[x]$, $r = f^k \frac{a}{b}$ for some unique $k \in \mathbb{N}$ and $a, b \in F[x]$ with $(a, f) = (b, f) = 1$. Define $\nu_f(r) = k$. The DVR is the localization $F[x]_f$ of $F[x]$ at f consisting of the rational functions in $F(x)$ whose denominator is not divisible by f.

3. $F((x))$: the field of formal Laurent series. $\nu(\sum_{i \geqslant n} a_i x^i) := n$. The DVR is the ring $F[[x]]$ of formal power series. (HW. 13)

4. Fix $z \in \mathbb{C}$ and let $K :=$ { functions meromorphic near z}. $\nu(f) := \operatorname{ord}_z f$. The DVR is the ring of holomorphic functions near z.

Proposition 2.6.2. Let R be a DVR with the valuation ν. Let π be an element in R such that $\nu(\pi) = 1$.

1. nonzero element $a \in R$ is a unit $\Leftrightarrow \nu(a) = 0$ (HW. 13)

2. Every element in R can be written uniquely as $u\pi^n$ for some unit u and $n \geqslant 0$

3. Nonzero ideals are of the form (π^n) for some $n \geqslant 0$. In particular, R is a PID. (HW. 15)

Definition. Let R be a DVR with the valuation ν. An element π with $\nu(\pi) = 1$ is called a **uniformizing parameter** or a **local parameter** of R.

Corollary 2.6.2.1. Let R be a DVR with the valuation.

1. R is a local ring with the unique maximal ideal $M = \{a \in K^\times \mid \nu(a) \geqslant 1\} \cup \{0\}$.
2. The only prime ideals of R are 0 and M. In particular, R has Krull dimension 1.

Theorem 2.6.3. TFAE:

1. R is a DVR.
2. R is a PID with a unique maximal ideal.
3. R is a UFD with a unique irreducible element π up to unit.
4. R is a local Noetherian integral domain whose unique maximal ideal is nonzero and principal.

Proof.

1. $(1 \Rightarrow 2, 3, 4)$ These are clear.
2. $(2 \Rightarrow 3)$ Recall that in a PID, (x) is a maximal ideal $\Leftrightarrow$ x is irreducible.
3. $(3 \Rightarrow 1)$ Define $\nu : R \to \mathbb{Z}$ by $\nu(u\pi^n) = n$.
4. Let M be the unique maximal ideal. We show that for each $x \in R$ there exists a unique integer $n \geqslant 0$ such that $x \in M^n$ but $x \notin M^{n+1}$. Then we may define $\nu : R \to \mathbb{Z}$ by setting $\nu(x) = n$. It suffices to show $M_0 := \bigcap_{n=1}^{\infty} M^n = 0$. Since $MM_0 = M_0$, we have $M_0 = 0$ by Nakayama's lemma (Theorem 2.2.27).

□

2.7 Commutative rings and algebraic geometry

- All rings are commutative rings with identity, and all algebra are commutative algebras.

We recall some basic fact for Noetherian rings:

Proposition 2.7.1. Let R be a Noetherian ring and I be any ideal of R.

1. R/I is Noetherian.
2. $R[x]$ is Noetherian. Thus $R[x_1, \ldots, x_n]$ is Noetherian.

Corollary 2.7.1.1. If k is a field, then $k[x_1, \ldots, x_n]$ is Noetherian.

Proposition 2.7.2. A ring R is a finitely generated k-algebra $\Leftrightarrow$ R is a quotient of some polynomial ring with finitely many variables.

Proof. The if part is clear. For the only if part, say $R = k[r_1, \ldots, r_n]$. Define

$$\begin{aligned} \phi : k[x_1, \ldots, x_n] &\longrightarrow R \\ x_i &\longmapsto r_i \end{aligned}$$

ϕ is clearly surjective, so by the isomorphism theorem we see $R \cong k[x_1, \ldots, x_n]/\ker\phi$. □

2.7.1 Affine algebraic sets

Definition. The set $\mathbb{A}^n$ of n-tuples of elements of k is called the **affine n-space** over k.

- The polynomial ring $k[x_1, \ldots, x_n]$, viewed as a set of functions on $\mathbb{A}^n$, is called the **coordinate ring** of $\mathbb{A}^n$, denoted by $k[\mathbb{A}^n]$.

Definition. Let $S \subseteq k[\mathbb{A}^n]$. The set $\mathcal{Z}(S) := \{p \in \mathbb{A}^n \mid \forall\, f \in S\,[f(p) = 0]\}$ the called the **zero locus/ vanishing set** of S in $\mathbb{A}^n$.

- We say $A \subseteq \mathbb{A}^n$ is an **affine algebraic set** if $A = \mathcal{Z}(S)$ for some $S \subseteq k[\mathbb{A}^n]$.
- When $S = \{f\}$ consists of a single nonconstant polynomial f, then the zero locus, denoted briefly by $\mathcal{Z}(f)$, is called a **hypersurface**.

Example 2.7.3. Let $k = \mathbb{R}$.

1. In $\mathbb{A}^2$, the x-axis is an affine algebraic set $\mathcal{Z}(y)$.

2. The circle $x^2 + y^2 = 1$ is $\mathcal{Z}(x^2 + y^2 - 1)$.

3. $\mathcal{Z}(xy - 1)$ is the hyperbola $xy = 1$.

4. $\mathcal{Z}(0) = \mathbb{A}^n$ and $\mathcal{Z}(1) = \varnothing$.

5. In $\mathbb{A}^1$, $\mathcal{Z}(f)$ is the zeros of f, and is a finite set if $f \neq 0$.

Property 2.7.4. $\mathcal{Z}$ assigns each subset of $k[\mathbb{A}^n]$ to an affine algebraic set, with the properties that

1. if $S \subseteq T \subseteq k[\mathbb{A}^n]$, then $\mathcal{Z}(T) \subseteq \mathcal{Z}(S)$.

2. if $I = (S)$, then $\mathcal{Z}(I) = \mathcal{Z}(S)$.

3. $\bigcap_{i \in I} \mathcal{Z}(S_i) = \mathcal{Z}\left(\bigcup_{i \in I} S_i\right)$.

4. $\mathcal{Z}(S) \cup \mathcal{Z}(T) = \mathcal{Z}(IJ)$, where $I = (S)$ and $J = (T)$.

Therefore every affine algebraic set A is the zero locus of some ideal $I \trianglelefteq k[\mathbb{A}^n]$. Since I a finitely generated, each A is an intersection of finitely many hypersurfaces.

Note that different ideals may have the same locus, e.g, $\mathcal{Z}(x) = \mathcal{Z}(x^2)$. Nevertheless, given an affine algebraic set A, there's a unique largest ideal

$$I = \{f \in k[\mathbb{A}^n] \mid \forall\, p \in \mathbb{A}^n\, [f(p) = 0]\}$$

such that $\mathcal{Z}(I) = A$.

Definition. For any subset $A \subseteq \mathbb{A}^n$, the set $\mathcal{I}(A) = \{f \in k[\mathbb{A}^n] \mid \forall\, p \in \mathbb{A}^n\, [f(p) = 0]\}$ is called the **defining ideal** of A.

Example 2.7.5.

1. In $\mathbb{A}^2$, $\mathcal{I}(x\text{-axis}) = (y)$.

2. $\mathcal{I}((a_1, \ldots, a_n)) = (x_1 - a_1, \ldots, x_n - a_n)$ is a maximal ideal since it's the kernel of the evaluation map at the point $(a_1, \ldots, a_n)$.

3. Let $V = \mathcal{Z}(y^2 - x^3)$. Let's determine $\mathcal{I}(V)$. Note that $V = \{(a^2, a^3) \mid a \in k\}$. Let $f \in k[\mathbb{A}^2]$; we can write it as

   $$f(x, y) = g_0(x) + y g_1(x) + (y^2 - x^3) g_2(x, y)$$

   (this can be seen by passing to the quotient.) Now if $f \in \mathcal{I}(V)$, then $0 = f(x, y) = g_0(a^2) + a^3 g_1(a^2)$ for all $a \in k$. If $\#k = \infty$, we have $g_0 = g_1 = 0$, implying that $\mathcal{I}(V) = (y^2 - x^3)$. Note that when $\#k < \infty$, it's not true. For instance, if $k = \mathbb{F}_2$, we have $V = \{(0, 0), (1, 1)\}$ and $\mathcal{I}(V) = (y - x, x(x - 1)) \neq (y^2 - x^3)$.

Property 2.7.6.

1. If $A \subseteq B \subseteq \mathbb{A}^n$, then $\mathcal{I}(B) \subseteq \mathcal{I}(A)$.
2. $\mathcal{I}(A \cup B) = \mathcal{I}(A) \cap \mathcal{I}(B)$.
3. $\mathcal{I}(\varnothing) = k[\mathbb{A}^n]$. If $\#k = \infty$, $\mathcal{I}(\mathbb{A}^n) = 0$.
4. If $A \subseteq \mathbb{A}^n$, then $A \subseteq \mathcal{Z}(\mathcal{I}(A))$. If $I \subseteq k[\mathbb{A}^n]$, then $I \subseteq \mathcal{I}(\mathcal{Z}(I))$
5. If $V = \mathcal{Z}(I)$, then $V = \mathcal{Z}(\mathcal{I}(V))$. If $I = \mathcal{I}(A)$, then $I = \mathcal{I}(\mathcal{Z}(I))$.

Thus, once we restrict $\mathcal{Z}$ to the defining ideals and $\mathcal{I}$ to the affine algebraic sets, $\mathcal{Z}$ and $\mathcal{I}$ are mutually inverse to each other.

Definition. If $V \subseteq \mathbb{A}^n$ is an affine algebraic set, then the quotient $k[V] := k[\mathbb{A}^n]/\mathcal{I}(V)$ is called the **coordinate ring** of V.

Definition. Let $V \subseteq \mathbb{A}^n$ and $W \subseteq \mathbb{A}^m$ be affine algebraic sets. A map $\varphi : V \to W$ is called a **morphism/ regular map/polynomial map** if there exist $\varphi_1, \ldots, \varphi_m \in k[\mathbb{A}^n]$ such that

$$\varphi(a_1, \ldots, a_n) = (\varphi_1(a_1, \ldots, a_n), \ldots, \varphi_m(a_1, \ldots, a_n))$$

for all $(a_1, \ldots, a_n) \in V$.

- If there exists a morphism $\psi : W \to V$ such that $\varphi \circ \psi = \mathrm{id}_W$ and $\psi \circ \varphi = \mathrm{id}_V$, we say φ is an **isomorphism**.

Let $\varphi : V \to W$ be a morphism. Now if $f \in \mathcal{I}(W)$, then for all $(a_1, \ldots, a_n) \in V$, we have

$$f(\varphi_1(a_1, \ldots, a_n), \ldots, \varphi_m(a_1, \ldots, a_n)) = 0$$

so that $f \circ \varphi \in \mathcal{I}(V)$. This show φ induces a well-defined k-algebra homomorphism

$$\tilde{\varphi} : k[W] \longrightarrow k[V]$$
$$f \longmapsto f \circ \varphi$$

Conversely, suppose we have a k-algebra homomorphism $\Phi : k[W] \to k[V]$. We'll see that Φ is identical with $\tilde{\varphi}$ for some $\varphi : V \to W$. For clarity, let $k[\mathbb{A}^n] = k[x_1, \ldots, x_n]$ and $k[\mathbb{A}^m] = k[y_1, \ldots, y_m]$. Set

$$F_i + \mathcal{I}(V) = \Phi(y_i + \mathcal{I}(W)),\ i = 1, \ldots, m$$

and define $\varphi : \mathbb{A}^n \to \mathbb{A}^m$ by $\varphi = (F_1, \ldots, F_m)$.

- For $g \in \mathcal{I}(W)$, we have $\Phi(g) \in \mathcal{I}(V)$. Also, since g is a polynomial and Φ is a k-algebra homomorphism, we have
$$\mathcal{I}(V) \ni \Phi(g(y_1, \ldots, y_m)) = g(\Phi(y_1), \ldots, \Phi(y_m))$$
so
$$g(F_1(x_1, \ldots, x_n), \ldots, F_m(x_1, \ldots, x_n)) \in \mathcal{I}(V)$$
This follows that for all $(a_1, \ldots, a_n) \in V = \mathcal{Z}(\mathcal{I}(V))$, we have
$$(g \circ \varphi)(a_1, \ldots, a_n) = g(F_1(a_1, \ldots, a_n), \ldots, F_m(a_1, \ldots, a_n)) = 0$$
and thus $\varphi(a_1, \ldots, a_n) \in \mathcal{Z}(\mathcal{I}(W)) = W$, proving that φ is a morphism from V to W.

- For all $g \in k[W]$, we have
$$\begin{aligned}\Phi(g) &= \Phi(g(y_1, \ldots, y_m)) + \mathcal{I}(V) = g(\Phi(y_1), \ldots, \Phi(y_m)) + \mathcal{I}(V) \\ &= g(F_1(x_1, \ldots, x_n), \ldots, F_m(x_1, \ldots, x_n)) + \mathcal{I}(V) \\ &= g \circ \varphi\end{aligned}$$
so that $\tilde{\varphi} = \Phi$.

- Different choices of F_i yield the same φ since the F_i is well-defined modulo $\mathcal{I}(V)$. This also shows the uniqueness of φ with $\tilde{\varphi} = \Phi$ since we must have $(y_i + \mathcal{I}(W)) \circ \varphi = \Phi(y_i + \mathcal{I}(W))$ for every $\varphi : V \to W$ with $\tilde{\varphi} = \Phi$.

Theorem 2.7.7. Let $V \subseteq \mathbb{A}^n$ and $W \subseteq \mathbb{A}^m$ be affine algebraic sets. Then there's a bijective correspondence

$$\{\text{morphisms from } V \text{ to } W\} \longleftrightarrow \{k\text{-algebra homomorphism from } k[W] \text{ to } k[V]\}$$

with the following properties:

1. Every morphism $\varphi : V \to W$ induces a k-algebra homomorphism $\tilde{\varphi} : k[W] \to k[V]$ defined by the pullback, i.e, $f \mapsto f \circ \varphi$.

2. Every k-algebra homomorphism $\Phi : V \to W$ is induced by a unique morphism $\varphi : V \to W$ defined by setting $(y_i + \mathcal{I}(W)) \circ \varphi = \Phi(y_i + \mathcal{I}(W))$.

3. $\varphi : V \to W$ is an isomorphism if and only if $\tilde{\varphi} : k[W] \to k[V]$ is an isomorphism.

Example 2.7.8. Let $\#k = \infty$, $V = \mathbb{A}^1$, $W = \mathcal{Z}(y^2 - x^3) = \{(a^2, a^3) \mid a \in k\}$. The map $\varphi : a \mapsto (a^2, a^3)$ is a bijective morphism, but $\operatorname{Im} \tilde{\varphi} = k + x^2 k[x]$, which is not surjective. Thus φ is not an isomorphism. The inverse map of φ is $\varphi^{-1} : (a, b) \mapsto \begin{cases} 0 & \text{, if } a = b = 0 \\ b/a & \text{, if } a \neq 0 \end{cases}$, which cannot be defined by polynomials.

Corollary 2.7.8.1. Let $\varphi : V \to W$ be a map of affine algebraic sets. Then φ is a morphism $\Leftrightarrow$ for all $f \in k[W]$, $f \circ \varphi$, as a k-valued function on V, coincides with some element in $k[V]$. When φ is a morphism, $\varphi(v) = w$ with $v \in V$ and $w \in W$ if and only if $\tilde{\varphi}^{-1}(\mathcal{I}(\{v\})) = \mathcal{I}(\{w\})$.

Proof. The only if part is clear. For the converse, we first show when $\tilde{\varphi}$ is a k-algebra homomorphism, we have

$$\varphi(v) = w \text{ for } v \in V \text{ and } w \in W \text{ if and only if } \tilde{\varphi}^{-1}(\mathcal{I}(\{v\})) = \mathcal{I}(\{w\})$$

Since $\{w\}$ is an algebraic set, $\{w\} = \mathcal{Z}(\mathcal{I}(\{w\}))$, and thus

$$\varphi(v) = w \text{ if and only if every polynomial } f \text{ vanishing at } w \text{ also vanishes at } \varphi(v)$$

This is equivalent to saying $\tilde{\varphi}(f)$ vanishes at v, so we have $\tilde{\varphi}(\mathcal{I}(\{w\})) \subseteq \mathcal{I}(\{v\})$, or $\mathcal{I}(\{w\}) \subseteq \tilde{\varphi}^{-1}\mathcal{I}(\{v\})$. Since $\mathcal{I}(\{w\})$ and $\mathcal{I}(\{v\})$ are maximal ideals (c.f. Example 2.7.5.2), it's equivalent to $\mathcal{I}(\{w\}) = \tilde{\varphi}^{-1}\mathcal{I}(\{v\})$, as wanted.

Let $\Phi : k[W] \ni f \mapsto f \circ \varphi \in k[V]$; this is clear a k-algebra homomorphism. The theorem above shows there exists a morphism $\varphi' : V \to W$ such that $\tilde{\varphi'} = \Phi$. We claim $\varphi' = \varphi$. Indeed, for each $v \in V$, by the first paragraph we have

$$\varphi'(v) = w = \varphi(v) \Leftrightarrow \tilde{\varphi'}^{-1}\mathcal{I}(\{v\}) = \mathcal{I}(\{w\}) = \tilde{\varphi}^{-1}\mathcal{I}(\{v\})$$

The RHS is clear since we have $\tilde{\varphi} = \Phi = \tilde{\varphi'}$. □

2.7.2 Radicals and affine varieties

For $A \subseteq \mathbb{A}^n$, if $f^k \in \mathcal{I}(A)$ for some $k \in \mathbb{N}$, then $f \in \mathcal{I}(A)$ since k is an integral domain. This suggests us to have the following definition.

Definition. Let $I \trianglelefteq R$ be an ideal.

1. The **radical** of I is the set $\sqrt{I} := \{a \in R \mid a^n \in I \text{ for some } n \in \mathbb{N}\}$.
2. $\sqrt{0}$ is called the **nilradical** of R, the set of nilpotent elements of R.
3. I is called **radical** is $I = \sqrt{I}$.

Property 2.7.9. Let I, J be ideals of R.

1. $\sqrt{I}$ is a ideal containing I.
2. $I \subseteq J \Rightarrow \sqrt{I} \subseteq \sqrt{J}$.

3. $\sqrt{\sqrt{I}} = \sqrt{I}$.

4. $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

5. $\sqrt{I} = (1) \Leftrightarrow I = (1)$.

6. $\sqrt{I + J} = \sqrt{\sqrt{I} + \sqrt{J}}$

7. If I is a prime, then $\sqrt{I} = I$.

8. $\sqrt{I}/I$ is the nilradical of R/I.

9. If $I \neq R$, then
$$\sqrt{I} = \bigcap_{\substack{P \,:\, \text{prime}' \\ I \subseteq P}} P$$
In particular, $\sqrt{0}$ is the intersection of all prime ideals of R.

Proof.

1. That $I \subseteq \sqrt{I}$ is clear. If $x, y \in \sqrt{I}$, say $x^n \in I$ and $y^m \in I$ for some $n, m \in \mathbb{N}$, then $(x+y)^{n+m} \in I$, so $x + y \in \sqrt{I}$. For all $a \in R$, $(ax)^n = a^n x^n \in I$ so $ax \in \sqrt{I}$.

2. Let $x \in \sqrt{I}$. Then $x^n \in I \subseteq J$ for some n, and thus $x \in \sqrt{J}$.

3. We have $\sqrt{I} \subseteq \sqrt{\sqrt{I}}$. For the reverse inclusion, let $x \in \sqrt{\sqrt{I}}$, then by definition there are $n, m \in \mathbb{N}$ such that $x^n \in \sqrt{I}$ and $(x^n)^m \in I$, i.e, $x^{nm} \in I$. Thus $x \in \sqrt{I}$.

4. We have $IJ \subseteq I \cap J$ so $\sqrt{IJ} \subseteq \sqrt{I \cap J}$. If $x \in \sqrt{I \cap J}$, say $x^n \in I \cap J \subseteq I, j$ for some n, then $x \in \sqrt{I} \cap \sqrt{J}$, so that $\sqrt{I \cap J} \subseteq \sqrt{I} \cap \sqrt{J}$. Now if $x \in \sqrt{I} \cap \sqrt{J}$, then there are $m, n \in \mathbb{N}$ such that $x^m \in I$ and $x^n \in J$. Then $x^{n+m} \in IJ$, i.e, $x \in \sqrt{IJ}$.

5. Since $I \subseteq \sqrt{I}$, $I = (1)$ implies $\sqrt{I} = (1)$. Now if $1 \in \sqrt{I}$, then $1 = 1^n \in I$ for some $n \in \mathbb{N}$ so that $I = (1)$.

6. We have $\subseteq$. If $x^n \in \sqrt{I} + \sqrt{J}$, then $x^{nM} \in I + J$ for $M \gg 0$, so that $x \in \sqrt{I + J}$.

7. If $x \in \sqrt{I}$, then $x^n \in I$ for some n. Since I is a prime, $x \in I$.

8. Let $x + I \in R/I$ be nilpotent. Then $x^n + I = I$ for some $n \in I$, i.e, $x^n \in I$. This means $x \in \sqrt{I}$, i.e, $x + I \in \sqrt{I}/I$.

9. Passing to the quotient R/I, it suffices to show the second assertion, which holds by Proposition 2.2.25.

□

Corollary 2.7.9.1. Prime ideals, and hence maximal ideals, are radical.

Corollary 2.7.9.2. If $\sqrt{I}$ and $\sqrt{J}$ are coprime, then I and J are coprime.

Proof. By 5. and 6., $1 = \sqrt{\sqrt{I} + \sqrt{J}} = \sqrt{I + J}$ so that $I + J = 1$. □

Proposition 2.7.10. Let R be Noetherian. Then $\sqrt{I}^n \subseteq I$ for some $n \in \mathbb{N}$. In particular, $\sqrt{0}$ is nilpotent.

Proof. This follows from the fact $\sqrt{I}$ is finitely generated. □

Zariski topology

Definition. Let's specify the *closed sets* of $\mathbb{A}^n$ to be the affine algebraic sets; by Property 2.7.4

1. $\varnothing = \mathcal{Z}(1)$, $\mathbb{A}^n = \mathcal{Z}(0)$.
2. $\bigcap \mathcal{Z}(I_i) = \mathcal{Z}\left(\bigcup I_i\right)$.
3. $\mathcal{Z}(I_1) \cup \mathcal{Z}(I_2) = \mathcal{Z}(I_1 I_2)$.

The topology thus obtained is called the **Zariski topology**.

- The Zariski topology of an affine algebraic set $V \subseteq \mathbb{A}^n$ is defined as the subspace topology inherited from $\mathbb{A}^n$.
- Note that if $I \trianglelefteq k[V]$ is an ideal, then

$$\mathcal{Z}_V(I) := \{(a_1, \ldots, a_n) \in V \mid f(a_1, \ldots, a_n) = 0 \text{ for all } f \in I\} = \mathcal{Z}(\pi^{-1}(I)) \cap V$$

  where $\pi : k[\mathbb{A}^n] \to k[V]$ is the canonical projection, and if $A \subseteq V$ is a subset, then

$$\mathcal{I}_V(A) := \{f \in k[V] \mid f(a_1, \ldots, a_n) = 0 \text{ for all } (a_1, \ldots, a_n) \in A\} = \pi(\mathcal{I}(A))$$

  We can define the Zariski topology in terms of $\mathcal{Z}_V$, and it's clearly the same as the one defined by subspace topology.

Remark 2.7.11. The Zariski topology is very coarse in the sense that there are few open sets. For instance, if $\#k = \infty$, then the Zariski topology is not Hausdorff, since any intersection of two nonempty open sets is nonempty. (Intuitively, a closed set has codimension at least 1.) Note that when $\#k < \infty$, it's precisely the discrete topology.

Proposition 2.7.12. A morphism $\varphi : V \to W$ is continuous with respect to Zariski topology.

Proof. Let $I \subseteq k[W]$ be an ideal. Then

$$\varphi^{-1}(\mathcal{Z}(I)) = \{p \in V \mid f(\varphi(p)) = 0 \text{ for all } f \in I\} = \mathcal{Z}(\tilde{\varphi}(I))$$

is Zariski closed in V. Thus φ is continuous. □

Example 2.7.13. Consider $\mathrm{M}_n(k)$ as $\mathbb{A}^{n^2}$. Then $\mathrm{SL}_n(k)$ is Zariski closed set and $\mathrm{GL}_n(k)$ is Zariski open set. (Note that the determinant is by definition a polynomial of its entries.)

Definition. Let $A \subseteq \mathbb{A}^n$. The **Zariski closure** $\overline{A}$ of A is the smallest closed set containing A. If $A \subseteq V$ for an algebraic set V, we say A is **Zariski dense** if the Zariski closure of A is V.

Proposition 2.7.14. The Zariski closure of a subset A in $\mathbb{A}^n$ is $\overline{A} = \mathcal{Z}(\mathcal{I}(A))$.

Proof. Let V be any algebraic set containing A. Then $\mathcal{Z}(\mathcal{I}(A)) \subseteq \mathcal{Z}(\mathcal{I}(V)) = V$ so that $\mathcal{Z}(\mathcal{I}(A))$ is the smallest closed set containing A. □

Example 2.7.15. As in general topology, a continuous morphism need not be a closed map. For example, consider the morphism $\begin{array}{c} \varphi : \mathcal{Z}(xy-1) \longrightarrow \mathbb{A}^1 \\ (x,y) \longmapsto x \end{array}$. Then $\operatorname{Im}\varphi = k^\times$, which is not closed when $\#k = \infty$.

Proposition 2.7.16. Let $\varphi : V \to W$ be a morphism.

1. $\ker\tilde{\varphi} = \mathcal{I}(\varphi(V))$.
2. $\overline{\varphi(V)} = \mathcal{Z}(\ker\tilde{\varphi}) \cap W$.

Proof.

1. $f \in \ker\tilde{\varphi} \Leftrightarrow f \circ \varphi \in \mathcal{I}(V) \Leftrightarrow f \in \mathcal{I}(\varphi(V))$.
2. $\overline{\varphi(V)} = \mathcal{Z}(\mathcal{I}(\varphi(V))) \cap W = \mathcal{Z}(\ker\tilde{\varphi}) \cap W$.

□

Example 2.7.17. $V = \mathcal{Z}(xy-1)$, $W = \mathbb{A}^1$, $\varphi : V \ni (x,y) \mapsto x \in W$. Then $\ker\tilde{\varphi} = 0$, $\varphi(V) = k^\times$. If $\#k = \infty$, $\mathcal{I}(V) = 0$ and $\mathcal{Z}(0) = A^1 = \overline{\varphi(V)}$.

Affine varieties

Definition. A topological space is **irreducible** if it cannot be written as a union of two proper closed subspaces.

- An irreducible affine algebraic set is called an **affine variety**. (some authors define affine varieties without the irreducibility.)

Proposition 2.7.18. Let V be an affine algebraic set.

1. V is irreducible if and only if $\mathcal{I}(V)$ is a prime ideal in $k[\mathbb{A}^n]$.
2. $V = V_1 \cup \cdots \cup V_m$ for unique irreducible algebraic sets V_j with $V_i \nsubseteq V_j$ if $i \neq j$.

Proof.

1. Let $fg \in \mathcal{I}(V)$. Then $V \subseteq \mathcal{Z}(fg) = \mathcal{Z}(f) \cup \mathcal{Z}(g)$ so that
$$V = (\mathcal{Z}(f) \cap V) \cup (\mathcal{Z}(g) \cap V)$$
The irreducibility implies either $\mathcal{Z}(f) \cap V = V$ or $\mathcal{Z}(g) \cap V = V$, i.e, either $V \subseteq \mathcal{Z}(f)$ or $V \subseteq \mathbb{Z}(g)$. Taking $\mathcal{I}$, we see $f \in \mathcal{I}(V)$ or $g \in \mathcal{I}(V)$. If V is reducible, say $V = V_1 \cup V_2$ with $V_1, V_2 \subsetneq V$. Then $\mathcal{I}(V) \subsetneq \mathcal{I}(V_i)$. Pick $f_i \in \mathcal{I}(V_i) \backslash \mathcal{I}(V)$. Then $f_1 f_2 \in \mathcal{I}(V)$.

2. Let
$$\mathcal{S} := \{\text{algebraic sets } W \mid W \text{ cannot be written as a union of irreducible algebraic sets}\}$$
and let $\mathcal{T} := \{\mathcal{I}(W) \mid W \in \mathcal{S}\}$. If $\mathcal{S}$ is nonempty, since $k[\mathbb{A}^n]$ is Noetherian, $\mathcal{T}$ has an maximal element, and thus $\mathcal{S}$ has a minimal element, say W. In particular, W is not irreducible, say $W = V_1 \cup V_2$ with $V_1, V_2 \subsetneq W$. Since V_1, V_2 are proper, $V_1, V_2 \notin \mathcal{S}$, so they're unions of irreducible algebraic sets, and so is W, a contradiction. Hence $\mathcal{S}$ is empty.

   Now write $V = V_1 \cup \cdots \cup V_m$; we may assume $V_i \nsubseteq V_j$ if $i \neq j$. Now suppose
$$V = V_1 \cup \cdots \cup V_m = U_1 \cup \cdots \cup U_\ell$$
with $V_i \nsubseteq V_j$ and $U_i \nsubseteq U_j$ if $i \neq j$. Consider the intersection
$$V_1 = V_1 \cap V = (V_1 \cap U_1) \cup \cdots \cup (V_1 \cap U_\ell)$$
Since V_1 is irreducible, $V_1 \cap U_j = V_1$ for some j, i.e, $V_1 \subseteq U_j$. Symmetrically, we have $U_j \subseteq V_{j'}$ for some j', so
$$V_1 \subseteq U_j \subseteq V_{j'}$$
and thus $1 = j'$ and $V_1 = U_j$ by our conditions imposed on V_j. Continuing in this way, we conclude $m = \ell$ and $\{V_1, \ldots, V_m\} = \{U_1, \ldots, U_\ell\}$.

□

Corollary 2.7.18.1. Let V be an affine algebraic set. Then V is irreducible if and only if $k[V]$ is an integral domain.

Proof. By Proposition above, V is irreducible $\Leftrightarrow \mathcal{I}(V)$ is a prime $\Leftrightarrow k[V] := k[\mathbb{A}^n]/\mathcal{I}(V)$ is an integral domain. □

Definition. Let V be an irreducible affine algebraic set. The fraction field $\operatorname{Frac} k[V]$ is called the **rational functions** of V and is denoted by $k(V)$.

- The **dimension** of V, denoted by $\dim V$, is defined to be $\operatorname{tr.deg}_k k(V)$.

Primary decomposition

Definition. A proper ideal Q of R is called **primary** if whenever $ab \in Q$ and $a \notin Q$, then $b \in \sqrt{Q}$.

- Equivalently, Q is primary if and only if the zero divisors of R/Q are nilpotent.

Property 2.7.19.

1. Prime ideals are primary.
2. If Q is primary, then $\sqrt{Q}$ is a prime and is the smallest prime containing Q.
3. If Q is an ideal such that $\sqrt{Q}$ is maximal, then Q is primary.
4. If M is a maximal ideal and Q is an ideal with $M^n \subseteq Q \subseteq M$ for some $n \geqslant 1$, then Q is primary and $\sqrt{Q} = M$.

Proof.

2. If $ab \in \sqrt{Q}$, then $a^n b^n \in Q$ for some $n \in \mathbb{N}$. Since Q is primary, $a^n \in Q$ or $b \in \sqrt{Q}$, i.e, $a \in \sqrt{Q}$ or $b \in \sqrt{Q}$. The second assertion follows from Proposition 2.7.9.9.
3. Let $ab \in Q$ but $a \notin Q$. We must show $b \in \sqrt{Q}$. If not, then $(b, \sqrt{Q}) = 1$, i.e, $tb + q = 1$ for some $t \in R$ and $q \in \sqrt{Q}$, so $tab + qa = a$ Thus $Q \ni (qa)^n = (a - tab)^n$ for some n. Expanding, since $ab \in Q$, we see $a \in Q$, a contradiction.
4. Taking radicals, we see $M = \sqrt{M^n} \subseteq \sqrt{Q} \subseteq \sqrt{M} = M$ so that $\sqrt{Q} = M$. By 3., Q is primary.

□

Definition. If Q is a primary ideal, then the prime ideal $P = \sqrt{Q}$ is called the **associated prime** of Q, and we say Q is P-primary.

Proposition 2.7.20. If $Q_1, \ldots, Q_m$ are P-primary, then so is $Q_1 \cap \cdots \cap Q_m$.

Proof. By Property 2.7.9.4, we have

$$\sqrt{Q_1 \cap \cdots \cap Q_m} = \sqrt{Q_1} \cap \cdots \cap \sqrt{Q_m} = P$$

□

Example 2.7.21.

1. In $\mathbb{Z}$, the primary ideals are 0 and (p^m) for p a prime and $m \geqslant 1$.
2. For any field k, (x) is an primary ideal of $k[x, y]$ since it's prime, and $(x, y)^m$ is primary since (x, y) is maximal.
3. $Q = (x^2, y)$ in $k[x, y]$ is primary since $(x, y)^2 \subseteq Q \subseteq (x, y)$ and (x, y) is maximal.
4. In general, however, powers of a prime might not be primary. For instance, $R = k[x, y, z]/(xy - z^2)$. Let $P = (\overline{x}, \overline{z}) \subseteq R$. P is a prime since $R/P \cong k[y]$ is an integral domain. But

   $$P^2 = (\overline{x}^2, \overline{xz}, \overline{xy}) = \overline{x}(\overline{x}, \overline{y}, \overline{z})$$

   is not primary for $\overline{xy} \in P^2$ but $\overline{x} \notin P^2$ and $\overline{y}^n \notin P$ for all $n \geqslant 1$.
5. Also, Q need not be primary when $\sqrt{Q}$ is only a prime. For instance, consider the ideal $I = (x^2, xy)$ in $k[x, y]$. We have $(x)^2 \subseteq I \subseteq (x)$ so $\sqrt{I} = (x)$. But I is not primary: $xy \in I$ but $x \notin I$ and $y^n \notin I$ for all $n \geqslant 1$.

   Though (x^2, xy) is not primary, $(x^2, xy) = (x) \cap (x, y)^2$ is an intersection of primary ideals.
6. Let R be a UFD and π an irreducible element of R. Then the (π) is a prime and (π^n) is primary for each $n \in \mathbb{N}$. Conversely, let Q be a (π)-primary ideal, and $n \in \mathbb{N}$ be the largest integer with $Q \subseteq (\pi^n)$ (n exists since $\sqrt{Q} = (\pi)$.) If $q \in Q \backslash (\pi^{n+1})$, then $q = r\pi^n$ for some $r \in R$ and $r \notin (\pi)$. Since Q is (π)-primary and $r \notin (\pi)$, we see $\pi^n \in Q$, and thus $Q = (\pi^n)$. This generalizes 1.

Definition.

1. An ideal I in R has a **primary decomposition** if it may by written as a finite intersection of primary ideals, that is,

   $$I = \bigcap_{i=1}^{m} Q_i$$

   with Q_i being primary.

2. A primary decomposition is **minimal/irredundant/reduced** if $\bigcap_{j\neq i} Q_j \nsubseteq Q_i$ and $\sqrt{Q_i} \neq \sqrt{Q_j}$ if $i \neq j$.

- If I has primary decomposition, then by Proposition 2.7.20, the decomposition can be made minimal by eliminating the superfluous primary ideals involved.

Definition. A proper ideal I is **irreducible** if I cannot be written as an intersection of two ideals strictly containing I.

Example 2.7.22.

1. A prime ideal P is irreducible: suppose $P = I \cap J$ for some $P \subsetneq I, J$. Then pick $a \in I\backslash P$, $b \in J\backslash P$; thus
$$ab \in IJ \subseteq I \cap J = P$$
Since P is a prime, $a \in P$ or $b \in P$, a contradiction.

2. The notion of irreducible ideals is related to that of irreducible affine algebraic sets as follows: If V is an irreducible affine algebraic set, then $\mathcal{I}(V)$ is a prime ideal, and hence irreducible. Conversely, when k is algebraically closed, if I is irreducible, then $\mathcal{Z}(I)$ is irreducible.

   Proof. By Proposition 2.7.18.1, it suffices to show $\mathcal{I}(\mathcal{Z}(I))$. By Hilbert's Nullstellensatz, $\mathcal{I}(\mathcal{Z}(I)) = \sqrt{I}$. By Lemma 2.7.24, I is primary, and thus $\sqrt{I}$ is a prime. □

3. The above is not true when k isn't algebraically closed. For instance, when $k = \mathbb{R}$, consider $f(x, y) = (x^2 - 1)^2 + y^2$ and its zero locus $\mathcal{Z}(f)$. We see f is irreducible over $k[x, y]$ so that (f) is prime by Proposition 2.3.22. By 1., (f) is irreducible. Also,
$$\mathcal{Z}(f) = \mathcal{Z}((x-1)^2 + y^2) \cup \mathcal{Z}((x+1)^2 + y^2)$$
so $\mathcal{Z}(f)$ is not irreducible. (One can see $\mathcal{Z}(f)$ is even not connected.)

4. Being irreducible is not necessarily prime. For instance, for p a prime in $\mathbb{Z}$, (p^n) is irreducible but not a prime: say $(p^n) = (a) \cap (b) = (\text{lcm}(a, b))$. Then one of (a), (b) is (p^n).

5. Being primary is not necessarily irreducible. For instance, $(x, y)^2 \subseteq k[x, y]$ is (x, y)-primary but not irreducible since $(x, y)^2 = (x^2, y) \cap (x, y^2)$.

Lemma 2.7.23. If R is Noetherian, then every ideal is a finite intersection of irreducible ideals of R.

Proof. Suppose otherwise, then the collection

$$\mathcal{S} = \{I \trianglelefteq R \mid I \text{ is not a finite intersection of irreducible ideals}\}$$

is nonempty, so $\mathcal{S}$ admits a maximal element, say I. Since I cannot be irreducible, $I = J \cap K$ for some $J, K \supsetneq I$. The maximality implies J, K can be written as finite intersections of irreducible ideals, and so is I, a contradiction. □

Lemma 2.7.24. If R is Noetherian, then every irreducible ideal is primary.

Proof. Let $I \trianglelefteq R$ be irreducible. Suppose $ab \in I$ and $a \notin I$. We must show $b \in \sqrt{I}$. Consider the ascending chain of ideals

$$(I : b) \subseteq (I : b^2) \subseteq \cdots$$

Since R is Noetherian, there's an integer n such that $(I : b^n) = (I : b^N)$ for all $N \geqslant n$.

Claim. $(a, I) \cap (b^n, I) = I$ (so that $b^n \in I$ since I is irreducible.)

Let $v \in (a, I) \cap (b^n, I)$. Then $v = ax + y = b^n z + w$ for some $x, z \in R$, $y, w \in I$. Multiplying b gives

$$vb = abx + by + b^{n+1}z + wb$$

so $b^{n+1}z = abx + by - wb \in I$, i.e, $z \in (I : b^{n+1}) = (I : b^n)$. Thus $v = b^n z + w = w \in I$. □

Lemma 2.7.25. Let Q be a P-primary ideal and $x \in R$. Then

1. $x \in Q \Rightarrow (Q : x) = (1)$.
2. $x \notin Q \Rightarrow (Q : x)$ is P-primary.
3. $x \notin P \Rightarrow (Q : x) = Q$.

Proof.

2. If $y \in (Q : x)$, then $xy \in Q$. Since $x \notin Q$, we have $y \in \sqrt{Q} = P$. Hence $Q \subseteq (Q : x) \subseteq P$. Taking radicals gives $P = \sqrt{(Q : x)}$. Now if $ab \in (Q : x)$ and $a \notin (Q : x)$, then $abx \in Q$, i.e, $a^n b^n x^n \in P$ for some $n \geqslant 1$. Since $x \notin P$, $a \notin (Q : x) \subseteq P$, we see $b^n \in P$, so $b \in P$.
3. If $a \in (Q : x)$, then $ax \in Q$. Since $x \notin \sqrt{Q} = P$, $a \in Q$.

□

Theorem 2.7.26. Let I has a minimal primary decomposition $I = Q_1 \cap \cdots \cap Q_m$. Let $P_i = \sqrt{Q_i}$ for $i = 1, \ldots, m$. Then the P_i are precisely the prime ideals occurring in the set $\{\sqrt{(I : x)} \mid x \in R\}$, so that the P_i are independent of the particular decomposition of I.

Proof. For $x \in R$, we have $(I : x) = (\bigcap Q_i : x) = \bigcap (Q_i : x)$ so that by Lemma 2.7.25 we have $\sqrt{(I : x)} = \bigcap P_i$. If $\sqrt{(I : x)}$ is a prime, then $\sqrt{(I : x)} = P_i$ for some i. Conversely, for each i there exists $x_i \in \bigcap_{j \neq i} Q_j \backslash Q_i$ since the decomposition is minimal, and thus $(Q_i : x)$ is P_i-primary by Lemma again. □

Corollary 2.7.26.1. Let R be Noetherian. Then every proper ideal admits a minimal primary decomposition, and is unique in the following sense: let $I = \bigcap_{m} Q_i = \bigcap_{n} Q'_j$ be minimal primary decompositions. Then

$$n = m \text{ and } \left\{\sqrt{Q_i}\right\} = \left\{\sqrt{Q_j}\right\}$$

and for prime ideals P that are minimal in the set above, the P-primary components of the decomposition are the same.

Proof. All assertions result from the above Lemma and Theorem except for the last one, which will be proved by localization in the follow section. □

Definition. The prime ideals P_i are called the **associated primes** of I. The minimal elements of the set $\{P_1, \ldots, P_m\}$ are called the **isolated primes** of I and the others are called **embedded primes**.

- The isolated primes of $I \trianglelefteq k[\mathbb{A}^n]$ correspond to the irreducible components of $\mathcal{Z}(I)$, maximal irreducible subspaces, and the embedded primes are irreducible subspaces of these components.

Proposition 2.7.27. Let I be a proper ideal in R. Suppose I has a minimal decomposition.

1. A prime ideal P contains I if and only if P contains one of the associated primes of I.
2. The isolated primes of I are precisely the minimal elements of the set of all primes containing I. In particular, there are only finitely many minimal prime ideals containing I.
3. $\sqrt{I} = \bigcap_{P\text{:ass. primes of } I} P = \bigcap_{P\text{:iso. primes of } I} P.$
4. If R is Noetherian, then there are primes $P_1, \ldots, P_m$ of R containing I such that $P_1 \cdots P_m \subseteq I$.

Proof. Let $I = Q_1 \cap \cdots \cap Q_n$ be a minimal primary decomposition of I and $P_i = \sqrt{Q_i}$ for $i = 1, \ldots, n$.

1. $I \subseteq P \Leftrightarrow Q_1 \cap \cdots \cap Q_n \subseteq P \Leftrightarrow P_1 \cap \cdots \cap P_n \subseteq P \Leftrightarrow P_i \subseteq P$ for some i.
2. These are clear.
3. This follows from 1., 2, and Property 2.7.9.4 and 9.
4. By Proposition 2.7.10, $\sqrt{I}^{\ell} \subseteq I$ for some $\ell \geqslant 1$. Then $P_1^{\ell} \cdots P_n^{\ell} \subseteq I$.

□

2.7.3 Integral extensions and Hilbert's Nullstellensatz

Definition. Let $R \subseteq S$ be commutative rings with $1_R = 1_S$.

1. $s \in S$ is said to be **integral over** R if there exists a monic polynomial $f \in R[x]$ such that $f(s) = 0$.
2. S is an **integral extension** of R if every element in S is integral over R.
3. The **integral closure of R in S** is the set $\{s \in S \mid s \text{ is integral over } R\}$.
4. R is **integrally closed in** S if the integral closure of R in S is R itself.
5. When R is an integral domain, we say R is **integrally closed/normal** if R is integrally closed over its fraction field $\operatorname{Frac} R$.

Example 2.7.28. $R = \mathbb{Z}[\sqrt{-3}]$ is not normal; $\dfrac{-1+\sqrt{3}i}{2} \notin R$ but it's a root of $x^2 + x + 1$.

Proposition 2.7.29. Let $R \subseteq S$ as before. TFAE:

1. $s \in S$ is integral over R.
2. $R[s]$ is a finitely generated R-module.
3. $s \in T$ and $R \subseteq T \subseteq S$ for some subring T of S that is also a finitely generated R-module.

Proof. The direction $1 \Rightarrow 2 \Rightarrow 3$ is clear. For $3 \Rightarrow 1$, let $T = \langle v_1, \ldots, v_n \rangle_R$. Since T is a ring, $sv_i \in T$ and thus

$$sv_i = \sum_{j=1}^{n} a_{ij} v_j,\ i = 1, \ldots, n$$

for some $a_{ij} \in R$. Hence

$$0 = \sum_{j=1}^{n} (s\delta_{ij} - a_{ij}) v_j,\ i = 1, \ldots, n$$

i.e, $0 = (s\delta_{ij} - a_{ij})_{ij} v$, where $v = (v_1 \ \cdots \ v_n)^t$. Multiplying by the adjoint of $(s\delta_{ij} - a_{ij})_{ij}$ to both sides, we obtain $\det(s\delta_{ij} - a_{ij})v = 0$. Since $1 \in T$, 1 is a R-combination of the v_i so that $\det(s\delta_{ij} - a_{ij}) = 0$. Hence s is a root of the monic polynomial $\det(x\delta_{ij} - a_{ij}) \in R[x]$. □

Corollary 2.7.29.1. Let $R \subseteq S$ as above.

1. If $s, t \in S$ are integral over R, then so are $s + t, as$.
2. The integral closure of R in S is a subring of S.

3. If $R \subseteq S \subseteq T$ with S integral over R and T integral over S, then T is integral over R.

Proof.

1. Since $R[s], R[t]$ are finitely generated R-modules, so are $R[s+t]$ and $R[st]$.
2. This follows from 1.
3. Let $t \in T$. Then $t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0 = 0$ for some $a_i \in S$. Since S is integral over R, $R[a_{n-1}, \ldots, a_0]$ is a finitely generated R-module, and thus $R[t, a_{n-1}, \ldots, a_0]$ is a finitely generated R-module. Since $R \subseteq R[t, a_{n-1}, \ldots, a_0] \subseteq T$, the above Proposition shows $t \in T$ is integral over R.

□

Corollary 2.7.29.2. The integral closure of R is S is integrally closed in S.

Proof. Let R' be the integral closure of R in S and R'' the one of R' in S. Now we have $R \subseteq R' \subseteq R''$. Corollary above shows R'' is integral over R so that $R'' \subseteq R'$, and thus $R' = R''$. □

Example 2.7.30. A finite field extension K of $\mathbb{Q}$ is called a **number field**. Then the ring of integers $\mathcal{O}_K$ of K over $\mathbb{Q}$ is integrally closed. For example, when $K = \mathbb{Q}[\sqrt{-3}]$, $\mathcal{O}_K = \mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$. (c.f. Example 2.1.8)

Example 2.7.31. Let $R \subseteq S$ as above.

1. If R, S are fields, then S is integral over R if and only if S/R is an algebraic extension.
2. If S is integral over R and $I \trianglelefteq S$ is an ideal, then S/I is integral over $R/R \cap I$.
3. If R is a UFD, then it's integrally closed. (Proposition 2.4.9.)
   - Since $\mathbb{Z}[\sqrt{-3}]$ is not integrally closed, $\mathbb{Z}[\sqrt{-3}]$ is not a UFD.
   - By Gauss' lemma, $k[x_1, \ldots, x_n]$ is a UFD, so it's integrally closed.
   - $k[x,y]/(y^2 - x^3)$ is not integrally closed, though it's an integral domain: $(\overline{y}/\overline{x})^2 - \overline{x} = 0$ but $\overline{y}/\overline{x} \notin k[x,y]/(y^2 - x^3)$.

Definition. Let $\varphi : R \to S$ be a ring homomorphism of commutative rings with 1.

1. If $I \trianglelefteq R$, then $I^e := \varphi(I)S \trianglelefteq S$ is called the **extension** of I to S.
2. If $J \trianglelefteq S$, then $J^c := \varphi^{-1}(J) \trianglelefteq R$ is called the **contraction** of J in R.

- When $R \subseteq S$ and $\varphi : R \to S$ is the inclusion, we have $I^e = IS$ and $J^c = J \cap R$.

Property 2.7.32. Let I, I_1, I_2 be ideals of R and J, J_1, J_2 ideals of S.

1. $I \subseteq I^{ec}$, $J \supseteq J^{ce}$.
2. $I = I^{ece}$, $J = J^{cec}$.
3. The set $\mathcal{C}$ of contracted ideals in R is $\{I \mid I^{ec} = I\}$ and the set $\mathcal{E}$ of extended ideals in R is $\{J \mid J^{ce} = J\}$. Moreover, $I \mapsto I^e$ is a bijective map of $\mathcal{C}$ onto $\mathcal{E}$, with inverse $J \mapsto J^c$.
4.
$$\begin{array}{cc} (I_1 + I_2)^e = I_1^e + I_2^e & (J_1 + J_2)^c \supseteq J_1^c + J_2^c \\ (I_1 \cap I_2)^e \subseteq I_1^e \cap I_2^e & (J_1 \cap J_2)^c = J_1^c \cap J_2^c \\ (I_1 I_2)^e = I_1^e I_2^e & (J_1 J_2)^c \supseteq J_1^c J_2^c \\ (I_1 : I_2)^e \subseteq (I_1^e : I_2^e) & (J_1 : J_2)^c \subseteq (J_1^c : J_2^c) \\ \sqrt{I}^e \subseteq \sqrt{I^e} & \sqrt{J}^c = \sqrt{J^c} \end{array}$$

Proof.

1. $\varphi(I) \subseteq I^e$ so that $I \subseteq \varphi^{-1}(\varphi(I)) \subseteq I^{ec}$. Since $J \supseteq \varphi(J^c)$ and J is an ideal, $J \supseteq J^{ce}$.
2. This follows from 1.
3. If $I \in \mathcal{C}$, say $I = J^c$, then $I^{ec} = J^{cec} = J^c = I$. If $J \in \mathcal{E}$, say $J = I^e$, then $J^{ce} = I^{ece} = I^e = J$. If $I_1, I_2 \in \mathcal{C}$ are such that $I_1^e = I_2^e$, then $I_1 = I_1^{ec} = I_2^{ec} = I_2$. For $J \in \mathcal{E}$, $J^c \in \mathcal{C}$ such that $(J^c)^e = J$. This shows the bijectivity of $I \mapsto I^e$ of $\mathcal{C}$ onto $\mathcal{E}$.
4.
   - Let $\varphi(r)s \in (I_1 : I_2)^e$ with $r \in (I_1 : I_2)$, $s \in S$. Then $\varphi(r)sI_2^e \subseteq \varphi(r)\varphi(I_2)S \subseteq \varphi(I_1)S = I_1^e$. If $r \in (J_1 : J_2)^c$, then $\varphi(r)J_2 \subseteq J_1$. Taking inverse image gives $rJ_2^c \subseteq J_1^c$.
   - Let $\varphi(r)s \in \sqrt{I}^e$ with $r \in \sqrt{I}$, $s \in S$. Then $r^n \in I$ for some $n \geqslant 1$ and $\varphi(r^n)s^n \in \varphi^I S = I^e$. Taking radicals gives $\varphi(r)s \in \sqrt{I^e}$. If $r \in \sqrt{J^c}$, then $r^n \in J^c$ for some $n \geqslant 1$ and $\varphi(r)^n \in J$. Taking radicals gives $\varphi(r) \in \sqrt{J}$, and thus $r \in \sqrt{J}^c$. For the reverse inclusion, let $r \in \sqrt{J}^c$. Then $\varphi(r)^n \in J$ for some $n \geqslant 1$, i.e, $r^n \in J^c$. Hence $r \in \sqrt{J^c}$. (the essence is that φ is a ring homomorphism.)

□

Example 2.7.33. The above inclusion can be strict. Here are some examples.

1. $\mathbb{Z} \subseteq \mathbb{Q}$, $I = n\mathbb{Z}$, $n \neq 0$. Then $n\mathbb{Z} = I \subsetneq I\mathbb{Q} \cap \mathbb{Z} = \mathbb{Z}$. Also, when $n = p$, $I\mathbb{Q}$ is either a prime ideal nor a maximal ideal.

2. $\mathbb{Z} \subseteq \mathbb{Z}[i]$, $J = (1+i)$. We have $J \cap \mathbb{Z} = (2)$ so that $(J \cap \mathbb{Z})Z[i] = 2\mathbb{Z}[i]$. We see $J \subsetneq 2\mathbb{Z}[i]$ is proper.

Lemma 2.7.34. Let $R \subseteq S$ be commutative rings with $1_S = 1_R$ and S be integral over R. If D is multiplicatively closed set in R containing 1, then $D^{-1}S$ is integral over $D^{-1}R$.

Proof. Let $\dfrac{x}{y} \in D^{-1}S$. Since $x \in S$, $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$ for some $a_i \in R$. Then

$$\left(\frac{x}{y}\right)^n + \frac{a_{n-1}}{y}\left(\frac{x}{y}\right)^{n-1} + \cdots + \frac{a_1}{y^{n-1}}\left(\frac{x}{y}\right) + \frac{a_0}{y^n} = 0$$

so that $\dfrac{x}{y} \in D^{-1}S$ is integral over $D^{-1}R$. □

Theorem 2.7.35. Let $R \subseteq S$ be commutative rings with $1_S = 1_R$ and S be integral over R.

1. If S is an integral domain, then S is a field if and only if R is a field.
2. For P a prime in R, there exists a prime Q in S such that $Q \cap R = P$. Moreover, P is maximal if and only if Q is maximal.
3. (Going-up) If $P_1 \subseteq P_2$ are primes of R and Q_1 is a prime of S such that $Q_1 \cap R = P_1$, then there's a prime Q_2 of S such that $Q_1 \subseteq Q_2$ and $Q_2 \cap R = P_2$.
4. (Going-down) Suppose S is an integral domain and R is integrally closed in R. If $P_1 \subseteq P_2$ are primes of R and Q_2 is a prime of S such that $Q_2 \cap R = P_2$, then there's a prime Q_1 of S such that $Q_1 \subseteq Q_2$ and $Q_1 \cap R = P_1$.

Proof.

1. Let $r \in R\backslash\{0\}$. Then $r^{-1} \in S$ so that $(r^{-1})^n + a_{n-1}(r^{-1})^{n-1} + \cdots + a_1 r^{-1} + a_0 = 0$ for some $a_i \in R$. Multiplying by r^{n-1} gives $r^{-1} = -(a_0 r^{n-1} + \cdots + a_{n-1}) \in R$. Conversely, let $s \in S\backslash\{0\}$. Then $s^n + a_{n-1}s^{n-1} + \cdots + a_1 s + a_0 = 0$ for some $a_i \in R$; assume that $a_0 \neq 0$ (it's the step that being an integral domain matters). Then $s \cdot \dfrac{-1}{a_0}(s^{n-1} + \cdots + a_1) = 1$ so that s is invertible.
2. We first prove the second part. Since Q is a prime, S/Q is an integral domain, and since S is integral over R, S/Q is integral over $R/Q^c = R/P$. By 1., S/Q is a field if and only if R/P, i.e, Q is maximal if and only if P is maximal. For the first part, let $D = R\backslash P$. Consider the commutative diagram

$$\begin{array}{ccc} D^{-1}R & \hookrightarrow & D^{-1}S \\ \uparrow{\scriptstyle \alpha} & & \uparrow{\scriptstyle \beta} \\ R & \hookrightarrow & S \end{array}$$

By Lemma, $D^{-1}S$ is integral over $D^{-1}R$. Let M be a maximal ideal of $D^{-1}S$. Then $M^c = M \cap D^{-1}R$ is also maximal by the second part. Since $D^{-1}R$ is a local ring, $M^c = D^{-1}P$ is the unique maximal ideal. Then the prime ideal $\beta^{-1}(M)$ has the property that $\beta^{-1}(M) \cap R = \alpha^{-1}(M^c) = P$, as wanted.

3. S/Q_1 is integral over R/P_1 and P_2/P_1 is a prime of R/P_1. The result follows from 2.

4. (...)

□

Remark 2.7.36. The prime ideal in 2. is not unique. For example, $R = \mathbb{Z}$, $S = \mathbb{Z}[i]$, $P = 5\mathbb{Z}$. Then Q can be $(1 + 2i)$ or $(1 - 2i)$.

Theorem 2.7.37. Let $R \subseteq S$ be commutative rings with $1_S = 1_R$ and assume S is integral over R and is a finitely generated R-algebra. If P is maximal, then

$$0 < \#\{Q \trianglelefteq S \mid Q \text{ is maximal}, Q \cap R = P\} < \infty$$

Proof. The nonzero part follows from 2. of the Theorem above. Now if Q is maximal in S such that $Q \cap R = P$, then $R/P \subseteq S/Q$ is a field extension. Since S/Q is integral over R/P, it's also algebraic. Denote by $\overline{R/P}$ an algebraic closure of R/P. Each maximal ideal Q of S such that $Q \cap R = P$ gives rise to a distinct pair (K, ϕ), where $K \subseteq \overline{R/P}$ is a subfield and $\phi : S \to K$ is a ring homomorphism such that $\phi|_R = \bmod P$, pictorially

$$\begin{array}{ccccc} R & \hookrightarrow & S & \xrightarrow{\phi} & S/Q =: K \subseteq \overline{R/P} \\ \uparrow & & \uparrow & & \\ P = Q \cap R & \hookrightarrow & Q & & \end{array}$$

so that

$$\#\{Q \trianglelefteq S \mid Q \text{ is maximal}, Q \cap R = P\} \leqslant \#\{(K, \phi) \mid K \subseteq \overline{R/P},\ \phi \in \mathrm{Hom}_{(\mathbf{Ring})}(S, K) \text{ with } \phi|_R = \bmod P\}$$

Let $\mathcal{F} = \{(K, \phi) \mid K \subseteq \overline{R/P},\ \phi \in \mathrm{Hom}_{(\mathbf{Ring})}(S, K) \text{ with } \phi|_R = \bmod P\}$. We contend $\mathcal{F}$ is a finite set. Assume $S = R[s_1, \ldots, s_m]$. Since S is integral over R, there are monic polynomial $f_j = x^{n_j} + \cdots + a_{j,0} \in R[x]$ such that $f_j(s_j) = 0$. If $(K, \phi) \in \mathcal{F}$, then $0 = \phi(f_j(s_j)) = \phi(s_j)^{n_j} + \cdots + \overline{a_{j,0}}$ (here $\overline{a_{j,i}} := a_{j,i} \bmod P$). This means $\phi(s_j)$ is a root of $\overline{f_j(x)}$ in $\overline{R/P}$. Since there are only finitely many roots of $\overline{f_j}$, we conclude $\#\mathcal{F} < \infty$. □

Example 2.7.38. Given a prime P in R, we make use of the proof above to find primes Q in S lying over P.

1. $R = \mathbb{Z}$, $S = \mathbb{Z}[i]$, $P = 5\mathbb{Z}$, $R/P = \mathbb{F}_5$, $f(x) = x^2 + 1$. Then $\phi(i) \in \{\text{roots of } x^2+1 \text{ in } \overline{\mathbb{F}_5}\} = \{2, -2\}$.
   - $\phi(i) = 2$ so that $\phi(i-2) = 0$. This means $i - 2 \in Q$, and thus $Q = (5, i-2) = (1+2i)$.
   - $\phi(i) = -2 \rightsquigarrow Q = (5, i+2) = (1-2i)$.
2. $R = \mathbb{Z}$, $S = \mathbb{Z}[i]$, $P = 2\mathbb{Z}$, $R/P = \mathbb{F}_2$, $f(x) = x^2 + 1 = (x-1)^2$ in $\overline{\mathbb{F}_2}$. Then $Q = (2, i-1) = (1+i)$. (Note that $2\mathbb{Z}[i] = (1+i)^2$). If $P = 7\mathbb{Z}$, x^2+1 has not root in $\mathbb{F}_7$ but in $\mathbb{F}_{49}$. We then see $Q = (7)$.
3. $R = \mathbb{Z}$, $S = \mathbb{Z}[\sqrt[3]{2}]$, $f(x) = x^3 - 2$, $P = 5\mathbb{Z}$. We have $x^3 - 2 = (x-3)(x^2 - 2x - 1)$ in $\mathbb{F}_3$. Thus $Q = (5, \sqrt[3]{2} - 3) = (\sqrt[3]{4} + 1)$ or $Q = (5, \sqrt[3]{4} - 2\sqrt[3]{2} - 1) = (\sqrt[3]{4} - 2\sqrt[3]{2} - 1)$.

Algebraic integers

Proposition 2.7.39. An element α in some field extension of $\mathbb{Q}$ is an algebraic integer if and only if it's algebraic over $\mathbb{Q}$ and $m_{\alpha,\mathbb{Q}} \in \mathbb{Z}[x]$.

Proof. The if part is clear. For the converse, let $g(x) \in \mathbb{Z}[x]$ be a monic polynomial such that $g(\alpha) = 0$; suppose g has the minimal degree. If g is reducible over $\mathbb{Q}$, then by Gauss' lemma, g is reducible over $\mathbb{Z}$, contradicting to the minimality of g. Hence g is irreducible over $\mathbb{Q}$. Since $m_{\alpha,\mathbb{Q}} \mid g$, we conclude $g = m_{\alpha,\mathbb{Q}}$. □

Proposition 2.7.40. Let K be a number field.

1. As a vector space over $\mathbb{Q}$, K has a basis consisting of elements in $\mathcal{O}$.
2. Let $I \subset \mathcal{O}_K$ be a non-trivial ideal. Then as an abelian group, it is of rank $[K : \mathbb{Q}]$. In particular, $\mathcal{O}_K$ is Noetherian.
3. $\mathcal{O}_K$ is a Dedekind domain, i.e, Noetherian, integrally closed and of Krull dimension 1.

Proof.

1. Let $\alpha \in K \backslash \mathbb{Q}$ and $m_{\alpha,\mathbb{Q}}(x) = a_n x^n + \cdots + a_1 x + a_0$. Consider the polynomial
$$(a_n x)^n + a_{n-1}(a_n x)^{n-1} + \cdots + a_n^{n-2} a_1 (a_n x) + a_n^{n-1} a_0$$
From this, we see that $a_n x$ is a root of the monic polynomial
$$y^n + a_{n-1} y^{n-1} + \cdots + a_n^{n-2} a_1 y + a_n^{n-1} a_0$$
implying that $a_n x \in \mathcal{O}$. We've proved that for any $\alpha \in K$, $m\alpha \in \mathcal{O}$ for some $m \in \mathbb{Q}^\times$. Now given any basis $\{\alpha_1, \ldots, \alpha_n\}$ for $K/\mathbb{Q}$, $\{m_i \alpha_i \mid i = 1, \ldots, n\}$ is a basis for $K/\mathbb{Q}$, where $m_i \in \mathbb{Q}^\times$ is such that $m_i \alpha_i \in \mathcal{O}$.

2. Let $\{v_1, \ldots, v_n\} \subseteq \mathcal{O}$ be a basis of $K/\mathbb{Q}$; this exists by (a). Put $\mathrm{Emb}(K/\mathbb{Q}) = \{\sigma_1, \ldots, \sigma_n\}$. For $x \in \mathcal{O}$, write

$$x = a_1 v_1 + \cdots + a_n v_n$$

where $a_i \in \mathbb{Q}$ is to be determined. Applying σ_i gives a system a equations

$$\begin{cases} \sigma_1(x) = & a_1\sigma_1(v_1) + \cdots + a_n\sigma_1(v_n) \\ \sigma_2(x) = & a_1\sigma_2(v_1) + \cdots + a_n\sigma_2(v_n) \\ \quad \vdots & \\ \sigma_n(x) = & a_1\sigma_n(v_1) + \cdots + a_n\sigma_n(v_n) \end{cases}$$

Put $D = \det(\sigma_i v_j)$ and D_i to be the determinant of the matrix obtained by replacing the i-th column of the matrix $(\sigma_i v_j)$ by $(\sigma_1(x) \cdots \sigma_n(x))^t$. By Cramer's rule, we have $a_i = D_i/D$ for $i = 1, \ldots, n$, i.e, $a_i D^2 = D_i D$. Since $x, v_j \in \mathcal{O}$, so are $\sigma_i(x), \sigma_i(v_j) \in \mathcal{O}$, and thus $D_i, D \in \mathcal{O}$. Also, note that $(\sigma_i v_j)(\sigma_i v_j)^t = (\mathrm{tr}_{K/\mathbb{Q}}(v_i v_j))$ and $\mathrm{tr}_{K/\mathbb{Q}}(v_i v_j) \in \mathbb{Q}$, so that $D^2 = \det(\mathrm{tr}_{K/\mathbb{Q}}(v_i v_j)) \in \mathbb{Q}$. Hence $a_i D^2 = D_i D \in \mathbb{A} \cap \mathbb{Q} = \mathbb{Z}$.

So far we've shown that for each $x \in \mathcal{O}$, there exist $m_i \in \mathbb{Z}$ such that

$$x = \frac{1}{D^2}(m_1 v_1 + \cdots + m_n v_n)$$

equivalently, $\mathcal{O} \subseteq \dfrac{1}{D^2}\mathbb{Z}\langle v_1, \ldots, v_n\rangle$. On the other hand, we have $\mathbb{Z}\langle v_1, \ldots, v_n\rangle \subseteq \mathcal{O}$. Combining these gives

$$\mathbb{Z}\langle v_1, \ldots, v_n\rangle \subseteq \mathcal{O} \subseteq \frac{1}{D^2}\mathbb{Z}\langle v_1, \ldots, v_n\rangle$$

Both RHS and LHS are free abelian groups of rank n, forcing $\mathcal{O}$ itself to be a free abelian group of rank n, as wanted.

For each $\alpha \in I$, we have $\alpha\mathcal{O} \subseteq I \subseteq \mathcal{O}$. Again, RHS and LHS are free abelian groups of rank n, and thus so is I. In particular, I is finitely generated $\mathbb{Z}$-module. Hence $\mathcal{O}$ is Noetherian.

3. Let $\alpha \in P \backslash \{0\}$. Then $m := \mathrm{N}_{K/\mathbb{Z}}(\alpha) = \alpha\beta \in \mathbb{Z}$ for some $\beta \in \mathcal{O}_K$, so $m \in P$, and thus $\mathcal{O}_K/P \subseteq \mathcal{O}_K/(m)$. Since $\mathcal{O}_K$ has rank n, $\#\mathcal{O}_K/(m) = m^n < \infty$, and thus $\mathcal{O}_K/P$ is a finite integral domain, i.e, a field. Hence P is a prime.

It remains to show $\mathcal{O}_K$ is integrally closed. Since $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K, $\mathcal{O}_K$ is integrally closed in K. Since $K = \mathrm{Frac}\,\mathcal{O}_K$, we are done.

□

Definition. A $\mathbb{Z}$-basis for $\mathcal{O}_K$ is called an **integral basis** for $\mathcal{O}_K$ (or K).

Example 2.7.41.

1. Let $D \neq 1$ be square-free. Then an integral basis for $\mathbb{Q}[\sqrt{D}]$ is $\{1, \omega\}$, where

$$\omega = \begin{cases} \sqrt{D} & , \text{if } D \equiv 2, 3 \pmod 4 \\ \dfrac{1+\sqrt{D}}{2} & , \text{if } D \equiv 1 \pmod 4 \end{cases}$$

   (c.f. Example 2.1.8.)

2. An integral basis for $\mathbb{Q}(\zeta) = \mathbb{Q}(e^{2\pi i/n})$ is $1, \zeta, \ldots, \zeta^{\phi(n)-1}$.

Hilbert's Nullstellensatz

Theorem 2.7.42 (Noether's normalization lemma)**.** Let $A = k[r_1, \ldots, r_m]$ be a finitely generated k-algebra. Then there exist $y_1, \ldots, y_d \in A\,(0 \leqslant d \leqslant m)$ such that the y_i are algebraically independent and A is integral over $k[y_1, \ldots, y_d]$.

Proof. We prove this by induction on m.

1° $m = 1$: Suppose $A = k[r]$. If r is algebraically independent over k, pick $y_1 = r$. Otherwise, r is algebraic over k so that A is integral over k.

2° $m > 1$: If $r_1, \ldots, r_m$ is algebraically independent over k, then done. Otherwise, there's a nonzero $f \in k[x_1, \ldots, x_m]$ such that $f(r_1, \ldots, r_m) = 0$. Renumbering the subscripts, if necessary, we assume $f(x_1, \ldots, x_m)$ is not a constant in the variable x_m. Let $d = \deg f$, the maximum of the total monomial degrees. For $j = 1, \ldots, m-1$, define

$$X_j := x_j - x_m^{(1+d)^j}$$

For each monomial $x_1^{e_1} \cdots x_m^{e_m}$, we have

$$\begin{aligned} x_1^{e_1} \cdots x_m^{e_m} &= (X_1 + x_m^{1+d})^{e_1} \cdots (X_{m-1} + x_m^{(1+d)^{m-1}})^{e_{m-1}} x_m^{e_m} \\ &= x_m^{e_m + e_1(1+d) + \cdots + e_{m-1}(1+d)^{m-1}} + \cdots \end{aligned}$$

Note that different $(e_1, \ldots, e_m)$ give polynomials in $X_1, \ldots, X_{m-1}, x_m$ with the different highest degrees of x_m.

Now write

$$g(X_1, \ldots, X_{m-1}, x_m) = f(X_1 + x_m^{e_1(1+d)^1}, \ldots, x_m^{e_m}) = c x_m^N + \sum_{j=0}^{N-1} h(X_1, \ldots, X_{m-1}) x_m^j$$

for non-zero $c \in k$. For $j = 1, \ldots, m-1$, let $s_j = r_j - r_m^{(1+d)^j}$. Then $\frac{1}{c}g(s_1, \ldots, s_{m-1}, r_m) = \frac{1}{c}f(r_1, \ldots, r_m) = 0$, i.e, r_m is integral over $B := k[s_1, \ldots, s_{m-1}]$. By induction hypothesis, there exists $y_1, \ldots, y_d$, $(0 \leqslant d \leqslant m-1)$ such that $y_1, \ldots, y_d$ are algebraically independent over k and B is integral over $k[y_1, \ldots, y_d]$ and thus A is integral over $k[y_1, \ldots, y_d]$.

□

Corollary 2.7.42.1 (Zariski's lemma)**.** Let K/k be a field extension. If K is finitely generated as k-algebras, it's a finite field extension.

Proof. By normalization lemma, $k \subseteq k[y_1, \ldots, y_d] \subseteq K$ with K integral over $k[y_1, \ldots, y_d]$ for some algebraically independent elements $y_1, \ldots, y_d$ over k. Since K is a field, Theorem 2.7.35.1 implies $k[y_1, \ldots, y_d]$ is a field, and thus $d = 0$, i.e, K is algebraic over k. Since K is finitely generated as k-algebra, $[K : k]$ is finite. □

Theorem 2.7.43 (Hilbert's Nullstellensatz - Weak form)**.** Let k be an algebraically closed field. Then $M \trianglelefteq k[x_1, \ldots, x_n]$ is a maximal ideal if and only if $M = (x_1 - a_1, \ldots, x_n - a_n)$ for some $a_i \in k$. Equivalently, we have the bijection

$$\{\text{points in } \mathbb{A}^n\} \underset{\mathcal{Z}}{\overset{\mathcal{I}}{\rightleftarrows}} \{\text{maximal ideals in } k[\mathbb{A}^n]\}$$

Moreover, if I is any proper ideal of $k[x_1, \ldots, x_n]$, then $\mathcal{Z}(I) \neq \varnothing$.

Proof. Clearly, $M = (x_1 - a_1, \ldots, x_n - a_n)$ is a maximal ideal. Conversely, let M be any maximal ideal of $k[x_1, \ldots, x_n]$. Then $K := k[x_1, \ldots, x_n]/M$ is a field of finite degrees. By Noether's normalization lemma, there exist $y_1, \ldots, y_d \in K$, $(0 \leqslant d \leqslant n)$ being algebraically independent over k such that K is integral over $k[y_1, \ldots, y_d]$. Since K is a field, so is $k[y_1, \ldots, y_d]$, and thus $d = 0$, i.e, K is algebraic over k. Since k is algebraically closed, $K = k$, i.e, $k[x_1, \ldots, x_m]/M \cong k$. Then for each j, $x_i - a_j \in M$ for some $a_j \in k$. Hence $M = (x_1 - a_1, \ldots, x_n - a_n)$. The moreover part is clear. □

Theorem 2.7.44 (Hilbert's Nullstellensatz)**.** Let k be an algebraically closed field. Then $\mathcal{I}(\mathcal{Z}(I)) = \sqrt{I}$ for every ideal of $I \trianglelefteq k[x_1, \ldots, x_n]$. Moreover, we have the bijection

$$\{\text{affine algebraic sets}\} \underset{\mathcal{Z}}{\overset{\mathcal{I}}{\rightleftarrows}} \{\text{radical ideals in } k[\mathbb{A}^n]\}$$

Proof. It remains to show $\mathcal{I}(\mathcal{Z}(I)) \subseteq \sqrt{I}$. Assume $g \in \mathcal{I}(\mathcal{Z}(I))$ and $I = (f_1, \ldots, f_m)$. Introduce a new indeterminate x_{m+1}, and consider the ideal

$$I' = (f_1, \ldots, f_m, gx_{m+1} - 1) \trianglelefteq k[x_1, \ldots, x_n, x_{n+1}]$$

Then $\mathcal{Z}(I') = \varnothing$. By the weak form, $(f_1, \ldots, f_m, gx_{m+1} - 1) = k[x_1, \ldots, x_n, x_{n+1}]$. In particular, $1 = a_1 f_1 + \cdots + a_m f_m + a_{m+1}(gx_{m+1} - 1)$ for some $a_j \in k[x_1, \ldots, x_{m+1}]$. Let $y = \dfrac{1}{x_{m+1}}$. Then

$$y^N = b_1 f_1 + \cdots + b_m f_m + b_{m+1}(g - y)$$

for $N >> 0$ and $b_i \in k[x_1, \ldots, x_m, y]$. Substituting g for y gives $g^N \in I \subseteq k[x_1, \ldots, x_n]$, i.e, $g \in \sqrt{I}$. □

Corollary 2.7.44.1. If k is a field with algebraic closure $\overline{k}$ and $I \trianglelefteq k[x_1, \ldots, x_n]$, the $\mathcal{I}_k(\mathcal{Z}_{\overline{k}}(I)) = \sqrt{I}$, where $\mathcal{Z}_{\overline{k}}(I)$ is the zero locus of I in $\overline{k}^n$ and $\mathcal{I}_k(\mathcal{Z}_{\overline{k}}(I))$ is the defining ideal of $\mathcal{Z}_{\overline{k}}(I)$ in $k[x_1, \ldots, x_n]$. Moreover, $I = (1)$ if and only if there are no common zeros in $\overline{k}^n$ of I.

Proof. It follows from Theorem 2.7.35.2 and Property 2.7.9.9 that if $R \subseteq S$ are commutative rings with $1_S = 1_R$ and S is integral over R, then

$${}_S\sqrt{IS} \cap R =_R \sqrt{I}$$

Since $\overline{k}[x_1, \ldots, x_n]$ is integral over $k[x_1, \ldots, x_n]$, the result follows from the Nullstellensatz.

□

2.7.4 Localization

Chapter 3

Field theory and Galois theory

3.1 Field Extensions

Definition. The **characteristic** of a ring R with 1 is defined to be the smallest positive p, denoted by $\operatorname{Char} R$ such that $\underbrace{1+1+\cdots+1}_{p} = 0$. If no such integer exists, we define the characteristic to be 0.

Proposition 3.1.1. If R is an integral domain with $1 \neq 0$, then $\operatorname{Char} R = 0$ or a prime. Moreover, if $\operatorname{Char} R = p$, then $p\alpha = 0$ for all $\alpha \in R$. (HW. 14)

Proposition 3.1.2. Let F be a field. If $\operatorname{Char} F = 0$, then F contains a subfield isomorphic to $\mathbb{Q}$. If $\operatorname{Char} F = p$, then F contains a subfield isomorphic to $\mathbb{Z}/p\mathbb{Z}$. (HW. 15)

Definition. In the preceding proposition, $\mathbb{Q}$ or $\mathbb{Z}/p\mathbb{Z}$ is called the **prime field** of F.

Notation 3.1.3. We denote $\mathbb{Z}/p\mathbb{Z}$ as $\mathbb{F}_p$, a field of order p.

Definition. If K is a field containing a subfield F, we say K **is an extension field of** F and denote it by K/F (not confused with the quotient). Sometimes we call F the **base field** of the extension.

Definition. Given K/F and $\alpha, \beta, \gamma, \ldots \in K$, the smallest subfield of K containing $\alpha, \beta, \gamma, \ldots$ is called the **subfield generated by** $\alpha, \beta, \gamma, \ldots$ **over** F, and is denoted by $F(\alpha, \beta, \gamma, \ldots)$.

- If $K = F(\alpha)$ for some $\alpha \in K$, we say K is a **simple extension of** F and α is the **primitive element** for the extension K/F.
- Note that we may regard K as a *vector space over* F, and we call $\dim_F K$ the **degree of the extension**, and denote it by $[K : F]$.
- We say K/F is a **finite extension** if $[K : F] < \infty$.

Proposition 3.1.4. If $\varphi : F \to F'$ is a field homomorphism, i.e, a ring homomorphism that sends 1 to 1, then either $\varphi \equiv 0$ or φ is injective. Hence, either $\varphi(F) = 0$ or $\varphi(F) \cong F$.

Theorem 3.1.5. Let $p \in F[x]$ be irreducible. Then there exists an extension field K/F such that p has a root in K. More precisely, there's a field K containing a subfield $\tilde{F} \cong F$ and $\tilde{p}$ has a root in K, where $\tilde{p}$ is the image of p under the natural isomorphism $F[x] \cong \tilde{F}[x]$.

Proof. Let $K = F[x]/(p(x))$. Then $x + (p(x))$ is a root of p in K. □

Definition. Given K/F, an element $\alpha \in K$ is called **algebraic over** F if α is a root of some nonzero polynomial in $F[x]$. Otherwise, α is called transcendental over F.

- If all elements of K are algebraic over F, then we say K is an **algebraic extension** of F.

- When speaking of **algebraic numbers**, we always refer to those that are algebraic over $\mathbb{Q}$.

Example 3.1.6. 1. π is transcendental over $\mathbb{Q}$. (Lindemann)

2. e is transcendental over $\mathbb{Q}$. (Hermite)

3. $\sqrt{\pi}$ is algebraic over $\mathbb{Q}(\pi)$.

Proposition 3.1.7. Let α be algebraic over F. Then there's a unique monic irreducible polynomial, denoted as $m_{\alpha,F}$, in $F[x]$ such that α is a root of it. Moreover, if α is a root of $f \in F[x]$, then $m_{\alpha,F} \mid f$.

Proof. Let $I_\alpha = \{f \in F[x] \mid f(\alpha) = 0\}$. Clearly $I_\alpha \trianglelefteq F[x]$, and thus there's a unique monic polynomial $m_{\alpha,F}$ such that $I_\alpha = (m_{\alpha,F}(x))$. That $m_{\alpha,F}$ is irreducible follows from the uniqueness. □

Definition. The polynomial $m_{\alpha,F}$ in the preceding proposition is called the **minimal polynomial of** α **over** F.

- The **degree of** α **over** F is defined to be $\deg_F \alpha := \deg m_{\alpha,F}$.

Theorem 3.1.8. Let α be algebraic over F and $n := \deg_F \alpha$. Then

1. $F(\alpha) \cong F[x]/(m_{\alpha,F}(x))$.

2. $1, \alpha, \ldots, \alpha^{n-1}$ form a basis for $F(\alpha)$ over F. In particular, $[F(\alpha) : F] = n$.

Proof. Consider the homomorphism

$$\phi : F[x] \ni f(x) \mapsto f(\alpha) \in F(\alpha)$$

Note $\ker \phi = (m_{\alpha,F}(x))$, so $F[x]/(m_{\alpha,F}(x)) \cong \operatorname{Im} \phi$. Also, $\operatorname{Im} \phi$ contains F and α, so ϕ is surjective, implying that $F[x]/(m_{\alpha,F}(x)) \cong \operatorname{Im} \phi = F(\alpha)$. For the second statement, it's clear that every element in $F[x]/(m_{\alpha,F}(x))$ can be represented by some polynomial of degree $\leqslant n-1$. In view of the isomorphism $F[x]/(m_{\alpha,F}(x)) \cong F(\alpha)$, this means $1, \alpha, \ldots, \alpha^{n-1}$ spans $F(\alpha)$. To show the linear independence, let $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = 0$ for $a_j \in F$. Then $\underbrace{m_{\alpha,F}}_{\deg = n} \mid \underbrace{a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}}_{\deg \leqslant n-1}$, and thus $a_j = 0$. □

Example 3.1.9. 1. $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$, $\deg = 2$

2. $\mathbb{Q}[x]/(x^2-2) \cong \mathbb{Q}(\sqrt{2})$, $\deg = 2$

3. $\mathbb{Q}[x]/(x^3-2) \cong \mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q}(\sqrt[3]{(e^{2\pi i/3})}) \cong \mathbb{Q}(\sqrt[3]{(e^{-2\pi i/3})})$, $\deg = 3$

4. $\mathbb{F}_2/(x^2+x+1)$ is a field of 4 elements since the degree of the extension over $\mathbb{F}_2$ is 2.

Proposition 3.1.10. α is algebraic over $F \Leftrightarrow [F(\alpha) : F] < \infty$.

Proof. The only if part follows from Theorem 3.1.8. If α is transcendental, then $1, \alpha, \alpha^2, \ldots$ are linearly independent over F, implying that $[F(\alpha) : F] = \infty$. □

Corollary 3.1.10.1. If $[K : F] < \infty$, then K/F is an algebraic extension.

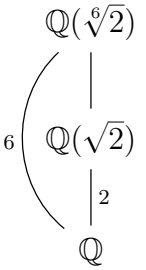
Theorem 3.1.11. For extensions $L \text{ —— } K \text{ —— } F$, it satisfies $[L : F] = [L : K][K : F]$.

Proof. The cases $[L : K]$ or $[K : F]$ is infinity are trivial. Suppose that $[L : K] = m$ and $[K : F] = n$, say $\{\alpha_1, \ldots, \alpha_m\}$ is a basis for L over K and $\{\beta_1, \ldots, \beta_n\}$ for K over F.

Claim. $S = \{\alpha_i \beta_j \mid i = 1, \ldots, m,\ j = 1, \ldots, n\}$ is a basis for L over F.

□

Example 3.1.12. 1. $\sqrt[3]{2} \notin \mathbb{Q}[\sqrt{2}]$ since $\deg_{\mathbb{Q}} \sqrt[3]{2} = 3$ but $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

2. 

, and thus $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}(\sqrt{2})] = 3 \Rightarrow \deg_{\mathbb{Q}(\sqrt{2})} \sqrt[6]{2} = 3$ and $m_{\sqrt[6]{2}, \mathbb{Q}(\sqrt{2})}(x) = x^3 - \sqrt{2}$

Theorem 3.1.13. An extension K/F is finite $\Leftrightarrow$ K is generated by a finite number of algebraic numbers over F. Moreover, a field generated by $\alpha_1, \ldots, \alpha_k$ of degree $n_1, \ldots, n_k$ over F has degree $\leqslant n_1 \cdots n_k$ over F.

Proof. Consider field extensions

$$F \subseteq F(\alpha_1) \subseteq F(\alpha_1, \alpha_2) \subseteq \cdots \subseteq F(\alpha_1, \alpha_2, \ldots, \alpha_k) = K$$

By Theorem 3.1.11,

$$[K : F] = [F(\alpha_1) : F][F(\alpha_1, \alpha_2) : F(\alpha_1)] \cdots [K : F(\alpha_1, \alpha_2, \ldots, \alpha_{k-1})] \leqslant n_1 n_2 \cdots n_k < \infty$$

□

Corollary 3.1.13.1. If α, β are algebraic over F, so are $\alpha \pm \beta,\ \alpha\beta,\ \dfrac{\alpha}{\beta}\,(\beta \neq 0)$. In particular, given K/F, the set of elements in K algebraic over F forms a subfield of K.

Example 3.1.14. Let $\overline{\mathbb{Q}}$ be the set of all algebraic numbers in $\mathbb{C}$. Then $\overline{\mathbb{Q}}$ is an algebraic extension of $\mathbb{Q}$ but not a finite extension of $\mathbb{Q}$ since, for instance, $\overline{\mathbb{Q}}$ contains $\sqrt[n]{2}$ for any $n \in \mathbb{N}$.

Theorem 3.1.15. If L/K and K/F are algebraic, so is L/F.

Proof. Let $\alpha \in L$ and put $m_{\alpha,K}(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. Then $\deg_{F(\alpha,a_0,\ldots,a_{n-1})} \alpha = n$, and thus

$$\begin{aligned}
[F(\alpha), F] &\leqslant [F(\alpha, a_0, \ldots, a_{n-1}) : F] \\
&\leqslant [F(\alpha, a_0, \ldots, a_{n-1}) : F(a_0, \ldots, a_{n-1})][F(a_0, \ldots, a_{n-1}), F] \\
&\leqslant n \prod_{j=0}^{n-1} \deg_F a_j < \infty \text{ since } a_j \in K \text{ and } K/F \text{ is algebraic}
\end{aligned}$$

□

Definition. Let K_1, K_2 be subfields of K. The **composite of K_1 and K_2**, denoted by K_1K_2, is the smallest subfield of K containing K_1, K_2.

Proposition 3.1.16. Let K_1, K_2 be subfields of K containing F. Then $[K_1K_2 : F] \leqslant [K_1 : F][K_2 : F]$. Moreover, the equality holds when $\gcd([K_1 : F], [K_2 : F]) = 1$.

Proof. Put $m = [K_1 : F]$ and $n = [K_2 : F]$. Let $\{\alpha_1, \ldots, \alpha_m\}$ and $\{\beta_1, \ldots, \beta_n\}$ be bases for K_1 and K_2 over F, respectively.

Claim. $\{\alpha_i\beta_j \mid 1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant n\}$ spans K_1K_2.

If $\gcd([K_1 : F], [K_2 : F]) = 1$, $m, n \mid [K_1K_2 : F]$ implies $mn \mid [K_1K_2 : F]$, and hence $mn \leqslant [K_1K_2 : F]$. □

3.1.1 Constructible numbers

Definition. A real number is **constructible** if it can be constructed using a straightedge and a compass.

- The three geometric problems of ancient Greek mathematics
  1. Doubling a cube $\rightsquigarrow$ whether $\sqrt[3]{2}$ is constructible.
  2. Trisecting an angle $\rightsquigarrow$ whether $\cos\dfrac{\theta}{3}$ is constructible given any $\cos\theta$.
  3. Squaring a cube $\rightsquigarrow$ whether $\sqrt{\pi}$ is constructible.
- Note that if a, b are constructible, so are $a \pm b, ab, \dfrac{a}{b}$ and $\sqrt{a}$.

Proposition 3.1.17. α is constructible $\Leftrightarrow [\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^k$ for some $k \in \mathbb{N}$.

Example 3.1.18. The minimal polynomial for $e^{2\pi i/7}$ over $\mathbb{Q}$ is $x^6+x^5+\cdots+1$, and thus $[\mathbb{Q}(e^{2\pi i/7}) : \mathbb{Q}] = 6$. Also, $[\mathbb{Q}(e^{2\pi i/7}) : \mathbb{Q}(\cos\frac{2\pi}{7})] = 2$ since $2\cos\frac{2\pi}{7} = e^{2\pi i/7} + e^{-2\pi i/7}$. Hence $[\mathbb{Q}(\cos\frac{2\pi}{7}) : \mathbb{Q}] = 3$, implying that $\cos\frac{2\pi}{7}$ is not constructible by Proposition 3.1.17.

Question 3.1.19. For which n can we draw a regular n-gon using a straightedge and a compass? Equivalently, for which n is $\cos\frac{2\pi}{n}$ constructible, i.e, $[\mathbb{Q}(\cos\frac{2\pi}{n}) : \mathbb{Q}]$ a power of 2, i.e,

$$\textit{for which } n \textit{ is } [\mathbb{Q}(e^{2\pi i}/n) : \mathbb{Q}] \textit{ a power of } 2\textit{?}$$

We'll see that

$$[\mathbb{Q}(e^{2\pi i}/n) : \mathbb{Q}] = \phi(n)$$

and clearly, $\phi(n) = 2^k \Leftrightarrow n = 2^m p_1 \dots p_k$ with $p_i - 1 = 2^{m_i}$, $m_i \geqslant 1$.

Definition. A prime of the form $2^k + 1$ is called a **Fermat prime**.

Observation 3.1.20. If k is divisible by any odd integer $\geqslant 3$, then 2^k+1 is composite, via the factorization $x^m + 1 = (x + 1)(x^{m-1} - x^{m-2} + \cdots + 1)$.

- Hence, a Fermat prime is necessarily of the form $2^{2^k} + 1$, which we will denote by F_k.
- $F_0 = 3,\ F_1 = 5,\ F_2,\ F_3 = 257,\ F_4 = 65537$ are primes.
- Fermat conjectured that all F_k are primes; however, this conjecture is way off. In fact, now it's believed that those above are the only Fermat primes.

3.1.2 Splitting Fields and Algebraic Closures

Definition. Let $f \in F[x]$. If K is an extension field of F such that f *splits completely* in $K[x]$ and no proper subfield of K possesses this property, we say K is a **splitting field of f over F**.

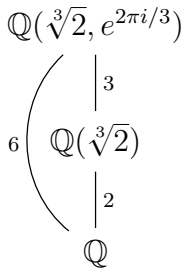
Theorem 3.1.21. A splitting field for $f \in F[x]$ exists.

Proof. We prove this by induction on $n = \deg f$ for each polynomial over any field. The case $n = 1$ is trivial. In general, let g be an irreducible factor of f over F. By Theorem 3.1.5, there exists an extension E/F such that g admits a root α_1 in E. Write $f(x) = (x - \alpha_1)f_1(x)$ for some $f_1 \in E[x]$. Now $\deg f_1 = \deg f - 1 < \deg f$, so by the induction hypothesis, there exists an extension E'/E such that E' is a splitting field for f_1 over E. Hence, f splits completely in $E'[x]$. Let K be the smallest subfield of E' containing all roots of f and F. Such K is what we desire. □

Proposition 3.1.22. If K is a splitting field for $f \in F[x]$, then $[K : F] \leqslant n!$, where $n = \deg f$.

Remark 3.1.23. The bound is in general the best. Consider $x^3 - 2 \in \mathbb{Q}[x]$. Its splitting field is

$$\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}e^{2\pi i/3}, \sqrt[3]{2}e^{-2\pi i/3}) = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$$

Then 

, and thus $[\mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3}) : \mathbb{Q}] = 6 = 3!$.

Example 3.1.24. Let p be a prime. A splitting field of $x^{p-1} + \cdots + 1 = \dfrac{x^p - 1}{x - 1}$ over $\mathbb{Q}$ is $\mathbb{Q}(e^{2\pi i/p})$ since all roots are of the form $e^{2\pi ik/p}$, $k = 1, \ldots, p-1$, and thus $[\mathbb{Q}(e^{2\pi i/p}), \mathbb{Q}] = p - 1$.

Definition. If K/F is an algebraic extension such that K is a splitting field for a collection of polynomial in $F[x]$, then we say K is a **splitting field**, or **normal field**, of F.

Lemma 3.1.25. Assume that $F \cong_\phi F'$, let p be an irreducible polynomial in $F[x]$ and put $p' = \phi(p) \in F'[x]$. Let α, α' be roots of p, p' in some extension fields, respectively. Then ϕ can be extended to an isomorphism from $F(\alpha)$ to $F'(\alpha')$.

Proof. Consider the isomorphism

$$\Phi : F(\alpha) \cong F[x]/(p(x)) \cong_\phi F'[x]/(p'(x)) \cong F'(\alpha')$$

where the first and the third isomorphisms are as in Theorem 3.1.8. Then Φ is an extension of ϕ. □

Theorem 3.1.26. Assume that $F \cong_\phi F'$ and extend ϕ to $F[x]$ naturally. Let $f \in F[x]$ and put $f' := \phi(f)$. Let E, E' be splitting fields of f, f' over F, F', respectively. Then ϕ can be extended to an isomorphism from E to E'.

Proof. We prove this by induction on $n = \deg f$ for each polynomial over any field. The case $n = 1$ is simply Lemma 3.1.25. For the general case, let g be an irreducible factor of f in $F[x]$ and put $g' = \phi(g)$. Then g' is an irreducible factor of f' in $F'[x]$. Let α, α' be roots of g, g' in E, E', respectively. By Lemma 3.1.25, ϕ can be extended to an isomorphism, denoted by ϕ_1, from $F_1 := F(\alpha)$ to $F_1' := F'(\alpha')$. Now write $f(x) = (x - \alpha)h(x)$ and $f'(x) = (x - \alpha')h'(x)$ for some $h \in F_1[x]$ and $h' \in F_1'[x]$. Note that $\deg h = \deg f - 1 < \deg f$ and $h' = \phi_1(h)$. By the induction hypothesis, ϕ_1 can be extended to an isomorphism, denoted by Φ, from E, a splitting field of h, to E', a splitting field of h'. Then $\Phi : E \to E'$ is an isomorphism extending ϕ. □

Corollary 3.1.26.1. Any splitting fields for $f \in F[x]$ are isomorphic, and the isomorphism may be chosen so that it fixes F pointwise.

Proof. This follows from Theorem 3.1.26 with $\phi = \mathrm{id}_F$. □

Definition. An **algebraic closure** of a field F, denoted by $\overline{F}$, is an algebraic extension of F such that each polynomial over F splits completely over $\overline{F}$.

Definition. A field K is **algebraically closed** if each polynomial over K admits a root in K.

Proposition 3.1.27. An algebraic closure of a field is algebraically closed.

Proof. Let F be a field, $f(x) = \sum_{i=0}^{n} a_i x^i \in \overline{F}[x]$ and α be a root of f in some extension of $\overline{F}$. Then α is algebraic over $K = F(a_0, \ldots, a_n)$, and K is algebraic over F, so α is algebraic over F. Hence $\alpha \in \overline{F}$. □

Example 3.1.28.

1. $\overline{\mathbb{Q}} = \{\text{algebraic numbers}\}$ is an algebraic closure of $\mathbb{Q}$.
2. The *Fundamental theorem of algebra* states that $\mathbb{C}$ is algebraically closed.

Theorem 3.1.29. Let F be a field. Then an algebraic closure of F exists. Moreover, if K, K' are two algebraic closures of F, then there exists a field isomorphism between K and K' that fixes F pointwise.

Proof. Let $S := \{\text{algebraic extensions of } F\}$, partially ordered by set-theoretic inclusion. By the Zorn's lemma S has a maximal element, say, K. Then K is an algebraic closure of F, which can be shown by an argument similar to the proof of Proposition 3.1.27. For the moreover part, we let

$$T := \{(E, \psi) \mid E \text{ is a subfield of } K,\ \psi : E \cong E' \text{ for some subfield } E' \text{ of } K'\}$$

and define a partial order on T by

$$(E_1, \psi_1) \leqslant (E_2, \psi_2) \Leftrightarrow E_1 \subseteq E_2 \ \wedge\ \psi_2|_{E_2} = \psi_1$$

Let $\mathcal{C}$ be a chain in T. Let $E_0 = \bigcup_{(E,\psi)\in\mathcal{C}} E$, $E_0' = \bigcup_{(E,\psi)\in\mathcal{C}} E'$ and define $\psi_0 : E_0 \to E_0'$ by for all $x \in E_0$, $\psi_0(x) := \psi(x)$ for some ψ whose associated subfield E contains x.

- ψ_0 is well-defined by the definition of $\leqslant$ on T.
- ψ_0 is clearly an isomorphism from E_0 to E_0'.
- $(E, \psi) \leqslant (E_0, \psi_0)$ for each $(E, \psi) \in \mathcal{C}$.

Hence $(E_0, \psi_0) \in T$ is an upper bound for $\mathcal{C}$. By the Zorn's lemma, T has a maximal element, say, (K_0, ϕ_0).

Claim. $K_0 = K$ and $\operatorname{Im}\phi_0 = K'$.

- Suppose otherwise that $K_0 \subsetneq K$. Pick $\alpha \in K \setminus K_0$ and put $p := m_{\alpha,K_0} \in K_0[x]$. Also, put $p' := \phi_0(p)$ and let α' be a root of p' in K'. Then by Lemma 3.1.25 we can extend ϕ_0 to an isomorphism from $K_0(\alpha) \supsetneq K_0$ to $K_0'(\alpha') \subseteq K'$, a contradiction to the maximality of (K_0, ϕ_0).
- Note that $\operatorname{Im}\phi_0 \subseteq K'$ is also an algebraic closure of F, which forces that $\operatorname{Im}\phi_0 = K'$ since it cannot be extended algebraically.

□

3.1.3 Separable and Inseparable Extensions

Example 3.1.30. $x^2 - 2 \in \mathbb{Q}[x]$ defines an extension $\mathbb{Q}(\sqrt{2})$ of degree 2 over $\mathbb{Q}$, and has two distinct roots $\pm\sqrt{2}$ in $\mathbb{Q}(\sqrt{2})$. On the other hand, $x^2 - t \in \mathbb{F}_2(t)[x]$ also defines an extension $\mathbb{F}_2(t)(\sqrt{t}) = \mathbb{F}_2(\sqrt{t})$ of degree 2 over $\mathbb{F}_2(t)$; however, $x^2 - t = (x - \sqrt{t})^t$ has a (and the only) repeated root $\sqrt{t}$ in $\mathbb{F}_2(\sqrt{t})$.

Definition. A polynomial over a field is **separable** if it has no repeated roots in its splitting field. A polynomial which is not separable is called **inseparable**.

Definition. Let $f(x) = \sum_{i=0}^{n} a_i x^i \in F[x]$. The **formal derivative** Df of f is $Df := \sum_{i=1}^{n} i a_i x^{i-1} \in F[x]$.

Property 3.1.31. Let $f, g \in F[x]$.

1. $D(f+g) = Df + Dg$
2. $D(fg) = fDg + gDf$

Proposition 3.1.32. $f \in F[x]$ has a repeated root $\alpha \Leftrightarrow Df(\alpha) = 0$. In particular, f is separable if and only if f and Df are relatively prime.

Corollary 3.1.32.1. Every irreducible polynomial over a field of characteristic 0 is separable.

Corollary 3.1.32.2. An irreducible polynomial f over a field F of characteristic p is inseparable if and only if $f(x) = g(x^p)$ for some $g \in F[x]$.

Example 3.1.33. In $\mathbb{F}_2(t)[x]$, $D(x^2 - t) = 2x = 0$. Thus $x^2 - t$ has a repeated root.

Proposition 3.1.34. Let F be a field of characteristic p. Then $F \ni a \mapsto a^p$ is a field endomorphism on F.

Corollary 3.1.34.1. If F is a finite field of characteristic p, then $F \ni a \mapsto a^p$ is a field automorphism on F.

Definition. The function $F \ni a \mapsto a^p$ is called the **Frobenius endomorphism** of F.

Example 3.1.35. The Frobenius endomorphism on $\mathbb{F}_2(\sqrt{t})$, which has image $\mathbb{F}_2(t)$, is not surjective. This also gives us an example that a field is isomorphic to its proper subgroup.

Proposition 3.1.36. Every irreducible polynomial over a finite field F (of characteristic p) is separable.

Proof. If $f \in F[x]$ is inseparable, by Corollary 3.1.32.2, $f(x) = g(x^p)$ for some $g \in F[x]$, say $g(x) = a_n x^n + \cdots + a_0$. Since $x \mapsto x^p$ is an automorphism, $a_i = b_i^p$ for some b_i for each i. Hence

$$f(x) = a_n x^{np} + \cdots + a_1 x^p + a_0 = (b_n x^n)^p + \cdots + (b_1 x)^p + b_0^p = (b_n x^n + \cdots + b_1 x + b_0)^p$$

and thus f isn't irreducible over F. □

Definition. A field is said to be **perfect** is every irreducible polynomial over it is separable.

Example 3.1.37. Fields of characteristic 0 and field of characteristic p such that $x \mapsto x^p$ is an automorphism are perfect.

Theorem 3.1.38. Let p be a prime. Then for each positive integer n there exists a finite field of p^n elements. Moreover, any two finite fields of p^n elements are isomorphic, which will be denoted by $\mathbb{F}_{p^n}$. Precisely, $F := \{\alpha \in \overline{\mathbb{F}_p} \mid \alpha^{p^n} - \alpha = 0\}$ is a finite field of p^n elements.

Proof. Since $D(x^{p^n} - x) = -1$, $x^{p^n} - x$ has no repeated roots, i.e, $\#F = p^n$. Also, for all $a, b \in F$, $a \pm b, ab \in F$ and $\frac{a}{b} \in F$ if $b \neq 0$, so F is a field. Suppose F' is another field of p^n elements, then $x^{p^n - 1} = 1$ for each $0 \neq x \in F$, and thus each element of F' is precisely a root of $x^{p^n} - x$. Therefore, F and F' are splitting fields of $x^{p^n} - x$, and hence, by Corollary 3.1.26.1, $F \cong F'$. □

Proposition 3.1.39. Let f be an irreducible polynomial over a field F of characteristic p. Then there exist a unique integer $k \geqslant 0$ and a unique separable irreducible polynomial $f_{sep} \in F[x]$ such that $f(x) = f_{sep}(x^{p^k})$.

Proof. If f is separable, we are done with $k = 0$ and $f_{sep} = f$. Otherwise, by Corollary 3.1.32.2, $f(x) = f_1(x^p)$ for some $f_1 \in F[x]$. If f_1 is separable, we are done with $k = 1$ and $f_{sep} = f_1$. Otherwise, continuing this way, and since $\deg f < \infty$, this must stop in a finite stage. □

Definition. In the preceding proposition, the integer p^k, denoted by $\deg_i f$, is called the **inseparable degree of** f, and the integer $\deg f_{sep}$, denoted by $\deg_s f$, is called the **separable degree**.

Remark 3.1.40. Clearly, $\deg f = (\deg_i f)(\deg_s f)$. Note that we only define these degrees over irreducible polynomials. For example, we cannot say what they should be for $f(x) = (x^p - t)(x^{p^2} - t)$.

Example 3.1.41.

1. $p(x) = x^p - t$ is irreducible over $\mathbb{F}_p(t)$ by the Eisenstein's criterion, and is separable since it has zero derivative. Hence $p_{sep}(x) = x - t$, $\deg_s = 1$ and $\deg_i = p$.

2. $p(x) = x^{p^n} - t$ is irreducible over $\mathbb{F}_p(t)$ with $p_{sep} = x - t$ and $\deg_i p = p^n$.

Definition. An algebraic extension K/F is said to be a **separable extension** if $m_{\alpha,F}$ is separable for each $\alpha \in K$.

Example 3.1.42. Each algebraic extension of a perfect field is separable. In particular, any finite extension of either $\mathbb{Q}$ or a finite field is separable.

3.1.4 Cyclotomic Polynomials and Extensions

Definition. Let n be a positive integer.

1. $\zeta_n := e^{2\pi i/n}$.

2. $\mu_n := \{\zeta_n^k \mid k = 0, \ldots, n-1\}$ is the group of n-th roots of unity over $\mathbb{Q}$.

3. $\zeta \in \mu_n$ is a **primitive** if $\mu_n = \langle \zeta \rangle$, i.e, $\gcd(k, n) = 1$.

4. $\Phi_n(x) = \prod_{\substack{\gcd(k,n)=1 \\ 1 \leqslant k \leqslant n}} (x - \zeta_n^k)$ is called the **n-th cyclotomic polynomial**.

Lemma 3.1.43. $x^n - 1 = \prod_{d|n} \Phi_d(x)$.

Proof.

$$x^n - 1 = \prod_{k=1}^{n} \left(x - e^{2k\pi i/n}\right) = \prod_{d'|n} \prod_{\substack{\gcd(k,n)=d' \\ 1 \leqslant k \leqslant n}} \left(x - e^{2k\pi i/n}\right)$$

$$(\text{Let } d = \frac{n}{d'},\ k' = \frac{k}{d'}) = \prod_{d|n} \prod_{k' \in (\mathbb{Z}/d\mathbb{Z})^\times} \left(x - e^{2k'\pi i/d}\right) = \prod_{d|n} \Phi_d(x)$$

□

Lemma 3.1.44. $\Phi_n \in \mathbb{Z}[x]$ is monic of degree $\phi(n)$.

Proof. That Φ_n is monic of degree $\phi(n)$ is clear. We prove it by induction on n. The result is clear when $n = 1$. Suppose $\Phi_k \in \mathbb{Z}[x]$ when $1 \leqslant k < n$. By Lemma 3.1.43 we have $x^n - 1 = f(x)\Phi_n(x)$, where $f(x) = \prod_{d|n,\, d \neq n} \Phi_d(x)$. Since $f \in \mathbb{Z}[x]$ by the induction hypothesis and is monic, $\Phi_n \in \mathbb{Z}[x]$ by the division, and thus the induction stage is completed. □

Definition. For each $n \geqslant 2$, we write $n = p_1^{e_1} \cdots p_k^{e_k}$, where each p_i is prime and $e_i \geqslant 1$. We define the **Möbius function** $\mu : \mathbb{N} \to \{-1, 0, 1\}$ by setting

$$\mu(n) = \begin{cases} 1 & \text{, if } n = 1 \\ (-1)^k & \text{, if } e_i = 1 \text{ for each } i \\ 0 & \text{, if } e_i > 1 \text{ for some } i \end{cases}$$

Proposition 3.1.45. Let $G := \{f : \mathbb{N} \to \mathbb{R} \mid f(1) \neq 0\}$. Define the operation $*$ on G by setting

$$(f * g)(n) := \sum_{d|n} f(d) g(\frac{n}{d})$$

for each $f, g \in G$. Then $(G, *)$ is an abelian group with identity δ_{1n}.

Proposition 3.1.46. Let $f, g : \mathbb{N} \to \mathbb{R}$ with $f(1), g(1) \neq 0$. TFAE:

1. $f(n) = \sum_{d|n} g(d)$
2. $g(n) = \sum_{d|n} \mu(\frac{n}{d}) f(d)$

Equivalently, $\mu * 1 = \delta_{1n}$, where $1 : \mathbb{N} \ni n \mapsto 1$.

Proposition 3.1.47. $\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(\frac{n}{d})}$.

Proof. This follows from Lemma 3.1.43 and Proposition 3.1.46, by exponentiating. □

Remark 3.1.48. This also gives a proof for Lemma 3.1.44.

Theorem 3.1.49. Φ_n is irreducible over $\mathbb{Q}$.

Proof. Suppose that $\Phi_n(x) = f(x)g(x)$, where $f, g \in \mathbb{Q}[x]$. By the Gauss' lemma, we may assume that $f, g \in \mathbb{Z}[x]$. We also assume $f = m_{\zeta_n, \mathbb{Q}}$.

Claim. If p is a prime such that $\gcd(p, n) = 1$, then $f(\zeta_n^p) = 0$.

Note that ζ_n^p is also a root of Φ_n. Suppose otherwise $f(\zeta_n^p) \neq 0$. Then $g(\zeta_n^p) = 0$, implying that $f(x) = m_{\zeta_n, \mathbb{Q}}(x) \mid g(x^p)$, say $g(x^p) = f(x)h(x)$ for some $h \in \mathbb{Q}[x]$. Since f is monic, $h \in \mathbb{Z}[x]$. Consider the reduction modulo p. We have $\overline{g(x)}^p = \overline{g(x^p)} = \overline{f(x)} \cdot \overline{h(x)}$. Since $\mathbb{F}_p[x]$ is a UFD, $\overline{f}, \overline{g}$ have common factor of degree $\geqslant 1$ in $\mathbb{F}_p[x]$. This implies that $\overline{\Phi_n}$ has a repeated irreducible factor in $\mathbb{F}_p[x]$, so does $x^n - 1$, which leads to a contradiction since $x^n - 1, D(x^n - 1) = (x^n - 1, nx^{n-1}) = (1)$ in $\mathbb{F}_p$ with $\gcd(n, p) = 1$. Hence the proof of the claim is completed.
Now for all $a \in \mathbb{N}$ such that $\gcd(a, n) = 1$, write $a = p_1 \cdots p_k$, where each p_i is prime. Then the claim implies that $\zeta_n, \zeta_n^{p_1}, \ldots, \zeta_n^{p_1 \cdots p_k} = \zeta_n^a$ are roots of $f(x)$. Hence $f = \Phi_n$, i.e, $\Phi_n = m_{\zeta_n, \mathbb{Q}}$. □

3.1.5 Wedderburn's theorem

Theorem 3.1.50 (Wedderburn's)**.** Every finite division ring is a field.

Proof. Let R be a finite division ring. For any $a \in R$, denote

$$C(a) := \{r \in R \mid ar = ra\}$$

and

$$Z(R) := \bigcap_{a \in R} C(a).$$

Note that $Z(R)$ is a finite *commutative* division ring, so $Z(R)$ is a field. Put $\mathbb{F} = Z(R)$ and $q = |\mathbb{F}|$. Also note that R and $C(a)$ are both vector spaces over $\mathbb{F}$. Since R and $C(a)$ are finite, $R \cong \mathbb{F}^n$ and $C(a) \cong \mathbb{F}^{n_a}$ for some $n, n_a \in \mathbb{N}$.

- $R^\times = R \backslash \{0\}$ is a multiplicative group, so we may consider the class equation:

  $$|R^\times| = |Z(R^\times)| + \sum_{|[a]| \neq 1} \frac{|R^\times|}{|C_{R^\times}(a)|}$$

  i.e,

  $$q^n - 1 = (q-1) + \sum_{|[a]| \neq 1} \frac{q^n - 1}{q^{n_a} - 1}$$

  The last term on the RHS implies that $n_a \mid n$ since $q^{n_a} - 1 \,\Big|\, q^n - 1$.

- On the other hand,

  $$q^n - 1 = \prod_{d \mid n} \Phi_d(q) = \Phi_n(q) \underbrace{\prod_{d \mid n_a} \Phi_d(q)}_{q^{n_a} - 1} \underbrace{\prod_{n_a < d \mid n, d \neq n} \Phi_d(q)}_{=: A \in \mathbb{Z}}$$

  and hence $\dfrac{q^n - 1}{q^{n_a} - 1} = A\Phi_n(q)$, implying $|\Phi_n(q)| \,\Big|\, |\dfrac{q^n - 1}{q^{n_a} - 1}|$.

Hence, we must have $|\Phi_n(q)| \,\Big|\, (q-1)$. Thus

$$q - 1 \geqslant |\Phi_n(q)| = |\prod_{k \in (\mathbb{Z}/n\mathbb{Z})^\times} \left(x - \exp \frac{2k\pi i}{n}\right)| \;\; \geqslant \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^\times} (|q| - 1) = (|q| - 1)^{\varphi(n)}$$

If $q = 2$, then all inequalities turn out being equalities, and thus $n = 1$. Otherwise, we have $\varphi(n) = 1$, implying that $n = 1, 2$ and hence $n = 1$ for $\Phi_2(q) = q + 1$. Hence, we have $R \cong \mathbb{F}^n = \mathbb{F}$ is commutative, and thus a field. □

3.2 Galois Theory

3.2.1 Separable extensions

Let F be a field and $\alpha \in \overline{F}$. Recall that we have $F(\alpha) \cong F[x]/(m_{\alpha,F}(x))$. If β is another root of $m_{\alpha,F}$, then $F(\beta) \cong F[x]/(m_{\alpha,F}(x)) \cong F(\alpha)$. This gives the isomorphism

$$\phi_{\alpha,\beta} : F(\alpha) \longrightarrow F(\beta)$$

$$\alpha \longmapsto \beta$$

Definition. For $\alpha, \beta \in \overline{F}$, we say α and β are **conjugates** over F if $m_{\alpha,F} = m_{\beta,F}$.

Proposition 3.2.1. $\phi : F(\alpha) \hookrightarrow \overline{F}$ be an isomorphism from F is a subfield of $\overline{F}$ such that ϕ fixes F pointwise. Then $\phi(\alpha)$ is a conjugate of α over F.

Definition. Let $F \subseteq E \subseteq \overline{F}$ be fields.

1. An **embedding** of E into $\overline{F}$ is a nontrivial (injective) field homomorphism from E to $\overline{F}$.
2. $\mathrm{Emb}(E/F) := \{\text{embeddings of } E \text{ into } \overline{F} \text{ that fix } F \text{ pointwise}\}$.
3. $\{E : F\} := \#\,\mathrm{Emb}(E/F)$

Corollary 3.2.1.1. Let F be a field and $\alpha \in \overline{F}$. Then $\{F(\alpha) : F\} = \#$ of distinct roots of $m_{\alpha,F} = \deg_s m_{\alpha,F}$.

Theorem 3.2.2. Let $F \subseteq K \subseteq E$ and $[E : F] < \infty$, then $\{E : F\} = \{E : K\}\{K : F\}$.

Proof. Note that if $\tau \in \mathrm{Emb}(E/F)$, then $\tau|_K \in \mathrm{Emb}(K/F)$.

Claim. For all $\sigma \in \mathrm{Emb}(K/F)$, there are $\{E : K\}$ embeddings $\tau \in \mathrm{Emb}(E/F)$ such that $\tau|_K = \sigma$.

In fact, we will prove a stronger statement:

Claim.

$$\begin{aligned} \text{For all } \sigma_1, \sigma_2 \in \mathrm{Emb}\, K/F, \quad & \#\text{ of } \tau_1 \in \mathrm{Emb}(E/F) \text{ such that } \tau_1|_K = \sigma_1 \\ = \ & \#\text{ of } \tau_2 \in \mathrm{Emb}(E/F) \text{ such that } \tau_2|_K = \sigma_2 \\ = \ & \#\text{ of } \tau \in \mathrm{Emb}(E/F) \text{ such that } \tau|_K = \mathrm{id}_K = \{E : K\} \end{aligned}$$

Let $\sigma_i : K \to K_i$, $i = 1, 2$. Extend them to isomorphisms $\overline{\sigma}_i : \overline{F} \to \overline{F}$ by Zorn's lemma, as in the proof of Theorem 3.1.29. Let $\lambda = \overline{\sigma}_2 \circ \overline{\sigma}_1^{-1}$. Then for any $\tau_1 \in \mathrm{Emb}(E/F)$ such that $\tau_1|_K = \sigma_1$, $(\lambda \circ \tau_1)|_K = \sigma_2$. Conversely, for any $\tau_2 \in \mathrm{Emb}(E/F)$ such that $\tau_2|_K = \sigma_2$, $(\lambda^{-1} \circ \tau_2)|_K = \sigma_1$. Thus λ induces a bijection from $\{\tau_1 \in \mathrm{Emb}(E/F) \mid \tau_1|_K = \sigma_1\}$ to $\{\tau_2 \in \mathrm{Emb}(E/F) \mid \tau_2|_K = \sigma_2\}$. □

Definition. Let F be a field and $\alpha \in \overline{F}$.

1. α is **separable over** F is $\{F(\alpha) : F\} = [F(\alpha) : F]$, i.e, $m_{\alpha,F}$ is separable over F.
2. Let $F \subseteq E \subseteq \overline{F}$. E/F is a **separable extension** if each element in E is separable over F.
3. Let $F \subseteq E \subseteq \overline{F}$. E/F is a **purely inseparable extension** if $m_{\beta,F}$ has only one root for all $\beta \in E$.

- In the case E/F is finite, E/F is separable if and only if $\{E : F\} = [E : F]$.
- If α is separable over F, then $F(\alpha)/F$ is a separable extension. Indeed, let $\beta \in F(\alpha)$, then

$$\{F(\beta) : F\} = \frac{\{F(\alpha) : F\}}{\{F(\alpha) : F(\beta)\}} = \frac{[F(\alpha) : F]}{[F(\alpha) : F(\beta)]} = [F(\beta) : F]$$

  in which the second equality holds since if α is separable over F, it remains separable over any intermediate field of $F \subseteq F(\alpha)$.
- If F has characteristic 0, then every algebraic extension of F is separable (see Corollary 3.1.32.1). In general, any algebraic extension of a perfect field is separable.

Corollary 3.2.2.1. Let F be a field and $\alpha, \beta \in \overline{F}$ are separable over F, then $F(\alpha, \beta)/F$ is separable. In particular, $\alpha \pm \beta$, $\alpha\beta$, $1/\alpha$ are separable.

Definition. Let $F \subseteq E \subseteq \overline{F}$ be fields.

1. $E_s := \{\alpha \in E \mid \alpha \text{ is separable over } F\}$ is a subfield of E, called the **separable closure of** F in E.
2. $[E_s : F]$ is called the **separable degree** of E/F, denoted as $\deg_s E/F$.
3. $[E : E_s]$ is called the **inseparable degree** of E/F, denoted as $\deg_i E/F$.

Proposition 3.2.3. Let E/F be an inseparable algebraic extension and $p = \operatorname{Char} E$. Then E_s/F is separable and E/E_s is purely inseparable.

Proof. The first is clear by definition. Let $\alpha \in E$. By Proposition 3.1.39, there's a $k \geqslant 0$ and an irreducible separable polynomial $f \in F[x]$ such that $m_{\alpha,F}(x) = f(x^{p^k})$, and thus α^{p^k} is separable over F, i.e, $\alpha^{p^k} \in E_s$. Hence m_{α,E_s} has only one root, and thus E/E_s is purely inseparable. □

Corollary 3.2.3.1. Let E/F be algebraic and $p = \operatorname{Char} F$. Then E/F is purely inseparable if and only if for each element $\alpha \in E$, α^q is separable over F for some $q = p^k$, $k \geqslant 0$.

Proof. This can be seen from the proof above. □

Traces and norms

Definition. Let L/K be a finite field extension. For each $x \in L$ we associate it with a translation $T_x : L \to L$ defined by $y \mapsto xy$; T_x is a K-linear map.

1. The **trace** $\mathrm{Tr}_{L/K}(x)$ is defined to be the trace of T_x.
2. The **norm** $\mathrm{N}_{L/K}(x)$ is defined to be the determinant of T_x.

- One can see the trace is additive and the norm is multiplicative.

Proposition 3.2.4. Let L be a finite separable extension of K of degree n. Let α be an element of L. (HW. 1)

1. The minimal polynomial for α over K is the same as the minimal polynomial for the linear transformation T_α. (Moreover, the characteristic polynomial of T_α is a power of its minimal polynomial.)
2. $\mathrm{Tr}_{L/K}(\alpha) = \sum_{\sigma \in \mathrm{Emb}(L/K)} \sigma(\alpha) \in K$
3. $\mathrm{N}_{L/K}(\alpha) = \prod_{\sigma \in \mathrm{Emb}(L/K)} \sigma(\alpha) \in K$

Proof.

1. Let $f(x) = m_{\alpha,K}(x)$ and $g(x)$ be the minimal polynomial of T_α; by definition $g(x) \in K[x]$. By definition, we have $g(T_\alpha)\beta = 0$ for all $\beta \in K$, and thus $g(\alpha) = 0$, implying $f(x) \mid g(x)$. Conversely, $f(\alpha) = 0$ implies $f(\alpha)\beta = 0$ for all $\beta \in K$, i.e, $f(T_\alpha) = 0$. Hence $g(x) \mid f(x)$. To sum up, we obtain $f = g$.

2. Let $d = \deg_K \alpha$. Clearly, we have $d \mid n$. Let $t(\alpha)$ and $n(\alpha)$ be the sum and product of conjugates of α over K, respectively. Obviously, we have
$$\mathrm{Tr}_{L/F}(\alpha) = \frac{n}{d} t(\alpha)$$
$$\mathrm{N}_{L/F}(\alpha) = n(\alpha)^{n/d}$$
Let $\{\beta_1, \ldots, \beta_d\}$ be a basis for $L/K(\alpha)$. Then $\beta := \{\alpha^i \beta_j \mid 0 \leqslant i \leqslant d-1,\ 1 \leqslant j \leqslant d\}$ is a basis for L/K. Ordering β appropriately, we have $[T_\alpha]_\beta = A \oplus \cdots \oplus A \in M_n(K)$, where
$$A = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & & 0 & -a_1 \\ & \ddots & & & \vdots \\ & & \ddots & & \vdots \\ & & & 1 & -a_{d-1} \end{pmatrix} \in M_d(K)$$

and $g(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$. Thus

$$\mathrm{tr}(T_\alpha) = \frac{-a_{d-1}n}{d} = \frac{n}{d}t(\alpha) = \mathrm{Tr}_{L/K}(\alpha)$$

3. As in 2., we have

$$\det(T_\alpha) = ((-1)^d a_0)^{n/d} = n(\alpha)^{n/d} = \mathrm{N}_{L/K}(\alpha)$$

□

Proposition 3.2.5. Let L/K be a finite extension and V a finite dimensional vector space over L. Let $\varphi : V \to V$ be an L-linear map. Then

$$\mathrm{tr}_K(\varphi) = \mathrm{Tr}_{L/K}(\mathrm{tr}_L(\varphi))$$

$$\det_K(\varphi) = \mathrm{N}_{L/K}(\det_L(\varphi))$$

Proof.

1. Let $\{v_1, \ldots, v_n\}$ be an L-basis for V. By linearity of the first asserted identity, assume $\varphi(v_t) = av_s$ and $\varphi(v_i) = 0$ for $i \neq t$. Let $\{\alpha_1, \ldots, \alpha_m\}$ be a K-basis for L. Then $\varphi(\alpha_i v_j) = \delta_{tj} a\alpha_i v_s = \delta_{tj} T_a(\alpha_i)v_s$, and hence

$$\mathrm{tr}_K(\varphi) = \mathrm{tr}_K\, T_a = \mathrm{Tr}_{L/K}(a) = \mathrm{Tr}_{L/K}(\mathrm{tr}_L(\varphi))$$

when $t = s$ and

$$\mathrm{tr}_K(\varphi) = 0 = \mathrm{Tr}_{L/K}(0) = \mathrm{Tr}_{L/K}(\mathrm{tr}_L(\varphi))$$

when $t \neq s$.

2. We may assume φ is invertible. Also, by multiplicativity, we may assume φ is an elementary matrix.

   - Assume $\varphi(v_t) = v_t + av_s$ and $\varphi(v_i) = v_i$ for $i \neq t$. Then $\varphi(\alpha_i v_j) = \alpha_i v_j + \delta_{tj} T_a(\alpha_i)v_s$ so that

$$\det_K(\varphi) = 1 = \mathrm{N}_{L/K}(1) = \mathrm{N}_{L/K}(\det_L(\varphi))$$

   - Assume $\varphi(v_t) = av_t$ and $\varphi(v_i) = v_i$ for $i \neq t$. Then $\varphi(\alpha_i v_t) = a\alpha_i v_t = T_a(\alpha_i)v_t$ so that $[\varphi] = [T_a] \oplus I$ in terms of the basis $\{\alpha_i v_j\}$, and thus

$$\det_K(\varphi) = \det_K T_a = \mathrm{N}_{L/F}(a) = \mathrm{N}_{L/K}(\det_L(\varphi))$$

□

Definition. Let L/K be a finite extension of degree n and $\{x_1, \ldots, x_n\}$ be elements of L. The **discriminant** $\mathrm{disc}(x_1, \ldots, x_n)$ is the determinant of the matrix $(\mathrm{Tr}_{L/K}(x_i x_j))_{ij}$.

- Suppose L/K is separable. Let $\mathrm{Emb}(L/K) = \{\sigma_1, \ldots, \sigma_n\}$. Then $\mathrm{disc}(x_1, \ldots, x_n) = \det(\sigma_i(x_j))^2$.

Theorem 3.2.6. Let L/K be a finite extension of degree n. TFAE:

1. L/K is separable.
2. $\mathrm{Tr}_{L/K}$ is not identically zero.
3. The pairing $Q = \mathrm{Tr}_{L/K} : L \times L \to K$ is nondegenerate.

Proof.

1. $(3 \Rightarrow 2)$ This is clear.
2. $(2 \Rightarrow 3)$ Pick $y \in L$ such that $\mathrm{Tr}_{L/K}(y) \neq 0$. Then for all $x \neq 0$, $Q(x, y/x) \neq 0$. This shows Q is nondegenerate.
3. $(2 \Rightarrow 1)$ Suppose L/K is inseparable. Say $\mathrm{Char}\, K = p$ for some prime p. By Proposition 3.2.3, L_s/K is separable and and L/L_s is purely inseparable. By Proposition 3.2.5, the trace is identically zero since L/L_s is purely inseparable.
4. $(1 \Rightarrow 2)$ Suppose L/K is separable. Use induction on n we show the trace map is not identically zero. By Proposition 3.2.5 we may assume $L = K(\alpha)$ for some $\alpha \in L$. Let $\alpha_1, \ldots, \alpha_n$ be the conjugates of α over K; they're distinct by separability. Note also that they are the eigenvalues of the linear transformation induced by α. Consider the map $\pi_i : r \mapsto \alpha_i^r$; this is a character from the group $\mathbb{Z}$ to $L^\times$. Proposition 3.2.9 shows $\pi_1(e) + \cdots + \pi_n(e) \neq 0$ for some $e \in \mathbb{Z}$, i.e, $\mathrm{Tr}_{L/K}(\alpha^e) \neq 0$.

□

3.2.2 Galois extensions

Definition. Let F be a field.

1. An algebraic extension E/F is **normal** if $\sigma(E) = E$ for all $\sigma \in \mathrm{Emb}(E/F)$; equivalently, for any $\alpha \in E$, conjugates of α over F all lie in E.
2. If E/F is an extension, let

$$\mathrm{Aut}(E) := \{\sigma : E \to E \mid \sigma \text{ is a field isomorphism}\}$$

and let

$$\mathrm{Aut}(E/F) := \{\sigma \in \mathrm{Aut}(E) \mid \sigma \text{ fixes } F \text{ (pointwise)}\}$$

- Note that $\mathbb{F}_p \subseteq E$ if $\operatorname{Char} E = p$. Since $\sigma(1) = 1$ for all $\sigma \in \operatorname{Aut}(E)$, σ fixes $\mathbb{F}_p$. Hence $\operatorname{Aut}(E) = \operatorname{Aut}(E/\mathbb{F}_p)$. Likewise, $\operatorname{Aut}(E) = \operatorname{Aut}(E/\mathbb{Q})$ if $\operatorname{Char} E = 0$.
- An algebraic extension E/F is normal if and only if $\operatorname{Emb}(E/F) = \operatorname{Aut}(E/F)$.
- The splitting field of a collection of polynomials of $F[x]$ over F is a normal extension of F.

Proposition 3.2.7. Let E be the splitting filed of a collection of polynomials in $F[x]$ over F. Then E/F is normal.

Proof. Note $\operatorname{Emb}(E/F) \subseteq \operatorname{Aut}(E/F)$, so $\operatorname{Emb}(E/F) = \operatorname{Aut}(E/F)$. Now if $\alpha \in E$ and β is a conjugate of α over F, there exists a field isomorphism $\phi : F(\alpha) \to F(\beta)$ sending α to β. Extend ϕ to an element $\sigma \in \operatorname{Emb}(E/F) = \operatorname{Aut}(E/F)$. Thus $\beta = \phi(\alpha) = \sigma(\alpha) \in E$. □

Definition. Let F be a field. If E/F is separable and normal, we say E/F is a **Galois extension** . In this case, we write $\operatorname{Gal}(E/F) := \operatorname{Aut}(E/F)$, and call it the **Galois group** of E/F.

- In the case E/F is finite, E/F is Galois if and only if $\#\operatorname{Aut}(E/F) = [E : F]$.
- If $f \in F[x]$ is separable, "the Galois group of f" refers to the Galois group of the splitting field of f over F.

Example 3.2.8.

1. Quadratic extensions of a field of characteristic $\neq 2$ are Galois.
2. $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not Galois (not normal), but $\mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$ is; it's the splitting field of $x^3 - 2$ over $\mathbb{Q}$.
3. A Galois extension of a Galois extension may not be Galois. For instance, $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})$.
4. $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois since it's the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$. Let $\sigma : a \mapsto a^p$ be the Frobenius automorphism on $\mathbb{F}_{p^n}$. Clearly, $\sigma^n = \mathrm{id}_{\mathbb{F}_{p^n}}$. On the other hand, $x^{p^k} - x$ has at most p^k roots, so σ^k cannot fix every element of $\mathbb{F}_{p^n}$ if $k < n$. This means the order of $\sigma = n = [\mathbb{F}_{p^n} : \mathbb{F}_p] = \#\operatorname{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. Thus $\operatorname{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle\sigma\rangle$.

3.2.3 The fundamental theorem of Galois theory

Definition. Let K be a field and S be a subset of $\operatorname{Aut}(K)$. Then the set

$$K^S := \{\alpha \in K \mid \sigma\alpha = \alpha \text{ for all } \sigma \in S\}$$

is a subfield of K, called the **fixed field** of S.

Definition. Let G be a group and K be a field. A **character** of G with values in K is a group homomorphism $\chi : G \to K^\times$.

- Each homomorphism from E ot K may be viewed as a character of $E^\times$ with values in $K^\times$. In particular, embeddings and automorphism of a field are characters.

Proposition 3.2.9. Let G be a group and K be a field. If $\chi_1, \dots, \chi_n$ are distinct characters of G with values in K, they're K-linearly independent.

Corollary 3.2.9.1. Let K/F be a finite separable field extension. Then the trace $\mathrm{Tr}_{K/F} : K \to F$ is surjective.

Theorem 3.2.10. Let K be a field and $G = \{\sigma_1 = \mathrm{id}_K, \sigma_2, \dots, \sigma_n\} \leqslant \mathrm{Aut}(K)$ be a finite subgroup. Then $[K : K^G] = \#G$.

Proof. Let $m = [K : K^G]$ and let $\alpha_1, \dots, \alpha_m$ be a basis for K/F.

1. $n > m$: consider the system of equations

$$(*) : \begin{cases} \sigma_1(\alpha_1)x_1 + \cdots + \sigma_n(\alpha_1)x_n = 0 \\ \sigma_1(\alpha_2)x_1 + \cdots + \sigma_n(\alpha_2)x_n = 0 \\ \qquad\qquad \vdots \\ \sigma_1(\alpha_m)x_1 + \cdots + \sigma_n(\alpha_m)x_n = 0 \end{cases}$$

   Since $n > m$, $(*)$ has a nontrivial solution $(\beta_1, \dots, \beta_n) \in K^n$. Since the α_i form a basis for K/F, we have

$$(**) : \sigma_1(\alpha)\beta_1 + \cdots + \sigma_n(\alpha)\beta_n = 0, \, \forall\, \alpha \in K$$

   WLOG, suppose $(\beta_1, \dots, \beta_n)$ is a solution of all nontrivial solutions of $(*)$ such that the number of nonzero entries is minimal; say $\beta_1, \dots, \beta_r \neq 0$ and $\beta_{r+1}, \dots, \beta_n = 0$. Pick $\alpha_0 \in K^\times$ so that $\sigma_1(\alpha_0) \neq \sigma_r(\alpha_0)$. Replacing α by $\alpha_0\alpha$ in $(**)$, we obtain

$$\sigma_1(\alpha)\sigma_1(\alpha_0)\beta_1 + \cdots + \sigma_r(\alpha)\sigma_r(\alpha_0)\beta_r = 0$$

   On the other hand, by multiplying $\sigma_r(\alpha_0)$ to both side of $(*)$, we obtain

$$\sigma_1(\alpha)\sigma_n(\alpha_0)\beta_1 + \cdots + \sigma_r(\alpha)\sigma_r(\alpha_0)\beta_r = 0$$

   Subtracting the latter from the former, we have

$$\sigma_1(\alpha)[\sigma_1(\alpha_0) - \sigma_r(\alpha_0)]\beta_1 + \cdots + \sigma_{r-1}(\alpha)[\sigma_{r-1}(\alpha_0) - \sigma_r(\alpha_0)]\beta_{r-1} = 0$$

   which contradicts to the minimality of r.

2. $m > n$: consider the system of equations:

$$\begin{cases} \sigma_1(\alpha_1)x_1 + \cdots + \sigma_1(\alpha_m)x_m = 0 \\ \sigma_2(\alpha_1)x_1 + \cdots + \sigma_2(\alpha_m)x_m = 0 \\ \qquad\qquad \vdots \\ \sigma_n(\alpha_1)x_1 + \cdots + \sigma_n(\alpha_m)x_m = 0 \end{cases}$$

Again, since $m > n$, it has a nontrivial solution $(\beta_1, \ldots, \beta_m) \in K^m$; WLOG, suppose the number of its nonzero entries is minimal, and say $\beta_1, \ldots, \beta_r \neq 0$ and $\beta_{r+1}, \ldots, \beta_m = 0$. Furthermore, replace β_j by β_j/β_r so that $\beta_r = 1$. Thus

$$(***) : \sigma_j(\alpha_1)\beta_1 + \cdots + \sigma_j(\alpha_{r-1})\beta_{r-1} + \sigma_j(\alpha_r) = 0,\ j = 1, \ldots, n$$

Note that $\beta_1, \ldots, \beta_r$ cannot all lie in F, for otherwise the α_i wouldn't be linearly independent, by taking $j = 1$ in $(***)$; WLOG, say $\beta_1 \notin F$. Let $\sigma_i \in G$ so that $\sigma_i(\beta_1) \neq \beta_1$. Applying σ_i to $(***)$, we obtain

$$\sigma_i\sigma_j(\alpha_1)\sigma_i(\beta_1) + \cdots + \sigma_i\sigma_j(\alpha_{r-1})\sigma_i(\beta_{r-1}) + \sigma_i\sigma_j(\alpha_r) = 0,\ j = 1, \ldots, n$$

i.e,

$$\sigma_j(\alpha_1)\sigma_i(\beta_1) + \cdots + \sigma_j(\alpha_{r-1})\sigma_i(\beta_{r-1}) + \sigma_j(\alpha_r) = 0,\ j = 1, \ldots, n$$

Subtracting $(***)$ from the latter, we have

$$\sigma_j(\alpha_1)[\sigma_i(\beta_1) - \beta_1] + \cdots + \sigma_j(\alpha_{r-1})[\sigma_i(\beta_{r-1}) - \beta_{r-1}] = 0,\ j = 1, \ldots, n$$

which contradicts to the minimality of r.

Hence, we must have $n = m$. □

Corollary 3.2.10.1. Under the notations of above theorem, we have K/K^G is Galois with Galois group G.

Proof. By the definition of K^G, we have $G \leqslant \mathrm{Aut}(K/K^G)$. The preceding theorem shows that $\#G = [K : K^G]$, and this forces $G = \mathrm{Aut}(K/K^G)$; in the mean while, this shows $[K : K^G] = \#\,\mathrm{Aut}(K/K^G)$, i.e, K/K^G is Galois. □

Corollary 3.2.10.2 (Hilbert theorem 90)**.** Let K be a Galois extension of F with cyclic Galois group of order n generated by σ. If $\alpha \in K$ has $\mathrm{N}_{K/F}(\alpha) = 1$, then $\alpha = \sigma^{-1}(\beta)\beta$ for some $\beta \in K^\times$.

Proof. Since $1, \sigma, \sigma^2, \ldots, \sigma^{n-1}$ are linearly independent over K, we have

$$1 + \alpha\sigma + (\alpha\sigma\alpha)\sigma^2 + \cdots + (\alpha\sigma\alpha\cdots\sigma^{n-2}\alpha)\sigma^{n-1} \neq 0$$

Thus

$$\beta = \theta + \alpha\sigma\theta + (\alpha\sigma\alpha)\sigma^2\theta + \cdots + (\alpha\sigma\alpha\cdots\sigma^{n-2}\alpha)\sigma^{n-1}\theta \neq 0$$

for some $\theta \in K$. Then

$$\begin{aligned}
\frac{\beta}{\sigma\beta} &= \frac{\theta + \alpha\sigma(\theta) + (\alpha\sigma(\alpha))\sigma^2(\theta) + \cdots + (\alpha\sigma(\alpha)\cdots\sigma^{n-2}(\alpha))\sigma^{n-1}(\theta)}{\sigma(\theta) + \sigma(\alpha)\sigma^2(\theta) + (\sigma(\alpha)\sigma^2(\alpha))\sigma^3(\theta) + \cdots + (\sigma(\alpha)\sigma^2(\alpha)\cdots\sigma^{n-1}(\alpha))\sigma^n(\theta)} \\
&= \frac{\theta + \alpha\sigma(\theta) + (\alpha\sigma(\alpha))\sigma^2(\theta) + \cdots + (\alpha\sigma(\alpha)\cdots\sigma^{n-2}(\alpha))\sigma^{n-1}(\theta)}{\sigma\theta + \sigma(\alpha)\sigma^2(\theta) + (\sigma(\alpha)\sigma^2(\alpha))\sigma^3(\theta) + \cdots + \alpha^{-1}\theta} \\
&= \alpha
\end{aligned}$$

where the second equality results from the assumption $1 = \mathrm{N}_{K/F}(\alpha) = \alpha\sigma(\alpha)\cdots\sigma^{n-2}(\alpha)\sigma^{n-1}(\alpha)$. □

Corollary 3.2.10.3 (Additive Hilbert theorem 90)**.** Let K be a Galois extension of F with cyclic Galois group of order n generated by σ. If $\alpha \in K$ has $\mathrm{Tr}_{K/F}(\alpha) = 0$, then $\alpha = \beta - \sigma(\beta)$ for some $\beta \in K$.

Proof. The linear independence of $1, \sigma, \sigma^2, \ldots, \sigma^{n-1}$ shows that

$$\mathrm{Tr}_{K/F}(\theta) = \theta + \sigma(\theta) + \sigma^2(\theta) + \cdots + \sigma^{n-1}(\theta) \neq 0$$

for some $\theta \in K$. Now let

$$\beta := \frac{1}{\mathrm{Tr}_{K/F}(\theta)}(\alpha\sigma(\theta) + (\alpha + \sigma(\alpha))\sigma^2(\theta) + \cdots + (\alpha + \sigma(\alpha) + \cdots + \sigma^{n-2}(\alpha))\sigma(\theta))$$

Then

$$\begin{aligned}
\beta - \sigma\beta &= \frac{1}{\mathrm{Tr}_{K/F}(\theta)}(\alpha(\sigma^2(\theta) + \cdots + \sigma^{n-1}(\theta)) - (\sigma(\alpha) + \cdots + \sigma^{n-1}(\alpha))\theta) \\
&= \frac{1}{\mathrm{Tr}_{K/F}(\theta)}(\alpha(\sigma^2(\theta) + \cdots + \sigma^{n-1}(\theta)) + \alpha\theta) \\
&= \frac{1}{\mathrm{Tr}_{K/F}(\theta)}(\alpha(\theta + \sigma^2(\theta) + \cdots + \sigma^{n-1}(\theta))) \\
&= \alpha
\end{aligned}$$

where the second equality comes from the assumption $0 = \mathrm{Tr}_{K/F}(\alpha) = \alpha + \sigma(\alpha) + \cdots + \sigma^{n-1}(\alpha)$. □

Theorem 3.2.11 (Fundamental theorem for Galois theory)**.** Let K/F be a *finite* Galois extension.

1. If $F \subseteq E \subseteq K$, then K/E is Galois with $\mathrm{Gal}(K/E) \leqslant \mathrm{Gal}(K/F)$ and $\#\,\mathrm{Gal}(K/E) = [K : E]$, i.e, $[E : F] = [\mathrm{Gal}(K/F) : \mathrm{Gal}(K/E)]$.

2. There's a one-to-one inclusion-reversing correspondence

$$\begin{aligned} \{E \mid F \subseteq E \subseteq K\} &\longrightarrow \{H \mid 1 \leqslant H \leqslant \mathrm{Gal}(K/F)\} \\ E &\longmapsto \lambda(E) := \mathrm{Gal}(K/E) \\ K^H &\longleftarrow\!\shortmid H \end{aligned}$$

   where the mappings above are mutually inverses.

3. If $F \subseteq E_1 \subseteq E_2 \subseteq K$, then $\lambda(E_1 \cap E_2) = \langle \lambda(E_1), \lambda(E_2) \rangle$ and $\lambda(E_1 E_2) = \lambda(E_1) \cap \lambda(E_2)$.

4. For $F \subseteq E \subseteq K$,

$$E/F \text{ is Galois} \Leftrightarrow \mathrm{Gal}(K/E) \trianglelefteq \mathrm{Gal}(K/F)$$

   If it occurs, $\mathrm{Gal}(E/F) \cong \mathrm{Gal}(K/F)/\mathrm{Gal}(K/E)$.

Proof.

1. Since K/F is normal separable, K/E is automatically normal and separable, and hence Galois. The remaining is clear.

2. Let $F \subseteq E \subseteq K$ and $H := \lambda(E) = \mathrm{Gal}(K/E)$. Clearly, $E \subseteq K^H$. 1. and the previous theorem show that $[K : E] = \#H = [K : K^H]$, so $E = K^H$. Vice versa.

3. This is clear.

4. Note that E/F is clearly separable, so it suffices to show E/F is normal if and only if $\lambda(E) \trianglelefteq \lambda(F)$. Nevertheless,

$$E/F \text{ is normal} \Leftrightarrow \sigma(E) = E \text{ for all } \sigma \in \mathrm{Emb}(E/F) = \mathrm{Aut}(E/F)$$

   Note that for all $\sigma \in \mathrm{Emb}(E/F)$, $\sigma(E)$ is the fixed field of $\sigma\,\mathrm{Gal}(K/E)\sigma^{-1}$. The results follows.

□

Example 3.2.12.

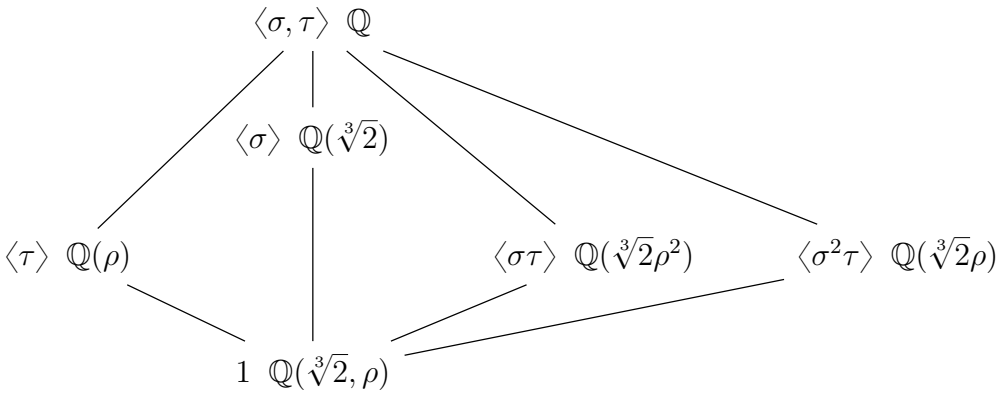
1. $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$:

$$\begin{array}{ccc} \mathbb{Q}(\sqrt{2}) & & 1 \\ | & & | \\ \mathbb{Q} & \langle\sigma\rangle & \sigma : \sqrt{2} \mapsto -\sqrt{2} \end{array}$$

2. $\mathbb{Q}(\sqrt[3]{2}, \rho)/\mathbb{Q}$, where $\rho = e^{2\pi i/3}$: Let

$$\sigma : \begin{cases} \sqrt[3]{2} & \mapsto \sqrt[3]{2}\rho \\ \rho & \mapsto \rho \end{cases} \qquad \tau : \begin{cases} \sqrt[3]{2} & \mapsto \sqrt[3]{2} \\ \rho & \mapsto \rho^{-1} \end{cases}$$

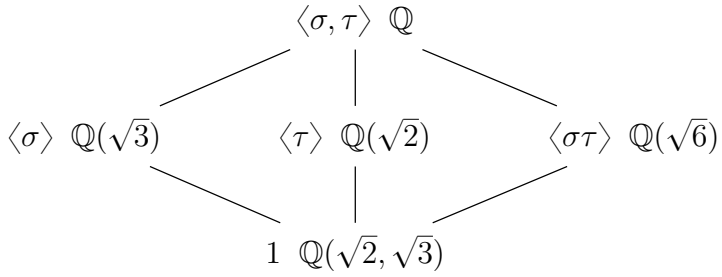
Then $\sigma\tau = \tau\sigma^2$; this shows $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \rho)/\mathbb{Q}) \cong S_3$.



3. $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$: Let

$$\sigma : \begin{cases} \sqrt{2} & \mapsto -\sqrt{2} \\ \sqrt{3} & \mapsto \sqrt{3} \end{cases} \qquad \tau : \begin{cases} \sqrt{2} & \mapsto \sqrt{2} \\ \sqrt{3} & \mapsto -\sqrt{3} \end{cases}$$

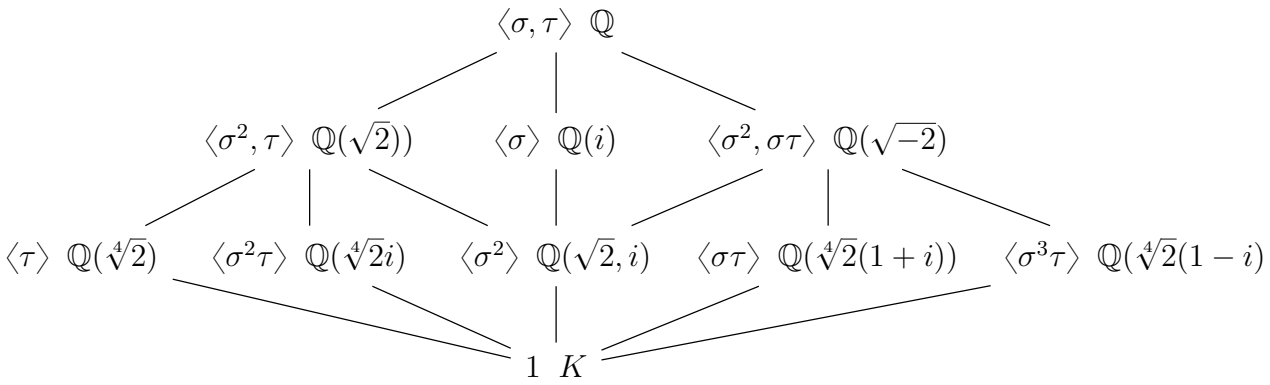
Then



4. Let K be the splitting field of $x^4 - 2$ over $\mathbb{Q}$; $K = \mathbb{Q}(\sqrt[4]{2}, i)$. Let

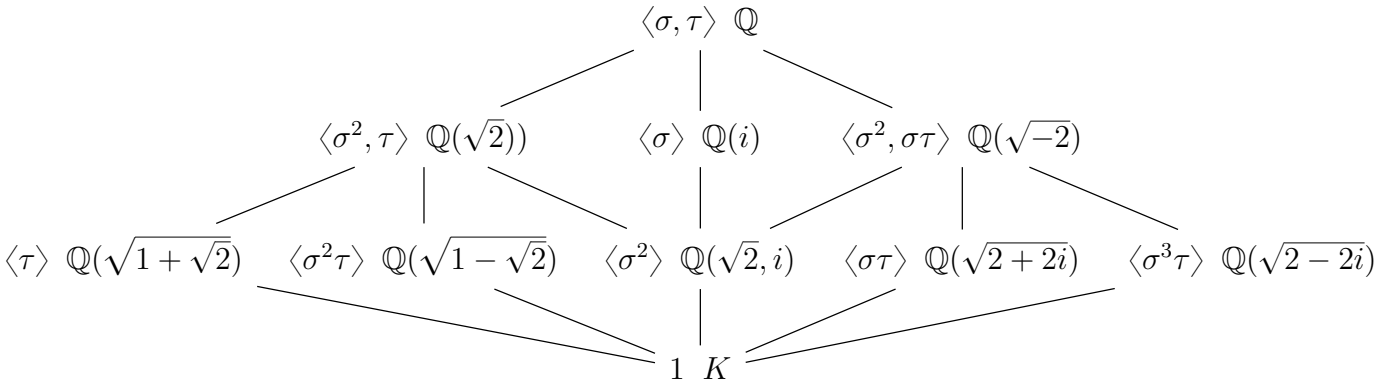
$$\sigma : \begin{cases} \sqrt[4]{2} & \mapsto \sqrt[4]{2}i \\ i & \mapsto i \end{cases} \qquad \tau : \begin{cases} \sqrt[4]{2} & \mapsto \sqrt[4]{2} \\ i & \mapsto -i \end{cases}$$

Then $\sigma\tau = \tau\sigma^3$; this shows $\mathrm{Gal}(K/\mathbb{Q}) \cong D_8$.



We elaborate how to find the fixed field of $\langle\sigma\tau\rangle$. A technique is to find $\alpha \in K$ such that $\sigma\tau(\alpha)+\alpha \neq 0$. Then clearly, $\sigma\tau(\alpha) + \alpha$ is fixed by $\sigma\tau$.

5. Let K be the splitting field of $x^4 - 2x^2 - 1$ over $\mathbb{Q}$; $K = \mathbb{Q}(\sqrt{1+\sqrt{2}}, \sqrt{1-\sqrt{2}}) = \mathbb{Q}(\sqrt{1+\sqrt{2}}, i)$. Let
$$\sigma : \begin{cases} \sqrt{1+\sqrt{2}} & \mapsto \sqrt{1-\sqrt{2}} \\ i & \mapsto i \end{cases} \qquad \tau : \begin{cases} \sqrt{1+\sqrt{2}} & \sqrt{1+\sqrt{2}} \\ i & \mapsto -i \end{cases}$$
Then $\sigma\tau = \tau\sigma^3$. This shows $K \cong D_8$.



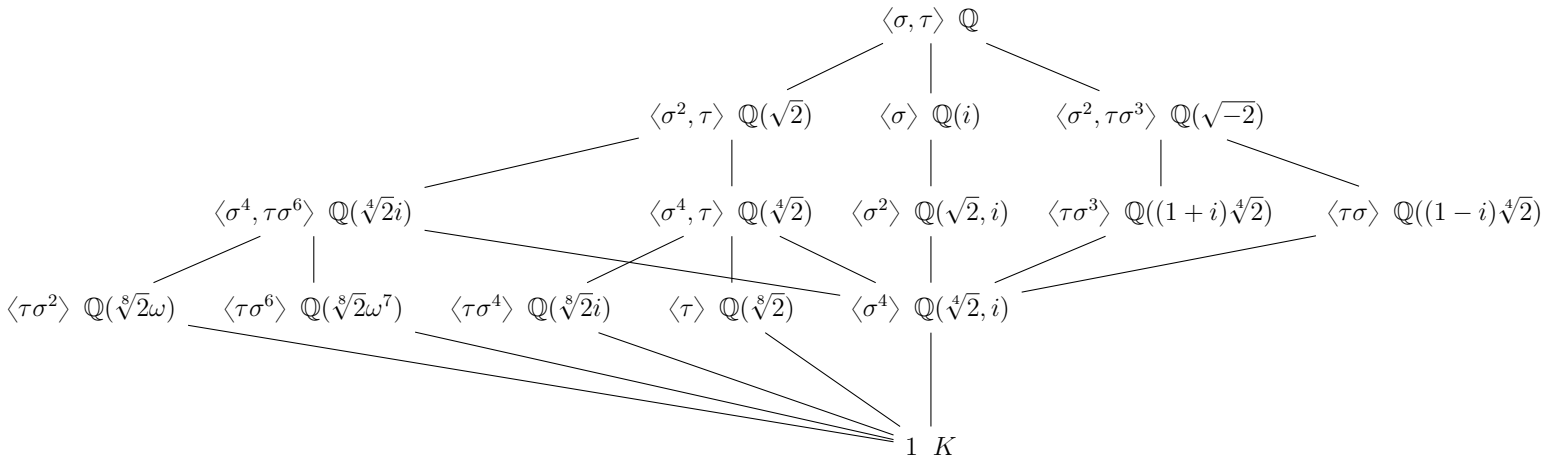
- Since $\sigma^2\tau = \sigma\tau\sigma^{-1}$, the fixed field of $\langle\sigma^2\tau\rangle$ is σ(fixed field of $\langle\tau\rangle$) $= \sigma(\mathbb{Q}(\sqrt{1+\sqrt{2}})) = \mathbb{Q}(\sqrt{1-\sqrt{2}})$.
- To find the fixed field of $\langle\sigma\tau\rangle$, let $\alpha = \sqrt{1+\sqrt{2}}$. Then $\sigma\tau\alpha + \alpha \neq 0$ is fixed by $\sigma\tau$; note that $\sqrt{1+\sqrt{2}} + \sqrt{1-\sqrt{2}} = \sqrt{2+2i}$. Counting the degree, we see $\mathbb{Q}(\sqrt{2+2i})$ is the fixed field of $\langle\sigma\tau\rangle$.

6. Let K be the splitting field of $x^8 - 2$ over $\mathbb{Q}$; $K = \mathbb{Q}(\sqrt[8]{2}, e^{2\pi i/8}) = \mathbb{Q}(\sqrt[8]{2}, i)$. Let $\omega = e^{2\pi i/8}$ and define

$$\sigma : \begin{cases} \sqrt[8]{2} & \mapsto \sqrt[8]{2}\omega \\ i & \mapsto i \end{cases} \qquad \tau : \begin{cases} \sqrt[8]{2} & \mapsto \sqrt[8]{2} \\ i & \mapsto -i \end{cases}$$

Then $\tau\sigma\tau = \sigma^3$. It's easy to see that

$$\mathrm{Gal}(\mathbb{Q}(\sqrt[8]{2}, i)/\mathbb{Q}) = \{\sigma, \tau \mid \sigma^8 = \tau^2 = 1,\ \tau\sigma\tau = \sigma^3\}$$



- The fixed field of $\langle\tau\rangle$ can be sought out easily. Note that $\sigma\tau\sigma^{-1} = \tau\sigma^2$, so its fixed field can be obtained by applying σ to that of $\langle\tau\rangle$. Similar for $\langle\tau\sigma^6\rangle$ and $\langle\tau\sigma^4\rangle$.
- Once the fixed fields of degree 2 are determined, it's not hard to determine those of $\langle\sigma^4, \tau\sigma^6\rangle$ and $\langle\sigma^4, \tau\rangle$, by the fundamental theorem.
- It's not so easy to determine the fixed fields of $\langle\tau\sigma^3\rangle$ and $\langle\tau\sigma\rangle$; but once one of them is found, the other can be determined easily, since $\sigma(\tau\sigma)\sigma^{-1} = \tau\sigma^3$. We strive to seek the fixed field of $\langle\tau\sigma\rangle$. Let $H = \langle\tau\sigma\rangle$; it's a cyclic group of order 4. The lattice above shows $\langle\sigma^4\rangle$ is a normal subgroup of H of index 2, with representatives $1, \tau\sigma$ for the cosets. Consider the element

$$\alpha := (1 + \tau\sigma)\sqrt[4]{2} = (1 - i)\sqrt[4]{2}$$

Then α is fixed by σ^4. *Also*, α is fixed by $\tau\sigma$:

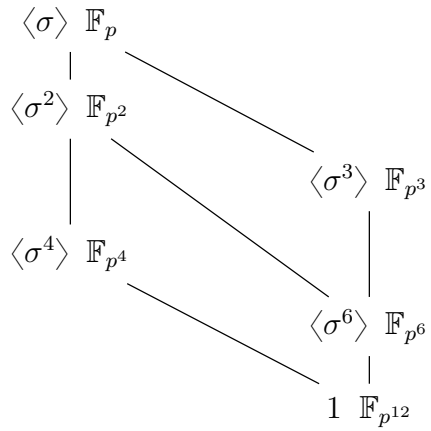
$$\begin{aligned} \tau\sigma\alpha = (\tau\sigma + (\tau\sigma)^2)\sqrt[4]{2} &= (\tau\sigma + \sigma^4)\sqrt[4]{2} \\ &= (\tau\sigma + 1)\sqrt[4]{2} \end{aligned}$$

the last equality holds since σ^4 fixes $\sqrt[4]{2}$. This shows that α is in the fixed field of H. However,

$$\tau\sigma^3\alpha = \tau\sigma^3((1 - i)\sqrt[4]{2}) = (1 + i)\sqrt[4]{2}\omega \neq \alpha$$

which means the fixing subgroup of $\mathbb{Q}(\alpha)$ is not larger than H, and thus is H. In conclusion, the fixed field of H is $\mathbb{Q}(\alpha) = \mathbb{Q}((1-i)\sqrt[4]{2})$

7. $\mathbb{F}_{p^n}/\mathbb{F}_p$: We have seen that $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle\sigma\rangle$, where σ is the Frobenius automorphism. We draw its lattice when $n = 12$:



3.2.4 Simple extensions and composite extensions

Proposition 3.2.13. Let K/F be a finite extension. Then K/F is simple if and only if there are only finitely many subfields of K containing F.

Proof. ($\Rightarrow$) Say $K = F(\alpha)$. Let $F \subseteq E \subseteq K$; then $m_{\alpha,E} \mid m_{\alpha,F}$. Let $E' = F(\text{coefficients of } m_{\alpha,E})$.

Claim. $E = E'$

Clearly, we have $E' \subseteq E$. On the other hand, $m_{\alpha,E} \in E'[x]$ is irreducible over E', which implies $m_{\alpha,E} = m_{\alpha,E'}$. Thus $[K : E] = [K : E']$, and hence $E' = E$.
This means E is the subfield generated by F and coefficients of some monic irreducible factor of $m_{\alpha,F}$. The result follows.
($\Leftarrow$) If F is a finite field, K/F is of course simple. Now suppose F is infinite. By virtue of the finiteness of K/F, write $K = F(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_1, \ldots, \alpha_n$. By induction, it suffices to show the case $K = F(\alpha, \beta)$. Consider the field $F(\alpha + c\beta)$, $c \in F$. Since F is infinite and there are only finitely many intermediate fields, $F(\alpha + c_1\beta) = F(\alpha + c_2\beta)$ for some distinct $c_1, c_2 \in F$. This means $F(\alpha, \beta) = F(\alpha + c_1\beta)$. □

Example 3.2.14. Let $F = \overline{\mathbb{F}}_p(x^p, y^p)$ and $K = \overline{\mathbb{F}}_p(x, y)$. We have $[K : F] = p^2$. For any $c \in \overline{\mathbb{F}}_p$, $[F(x + cy) : F] = p$, since $(x + cy)^p = x^p + c^p y^p \in F$. Thus $F(x + cy) \neq K$. Also, different choices of c gives different fields. The previous proposition then shows that K/F is not simple. (HW. 20)

Theorem 3.2.15 (Primitive element theorem, PET)**.** If K/F is finite separable, then K/E is simple.

Proof. Since K/F, $K = F(\alpha_1, \ldots, \alpha_n)$. Let L be the splitting field of $m_{\alpha_1,F}, \ldots, m_{\alpha_n,F}$. Then L/F is separable normal, and hence Galois. Since L/F is finite Galois, each intermediate fields corresponds to a subgroup of $\mathrm{Gal}(L/E)$, so they're in finite number. The previous proposition shows that K/F is simple. □

Proposition 3.2.16. Let K/F be a finite Galois extension and F'/F be any field extension. Then KF'/F' is Galois and $\mathrm{Gal}(KF'/F') \cong \mathrm{Gal}(K/K \cap F')$.

Proof. PET shows that $K = F(\alpha)$ for some $\alpha \in K$. Then KF' is the splitting field of $m_{\alpha,F'}$, which is separable. Hence KF'/F' is Galois. Consider the map

$$\Phi : \mathrm{Gal}(KF'/F') \longrightarrow \mathrm{Gal}(K/F)$$

$$\sigma \longmapsto \sigma|_K$$

Note that $\ker \Phi = \{\sigma \mid \sigma|_K = \mathrm{id}_K\} = \mathrm{id}_{KF'}$; Φ is injective. Let $H = \mathrm{Im}\,\Phi$. Clearly, we have $K \cap F' \subseteq K^H$. On the other hand, $K^H F'$ is fixed by $\mathrm{Gal}(KF'/F')$, so $K^H F' \subseteq F'$, implying $K^H \subseteq F'$. Since $K^H \subseteq K$, $K^H = K \cap F'$. In conclusion, $K^H = K \cap F'$. Hence $H \cong \mathrm{Gal}(K/K \cap F')$. □

Corollary 3.2.16.1. Let K, F' as above. Then $[KF' : F] = \dfrac{[K : F][F' : F]}{[K \cap F' : F]}$.

Remark 3.2.17. The condition imposed above is not superfluous. For instance, consider $K = \mathbb{Q}(\sqrt[3]{2})$, $F' = \mathbb{Q}(\sqrt[3]{2}e^{2\pi i/3})$ and $F = \mathbb{Q}$. Then $KF' = \mathbb{Q}(\sqrt[3]{2})$, $[KF' : F] = 6$, but $\dfrac{[K : F][F' : F]}{[K \cap F' : F]} = 9$.

Proposition 3.2.18. Let K_i/F be finite Galois, $i = 1, 2$. Then

1. $K_1 \cap K_2$ is Galois over F.
2. K_1K_2 is Galois over F, with

$$\mathrm{Gal}(K_1K_2/F) \cong \{(\sigma, \tau) \in \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F) \mid \sigma|_{K_1 \cap K_2} = \tau|_{K_1 \cap K_2}\}$$

Proof.

1. This is clear.
2. That K_1K_2 is Galois over F is clear. Consider the map

$$\Phi : \mathrm{Gal}(K_1K_2/F) \longrightarrow \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$$

$$\sigma \longmapsto (\sigma|_{K_1}, \sigma|_{K_2})$$

Note that $\ker \Phi = \{\sigma \mid \sigma|_{K_i} = \mathrm{id}_{K_i},\ i = 1, 2\} = 1$; Φ is injective. Put $H := \{(\sigma, \tau) \in \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F) \mid \sigma|_{K_1 \cap K_2} = \tau|_{K_1 \cap K_2}\}$. It's clear that $\mathrm{Im}\,\Phi \leqslant H$. We count their cardinality. $\#\,\mathrm{Im}\,\Phi = [K_1K_2 : F]$ and

$$\begin{aligned} \#H &= \sum_{\sigma \in \mathrm{Gal}(K_1/F)} \#\{\tau \in \mathrm{Gal}(K_2/F) \mid \sigma|_{K_1 \cap K_2} = \tau|_{K_1 \cap K_2}\} \\ &= [K_1 : F][K_2 : K_1 \cap K_2] = \frac{[K_1 : F][K_2 : F]}{[K_1 \cap K_2 : F]} \end{aligned}$$

where the second equality holds as in the proof of Theorem 3.2.2. The previous corollary shows $\#H = \#\,\mathrm{Im}\,\Phi$, and thus $\mathrm{Im}\,\Phi = H$.

□

Corollary 3.2.18.1. With the same condition above, if $K_1 \cap K_2 = F$, then $\mathrm{Gal}(K_1K_2/F) \cong \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$. Conversely, if $\mathrm{Gal}(K/F) = G_1 \times G_2$ for some $G_1, G_2 \trianglelefteq \mathrm{Gal}(K/F)$, then $K = K^{G_1}K^{G_2}$ with $K^{G_1} \cap K^{G_2} = F$.

Corollary 3.2.18.2. Let E/F be finite separable. Then

$$\bigcap_{\substack{E \subseteq K \subseteq \overline{F} \\ K/F\text{: Galois}}} K$$

is Galois over F, which is the smallest Galois extension of F containing E, called the **Galois closure** of E/F.

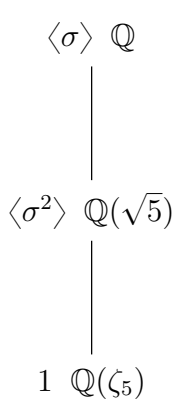
3.2.5 Cyclotomic extensions and abelian extensions

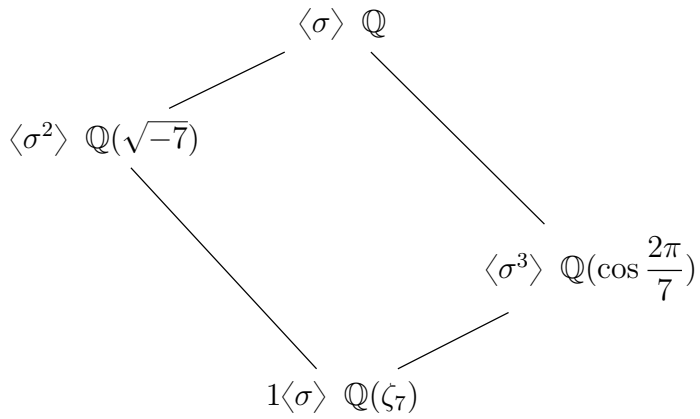
Definition. Let ζ_n be a primitive n-th root of unity. We call $\mathbb{Q}(\zeta_n)$ the **n-th cyclotomic field**.

- It's Galois over $\mathbb{Q}$ since all conjugates of ζ_n over $\mathbb{Q}$ have the form ζ_n^d, $(d, n) = 1$.
- $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, where the isomorphism is given by $(\mathbb{Z}/n\mathbb{Z})^\times \ni a \mapsto [\sigma_a : \zeta_n \mapsto \zeta_n^a]$.
- Consequently, if $n = p_1^{a_1} \cdots p_k^{a_k}$ is the prime decomposition of n, then

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_{p_1}^{a_1})/\mathbb{Q}) \times \cdots \times \mathrm{Gal}(\mathbb{Q}(\zeta_{p_k}^{a_k})/\mathbb{Q})$$

Example 3.2.19. $n = 5 : (\mathbb{Z}/5\mathbb{Z})^\times = (2)$. Let $\sigma = \sigma_2$. Note that $\sqrt{5} = \zeta_5 + \sigma^2\zeta_5$ is fixed by σ^2.





Example 3.2.20. $n = 7$: $(\mathbb{Z}/7\mathbb{Z})^\times = (3)$. Let $\sigma = \sigma_3$. Note $2\cos\frac{2\pi}{7} = \zeta_7 + \sigma^3\zeta_7 = \zeta_7 + \zeta_7^{-1}$ is fixed by σ^3.

Let's find the minimal polynomial of $2\cos\frac{2\pi}{7}$. The conjugates of $\zeta_7 + \zeta_7^{-1}$ over $\mathbb{Q}$ are $\sigma(\zeta_7 + \zeta_7^{-1})$ and $\sigma^2(\zeta_7 + \zeta_7^{-1})$. Thus $m_{2\cos(2\pi/7),\mathbb{Q}}(x) = x^3 + x^2 - 2x - 1$.

Exercise. Let p be an odd prime. Then $\mathbb{Q}(\zeta_p)$ contains $\begin{cases} \mathbb{Q}(\sqrt{p}) & \text{if } p \equiv 1 \pmod p \\ \mathbb{Q}(\sqrt{-p}) & \text{if } p \equiv 3 \pmod p \end{cases}$

Definition. An extension E/F is called an **abelian extension** if E/F is Galois and $\mathrm{Gal}(E/F)$ is abelian.

Proposition 3.2.21. Let G be a finite abelian group. Then there exists a Galois extension $K/\mathbb{Q}$ with Galois group isomorphic to G.

Proof. By FTFGAG, say $G \cong C_{n_1} \times \cdots \times C_{n_k}$. By Dirichlet's theorem on primes in arithmetic progression, there are primes p_j such that $p_j \equiv 1 \pmod{n}_j$. Now $(\mathbb{Z}/p_j\mathbb{Z})^\times$ is cyclic of order $p_j - 1$, so it contains a subgroup of index n_j, and thus $\mathbb{Q}(\zeta_{p_j})$ contains a subfield K_j of degree n_j over $\mathbb{Q}$. Then the composite $K = K_1 \cdots K_k$ satisfies that $K/\mathbb{Q}$ is Galois and $\mathrm{Gal}(K/\mathbb{Q}) \cong G$, since $K_i \cap K_j = \mathbb{Q}$ if $i \neq j$. □

Theorem 3.2.22 (Kronecker-Weber)**.** Any abelian extension of $\mathbb{Q}$ is a subfield of some cyclotomic field.

Exercise. Let D be a squarefree integer. We know $\mathbb{Q}(\sqrt{D})$ is contained in some cyclotomic field. Find one.

Remark 3.2.23.

1. The Kronecker-Weber theorem basically says {abelian extensions of $\mathbb{Q}$} corresponds to {subgroups of $(\mathbb{Z}/n\mathbb{Z})^\times$}. More generally, the *class field theory* says that if F is a number field and $\mathcal{O}$ is its ring of integers, then {abelian extensions of F} corresponds to {$(\mathcal{O}/(\text{nonzero ideal}))^\times$}.

2. ζ_n is a value of analytic function $e^{2\pi ix}$ at torsion points of $\mathbb{R}/\mathbb{Z}$, i.e, $\mathbb{Q}/\mathbb{Z}$. Thus, every abelian extension of $\mathbb{Q}$ can be obtained by *adjoining* special values of some analytic functions to $\mathbb{Q}$.

Kronecker's Jugendtraum (Youth dream in English), aka Hilbert's twelfth problem, asks given a number field F, find analytic functions such that every abelian extension of F can be obtained by adjoining some special values of these functions to F. For example, $F = \mathbb{Q}(\sqrt{D})\,(D > 0)$ can be obtained by adjoining elliptic functions and modular functions. For general F, only for CM field case we know such functions exist (but not constructive).

Example 3.2.24. Recall that a regular 17-gon is constructible. Let $\sigma = \sigma_3$.

$$\begin{array}{c} \langle\sigma\rangle \;\; \mathbb{Q} \\ | \\ \langle\sigma^2\rangle \;\; \mathbb{Q}(\sqrt{17}) \\ | \\ \langle\sigma^4\rangle \;\; K \\ | \\ \langle\sigma^8\rangle \;\; \mathbb{Q}(\cos\frac{2\pi}{17}) \\ | \\ 1 \;\; \mathbb{Q}(\zeta_{17}) \end{array}$$

Let $\eta_1 = \zeta + \sigma^2\zeta + \sigma^4\zeta + \cdots = \zeta + \zeta^9 + \zeta^{13} + \zeta^{15} + \zeta^{16} + \zeta^8 + \zeta^4 + \zeta^2$ and $\eta_2 = \sigma\eta_2 = \zeta^3 + \zeta^{10} + \cdots$. Then $\eta_1 + \eta_2 = -1$ and $\eta_1\eta_2 = -4$; to determine the value of η_1, note that

$$\begin{aligned} \eta_1 &= (\zeta + \zeta^{-1}) + (\zeta^2 + \zeta^{-2}) + (\zeta^4 + \zeta^{-4}) + (\zeta^8 + \zeta^{-8}) \;\sim\; 1.562 > 0 \\ \eta_2 &= (\zeta^3 + \zeta^{-3}) + (\zeta^5 + \zeta^{-5}) + (\zeta^6 + \zeta^{-6}) + (\zeta^7 + \zeta^{-7}) \sim -2.562 < 0 \end{aligned}$$

thus

$$\eta_1 = \frac{-1+\sqrt{17}}{2} \text{ and } \eta_2 = \frac{-1-\sqrt{17}}{2}$$

This shows the fixed field of $\langle\sigma^2\rangle$ is $\mathbb{Q}(\sqrt{17})$.

In general, for a Fermat prime $n = 2^{2^N} + 1$, $N \geqslant 1$, we consider the **periods** of $\zeta = \zeta_n$: first, choose a generator of $\mathbb{F}_n^\times$; we may pick 3 as a generator since 3 is not a quadratic residue mod n, for $\left(\frac{3}{n}\right) = \left(\frac{n}{3}\right) = \left(\frac{2}{3}\right) = -1$, and $\mathbb{F}_n^\times$ has order a power of 2. Let $\sigma = \sigma_3$, $n = k\ell$, and for $0 \leqslant r \leqslant k-1$, put

$$\eta_r = (1 + \sigma^k + \cdots + \sigma^{k(\ell-1)})\sigma^r\zeta = \zeta^{3^r} + \zeta^{3^{r+k}} + \cdots + \zeta^{3^{r+k(\ell-1)}}$$

Let $H_\ell = \langle\sigma^k\rangle \leqslant \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ be the subgroup of order ℓ, and let $K_\ell = \mathbb{Q}(\zeta)^{H_\ell}$ be its fixed field. Then the η_r are fixed by σ_k and we see $\{\eta_0, \eta_1, \ldots, \eta_{k-1}\}$ is a basis for $K_\ell/\mathbb{Q}$, and we call them the **periods of ℓ terms**. Also, we define $\eta^{(t)} := \zeta^t + \zeta^{t3^k} + \cdots + \zeta^{t3^{k(\ell-1)}}$ for η a period of ℓ term, for $0 \leqslant t \leqslant n-1$; note that $\eta^{(t)}$ is the η_r in which ζ^t appears.

We resume our work on finding fixed fields of subgroups. As the terminology above, we establish the periods of 8 terms ($k = 2$)

$$\begin{aligned} \eta_0 &= \zeta^{3^0} + \zeta^{3^{0+2}} + \zeta^{3^{0+4}} + \cdots + \zeta^{3^{0+14}} &&= \zeta + \zeta^9 + \zeta^{13} + \zeta^{15} + \zeta^{16} + \zeta^8 + \zeta^4 + \zeta^2 \\ \eta_1 &= \zeta^{3^1} + \zeta^{3^{1+2}} + \zeta^{3^{1+4}} + \cdots + \zeta^{3^{1+14}} &&= \zeta^3 + \zeta^{10} + \zeta^5 + \zeta^{11} + \zeta^{14} + \zeta^7 + \zeta^{12} + \zeta^6 \end{aligned}$$

Then $\eta_0 + \eta_1 = -1$ and

$$\eta_0\eta_1 = \eta^{(4)} + \eta^{(11)} + \eta^{(6)} + \eta^{(12)} + \eta^{(15)} + \eta^{(8)} + \eta^{(13)} + \eta^{(7)} = 4\eta_0 + 4\eta_1 = -4$$

As shown in above, we have

$$\eta_0 = \frac{-1+\sqrt{17}}{2} \text{ and } \eta_1 = \frac{-1-\sqrt{17}}{2}$$

Next, consider the period of 4 terms ($k = 4$)

$$\begin{array}{lll}
\eta'_0 &= \zeta^{3^0} + \zeta^{3^{0+4}} + \zeta^{3^{0+8}} + \zeta^{3^{0+12}} &= \zeta + \zeta^{13} + \zeta^{16} + \zeta^4 \\
\eta'_1 &= \zeta^{3^1} + \zeta^{3^{1+4}} + \zeta^{3^{1+8}} + \zeta^{3^{1+12}} &= \zeta^3 + \zeta^5 + \zeta^{14} + \zeta^{12} \\
\eta'_2 &= \zeta^{3^2} + \zeta^{3^{2+4}} + \zeta^{3^{2+8}} + \zeta^{3^{2+12}} &= \zeta^9 + \zeta^{15} + \zeta^8 + \zeta^2 \\
\eta'_3 &= \zeta^{3^3} + \zeta^{3^{3+4}} + \zeta^{3^{3+8}} + \zeta^{3^{3+12}} &= \zeta^{10} + \zeta^{11} + \zeta^7 + \zeta^6
\end{array}$$

We have $\eta'_0 + \eta'_2 = \eta_0$, $\eta'_1 + \eta'_3 = \eta_1$

$$\begin{array}{llll}
\eta'_0\eta'_2 &= \eta'^{(10)} + \eta'^{(16)} + \eta'^{(9)} + \eta'^{(3)} &= \eta'_0 + \eta'_1 + \eta'_2 + \eta'_3 &= -1 \\
\eta'_1\eta'_3 &= \eta'^{(13)} + \eta'^{(14)} + \eta'^{(10)} + \eta'^{(9)} &= \eta'_0 + \eta'_1 + \eta'_2 + \eta'_3 &= -1
\end{array}$$

Also,

$$\begin{array}{lll}
\eta'_0 &= \zeta + \zeta^{13} + \zeta^{16} + \zeta^4 &= 2(\cos\frac{2\pi}{17} + \cos\frac{8\pi}{17}) > 0 \\
\eta'_1 &= \zeta^3 + \zeta^5 + \zeta^{14} + \zeta^{12} &= 2(\cos\frac{6\pi}{17} + \cos\frac{10\pi}{17}) > 0 \\
\eta'_2 &= \zeta^9 + \zeta^{15} + \zeta^8 + \zeta^2 &= 2(\cos\frac{4\pi}{17} + \cos\frac{16\pi}{17}) < 0 \\
\eta'_3 &= \zeta^{10} + \zeta^{11} + \zeta^7 + \zeta^6 &= 2(\cos\frac{12\pi}{17} + \cos\frac{14\pi}{17}) < 0
\end{array}$$

Thus

$$\begin{array}{lll}
\eta'_0 &= \dfrac{\eta_0 + \sqrt{\eta_0^2 + 4}}{2} &= \dfrac{-1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}}}{4} \\
\eta'_2 &= \dfrac{\eta_0 - \sqrt{\eta_0^2 + 4}}{2} &= \dfrac{-1 + \sqrt{17} - \sqrt{34 - 2\sqrt{17}}}{4} \\
\eta'_1 &= \dfrac{\eta_1 + \sqrt{\eta_1^2 + 4}}{2} &= \dfrac{-1 - \sqrt{17} + \sqrt{34 + 2\sqrt{17}}}{4} \\
\eta'_3 &= \dfrac{\eta_1 + \sqrt{\eta_1^2 + 4}}{2} &= \dfrac{-1 - \sqrt{17} - \sqrt{34 + 2\sqrt{17}}}{4}
\end{array}$$

This shows $K = \mathbb{Q}(\sqrt{34 - 2\sqrt{17}})$. Last, consider two period of 2 terms ($k = 8$)

$$\begin{array}{llll}
\eta''_0 &= \zeta^{3^0} + \zeta^{3^{0+8}} &= \zeta + \zeta^{16} &= 2\cos\frac{2\pi}{17} \\
\eta''_4 &= \zeta^{3^{0+4}} + \zeta^{3^{0+12}} &= \zeta^{13} + \zeta^4 &= 2\cos\frac{8\pi}{17}
\end{array}$$

Clearly, $\eta''_0 + \eta''_4 = \eta'_0$ and $\eta''_0\eta''_4 = \eta^{14} + \eta^{12} + \eta^5 + \eta^3 = \eta'_1$. We finally arrive at the expression

$$\begin{aligned}
\cos\frac{2\pi}{17} = \frac{\eta''_0}{2} &= \frac{\eta'_0 + \sqrt{\eta'^2_0 - 4\eta'_1}}{4} \\
&= \frac{-1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}} + 2\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}}{16}
\end{aligned}$$

3.2.6 Galois groups of polynomials

Let $f(x)$ be a separable polynomial over F of degree n, $\alpha_1, \ldots, \alpha_n$ be its roots, and K its splitting field over F. Clearly, we can embed $\mathrm{Gal}(K/F)$ into S_n.

- If f is irreducible over F, then $\mathrm{Gal}(K/F) \leqslant S_n$ is transitive.

Example 3.2.25. $n = 4$: The Galois group of an irreducible separable polynomial over F can only be S_4, A_4, D_8, C_4, V_4.

We consider a general setting : Let $x_1, \ldots, x_n$ be indeterminates, and put $L = F(x_1, \ldots, x_n)$. Let

$$\begin{aligned} s_1 &= \sum_{i=1}^{n} x_i && = x_1 + \cdots + x_n \\ s_2 &= \sum_{i<j} x_i x_j && = x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n \\ s_3 &= \sum_{i<j<k} x_i x_j x_k \\ &\vdots \\ s_n &= x_1 \cdots x_n \end{aligned}$$

Equivalently, let $f(X) := \prod_{i=1}^{n}(X - x_i) = X^n - s_1X^{n-1} + s_2X^{n-2} + \cdots + (-1)^n s_n \in L[X]$; the s_i are called the **i-th elementary symmetric function** of $x_1, \ldots, x_n$, and $f(X)$ is called the **general polynomial of degree** n.

Put $K = F(s_1, \ldots, s_n)$. Then clearly, L/K is Galois since L is the splitting field of $f(X)$ over K; this shows $[L : K] \leqslant n!$. On the other hand, every automorphism on L may be viewed as a permutation on subscripts of the x_i, so $S_n \leqslant \mathrm{Aut}(L)$. The symmetry makes K lie in the fixed field L^{S_n} of S_n. By Galois theory, $[L : K] \geqslant [L : L^{S_n}] = n!$. Thus, we conclude that $[L : K] = n!$, that is, $\mathrm{Gal}(L/K) \cong S_n$.

Theorem 3.2.26. The fixed field of S_n acting on the field $F(x_1, \ldots, x_n)$ of rational functions in n variables is the field $F(s_1, \ldots, s_n)$ of rational functions in elementary symmetric functions.

Corollary 3.2.26.1. Any symmetric function in $x_1, \ldots, x_n$ is a rational function in $s_1, \ldots, s_n$.

In fact, we have a stronger statement:

Theorem 3.2.27. Let A be a commutative ring with 1 and $R = A[x_1, \ldots, x_n]$. Regard S_n as a subgroup of $\mathrm{Aut}(R)$. Then $R^{S_n} = A[s_1, \ldots, s_n]$.

Proof. We define the lexicographical order on R by

1. $x_1 > x_2 > \cdots > x_n$

2. $x_1^{a_1}\cdots x_n^{a_n} > x_1^{b_1}\cdots x_n^{b_n}$ if and only if there exists $k \in \{1,\ldots,n\}$ such that $a_i = b_i$ for $i < k$ and $a_i > b_i$.

Let $f \in R^{S_n}$, let $x_1^{a_1}\cdots x_n^{a_n}$ be its leading monomial and $c \in R$ be its coefficient. By symmetric, we may assume $a_1 \geqslant \cdots \geqslant a_n$. Consider the polynomial $h = f - as_1^{a_1-a_2}s_2^{a_2-a_3}\cdots s_{n-1}^{a_{n-1}-a_n}s_n^{a_n}$. Then h has order less than f. The result follows by induction on order of f. □

Proposition 3.2.28. Let A be a UFD of characteristic $\neq 2$, $R = A[x_1,\ldots,x_n]$ and let

$$d = \prod_{i<j}(x_1 - x_j)$$

Let A_n act on R by $\sigma(x_i) = x_{\sigma(i)}$; thus, we may regard A_n as a subgroup of $\mathrm{Aut}(R)$. Then $R^{A_n} = R^{S_n}[d] = A[s_1,\ldots,s_n,d]$.

Proof. Let $f \in R^{A_n}$ and fix $\sigma \in S_n\backslash A_n$. Consider the expression

$$f = \frac{f+\sigma f}{2} + \frac{f-\sigma f}{2}$$

If $\tau \in A_n$, then

$$\tau\left(\frac{f\pm\sigma f}{2}\right) = \frac{\tau f \pm \sigma(\sigma^{-1}\tau\sigma)f}{2} = \frac{f\pm\sigma f}{2}$$

if $\tau \in S_n\backslash A_n$, then

$$\tau\left(\frac{f\pm\sigma f}{2}\right) = \frac{\sigma(\sigma^{-1}\tau)f \pm \tau\sigma f}{2} = \frac{\sigma f \pm f}{2} = \pm\left(\frac{f\pm\sigma f}{2}\right)$$

Hence the former is in R^{S_n}, so it suffices to deal with the latter. Let $h \in R^{A_n}$ and $\sigma(h) = -h$ for all $\sigma \in S_n\backslash A_n$. We claim $h = dg$ for some $g \in R^{S_n}$. Note $(1\,2)h(x_1,x_2,\ldots,x_n) = h(x_2,x_1,\ldots,x_n)$, but since $(1\,2) \notin A_n$, $(1\,2)h = -h$; thus $h(x_1,x_2,\ldots,x_n) + h(x_2,x_1,\ldots,x_n) = 0$, which implies $x_1 - x_2 \mid h$. Similarly, $x_i - x_j \mid h$ for all $i \neq j$. Since R is a UFD and each $x_i - x_j$, $i<j$ is relatively prime, $d \mid h$, and thus $h = dg$ for some $g \in R$. Since $\sigma(h/d) = h/d$ for all $\sigma \in S_n$, we have $g \in R^{S_n}$. □

For $i \geqslant 0$, we consider $p_i = \sum_{j=1}^{n} x_j^i = x_1^i + \cdots + x_n^i$, the sum of the i-th powers. For convenience, we let $s_i = 0$ for $i > n$. Then we have the **Newton formulas**:

Theorem 3.2.29.

$$s_k(x_1,\cdots,x_n) = \frac{1}{k}\sum_{i=1}^{k}(-1)^{i-1}s_{k-i}(x_1,\cdots,x_n)p_i(x_1,\cdots,x_n),$$

$$p_k(x_1,\ldots,x_n) = (-1)^{k-1}ks_k(x_1,\cdots,x_n) + \sum_{i=1}^{k-1}(-1)^{k-1+i}s_{k-i}(x_1,\ldots,x_n)p_i(x_1,\ldots,x_n),$$

Proof. Let $R = \mathbb{Z}[x_1, \ldots, x_n]$. We may view $f(X) = \prod_{i=1}^{n}(1 - x_i X) = \sum_{k=0}^{n}(-1)^k s_k X^k \in R[[X]]$, the ring of formal power series. Formally differentiating $f(X)$ with respect to X and multiplying X, one obtain

$$\begin{aligned}
\sum_{k=0}^{n}(-1)^k k s_k X^k &= X\sum_{i=1}^{n}\left[-x_i\prod_{j\neq i}(1 - x_j X)\right] \\
&= -\left(\sum_{i=1}^{n}\frac{x_i X}{1 - x_i X}\right)\prod_{i=1}^{n}(1 - x_i X) \\
&= -\left(\sum_{i=1}^{n}\sum_{k=1}^{\infty}(x_i X)^k\right)\left(\sum_{k=0}^{n}(-1)^k s_k X^k\right) \\
&= \left(\sum_{k=1}^{\infty}p_k X^k\right)\left(\sum_{k=0}^{n}(-1)^{k-1} s_k X^k\right)
\end{aligned}$$

which is what we want. □

Definition. Define the **discriminant** Δ of $x_1, \ldots, x_n$ to be the product

$$\Delta = \prod_{i<j}(x_i - x_j)^2$$

For $f \in F[x]$, we define $\mathrm{disc}(f)$ to be the discriminant of its roots.

- By Corollary 2.4.29.1, we see $R_{f,f'} = \prod_{i=1}^{n} f'(x_i)$. Hence $\Delta = (-1)^{\frac{n(n-1)}{2}} R_{f,f'}$.

Proposition 3.2.30. Let F be a field of characteristic $\neq 2$ and $f \in F[x]$ be a separable polynomial of degree n. Then the Galois group of f over F is contained in A_n if and only if $\mathrm{disc}(f)$ is a square in F.

Proof. This is a consequence of Proposition 3.2.28. □

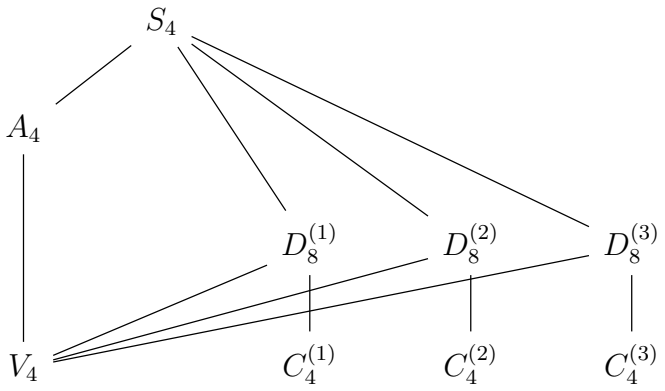
Example 3.2.31.

1. $f(x) = x^2 + ax + b$, $\mathrm{disc}(f) = a^2 - 4b$.
2. $f(x) = x^3 + ax^2 + bx + c$, $\mathrm{disc}(f) = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc$
   (i) $x^3 - 2$, disc $= -108$, which is not a square in $\mathbb{Q} \Rightarrow \mathrm{Gal} \cong S_3$
   (ii) $m_{2\cos(2\pi/7),\mathbb{Q}}(x) = x^3 + x^2 - 2x - 1$, disc $= 49 = 7^2 \Rightarrow \mathrm{Gal} \cong A_3$

   Let F be a field with $\mathrm{Char}(F) \neq 2$. Let $f \in F[x]$ and K be its splitting field over F. Let $\theta \in K$ be a root of f and put $G = \mathrm{Gal}(K/F)$.

- If f is reducible, the G is either trivial or C_2.
- If f is irreducible and $\operatorname{disc}(f)$ is a square in F, then $G = A_3 = C_3$ and $K = F(\theta)$; otherwise, if $\operatorname{disc}(f)$ is not a square in F, then $G = S_3$ and $K = F(\theta, \sqrt{\operatorname{disc}(f)})$.

3. $f(x) = x^4 + ax^3 + bx^2 + cx + d$. Let $\alpha_1, \ldots, \alpha_4$ be its roots, and K be its splitting field over $\mathbb{Q}$. Suppose f is irreducible; this implies $\operatorname{Gal}(K/\mathbb{Q}) \leqslant S_4$ is transitive. We list all transitive subgroups of S_4 below:



where $D_8^{(1)} = \langle (1\,3\,2\,4), (1\,2) \rangle$, $D_8^{(2)} = \langle (1\,2\,3\,4), (1\,3) \rangle$, $D_8^{(3)} = \langle (1\,2\,4\,3), (1\,4) \rangle$ are Sylow 4-subgroups and $V_4 = \{1, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$.

Consider the elements

$$\theta_1 = (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4) \in K^{D_8^{(1)}}$$
$$\theta_2 = (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4) \in K^{D_8^{(2)}}$$
$$\theta_3 = (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3) \in K^{D_8^{(3)}}$$

Any symmetric sum of the θ_i is invariant under S_4, so

$$\begin{aligned} g(x) &= (x - \theta_1)(x - \theta_2)(x - \theta_3) \in F[x] \\ &= x^3 - 2bx^2 + (b^2 + ac - 4d)x + (c^2 - abc + a^2 d) \end{aligned}$$

called the **resolvent cubic** of f. Equivalently, we may consider the elements

$$\theta_1' = \alpha_1\alpha_2 + \alpha_3\alpha_4 \in K^{D_8^{(1)}}$$
$$\theta_2' = \alpha_1\alpha_3 + \alpha_2\alpha_4 \in K^{D_8^{(2)}}$$
$$\theta_3' = \alpha_1\alpha_4 + \alpha_2\alpha_3 \in K^{D_8^{(3)}}$$

and similarly define the resolvent cubic

$$(x-\theta_1')(x-\theta_2')(x-\theta_3') = x^3 - bx^2 + (ac-4d)x + (4bd - c^2 - a^2 d) \in F[x]$$

The relation of two different resolvent is that $\theta_i + \theta_i' = b\,(i = 1, 2, 3)$. Notice that

$$\begin{aligned}
\theta_1 - \theta_2 &= -(\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3) \\
\theta_1 - \theta_3 &= -(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_4) \\
\theta_2 - \theta_3 &= -(\alpha_1 - \alpha_2)(\alpha_3 - \alpha_4)
\end{aligned}$$

so $\operatorname{disc}(g) = \operatorname{disc}(f)$. Thus

$$\begin{aligned}
\operatorname{disc}(f) = &- 128b^2d^2 - 4a^3c^3 + 16b^4d - 4b^3c^2 - 27a^4d^2 + 18abc^3 \\
&+ 144a^2bd^2 - 192acd^2 + a^2b^2c^2 - 4a^2b^3d - 6a^2c^2d \\
&+ 144bc^2d + 256d^3 - 27c^4 - 80ab^2cd + 18a^3bcd
\end{aligned}$$

Let E be the splitting field of the resolvent cubic g over $\mathbb{Q}$. We have $E \subseteq K$, so the Galois group of g is a quotient of that of f. Hence knowing the action of Galois group on the roots of g gives information above the Galois group of f. Let $G = \operatorname{Gal}(K/F)$.

- If g is irreducible over F, this means $3 \mid G \Rightarrow 12 \mid G$. If $\operatorname{disc}(f)$ is not a square in F, then $G = S_4$; otherwise, $G = A_4$.
- If g splits completely in F, this means $\theta_1, \theta_2, \theta_3 \in F$, and thus $G \subseteq D_8^{(1)} \cap D_8^{(2)} \cap D_8^{(3)} = V_4$. The only possible is $G = V_4$.
- If g has only one root in F, say $\theta_1 \in F$, we have $G \subseteq D_8^{(1)}$ but $G \nsubseteq V_4$, so whether $G = D_8^{(1)}$ or $G = C_4^{(1)}$. To distinguish them, recall that $F(\sqrt{\operatorname{disc}(f)})$ is the fixed field of A_4 and that $D_8 \cap A_4 = V_4$, $C_4 \cap A_4 = C_2$; the former group is transitive, while the latter is not. This indicates that is f is irreducible over $F(\sqrt{\operatorname{disc}(f)})$, then $G = D_8^{(1)}$; otherwise, $G = C_4^{(1)}$.

The criteria for D_8 and C_4 are hard to verify. However, when $\operatorname{Char}(F) \neq 2$, we have an alternative, which is quite elementary. Assume $\theta_1 \in F$ and $\theta_2, \theta_3 \notin F$. Consider the polynomial

$$h(x) = (x^2 + ax + \theta_1)(x^2 - (b - \theta_1)x + d) \in F[x]$$

in which the quadratic factors are picked so that the former has roots $\alpha_1 + \alpha_2$, $\alpha_3 + \alpha_4$ and the latter has roots $\alpha_1\alpha_2$, $\alpha_3\alpha_4$. If $G = C_4$, then $E = F(\sqrt{\operatorname{disc}(f)})$ is the only quadratic extension of F contained in K, so the quadratic factors of $h(x)$ splits in E. Conversely, if $h(x)$ splits completely in E, consider the quadratic polynomial $x^2 - (\alpha_1 + \alpha_2) + \alpha_1\alpha_2 \in E[x]$, and let M be its splitting field

over E. We have $\alpha_1, \alpha_2 \in M$, and since $\alpha_3 + \alpha_4 = -a - \alpha_1 - \alpha_2$ and $\alpha_3\alpha_4 = d/\alpha_1\alpha_2$, $\alpha_3, \alpha_4 \in M$; this shows $M = K$. Thus

$$\#G = [K : M][M : E][E : F] \leqslant 1 \cdot 2 \cdot 2 = 4 < \#D_8^{(1)}$$

and this forces $G = C_4^{(1)}$, and $E = F(\sqrt{\mathrm{disc}(f)})$.

(i) $x^4 + x^3 + x^2 + x + 1$. disc $= 125$. resolvent cubic $= x^3 - 2x^2 - 2x + 1 = (x + 1)(x^2 - 3x + 1)$. Also, $x^4 + x^3 + x^2 + x + 1 = (x^2 + \dfrac{1+\sqrt{5}}{2}x + 1)(x^2 + \dfrac{1-\sqrt{5}}{2}x + 1)$ is reducible in $\mathbb{Q}(\sqrt{5})$, so the Galois group is C_4.

(ii) $x^4 - 2x^2 - 1$. disc $= -1024$. resolvent cubic $= x(x^2 + 4x + 8)$. Also, $x^4 - 2x^2 - 1$ is irreducible over $\mathbb{Q}(i)$, so the Galois group is D_8.

(iii) In general, the polynomial $f(x) = x^4 + ax^2 + b \in F[x]$ has its resolvent cubic $g(x) = x^3 - 2ax^2 + (a^2 - 4b)x = x(x^2 - 2ax + (a^2 - 4b))$ splits in F, so its possible Galois group G is V_4, D_8, C_4. The discriminant of $f(x)$ is $\mathrm{disc}(g) = 16b(a^2 - 4b)^2$, so $G = V_4$ if and only if b is a square in F. Assume $\mathrm{Char}(F) \neq 2$ so that our criteria above apply. The remaining cases automatically satisfy that b is not a square in F. Let $h(x) = x^2(x^2 - ax + b)$ be the associated polynomial as above. Then $G = C_4$ if and only if $a^2 - 4b$ is a square in $F(\sqrt{b})$, if and only if $F(\sqrt{b}) = F(\sqrt{a^2 - 4b})$, if and only if $b(a^2 - 4b)$ is a square in F. Thus $G = D_8$ if and only if neither $b(a^2 - 4b)$ nor b is a square in F.

4. Let p be a prime and $f \in \mathbb{Q}[x]$ be an irreducible polynomial of degree p. Assume f has $p - 2$ distinct real roots and two non-real roots. Then $\mathrm{Gal}(f/\mathbb{Q}) \cong S_p$. Indeed, the irreducibility shows that $\mathrm{Gal}(f/\mathbb{Q}) \leqslant S_p$ is transitive, and thus $p \mid \mathrm{Gal}(f/\mathbb{Q})$. Cauchy's theorem indicates $\mathrm{Gal}(f/\mathbb{Q})$ has a p-cycle. The two non-real roots of f makes the complex conjugation lies in $\mathrm{Gal}(f/\mathbb{Q})$, so $\mathrm{Gal}(f/\mathbb{Q})$ has a 2-cycle. By conjugating, $\mathrm{Gal}(f/\mathbb{Q})$ admits all 2-cycles, and thus $\mathrm{Gal}(f/\mathbb{Q}) = S_p$.

   For instance, let $p \geqslant 5$ and pick $p - 2$ distinct even integers $n_1 < \cdots < n_{p-2}$ and m a positive even integer. Form the polynomial

$$f(x) = (x^2 + m)(x - n_1) \cdots (x - n_{p-2}) - 2$$

   If ℓ is any odd integer in some interval (n_i, n_{i+1}), then

$$|(k^2 + m)(k - n_1) \cdots (k - n_{p-2})| \geqslant k^2 + m \geqslant 3$$

   and therefore f has at least $p - 2$ distinct real roots. We will pick appropriate m so that f has exactly $p - 2$ real roots. Let

$$(x - \alpha_1) \cdots (x - \alpha_p) = (x^2 + m)(x - n_1) \cdots (x - n_{p-2}) - 2$$

Comparing the coefficients of x^{p-1} and x^{p-2}, we have $\sum_i \alpha_i = \sum_i n_i$ and $\sum_{i<j} \alpha_i\alpha_j = m + \sum_{i<j} n_i n_j$, so

$$\sum_i \alpha_i^2 = (\sum_i \alpha_i)^2 - 2\sum_{i<j} \alpha_i\alpha_j = (\sum_i n_i)^2 - 2\sum_{i<j} n_i n_j - 2m = \sum_i n_i^2 - 2m$$

Pick $2m > \sum_i n_i^2$ so that $\sum_i \alpha_i^2 < 0$; this will make some α_i non-real. We may pick $m = \sum_i n_i^2$, and thus

$$\left(x^2 + \sum_i n_i^2\right)(x - n_1)\cdots(x - n_{p-2}) - 2 \in \mathbb{Q}[x]$$

is a polynomial with Galois group S_p, $p \geqslant 5$.

Computation of Galois group over $\mathbb{Q}$

Let $f \in \mathbb{Z}[x]$. Consider the reduction $\overline{f}$ of f modulo p, p a prime. The Galois group of $\overline{f}$ over $\mathbb{F}_p$ will give us some information about the Galois group of f over $\mathbb{Q}$.

Theorem 3.2.32. For $p \nmid \operatorname{disc}(f)$, the Galois group of $\overline{f}$ over $\mathbb{F}_p$ is isomorphic to a subgroup of that of f over $\mathbb{Q}$.

Example 3.2.33.

1. $x^3 - 2$. Consider $p = 5$. Then $x^3 - 2 \equiv (x-3)(x^2 - 2x - 1) \pmod 5$, so the Galois group over $\mathbb{F}_5$ is C_2. This means there's a 2-cycle in the Galois group of $\mathbb{Q}$, and thus it's S_3.

2. $x^5 - x - 1$. $\operatorname{disc} = 19 \cdot 151$. For $p = 2$, we have $x^5 - x - 1 = (x^2 + x + 1)(x^3 + x^2 + 1)$, whose Galois group over $\mathbb{F}_2$ is C_6. This means the Galois group G of $x^5 - x - 1$ over $\mathbb{Q}$ has an element of order 6. In S_5, it must has form $(\cdot\cdot)(\cdot\ \cdot\ \cdot)$. Raising this element to the 3-rd power, we get a transposition, so G contains a 5-cycle and a 2-cycle, and thus is S_5.

More precisely, assume $f \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Q}$ and of degree n. Let K be its splitting field over $\mathbb{Q}$ and $\mathcal{O}_K$ be its ring of integers. Assume $p \nmid \operatorname{disc}(f)$. Pick a prime ideal Q of $\mathcal{O}_K$ containing p, which is always available since $\mathcal{O}_K$ is a Dedekind domain. Then there's a unique $\sigma \in \operatorname{Gal}(K/\mathbb{Q})$ such that $\sigma(a) \equiv a^p \pmod Q$ for all $a \in \mathcal{O}_K$ and $\operatorname{Gal}(f/\mathbb{F}_p) \cong \langle\sigma\rangle$. Different choices of Q yield conjugates of σ. Moreover, consider σ as an element of S_n and assume it has cycle type $n_1, n_2, \ldots, n_k$, including 1-cycles. Then the irreducible factors of $\overline{f}$ over $\mathbb{F}_p$ has degrees $n_1, \ldots, n_k$. Note that if $\operatorname{Gal}(K/\mathbb{Q})$ is abelian, then the condition $\sigma(a) \equiv a^p \pmod Q$ reduces to $\sigma(a) \equiv a^p \pmod{p\mathcal{O}_K}$. The correspondence $Q \mapsto \sigma$ is called the **Artin map**.

Example 3.2.34.

1. x^2+1.

   - $p \equiv 1 \pmod 4$, we have $i^p = i$ and $\sigma = \mathrm{id}$; $x^2+1 = (x-a)(x+a)$ for some $a \in \mathbb{F}_p$
   - $p \equiv 3 \pmod 4$, we have $i^p = -i$ and $\sigma = -\mathrm{id}$; x^2+1 is irreducible over $\mathbb{F}_p$.

2. Let $a \in \mathbb{Z}$ be squarefree and p a prime. Consider $x^2 - a$. $\sigma(\sqrt{a}) \equiv (\sqrt{a})^p \pmod p$. We have

$$\begin{aligned} \sigma = \mathrm{id} &\Leftrightarrow \sqrt{a} \equiv (\sqrt{a})^p \pmod p \\ &\Leftrightarrow a^{\frac{p-1}{2}} \equiv 1 \pmod p \\ &\Leftrightarrow a \text{ is a quadratic residue mod } p \end{aligned}$$

   This shows that the Artin map is a generalization of the Legendre symbol.

3. $x^3 - 2$. $\mathrm{disc} = -108$. Let p be a prime $\neq 2, 3$.

$$\mathrm{Gal} \cong \begin{cases} 1 \text{ or } A_3 & \text{if } \left(\dfrac{-108}{p}\right) = 1 \Leftrightarrow p \equiv 1 \pmod 3 \\ S_3 & \text{if } p \equiv 2 \pmod 3 \end{cases}$$

   If $p \equiv 2 \pmod 3$, the map $a \mapsto a^3$ is an automorphism on $\mathbb{F}_p^\times$. This means $x^3 - 2$ always has a solution a in $\mathbb{F}_p$. Then $x^3 - 2 \equiv (x-a)(x^2+bx+c) \pmod p$, with x^2+bx+c irreducible over $\mathbb{F}_p$.

Theorem 3.2.35 (Chebatarev's)**.** Let $f \in \mathbb{Z}[x]$ be irreducible over $\mathbb{Q}$ of degree n. Given a partition π if n, say $n = n_1 + \cdots + n_k$ with $n_i \geqslant n_{i+1}$. Let N_π be the number of elements in $\mathrm{Gal}(f/\mathbb{Q}) \leqslant S_n$ having cycle type π. Then the ratio

$$\frac{\#\{p \leqslant X \mid f(x) \equiv g_1(x) \cdots g_k(x) \mod p,\ g_i \text{ is irreducible over } \mathbb{F}_p \text{ of degree } n_i = 1, \ldots, k\}}{\#\{p \leqslant X\}}$$

tends to $\dfrac{N_\pi}{\#\,\mathrm{Gal}(f/\mathbb{Q})}$ as $X \to \infty$.

Example 3.2.36. $x^3 - 2$. The Galois group over $\mathbb{Q}$ is S_3, which has one 1-cycle, three 2-cycles and two 3-cycle. Let X be the 10000-th prime. Then we have

Type	Number
$(x-a)(x-b)(x-c)$	1634
irreducible	3354
$(x-a)(x^2+bx+c)$	5010

which demonstrates the above theorem.

Example 3.2.37. $x^5 + 15x + 12$. It's Eisenstein at 3, so it's irreducible. disc $= 2^{10} \cdot 3^4 \cdot 5^5$. Let X be the 10000-th prime.. Recall that all transitive subgroup of S_5 are S_5, A_5, F_{20}, D_{10}, C_5.

Cycle type	Number
5	1979
$4+1$	5022
$3+2$	0
$3+1+1$	0
$2+2+1$	2488
$2+1+1+1$	0
$1+1+1+1+1$	508

Note that $\frac{508}{10000} \sim \frac{1}{20}$. We guess its Galois group is F_{20}.

Exercise. Prove the Galois group of $x^5 + 15x + 12$ over $\mathbb{Q}$ is F_{20}.

3.2.7 Solvable and radical extensions

By F we mean a field.

Definition. If $K = F(\sqrt[n]{a})$ for some $a \in F$ and $n \in \mathbb{N}$, we say K/F is a **simple radical extension**.

- K/F is Galois if and only if $(*)$: $\begin{cases} \text{all } n\text{-th roots of unity are contained in } F \\ \text{Char}(F) \nmid n \end{cases}$

Proposition 3.2.38. Assume $(*)$ holds and $a \in F$. Then $\text{Gal}(F(\sqrt[n]{a})/F)$ is cyclic of order dividing n.

Proof. By our assumption, $F(\sqrt[n]{a})/F$ is Galois. Denote by μ_n the group of n-th roots of unity. For each $\sigma \in \text{Gal}(F(\sqrt[n]{a})/F)$, $\sigma(\sqrt[n]{a}) = \zeta_\sigma(\sqrt[n]{a})$ for some $\zeta_\sigma \in \mu_n$. We thus obtain a map

$$\begin{aligned} \text{Gal}(F(\sqrt[n]{a})/F) &\longrightarrow \mu_n \\ \sigma &\longmapsto \zeta_\sigma \end{aligned}$$

Note that $\mu_n \subseteq F$ by assumption, so the map above is a homomorphism. Its kernel consists of automorphisms fixing $\sqrt[n]{a}$, which turn out being identity; this means the kernel is trivial. This shows $\text{Gal}(F(\sqrt[n]{a})/F)$ can be embedded into μ_n, and this makes it a cyclic group of order dividing $n = \#\mu_n$. □

Definition. We say K/F is a **cyclic extension** if K/F is Galois with cyclic Galois group.

Proposition 3.2.39. Assume $(*)$ holds and that K/F is cyclic of degree n. Then $K = F(\sqrt[n]{a})$ for some $a \in F$.

Proof. Say $\mathrm{Gal}(K/F) = \langle\sigma\rangle$. Let ζ be a primitive n-th roots of unity in F. Proposition 3.2.9 guarantees the existence of an element $\alpha \in F$ such that

$$\beta := \alpha + \zeta\sigma(\alpha) + \zeta^2\sigma^2(\alpha) + \cdots + \zeta^{n-1}\sigma^(n-1)(\alpha) \neq 0$$

where the form on the RHS is called the **Lagrange resolvent**. Applying σ to both sides, we obtain $\sigma(\beta) = \zeta^{-1}\alpha$, and thus the smallest integer i such that $\sigma^i(\beta) = \beta$ is n, which implies β is not contained in any proper intermediate field of K/F, i.e, $\deg_F \beta = n$; this shows $K = F(\beta)$.

Now consider $\sigma(\beta)^n = (\zeta^{-1}\beta)^n = \beta^n$, so $a := \beta^n \in K$. Thus $K = F(\sqrt[n]{a})$. □

Remark 3.2.40.

1. Albeit $\mathbb{Q}(\cos\frac{2\pi}{7})/\mathbb{Q}$ is cyclic, it's not a simple radical extension.
2. By the same token, assume $(*)$ holds, then $K = F(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k})$ is a Galois extension over F with $\mathrm{Gal}(K/F)$ abelian and of exponent n. Conversely, assume $(*)$ holds, and K/F is an abelian extension with $\mathrm{Gal}(K/F)$ of exponent n. Then $K = F(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k})$ for some $a_j \in F$. Such an extension is called a **Kummer extension**, and one can show there's an one-to-one correspondence between Kummer extensions of F and finitely generated subgroups of $F^\times/(F^\times)^n$. See also *Artin-Schreier extensions*.

Definition.

1. We say K/F is a **radical extension** if there is a tower of extensions

   $$F = K_0 \subseteq K_1 \subseteq \cdots K_{s-1} \subseteq K_s = K$$

   such that K_{i+1}/K_i is simple radical for $i = 0, 1, \ldots, s-1$.
2. $\alpha \in \overline{F}$ is said to be **expressible by radicals** if $\alpha \in K$ for some radical extension K/F.
3. A polynomial $f \in F[x]$ can be **solved by radicals** if all its roots can be expressible by radicals.

Lemma 3.2.41. Assume $\mathrm{Char}(F) = 0$ and $\alpha \in \overline{F}$ is expressible by radicals, say $\alpha \in K$, where K/F is radical. Then there's a Galois radical extension K'/F containing K with

$$F = K'_0 \subseteq K'_1 \subseteq \cdots K'_{s-1} \subseteq K'_s = K'$$

such that K'_{i+1}/K'_i is cyclic. In particular, $\mathrm{Gal}(K'/F)$ is solvable.

Proof. We will use the fact (which can be verified easily):

♠ If E_1, E_2 are radical over F, so is E_1E_2/F.

Assume $F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_{t-1} \subseteq K_t = K$ such that each K_{i+1}/K_i is simple radical. Let L/F be the Galois closure of K/F. Recall that L is the composite of all $\sigma(K)$, $\sigma \in \mathrm{Emb}(K/F)$; by applying σ to the tower, we see $\sigma(K)/F$ is also a radical extension. By ♠, L/F is radical, say

$$F = L_0 \subseteq L_1 \subseteq L_{n-1} \subseteq L_n = L$$

with each L_{i+1}/L_i simple radical. Note that those quotients might not be Galois; to make it so, consider $F' = F(\text{all } n_i\text{-th roots of unity})$, where $n_i = [L_{i+1} : L_i]$ for $0 \leqslant i \leqslant n-1$. Establish the tower

$$F \subseteq F' = F'L_0 \subseteq F'L_1 \subseteq F'L_{n-1} \subseteq F'L_n = F'L$$

By Proposition 3.2.38, each $F'L_{i+1}/F'L_i$ is cyclic (it is the place that $\mathrm{Char}(F) = 0$ matters). Since $\mathrm{Gal}(F'/F)$ is abelian, it's solvable, so one may find a composition series of $\mathrm{Gal}(F'/F)$ with each composition factor being cyclic; thus there's tower of extensions

$$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_{m-1} \subseteq F_m = F'$$

such that F_{i+1}/F_i is cyclic. Hence, $K' := F'L$ has the desired property. □

Theorem 3.2.42. Assume $\mathrm{Char}(F) = 0$. The polynomial $f \in F[x]$ can be solved by radicals if and only if its Galois group over F is solvable.

Proof. ($\Rightarrow$) Let K/F be the splitting field of f. By Lemma above, there's a radical extension K'/F containing F such that $\mathrm{Gal}(K'/F)$ is solvable. Then $\mathrm{Gal}(K/F) \cong \mathrm{Gal}(K'/F)/\mathrm{Gal}(K'/K)$ is solvable.
($\Leftarrow$) Let K/F be the splitting field of f. Say $1 = G_t \trianglelefteq G_{t-1} \trianglelefteq \cdots \trianglelefteq G_1 \trianglelefteq G_0 = \mathrm{Gal}(K/F)$. Let

$$F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_{t-1} \subseteq K_t = K$$

be the corresponding tower such that each K_{i+1}/K_i is cyclic of order n_i. As in the proof of Lemma, consider $F' = F(\text{all } n_i\text{-th roots of unity})$ and the tower

$$F \subseteq F' = F'K_0 \subseteq F'K_1 \subseteq \cdots \subseteq F'K_{t-1} \subseteq F'K_t = F'K$$

The result ensues by following the proof of the previous lemma. □

Corollary 3.2.42.1. The general polynomial of degree $n \geqslant 5$ cannot be solved by radicals.

Proof. This follows from the previous theorem and the fact that S_n is not solvable for $n \geqslant 5$ (see Example 1.7.8). □

Remark 3.2.43. If K/F is Galois with Galois group being solvable, we say K/F is a solvable extension. It should be noted that a solvable extension may not be radical, but it's always contained in some radical extension of F. (This can be seen in the proof of the theorem above)

For instance, let $f(x) = x^3 + x^2 - 2x - 1 \in \mathbb{Q}[x]$ and K its splitting field over $\mathbb{Q}$; f is the minimal polynomial of $2\cos\dfrac{2\pi}{7}$, and $\mathrm{Gal}(K/\mathbb{Q}) = A_3$, which is solvable and implies all roots of f are real. Suppose, for contradiction, $K = \mathbb{Q}(a)$ for some $a \in K$ with $a^n \in \mathbb{Q}$. Consider the polynomial $x^n - a^n$. We have $f(x) \mid x^n - a^n$, since $[K : \mathbb{Q}] = 3 = \deg_{\mathbb{Q}} a$, and a is a root of f. Let r be another root of f. Then $\dfrac{r}{a}$ is a real root of unity, implying $r = \pm a$, a contradiction for this shows f has at most two roots. Hence $K/\mathbb{Q}$ is not a radical extension.

Cardano's formulas

Let F be a field with characteristic 0. We consider the irreducible cubic $f(x) = x^3 + ax^2 + bx + c \in F[x]$. By virtue of substitution $x \mapsto x - a/3$, we only need to deal with the case

$$g(x) = x^3 + px + q$$

Let $\Delta := \mathrm{disc}(g)$ be the discriminant. Over $F(\sqrt{\Delta})$, the Galois group of g is $A_3 = C_3$. By adjoining a primitive 3-rd root of unity ω, $F(\sqrt{\Delta}, \omega)/F(\omega)$ becomes a radical extension, with a generator of Galois group being a Lagrange resolvent, as in Proposition 3.2.39. Therefore, consider the elements

$$\begin{aligned} & \alpha + \beta + \gamma && = 0 \\ \theta_1 = \ & \alpha + \omega\beta + \omega^2\gamma \\ \theta_2 = \ & \alpha + \omega^2\beta + \omega\gamma \end{aligned}$$

where α, β, γ are the three roots of $g(x)$. Since $\omega^2 + \omega + 1 = 0$, we have

$$\begin{aligned} \theta_1 + \theta_2 &= 3\alpha \\ \omega^2\theta_1 + \omega\theta_2 &= 3\beta \\ \omega\theta_1 + \omega^2\theta_2 &= 3\gamma \end{aligned}$$

As shown in Proposition 3.2.39, the cube of these resolvents lies in $F(\sqrt{\Delta}, \omega)$. We compute them in terms of roots: one has

$$\begin{aligned} \sqrt{\Delta} &= (\alpha - \beta)(\alpha - \gamma)(\beta - \gamma) \\ &= (\alpha^2\beta + \beta^2\gamma + \gamma^2\alpha) - (\alpha\beta^2 + \beta\gamma^2 + \gamma\alpha^2) \end{aligned}$$

so

$$\begin{aligned}
\theta_1^3 &= (\alpha+\omega\beta+\omega^2\gamma)^3 \\
&= \alpha^3+\beta^3+\gamma^3+3\omega(\alpha^2\beta+\beta^2\gamma+\gamma^2\alpha)+3\omega^2(\alpha\beta^2+\beta\gamma^2+\gamma\alpha^2)+6\alpha\beta\gamma \\
&= \left(\alpha^3+\beta^3+\gamma^3-3\alpha\beta\gamma\right)+\frac{3\sqrt{-3}}{2}\left[(\alpha^2\beta+\beta^2\gamma+\gamma^2\alpha)-(\alpha\beta^2+\beta\gamma^2+\gamma\alpha^2)\right] \\
&\quad+\frac{-3}{2}\left[(\alpha^2\beta+\beta^2\gamma+\gamma^2\alpha)+(\alpha\beta^2+\beta\gamma^2+\gamma\alpha^2)\right]+9\alpha\beta\gamma \\
&= (\alpha+\beta+\gamma)(\dots\dots)+\frac{3\sqrt{-3}}{2}\sqrt{\Delta}+\frac{-3}{2}\left[(\alpha+\beta+\gamma)(\alpha\beta+\beta\gamma+\gamma\alpha)-3\alpha\beta\gamma\right]+9\alpha\beta\gamma \\
&= -\frac{27}{2}q+\frac{3}{2}\sqrt{-3}\sqrt{\Delta}
\end{aligned}$$

Similarly (by interchanging β and γ), we have

$$\theta_2^3 = -\frac{27}{2}q-\frac{3}{2}\sqrt{-3}\sqrt{\Delta}$$

Also, we have

$$\theta_1\theta_2 = \alpha^2+\beta^2+\gamma^2+\omega(\alpha\gamma+\beta\alpha+\gamma\beta)+\omega^2(\alpha\beta+\gamma\alpha+\beta\gamma) = -3p$$

At last, recall we have $\Delta = -4p^3-27q^2$, and let

$$A = \sqrt[3]{-\frac{27}{2}q+\frac{3}{2}\sqrt{-3}\sqrt{\Delta}} \qquad B = \sqrt[3]{-\frac{27}{2}q-\frac{3}{2}\sqrt{-3}\sqrt{\Delta}}$$

where the cubic roots are chosen so that $AB = -3p$. Then we have

$$\alpha = \frac{A+B}{3} \qquad \beta = \frac{\omega^2A+\omega B}{3} \qquad \gamma = \frac{\omega A+\omega^2B}{3}$$

Casus irreducibilis

Example 3.2.44. Consider the equation $x^3+x^2-2x-1=0$, the minimal polynomial of $2\cos\dfrac{2\pi}{7}$. Under substitution $x = y-\dfrac{1}{3}$, it becomes $y^3-\dfrac{7}{3}y-\dfrac{7}{27}=0$. Multiplying by 27 and letting $z=3y$, it becomes

$$z^3-21z-7=0$$

which has discriminant $-4(-21)^3-27(-7)^2 = 3^6\cdot 7^2$. We apply the Cardano's formula to solve the cubic; let

$$A = 3\sqrt[3]{\frac{7}{2}+\frac{21}{2}\sqrt{-3}} \qquad B = \sqrt[3]{\frac{7}{2}-\frac{21}{2}\sqrt{-3}}$$

Then the roots can be expressed by combinations of A, B using the formula above.

Let $f(x) = x^3 - 21x - 7$. It has Galois group A_3, and thus all roots of $f(x)$ are real; however, we see that the expressions of roots involves non-real numbers. We shall see, in fact, this always happens in the case $\Delta > 0$, called the *casus irreducibilis* (Latin for "the irreducible case").

Lemma 3.2.45. Let L be the Galois closure of the finite extension $\mathbb{Q}(\alpha)/\mathbb{Q}$. For any prime p dividing $\#\operatorname{Gal}(L/\mathbb{Q})$, there's subfield F of L with $[L : F] = p$ and $L = F(\alpha)$.

Proof. By Cauchy's theorem, there's subgroup P of $\operatorname{Gal}(L/\mathbb{Q})$ of order p; let F' be the corresponding subfield by Galois theory. If for all $\sigma \in \operatorname{Gal}(L/\mathbb{Q})$, $\sigma(\alpha) \in F'$, then $F' = L$, a contradiction. Hence $\sigma'(\alpha) \notin F'$ for some $\sigma' \in \operatorname{Gal}(L/\mathbb{Q})$, and $F'(\sigma'(\alpha)) = L$. Now put $F := \sigma^{-1}(F')$. Then $F(\alpha) = L$ and $[L : F] = p$. □

Lemma 3.2.46. Let F be a subfield of $\mathbb{R}$. Let $a \in F$ and $K = F(\sqrt[n]{a})$, where $\sqrt[n]{a}$ denotes a real n-th root of a. Then any Galois extension L/F contained in K has degree $[L : F] \leqslant 2$.

Proof. Put $[K : F] = d \leqslant n$. Let $F \subseteq E \subseteq K$ with $[E : F] = \ell$. Consider the norm $N_{K/E}\sqrt[n]{a} \in E$; since the only roots of unity in $\mathbb{R}$ are ± 1, we have $N_{K/E}\sqrt[n]{a} = \pm a^{\frac{d\ell}{n}}$. Note that $\deg_F a^{\frac{d}{n\ell}} = \ell$, so we have $E = F(a^{\frac{d}{n\ell}})$, by degree considerations.

Hence, all subextensions of K/F have the form $E = F(a^{\frac{d}{n\ell}})$ for some $\ell \in \mathbb{N}$. To make it Galois, F must possess enough roots of unity. Since ± 1 is the only roots of unity in F, we conclude that the only way to make it Galois is that $[E : F] \leqslant 2$. □

Theorem 3.2.47. If all roots of the irreducible polynomial $f \in \mathbb{Q}[x]$ are real, and one of these roots can be expressed by real radicals, then its Galois group is a 2-group.

Proof. Say α is the root of f that can be expressed by real radicals, i.e, there's a radical extension of real fields

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_m \subseteq \mathbb{R}$$

with $\alpha \in K_m$ and each K_{i+1}/K_i being simple radical. Let $L \subseteq \mathbb{R}$ be the Galois closure of $\mathbb{Q}(\alpha)/\mathbb{Q}$.

Suppose, for contradiction, that $[L : \mathbb{Q}]$ is divisible by some odd prime p. By Lemma 3.2.45, let F be a subfield of L with $[L : F] = p$ and $L = F(\alpha)$. Consider the composites $K_i' = FK_i$, $i = 0, 1, \ldots, m$; each K_{i+1}'/K_i is again real simple radical. We may assume each $[K_{i+1}' : K_i']$ is prime by inserting more simple radical extensions between any two successive subfields. Since $\alpha \notin F = FK_0$, there's an integer s such that $\alpha \notin K_{s-1}'$ but $\alpha \in K_s'$. Since the extensions are of prime degree, we have $K_s' = K_{s-1}(\alpha)$, and K_s'/K_{s-1}' is Galois of degree p, contradicting to Lemma 3.2.46. □

Corollary 3.2.47.1 (*casus irreducibilis*)**.** For an irreducible cubic equation over $\mathbb{Q}$, if it has the positive discriminant, then the expressions of the roots must involve radicals of non-real numbers.

Proof. Note that the positive discriminant indicates that all the roots are real. □

Quartic equations

Consider a quartic polynomial $f(x) = x^4 + ax^3 + bx^2 + cx + d \in F[x]$; under the substitution $x = y - \frac{a}{4}$, we may consider

$$h(y) = y^4 + py^2 + qy + r$$

Let

$$\begin{aligned}\theta_1 &= (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4)\\ \theta_2 &= (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4)\\ \theta_3 &= (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3)\end{aligned}$$

and form the resolvent cubic

$$\begin{aligned}g(x) &= (x - \theta_1)(x - \theta_2)(x - \theta_3) \in F[x]\\ &= x^3 - 2px^2 + (p^2 - 4r)x + q^2\end{aligned}$$

With the condition $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0$, we have

$$\begin{aligned}\alpha_1 + \alpha_2 &= \sqrt{-\theta_1} \qquad & \alpha_3 + \alpha_4 &= -\sqrt{-\theta_1}\\ \alpha_1 + \alpha_3 &= \sqrt{-\theta_2} \qquad & \alpha_2 + \alpha_4 &= -\sqrt{-\theta_2}\\ \alpha_1 + \alpha_4 &= \sqrt{-\theta_3} \qquad & \alpha_2 + \alpha_3 &= -\sqrt{-\theta_3}\end{aligned}$$

where the square roots are chosen so that $\sqrt{-\theta_1}\sqrt{-\theta_2}\sqrt{-\theta_3} = -q$. (Any two determines the third.) Therefore,

$$\begin{aligned}2\alpha_1 &= \sqrt{-\theta_1} + \sqrt{-\theta_2} + \sqrt{-\theta_3}\\ 2\alpha_2 &= \sqrt{-\theta_1} - \sqrt{-\theta_2} - \sqrt{-\theta_3}\\ 2\alpha_3 &= -\sqrt{-\theta_1} + \sqrt{-\theta_2} - \sqrt{-\theta_3}\\ 2\alpha_4 &= -\sqrt{-\theta_1} - \sqrt{-\theta_2} + \sqrt{-\theta_3}\end{aligned}$$

3.3 Transcendental extensions

3.3.1 Dependence relations

Definition. Let X be a nonempty set and let $\Delta \subseteq X \times 2^X$ be a binary relation. We write $x \prec S$ if $(x, S) \in \Delta$ and $S \prec T$ if $s \prec T$ for all $x \in S$. We say Δ is a **dependence relation** if it satisfies the following properties, for all $S, T, U \in 2^X$:

(I) (reflexivity) $S \prec S$

(II) (compactness) $x \prec S \Rightarrow x \prec S_0$ for some finite subset S_0 of S

(III) (transitivity) $S \prec T \wedge T \prec U \Rightarrow S \prec U$

(IV) (Steinitz exchange axiom) $x \prec S \wedge x \not\prec S \backslash \{s\} \Rightarrow s \prec (S \backslash \{s\}) \cup \{x\}$

We say x is **dependent on** S if $x \prec S$; otherwise, we say x is **independent of** S.

Definition. A subset $S \subseteq X$ is **dependent** if $s \prec S \backslash \{s\}$ for some $s \in S$. Otherwise, S is **independent**.

Property 3.3.1.

1. If $S \prec T$, then $S \prec T_0$ for all supersets T_0 of T.
2. Any superset of a dependent set is dependent.
3. Any subset of an independent set is independent.
4. If S is dependent set, then some finite subset of S is dependent. Equivalently, if every finite subset of T is independent, then T is independent.

Proof.

1. By (I), we have $T_0 \prec T_0$, i.e, $t \prec T_0$ for all $t \in T_0$; in particular, $t \prec T_0$ for all $t \in T$, i.e, $T \prec T_0$. By (III), we have $S \prec T_0$.
2. Let S be dependent and $T \supseteq S$. Since S dependent, $s \prec S \backslash \{s\}$ for some $s \in S$. By 1. we have $s \prec T \backslash \{s\}$.
3. This follows from 2.
4. Say $s \prec S \backslash \{s\}$ for some $s \in S$. By (II), $s \prec S_0$ for some finite subset S_0 of S. Then $S_0 \cup \{s\} \subseteq S$ is finite and dependent.

□

Proposition 3.3.2. If S is independent and $x \nprec S$, then $S \cup \{x\}$ is independent.

Proof. If $s \prec S \cup \{x\} \backslash \{s\}$ for some $s \in S \cup \{x\}$, by (V), we have $x \prec S \backslash \{s\}$. By Proposition 3.3.1.1, $x \prec S$, a contradiction. Hence $S \cup \{x\}$ is independent. □

Proposition 3.3.3. If S is dependent, then $S \prec S \backslash \{u\}$ for some $u \in S$.

Proof. The dependence of S shows that $u \prec S \backslash \{u\}$ for some u. By (I), we have $S \backslash \{u\} \prec S \backslash \{u\}$, and thus $S \prec S \backslash \{u\}$. □

Definition. A subset $B \subseteq X$ is called a **base** for X if B is independent and $X \prec B$.

Theorem 3.3.4. Let X be a nonempty set with a dependence relation $\prec$. For $B \subseteq X$, TFAE:

1. B is a base.
2. B is a maximal independent set in X.
3. B is a minimal set with respect to the property set $X \prec B$.

Proof.

1. 1. $\Rightarrow$ 2. : Pick $x \in X \backslash B$. Since $x \prec B$, we have $B \cup \{x\}$ is dependent.
2. 2. $\Rightarrow$ 3. : Take $x \in B$. If $X \prec B \backslash \{x\}$, then, in particular, $x \prec B \backslash \{x\}$, contradicting to the fact B is independent. Hence, B is minimal.
3. 3. $\Rightarrow$ 1. : Take $x \in B$. If B is dependent, then $X \prec B \prec B \backslash \{x\}$ by Proposition 3.3.3. Hence B is independent.

□

Theorem 3.3.5. Let X be a nonempty set with a dependence relation $\prec$. Let $S \subseteq T \subseteq X$ such that S is independent and $X \prec T$. Then there exists a base B for X such that $S \subseteq B \subseteq T$.

Proof. Put $\mathcal{A} = \{I \subseteq X \mid S \subseteq I \subseteq T \wedge \text{I is independent}\}$, partially ordered by inclusion. Let $\{I_n\}_{n \in \mathbb{N}}$ be a chain in $\mathbb{A}$. By Property 3.3.1.3 and .4, we see $\bigcup_n I_n$ is also independent. By Zorn's lemma, $\mathcal{A}$ has a maximal element, say B. We claim $X \prec B$. Since $B \subseteq T$, the maximality forces $T \prec B$, by Proposition 3.3.2; (III) implies $X \prec B$. □

Lemma 3.3.6. Let S be a finite dependent set and let $A \subseteq S$ be an independent subset of S. Then there exists $u \in S \backslash A$ such that $S \prec S \backslash \{u\}$.

Proof. By Theorem 3.3.5, let B be a base such that $A \subseteq B \subseteq S$. If $u \in S \backslash B$, then $u \prec B \prec S \backslash \{u\}$ by Property 3.3.1.1. (I) and (III) show $S \prec S \backslash \{u\}$. □

Theorem 3.3.7. 1. If B is a finite set for which $X \prec B$ and if C is independent in X, then $\#C \leqslant \#B$.

2. Any two bases with respect to $\prec$ for a set X have the same cardinality.

Proof.

1. Let $B = \{b_1, \ldots, b_m\}$. Pick $c_1 \in C$ and consider the set $C_1 = B \cup \{c_1\}$. By Lemma 3.3.6, with $A = \{c_1\}$, we have, say, $X \prec C_1 \prec \{c_1, b_1, \ldots, b_{m-1}\}$. Picking $c_2 \in C \backslash \{c_1\}$ and repeating the procedure above, we must exhaust the element of C first, for otherwise $X \prec C_0$ for some proper subset $C_0 \subseteq C$, contradicting to the independence of C. Hence $\#C \leqslant \#B$.

2. Let B, C be two bases for X. If they are finite, 1. indicates that $\#B = \#C$. Assume B, C are infinite. For each $c \in C$, we have $c \prec B$, and by (II), $c \prec B_c$ for some finite subset $B_c \subseteq B$. It follows $B = \bigcup_{c \in C} B_c$, for otherwise $b \prec C \prec \bigcup_{c \in C} B_c \prec B \backslash \{b\}$ for $b \in B \backslash \bigcup_{c \in C} B_c$, contradicting to the independence of B. Hence
$$\#B = \#\bigcup_{c \in C} B_c \leqslant \#(C \times \mathbb{N}) = \#C$$
Reversing the roles of B and C, we conclude $\#B = \#C$.

□

3.3.2 Transcendence extensions

In this section, $F \subseteq E$ always denotes a field extension.

Definition. $\alpha \in E$ is **transcendental** over F if t is not algebraic over F.

Definition. Let $S \subseteq E$. $\alpha \in E$ is **algebraically dependent on S over F**, written $\alpha \prec S$, if α is algebraic over $F(S)$. Otherwise, α is **algebraically independent of S over F**, written $\alpha \nprec S$.

- $\alpha \prec S$ if and only if $F(S) \subseteq F(S, \alpha)$ is algebraic. Also, the class of algebraic extensions is closed under any composite. Thus, for $A, S \subseteq E$, $A \prec S$ if and only if $F(S) \subseteq F(S, A)$ is algebraic, i.e, A is algebraic over $F(S)$.

- S is **algebraically dependent over** F if $s \prec S \backslash \{s\}$ for some $s \in S$. Otherwise, S is **algebraically independent over** F.

Definition. A subset $S \subseteq E$ is said to have a **nontrivial polynomial relationship** over F if $p(s_1, \ldots, s_n) = 0$ for some nonzero polynomial $p \in F[x_1, \ldots, x_n]$ and distinct $s_1, \ldots, s_n \in S$.

Theorem 3.3.8. Let $S \subseteq E$. S is algebraically dependent if and only if S has a nontrivial polynomial relationship over F.

Proof. ($\Rightarrow$) Let $s \in S$ such that $s \prec S\backslash\{s\}$, i.e, s is algebraic over $F(S\backslash\{s\})$. Hence, $f(s) = 0$ for some polynomial $f \in F(S\backslash\{s\})[x]$ of degree $n > 0$, say

$$f(x) = \sum_{i=1}^{n} \frac{p_i(s_1, \ldots, s_m)}{q_i(s_1, \ldots, s_m)} x^i$$

for distinct $s_1, \ldots, s_m \in S\backslash\{s\}$. Multiplying by the product of the denominators gives a nonzero polynomial satisfied by s.
($\Leftarrow$) Let $s_1, \ldots, s_m \in S$ such that $p(s_1, \ldots, s_m) = 0$ for some nonzero polynomial $p \in F[x_1, \ldots, x_n]$; WLOG, say m is the smallest number having such a property. Write

$$p(x_1, \ldots, x_m) = \sum_{i=1}^{n} p_i(x_2, \ldots, x_m) x_1^i$$

where $p_n \neq 0$. By the minimality, $p_n(s_2, \ldots, s_m) \neq 0$. Hence, s_1 satisfies the nonzero polynomial $p(x) := p(x, s_2, \ldots, s_m)$, i.e, $s_1 \prec S\backslash\{s_1\}$. □

Theorem 3.3.9. Algebraic dependence is a dependence relation.

Proof. The reflexivity holds trivially. Let $\alpha \prec S$ and $m_{\alpha, F(S)}(x) = a_n x^n + \cdots + a_1 x + a_0 \in F(S)[x]$. Put $C = \{a_0, \ldots, a_n\}$. Then $\alpha \prec C$, which proves the compactness. For the transitivity, let $\alpha \in S$. Then the tower $F(U) \subseteq F(U, T) \subseteq F(U, T, \alpha)$ is algebraic, proving that $F(U) \subseteq F(U, \alpha)$ is algebraic, i.e, $\alpha \prec U$. Finally, we verify the exchange axiom. Suppose $t \prec S$ but $t \not\prec S\backslash\{s\}$. Then t satisfies a polynomial $f \in F(S)[x]\backslash F(S\backslash\{s\})[x]$ of degree $n > 0$; write

$$f(x) = \sum_{i=1}^{n} \frac{p_i(s_1, \ldots, s_m)}{q_i(s_1, \ldots, s_m)} x^i$$

for distinct $s_1, \ldots, s_m \in S$ with, WLOG, $s = s_1$. Multiplying by the product of the denominators and setting $x = t$ gives a nonzero polynomial over $F(S\backslash\{s\}, t)$ satisfied by s, and thus $s \prec (S\backslash\{s\}) \cup \{t\}$ □

Property 3.3.10.
1. Any superset of an algebraically dependent set is algebraically dependent.
2. Any subset of an algebraically independent is algebraically independent.

3. If S is algebraically independent over F and α is transcendental over $F(S)$, then $S \cup \{\alpha\}$ is algebraically independent over F.

Definition. A **transcendence basis** for E over F is a subset $B \subseteq E$ which is algebraically independent over F and for which $F(B) \subseteq E$ is algebraic.

Theorem 3.3.11. Let $B \subseteq E$. TFAE:

1. B is a transcendental basis for E over F.
2. B is a maximal algebraically independent subset of E over F.
3. B is a minimal set with respect to the property that $F(B) \subseteq E$ is algebraic.

Theorem 3.3.12. Let $F \subseteq S \subseteq T \subseteq E$, where S is algebraically independent over F and $F(T) \subseteq E$ is algebraic. Then there exists a transcendental basis B for E over F satisfying $S \subseteq B \subseteq T$.

Theorem 3.3.13. Any two transcendental bases for E over F have the same cardinality, called the **transcendental degree** of E over F and denoted by $\mathrm{tr.deg}_F E$.

Theorem 3.3.14. Let $F \subseteq K \subseteq E$.

1. If $S \subseteq K$ is algebraically independent over F and $T \subseteq E$ is algebraically independent over K, then $S \cup T$ is algebraically independent over F.
2. If S is a transcendental bases for K over F and T is a transcendental bases for E over K, then $S \cup T$ is a transcendental bases for E over F.
3. The transcendence degree is additive in towers.

Proof.

1. Let $s_1, \ldots, s_m \in S, t_1, \ldots, t_n \in T$ and let $p \in F[x_1, \ldots, x_m, y_1, \ldots, y_n]$ such that $p(s_1, \ldots, s_m, t_1, \ldots, t_n) = 0$, where s_i, t_i are distinct. Write

$$p(x_1, \ldots, x_m, y_1, \ldots, y_n) = \sum_e \left(\sum_f a_f x_1^{f_1} \cdots x_m^{f_m} \right) y_1^{e_1} \cdots y_n^{e_n}$$

where $a_f = a_{f_1,\ldots,f_m} \in F$ and each $e = (e_1, \ldots, e_n)$ is distinct and for each e, each $f = (f_1, \ldots, f_m)$ is distinct. Consider the polynomial $q(y_1, \ldots, y_n) = p(s_1, \ldots, s_m, y_1, \ldots, y_n)$. Since T is algebraically independent over K, we obtain

$$\sum_f a_f s_1^{f_1} \cdots s_m^{f_m} = 0$$

Again, since S is algebraically independent over F, we obtain $a_f = 0$. In conclusion, $p \equiv 0$, i.e, $S \cup T$ is algebraically independent over F.

2. We must show $F(S \cup T) \subseteq E$ is algebraic. Since $F(S) \subseteq K$ and $K(T) \subseteq E$ are algebraic, each step in the tower $F(S \cup T) \subseteq K(T) \subseteq E$ is algebraic, and thus $F(S \cup T) \subseteq E$ is algebraic.

□

Definition. $F \subseteq E$ is **totally transcendental** if every element of $E \backslash F$ is transcendental over K.

- If $E = F(t)$ for some transcendence t over F, we say E/F is a **simple transcendental extension**.

Proposition 3.3.15. Let t be a transcendence over F. Let $s = \dfrac{p(t)}{q(t)} \in F(t) \backslash F$, where $(p, q) = 1$. Then $[F(t) : F(s)] = \max\{\deg p, \deg q\}$. (HW. 19)

Proof. Consider the polynomial $g(x) = q(x)s - p(x) \in F(s)[x]$. Then t is a root of $g(x)$, so $F(t)/F(s)$ is algebraic; this forces $F(s)/F$ to be transcendental. Regard s as an independent variable y. To show $g(x)$ is irreducible over $F(s)$, it suffices to show $g(x)y - f(x) \in F(y)[x]$ is irreducible over $F(y)$. By Gauss' lemma, we only need to show $h(y, x) = g(x)y - f(x) \in F[y][x]$ is irreducible in $F[y][x] = F[x, y] = F[x][y]$, which holds trivially since $(g, f) = 1$. Thus $[F(t) : F(s)] = \deg p = \max\{\deg p, \deg q\}$. The left is clear. □

Corollary 3.3.15.1. Let $F(t)/F$ be a simple transcendental extension. Then

$$\mathrm{Aut}(F(t)/F) = \left\{ \sigma_A : t \mapsto \frac{at + b}{ct + b} \,\middle|\, A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(F) \right\}$$

Furthermore, $A \mapsto \sigma_A$ is a surjective homomorphism from $\mathrm{GL}_2(F)$ to $\mathrm{Aut}(F(t)/F)$, with kernel equal to the group of all nonzero scalar matrices in $\mathrm{GL}_2(F)$, i.e, $\mathrm{Aut}(F(t)/F) \cong \mathrm{PGL}_2(F)$. (HW2. 1)

Proof. An automorphism f of $F(t)/F$ is uniquely determined by it action on t; suppose $f(t) = \dfrac{p(t)}{q(t)}$, where $p, q \in F[x]$, $q \neq 0$ and $(p, q) = 1$. Since it's an automorphism $F(t) = F(f(t))$, so $[F(t) : F(f(t))] = 1$. By Proposition 3.3.15, $\max\{\deg p, \deg q\} = 1$; say $p(x) = ax + b$ and $q(x) = cx + d$. If $c = 0$, then $a, d \neq 0$ and thus $ad \neq 0$. If $c \neq 0$, since $(p, q) = 1$, we have $ad - bc \neq 0$. Hence $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(F)$. □

Theorem 3.3.16 (Lüroth)**.** Let t be transcendental over F. If $F \subseteq K \subseteq F(t)$, then $K = F(s)$ for some $s \in F(t)$.

Proof. Assume $K \neq F$. By Proposition 3.3.15, for each $s \in K \backslash F$, the tower $F(s) \subseteq K \subseteq F(t)$ is algebraic; in particular, $F(t)/K$ is algebraic. Consider

$$p(x) = m_{t,K}(x) = x^n + \frac{a_1(t)}{b_1(t)} x^{n-1} + \cdots + \frac{a_n(t)}{b_n(t)}$$

where $a_i(t), b_i(t) \in F(t)$ are relatively prime; note that none of $a_i(t)/b_i(t) \in F$ thanks to the transcendence of t over F. We claim each $s = \dfrac{a_k(t)}{b_k(t)}$ is the desired element such that $K = F(s)$.

Consider the polynomial $h(x) = a_k(x) - \dfrac{a_k(t)}{b_k(t)} b_k(x) \in K[x]$. Since $s \notin F$, we have $h(x) \neq 0$. But $h(t) = 0$, we have $p \mid h$ over K, i.e, there exists $q \in K[x]$ so that

$$a_k(x) - \frac{a_k(t)}{b_k(t)} b_k(x) = q(x)p(x)$$

or

$$a_k(x)b_k(t) - a_k(t)b_k(x) = b_k(t)q(x)p(x)$$

Multiplying both sides by $r(t) = b_1(t) \cdots b_n(t)$ gives

$$r(t)[a_k(x)b_k(t) - a_k(t)b_k(x)] = b_k(t)q(x)r(t)p(x)$$

where

$$r(t)p(x) = b_1(t) \cdots b_n(t)x^n + \sum_{i=1}^{m} [b_1(t) \cdots b_{i-1}a_i(t)b_{i+1}(t) \cdots b_n(t)]x^{n-i}$$

Let $g(t)$ be the greatest common factor of the coefficients on the RHS. Since $g(t) \mid b_1(t) \cdots b_n(t)$ and $(b_i, a_i) = 1$, we have

$$g(t) \mid b_1(t) \cdots b_{k-1}(t)b_{k+1}(t) \cdots b_n(t)$$

for all k. Factoring out $g(t)$ gives

$$r(t)p(x) = g(t)p'(t, x)$$

where $p' \in F[t, x]$ is not divisible by any nonconstant polynomial in t $(*)$. Thus

$$\deg_t p'(t, x) \geqslant \max\{\deg a_k(t), \deg b_k(t)\} = [F(t) : F(s)]$$

and

$$r(t)[a_k(x)b_k(t) - a_k(t)b_k(x)] = b_k(t)q(x)g(t)p'(t, x)$$

Multiplying both sides by a polynomial $u(t)$ that clear all of the denominators of $q(x)$, we obtain

$$u(t)r(t)[a_k(x)b_k(t) - a_k(t)b_k(x)] = b_k(x)q'(t, x)p'(t, x)$$

where $q' \in F[t, x]$. By $(*)$, we have $a_k(x)b_k(t) - a_k(t)b_k(x) \mid p'(t, x)$, i.e, there exists $q''(t, x) \in F[t, x]$ so that

$$a_k(x)b_k(t) - a_k(t)b_k(x) = q''(t, x)p'(t, x)$$

Note that the degree of RHS with respect to t is at least $[F(t) : F(s)]$ and the RHS is at most $\max\{\deg a_k(t), \deg b_k(t)$ $[F(t) : F(s)]$. Hence $\deg_t q''(t, x) = 0$, i.e,

$$a_k(x)b_k(t) - a_k(t)b_k(x) = q''(x)p'(t, x)$$

for some $q'' \in F[x]$. Since the RHS is not divisible by any nonconstant polynomial of t, neither is the LHS. But the LHS is symmetric in x, t, so it cannot divisible by any nonconstant polynomial of x either. Hence $q''(x) \in F$, i.e,

$$a_k(x)b_k(t) - a_k(t)b_k(x) = q''p'(t, x)$$

for some $q'' \in F$. Finally, since the degree w.r.t. x and that w.r.t. t of the LHS agree, this holds for the RHS. Hence

$$n = \deg_x p'(t, x) = \deg_t p'(t, x) \geqslant [F(t) : F(s)] \geqslant n$$

and thus $[F(t) : F(s)] = n = \deg m_{t,K}(x)$, i.e, $K = F(s)$, completing the proof. □

Proposition 3.3.17. Every field extension is a totally transcendental extension of an algebraic extension.

Proof. Let $F \subseteq E$ be any field extension. Let $\mathcal{A} := \{\alpha \in E \mid \alpha \text{ is algebraic over } F\}$, which is a subfield of E containing F. If $\alpha \in E$ is algebraic over $\mathcal{A}$, then $\mathcal{A} \subseteq \mathcal{A}(\alpha)$ is algebraic, and thus $F \subseteq \mathcal{A}(\alpha)$ is algebraic, i.e, $\alpha \in \mathcal{A}$. Thus $\mathcal{A} \subseteq E$ is totally transcendental. □

Example 3.3.18. $F((x_i)_{i\in I})$ is totally transcendental over F with transcendence degree n over F.

Proof. First we show that $F(x)$ is totally transcendental over F. For clarity, we prove $F(\pi) \cong F(x)$ is totally transcendental over F, where π is a transcendence over F. Let $\alpha \in F(\pi)\backslash F$, so that $\alpha = \dfrac{p(\pi)}{q(\pi)}$ for some $p, q \in F[x]$. Then π satisfies $0 \neq \alpha q - p \in F(\alpha)[x]$, i.e, π is algebraic over $F(\alpha)$, i.e, $[F(\pi) : F(\alpha)] < \infty$. It forces that $[F(\alpha) : K] = \infty$, i.e, α is transcendental over F. Now $F(x_1, \ldots, x_n)$ is totally transcendental over F follows by induction on n. Finally, let $\alpha \in f/g \in F((x_i)_{i\in I})$ be algebraic over K. Since f, g have finitely nonzero zeros, $\alpha \in F((x_i)_{i\in J})$ for some finite subset $J \subseteq I$. Hence $\alpha \in F$. □

3.3.3 Purely transcendental extension

Definition. A extension $F \subseteq E$ is **purely transcendental** if E admits a transcendental base S over F such that $E = F(S)$.

- It's equivalent to saying that E is F-isomorphic to some $K((x_i)_{i\in I})$.

Proposition 3.3.19. If E/F is purely transcendental, then every $\alpha \in E\backslash F$ is transcendental over F.

Proof. Let B be a transcendence base for E/F such that $E = F(B)$. Assume $\alpha \in L := F(t_1, \ldots, t_n)$ for some finite subset $\{t_1, \ldots, t_n\} \subseteq B$, and also assume that $\alpha \notin K := F(t_1, \ldots, t_{n-1})$. Then $L = K(t_n)$ is a simple transcendental extension of K with $\alpha \in L \backslash K$. By Proposition 3.3.15, α is transcendental over K, and thus over F. □

Example 3.3.20. Let $n \geqslant 3$ and F be a field with $\mathrm{Char}(F) \nmid n$. Let u be transcendental over F and let v be a root of $p(x) = x^n + u^n - 1$. Put $E = F(u, v)$. Clearly, E/F is nor algebraic. We claim that E/F is not purely transcendental.

Proof. Since $F(u, v)/F(u)$ is algebraic, $\mathrm{tr.deg}_F F(u, v) = 1$. Suppose otherwise $E = F(t)$ for some transcendence t over F. Write $u = \dfrac{a(t)}{b(t)}$ and $v = \dfrac{c(t)}{d(t)}$ where $a, b, c, d \in F[x]$. Then

$$\frac{a(t)^n}{b(t)^n} + \frac{c(t)^n}{d(t)^n} = 1$$

or

$$(ad)^n + (bc)^n = (bd)^n$$

We rewrite it as

$$f(t)^n + g(t)^n = h(t)^n$$

where $f, g, h \in F[x] \backslash F$ are, say, pairwise relatively prime. Assume $\deg f \leqslant \deg g$; then $\deg h \leqslant \deg g$. Dividing by h^n and taking the derivative with respect to t, we obtain

$$f^{n-1}(f'h - fh') + g^{n-1}(g'h - gh') = 0$$

Since $(f, g) = 1$, we have $g^{n-1} \mid f'h - fh'$. While this implies

$$(n-1)\deg g \leqslant \deg(fh) - 1 = 2\deg(g) - 1$$

which is impossible for $n \geqslant 3$. Hence E/F is not purely transcendental. □

Example 3.3.21. If t is transcendental over $\mathbb{Q}$ then $\mathbb{Q}(t, \sqrt{t^3 - t})$ is not a purely transcendental extension of $\mathbb{Q}$.

Proof. Since $\mathbb{Q}(t) \subseteq \mathbb{Q}(t, \sqrt{t^3 - t})$ is algebraic, we see $\mathrm{tr.deg}_{\mathbb{Q}} \mathbb{Q}(t, \sqrt{t^3 - t}) = 1$. Suppose, for contradiction, that $\mathbb{Q}(u) = \mathbb{Q}(t, \sqrt{t^3 - t})$ for some transcendence u over $\mathbb{Q}$. Then $t = f(u)$, $\sqrt{t^3 - t} = g(u)$ for some $f, g \in \mathbb{Q}(x) \backslash \mathbb{Q}$; let us identify $\mathbb{Q}(u)$ with $\mathbb{Q}(x)$ for clarity. Thus, we have

$$g(x)^2 = f(x)^3 - f(x)$$

Write $f = \dfrac{a}{b}$, $g = \dfrac{c}{d}$ for some $a, b, c, d \in \mathbb{Q}[x]$ with $(a, b) = (c, d) = 1$; we assume $a, b, c, d \in \mathbb{Z}[x]$. Then we have

$$c^2 b^3 = d^2 a(a^2 - b^2)$$

Since $(a, b) = 1$ and $(c, d) = 1$, we have $b^3 \mid d^2$ and $d^2 \mid b^3$, thus, say, $b^3 = d^2$. Since $\mathbb{Z}[x]$ is a UFD, there's $w \in \mathbb{Z}[x]$ such that $w^6 = b^3 = d^2$; let $b = w^2$ and $d = w^3$. Now we have $f = \dfrac{a}{w^2}$ and $g = \dfrac{c}{w^3}$. Consider the rational function $\phi(x) = \dfrac{f'(x)}{g(x)}$. We have

$$\begin{aligned} \phi(x) &= \frac{f'(x)}{2g(x)} = \frac{a'w - 2aw'}{2c} \\ &= \frac{g'(x)}{3f(x)^2 - 1} = \frac{c'w - 3cw'}{3a^2 - w^4} \end{aligned}$$

where the first equality in the second row results from the fact $2g(x)g'(x) = 3f(x)^2 f'(x) - f'(x)$, obtained from differentiating the identity in f, g above. We contend that $\phi(x)$ is in fact a polynomial. Suppose that $x - \alpha$ is a factor of the denominator of ϕ. Then $c(\alpha) = 0 = 3a(\alpha)^2 - w(\alpha)^4$. $w(\alpha) \neq 0$ for otherwise $(w^3, a) \neq 1$, a contradiction. Thus $g(\alpha) = 0 = 3f(\alpha)^2 - 1$, together with $g(\alpha)^2 = f(\alpha)^3 - f(\alpha)$, which is impossible. Hence $\phi(x)$ is a polynomial.

Replace $f(x)$ and $g(x)$ by $f(1/x)$ and $g(1/x)$, respectively; by the same token, we may show

$$\varphi(x) := \frac{-x^{-2} f'(1/x)}{2g(1/x)} = \frac{-x^{-2} g'(1/x)}{3f(1/x)^2 - 1}$$

is a polynomial. On the other hand, we have $-x^{-2}\phi(1/x) = \varphi(x)$, which is impossible while both $\phi(x)$ and $\varphi(x)$ are polynomials at the same time. Hence $\mathbb{Q}(t, \sqrt{t^3 - t})$ is not purely transcendental.

□

Lemma 3.3.22. Let E, E' be two field and $K \subseteq E$, $K' \subseteq E'$ be subfield. Let I be an index set and $X = (x_i)_{i \in I} \subseteq E$ (resp. $X' = (x'_i)_{i \in I} \subseteq E'$) be algebraically independent over E (resp. over E'). If $u : K \to K'$ is a field isomorphism, then there's a unique field isomorphism $v : K(X) \to K'(X')$ extending u and sending x_i to x'_i for each $i \in I$.

Proof. The uniqueness is clear. For the existence, note the algebraic independence means that there is a ring isomorphism $w : K[X] \to K[X']$ sending $x_{i_1}^{\alpha_1} \cdots x_{i_n}^{\alpha_n}$ to $x_{i_1}'^{\alpha_1} \cdots x_{i_n}'^{\alpha_n}$ for $i_1, \ldots, i_n \in I$, $\alpha_j \in \mathbb{N}$, $n \in \mathbb{N}$. Passing to their fraction fields we obtain a field isomorphism $v : K(X) \to K'(X')$ with desired properties. □

Proposition 3.3.23. Let $K \subseteq E, F \subseteq \Omega$ be fields with Ω being algebraically closed. Then any K-isomorphism between E and F can be extended to some K-automorphism on Ω if and only if $\mathrm{tr.deg}_E \Omega = \mathrm{tr.deg}_F \Omega$.

Proof. The necessity is clear. The converse holds by Lemma above. □

Chapter 4

Module theory

4.1 Module theory

Definition. Let R be a ring.

1. A **left R-module** is an abelian group M on which R acts on the left by endomorphisms on M.
2. An **R-submodule** N of M is a subgroup of M stable under the action on R, i.e, $rN \subseteq N$ for all $r \in R$. In this case, we write $N \leqslant M$.

- Similarly, we may define a **right R-module**.
- If R has identity 1, we assume $1m = m$ for all $m \in M$. In this case, we say M is a **unital** R-module.
- Let S be a ring. An **(S, R)-bimodule** is a left S-module M that is also a right R-module at the same time on which two ring actions are compatible in the sense that $(sm)r = s(mr)$ for all $m \in M$, $s \in S$, $r \in R$.
- Unless indicated otherwise, by R-modules we mean left R-modules.

Example 4.1.1.

1. If $R = F$ is a field, then R-modules are simply F-vector spaces, and R-submodules are subspaces.
2. If $R = \mathbb{Z}$, unital R-modules are abelian groups, and R-submodules are subgroups.
3. R itself is an R-module, and R-submodules are left ideals.
4. More generally, $R^n := \{(a_1, \ldots, a_n) \mid a_i \in R\}$ is an R-module.
5. If S is a subring of R, then an R-module is automatically an S-module.
6. If M is an R-module and I is a left ideal of R such that $IM = 0$, then M is an (R/I)-module, with the (R/I)-action on M given by $(x + I)m := xm$ for all $x \in R$. For example, if A is an abelian group of exponent m, i.e, $(m\mathbb{Z})A = 0$, then A is a $\mathbb{Z}/m\mathbb{Z}$-module. In particular, if $m = p$ is a prime, then A is a $\mathbb{F}_p$-vector space. For example, V_4 is a $\mathbb{F}_2$-vector space of dimension 2.
7. Let F be a field. We consider the $F[x]$-module V. In particular, V is a F-vector space. Then the action of x defines a linear map $T : v \mapsto xv$, and determines the $F[x]$-action on V. Conversely, given a F-vector space V and $T \in \mathrm{End}(V)$, let $F[x]$ act on V by $p(x)v := p(t)v$ for all $p \in F[x]$.

   In conclusion, an $F[x]$-module corresponds to a F-vector space with an endomorphism T.

Definition. Let R be a commutative ring with 1_R. An **R-algebra** is a ring A with identity 1_A together with a ring homomorphism $f : R \to A$ such that $f(R) \subseteq Z(A)$ and $f(1_R) = 1_A$.

- Equivalently, an R-algebra is an R-module that is also a ring with identity such that the multiplication is R-bilinear.

Example 4.1.2.

1. Any commutative ring with 1 is a $\mathbb{Z}$-algebra.
2. If A is a ring with 1 and R is a subring of the center of A containing the same 1, then A is an R-algebra.

4.1.1 Module homomorphisms and quotient modules

Definition. Let R be a ring and M, N be R-modules.

1. A map $\phi : M \to N$ is an **R-module homomorphism** is ϕ is an abelian group homomorphism that respects the R-action on M and N, i.e ,$\phi(rm) = r\phi(m)$ for all $r \in R$, $m \in M$.
2. If ϕ is bijective, we say it's an **R-module isomorphism**, and write $M \cong N$.
3. $\ker \phi := \{m \in M \mid \phi(m) = 0\}$ and $\operatorname{Im} \phi := \phi(M)$.
4. $\operatorname{Hom}_R(M, N) := \{\phi : M \to N \mid \phi \text{ is an } R \text{ -module homomorphism}\}$.

Example 4.1.3.

1. $\mathbb{Z}$-module homomorphisms are just abelian group homomorphisms.
2. When F is a field, F-module homomorphisms are simply F-linear transformations.

Property 4.1.4. Let R be a ring and M, N be R-modules.

1. $\operatorname{Hom}_R(M, N)$ is an abelian group and a $Z(R)$-module. In particular, if R is commutative, it's an R-module.
2. $\operatorname{End}_R(M) := \operatorname{Hom}_R(M, M)$ is a ring with identity, with multiplication being function composition. If R is commutative with 1, then it's an R-algebra.

Property 4.1.5. Let R be a ring and N, M be R-modules with $N \subseteq M$. Then the quotient group M/N is an R-module on which R acts by $r(x + N) := rx + N$ for all $r \in R$. Also, the map $M \ni x \mapsto x + N$ is an R-module homomorphism with kernel N.

Definition. Let R be a ring and M be an R-module. For submodules A, B of M, define $A+B := \{a+b \mid a \in A, b \in B\}$, which is the **smallest submodule containing A and B.**

Proposition 4.1.6. Let R be a ring and N, M be R-modules.

1. $\phi \in \mathrm{Hom}_R(M,N) \Rightarrow M/\ker\phi \cong \mathrm{Im}\,\phi$.
2. $M+N/N \cong M/M \cap N$
3. $A \leqslant B \leqslant M \Rightarrow \dfrac{M/A}{B/A} \cong M/B$
4. If $N \leqslant M$, then there's a bijection between submodules of M/N and submodules of M containing N.

4.1.2 Generation of modules, direct sums and free modules.

Definition. Let R be a ring and M be an R-module.

1. Let $A \subseteq M$ be a subset. Define $RA := \{r_1a_1 + \cdots + r_na_n \mid n \in \mathbb{N},\, r_i \in R,\, a_j \in A\}$ to be the **module generated by** A. In this case, we say A is a generating set.
2. If $N \leqslant M$ such that $N = RA$ for some $A \subseteq M$ with $\#A < \infty$, we say N is **finitely generated**.
3. If $N = Ra$ for some $a \in M$, we say N is the **cyclic module generated by** a.

- If $A = \{a_1, \ldots, a_n\}$, we write $RA = Ra_1 + \cdots + Ra_n$.

Example 4.1.7.

1. If $R = \mathbb{Z}$, then $\mathbb{Z}a$ is just the cyclic group generated by a.
2. If $M = R$ is a ring, then cyclic submodules are precisely principal left ideals of R.
3. V is a cyclic $F[x]$-modules means precisely that V is a T-cyclic subspace generated by v for some $T \in \mathrm{End}(V)$, $v \in V$.

Definition. Let R be a ring and $M_1, \ldots, M_n$ be R-modules. Define an action of R on $M_1 \times \cdots \times M_n$ componentwise. The resulting R-module is called the **(external) direct sum** of $M_1, \ldots, M_n$, denoted as $M_1 \oplus \cdots \oplus M_n$.

Proposition 4.1.8. Let R be a ring and $N_1, \ldots, N_n \leqslant M$ be R-modules. TFAE:

1. $\begin{array}{rcl} \phi : N_1 \times \cdots \times N_k & \longrightarrow & N_1 + \cdots + N_k \\ (a_1, \ldots, a_k) & \longmapsto & a_1 + \cdots + a_k \end{array}$ is an isomorphism.

2. $N_j \cap \sum_{i \neq j} N_i = 0$ for any j.

3. Every element $x \in N_1 + \cdots + N_k$ can be written uniquely as $x = a_1 + \cdots + a_k$ for $a_j \in N_j$.

Definition. If any of the above holds, we say $N_1 + \cdots + N_k$ is the **(internal) direct sum** of the N_j, also denoted as $N_1 \oplus \cdots \oplus N_n$.

Remark 4.1.9. Let $(M_i)_{i \in I}$ be a family of R-modules. The **direct product** of the M_j is the set $\prod_{i \in I} M_i$ on which R acts componentwise, making it an R-module. The **direct sum** of the M_j is defined by the **restricted product**

$$\prod_{i \in I}^{*} M_i = \left\{ (a_i)_{i \in I} \in \prod_{i \in I} M_i \mid a_i = 0 \text{ for all but finitely many } i \in I \right\}$$

on which R acts componentwise.

The direct product has the following universal property. Let $\pi_j : \prod_{i \in I} M_i \to M_j$ be the j-th projection. Then given any family of R-module homomorphisms $f_j \in \mathrm{Hom}_R(A, M_j)$, there exists a unique $f \in \mathrm{Hom}_R(A, \prod_i M_i)$ such that $\pi_j \circ f = f_j$ for all $j \in I$.

The direct sum has the dual universal property. Let $\iota_j : M_j \to \bigoplus_{i \in I} M_i$ be the j-th inclusion. Then given any family of R-module homomorphisms $f_j \in \mathrm{Hom}_R(M_j, A)$, there exists a unique $f \in \mathrm{Hom}_R(\prod_i M_i, A)$ such that $f \circ \iota_j = f_j$ for all $j \in I$.

Definition. An R-module F is said to be **free on a subset** A if every $x \in I$ can be expressed uniquely as $x = r_1 a_1 + \cdots + r_n a_n$ with unique $a_j \in A$, $r_j \in R$. We say A is a **basis** or a set of **free generators** of F. When R is commutative, $\#A$ is called the **rank** of F.

- Let R be commutative with 1 and let I be a maximal ideal. Let $f : R^n \to R^m$ be an isomorphism. Then $\mathrm{id} \otimes f : R/I \otimes_R R^n \to R/I \otimes_R R^m$ is an isomorphism between vector spaces. Hence $n = m$.

Proposition 4.1.10. Let R be a ring and A be a set. Then there's a free R-module $F(A)$ on the set A satisfying the universal property: for any R-module M with a map $\phi : A \to M$, there's a unique $\Phi \in \mathrm{Hom}_R(F(A), M)$ such that $\Phi \circ \iota = \phi$, where $\iota : A \to F(A)$ is the inclusion.

Proof. It's clear that $F(A) := \bigoplus_{i \in A} R$ is the desired free module on A. Equivalently, one can construct it as

$$F(A) = \{ f : A \to M \mid f(x) = 0 \text{ for all but finitely many } x \in A \}$$

□

4.1.3 Tensor products of modules

Question 4.1.11. Suppose R, S are rings with $R \subseteq S$. Then any S-module is automatically an R-module. How above the converse? That is, given an R-module, can we make it a *nontrivial* S-module. The answer is generally negative. For example, $\mathbb{Z}$ is a $\mathbb{Z}$-module but fails to be a $\mathbb{Q}$-module.

How best can we do? Let M be an R-module. Consider the free abelian group $\mathbb{Z}(S \times M)$. To make it an S-module, we need to identify $(s_1 + s_2, m) - (s_1, m) - (s_2, m)$, $(s, m_1 + m_2) - (s, m_1) - (s, m_2)$ and $(sr, m) - (s, rm)$ with 0 for all $s, s_1, s_2 \in S$, $m, m_1, m_2 \in M$ and $r \in R$; let H be the subgroup of $\mathbb{Z}(S \times M)$ generated by the above identification. Define the **tensor product of S and M over R** to be the quotient

$$S \otimes_R M = \mathbb{Z}(S \times M)/H$$

and denote the coset of (s, m) by $s \otimes m$. Elements of $S \otimes_R M$ are called **tensors**, and those of the form $s \otimes m$ are called a **simple tensor**.

Proposition 4.1.12. Define the S-action on $S \otimes_R M$ by $s(\sum_i s_i \times m_i) := \sum_i ss_i \otimes m_i$. Then $S \otimes_R M$ becomes an S-module.

Example 4.1.13.

1. $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/a\mathbb{Z} = 0$.
2. More generally, if A is a torsion abelian group, then $\mathbb{Q} \otimes_{\mathbb{Z}} A = 0$.
3. $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z} = \mathbb{Q}$.

Theorem 4.1.14. Let $R \subseteq S$ be rings with 1 and let N be an R-module. Let $\iota : N \to S \otimes_R N$ be defined by $\iota(n) = 1 \otimes n$. Suppose L is an S-module and $\phi \in \mathrm{Hom}_R(N, L)$, then there's a unique $\Phi \in \mathrm{Hom}_S(S \otimes_R N, L)$ such that $\phi = \Phi \circ \iota$.

Corollary 4.1.14.1. Under the condition above, then $\ker \iota \subseteq \ker \phi$.

Corollary 4.1.14.2. Under the condition above, we have the bijection

$$\mathrm{Hom}_S(S \otimes_R N, L) \cong \mathrm{Hom}_R(N, \mathrm{Res}_R(L))$$

where $\mathrm{Res}_R : (S\textbf{-Mod}) \to (R\textbf{-Mod})$ is the forgetful functor.

Remark 4.1.15. The process of obtaining the S-module $S \otimes_R N$ from N is called the **extension of scalars**.

We next consider the tensor products of two modules. Let R be a ring, N be a left R-module and R a right R-module. Consider the free abelian group $\mathbb{Z}(M \times N)$ and let $H \leqslant \mathbb{Z}(M \times N)$ generated by $(m_1+m_2, n)-(m_1, n)-(m_2, n)$, $(m, n_1+n_2)-(m, n_1)-(m, n_2)$ and $(mr, n)-(m, rn)$ for all $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$ and $r \in R$. Then

$$M \otimes_R N := \mathbb{Z}(M \times N)/H$$

is called the **tensor product of M and N over R**. Note that $M \otimes_R N$ is, in general, just an abelian group, unless M is given the structure of some left module.

If M is an (S, R)-bimodule, then $M \otimes_R N$ can become a left S-module, where the S-action is given by $s(\sum_i m_i \otimes n_i) := \sum_i sm_i \otimes n_i$. In particular, if R is commutative, then we can make M an (R, R)-bimodule by setting $rm = mr$ for all $r \in R$, $m \in M$, and $M \otimes_R N$ is automatically an R-module.

Example 4.1.16.

1. Let $m, n \in \mathbb{N}$ and $d = \gcd(m, n)$. Then $\mathbb{Z}/m\mathbb{Z} \otimes_R \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/d\mathbb{Z}$ and is cyclic generated by $1 \otimes 1$.

2. $\mathbb{R}[x] \otimes_{\mathbb{R}} \mathbb{R}[y] \cong \mathbb{R}[x, y]$.

Definition. Let R be a ring, N a left R-module, R a right R-module and L an abelian group. A map $\phi : M \times N$ is **R-balanced**, or **R-middlelinear**, if it's bilinear as groups and $\phi(mr, n) = \phi(m, rn)$ for all $m \in M$, $n \in N$, $r \in R$.

Theorem 4.1.17. Let M, N, L, ϕ as above and $\iota : M \times N \to M \otimes_R N$ be an R-balanced map defined by $\iota(m, n) := m \otimes n$. Then there's a unique $\Phi \in \mathrm{Hom}_{\mathbb{Z}}(M \otimes_R N, L)$ such that $\phi = \Phi \circ \iota$.

Corollary 4.1.17.1. Let R, S be rings, M a right R-module, N an (R, S)-bimodule and L a right S-module. Then there's a bijection

$$\mathrm{Hom}_{(\textbf{Mod-}S)}(M \otimes_R N, L) \cong \mathrm{Hom}_{(\textbf{Mod-}R)}(M, \mathrm{Hom}_{(\textbf{Mod-}S)}(N, L))$$

Corollary 4.1.17.2. Let R be a commutative ring and M, N, L be R-modules. Then there's a bijection

$$\{\phi : M \times N \to L \mid \phi \text{ is } R\text{-bilinear}\} \cong \mathrm{Hom}_R(M \otimes_R N, L)$$

Example 4.1.18.

1. Let $f : R \to S$ be a ring homomorphism. This map induces a right R-module structure on S, given by $sr := sf(r)$ for all $s \in S, r \in R$. Then for any left R-module N, $S \otimes_R N$ changes the base from R to S.

2. If $f : R \to S$ is a ring homomorphism with $f(1_R) = 1_S$, then $S \otimes_R R \cong S$ via the map $s \otimes r \mapsto sf(r)$ with inverse $s \mapsto s \otimes 1$.

3. Let R be a ring, $I \trianglelefteq R$ a two-sided ideal and N an R-module. Then $(R/I) \otimes_R N \cong N/IN$.

4. A abelian group G is **divisible** if for all $n \in \mathbb{N}$ and $g \in G$, $ny = g$ for some $y \in G$. Then for any divisible abelian group A and torsion abelian group B, we have $A \otimes_{\mathbb{Z}} B = 0$.

   More generally, given a ring R with 1, we say an R-module M is **divisible** if for every non zero-divisor $r \in R$, the map $r \mapsto rm$ is a surjective endomorphism on M.

5. Let M, M' be right R-modules and N, N' be left R-modules. Let $\varphi : M \to M'$ and $\psi : N \to N'$ be R-module homomorphisms. Then we can define a group homomorphism $\varphi \otimes \psi : M \otimes_R N \to M' \otimes_R N'$ in a natural way, and this is unique. Furthermore, if M, M' are (S, R)-bimodules for some ring S and φ is an S-module homomorphism, then $\varphi \otimes \psi$ is an S-module homomorphism.

Proposition 4.1.19. Let R, S be rings, M a right R-module, N an (R, S)-bimodule and L a right S-module. Then there's a bijection

$$(M \otimes_R N) \otimes_S L \cong M \otimes_R (N \otimes_S L)$$

Proposition 4.1.20. Let R be a ring, M, M' be right R-modules and N, N' be left R-modules. Then

$$(M \oplus M') \otimes_R N \cong (M \otimes_R N) \oplus (M' \otimes_R N)$$

$$M \otimes_R (N \oplus N') \cong (M \otimes_R N) \oplus (M \otimes_R N')$$

Corollary 4.1.20.1. Let $R \subseteq S$ be rings with the same 1 and $n, m \in \mathbb{N}$. Then

$$S \otimes_R R^n \cong S^n$$

and

$$R^n \otimes_R R^m \cong R^{nm}$$

Proposition 4.1.21. Let R be a commutative ring and M, N be R-modules. Then

$$M \otimes_R N \cong N \otimes_R M$$

Proposition 4.1.22. Let R be a commutative ring and A, B be R-algebra. Then the tensor product of modules $A \otimes_R B$ has a structure of R-algebra, given by $(a \otimes a')(b \otimes b') := (ab \otimes a'b')$.

4.1.4 Exact sequences

Definition.

1. A pair of group/ring/module homomorphisms $X \xrightarrow{\alpha} Y \xrightarrow{\beta} Z$ is **exact** if $\ker \beta = \operatorname{Im} \alpha$.
2. A sequence $\cdots \to X_{i-1} \to X_i \to X_{i+1} \to \cdots$ is **exact** if it's exact at each X_i.
3. An exact sequence of the form $0 \to X \to Y \to Z \to 0$ is called a **short exact sequence**. Here 0 denotes the additive identity; if X, Y, Z are multiplicative groups, we write 1 instead.

- $0 \to X \xrightarrow{\alpha} Y$ is exact $\Leftrightarrow \alpha$ is injective.
- $Y \xrightarrow{\beta} Z \to 0$ is exact $\Leftrightarrow \beta$ is surjective.
- $0 \to X \xrightarrow{\alpha} Y \xrightarrow{\beta} Z \to 0$ is a short exact sequence $\Leftrightarrow Y/\alpha(X) \cong Z$.

Remark 4.1.23. We have the following short exact sequences:

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow (\mathbb{Z}/2\mathbb{Z})^3 \longrightarrow (\mathbb{Z}/2\mathbb{Z})^2 \longrightarrow 0$$

$$0 \longrightarrow \langle (2,0) \rangle \longrightarrow \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \longrightarrow (\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})/\langle (2,0) \rangle \longrightarrow 0$$

$$1 \longrightarrow \langle \sigma^2 \rangle \longrightarrow D_8 = \langle \sigma, \tau \rangle \longrightarrow D_8/\langle \sigma^2 \rangle \longrightarrow 1$$

$$1 \longrightarrow \langle -1 \rangle \longrightarrow Q_8 \longrightarrow Q_8/\langle -1 \rangle \longrightarrow 1$$

Those in the second column are isomorphic to $\mathbb{Z}/2\mathbb{Z}$ and those in the fourth column are isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$, but those in the middle column are not isomorphic.

This is a part of the classification of finite groups, which consists of

(i) classification of all finite simple groups

(ii) given any groups A, B, find all exact sequences $1 \to N \to G \to G/N \to 1$ such that $A \cong N$ and $B \cong G/N$.

Proposition 4.1.24. Consider the commutative diagram of modules with exact rows

$$\begin{array}{ccccc} A & \xrightarrow{\psi} & B & \xrightarrow{\varphi} & C \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} \\ A' & \xrightarrow{\psi'} & B' & \xrightarrow{\varphi'} & C' \end{array}$$

1. If φ, α are surjective and β is injective, then γ is injective.

2. If ψ', γ are injective and β is surjective, then α is surjective.

3. If ψ', α, γ are injective, then β is injective.

4. If φ, α, γ are surjective, then β is surjective.

Proposition 4.1.25 (five lemma)**.** Consider the commutative diagram of modules

$$\begin{array}{ccccccc} A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & D \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \delta} \\ A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & D' \end{array}$$

1. If β, δ are injective and α is surjective, then γ is injective.

2. If α, γ are surjective and δ is injective, then β is surjective.

Corollary 4.1.25.1. Consider the commutative diagram of modules

$$\begin{array}{ccccccccc} A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & D & \longrightarrow & E \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \delta} & & \downarrow{\scriptstyle \epsilon} \\ A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & D' & \longrightarrow & E' \end{array}$$

If β, δ are isomorphisms, α is surjective and ϵ is injective, then γ is an isomorphism.

Proposition 4.1.26 (snake lemma)**.** Consider the commutative diagram of modules

$$\begin{array}{ccccccccc} A & \xrightarrow{f} & B & \xrightarrow{g} & C & \xrightarrow{h} & D & \xrightarrow{j} & E \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \epsilon} & & \downarrow{\scriptstyle \eta} \\ A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & \xrightarrow{h'} & D' & \xrightarrow{j'} & E' \end{array}$$

with α surjective, η injective and two rows being exact. Then it induces a long exact sequence

$$\begin{array}{ccccccccc} \ker f'\alpha & \longrightarrow & \ker \beta & \longrightarrow & \ker \gamma & \longrightarrow & \ker \epsilon & & \\ & & & & & & & & \\ A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & D & \longrightarrow & E \\ \downarrow & & \downarrow & & \downarrow & \overset{\delta}{\searrow} & \downarrow & & \downarrow \\ A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & D' & \longrightarrow & E' \\ & & & & & & & & \\ \longrightarrow \operatorname{coker} \beta & \longrightarrow & \operatorname{coker} \gamma & \longrightarrow & \operatorname{coker} \epsilon & \longrightarrow & \operatorname{coker} \eta j. & & \end{array}$$

in which the map δ is called a **connecting homomorphism**.

Corollary 4.1.26.1. Consider the commutative diagram with exact rows

$$\begin{array}{ccccccccc} & & A & \xrightarrow{g} & B & \xrightarrow{h} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \epsilon} & & \\ 0 & \longrightarrow & A' & \xrightarrow{g'} & B' & \xrightarrow{h'} & C' & & \end{array}$$

Then it induces a long exact sequence

$$\ker \beta \longrightarrow \ker \gamma \longrightarrow \ker \epsilon \xrightarrow{\delta} \operatorname{coker} \beta \longrightarrow \operatorname{coker} \gamma \longrightarrow \operatorname{coker} \epsilon$$

Proposition 4.1.27 (3×3 lemma)**.** Consider the commutative diagram of modules

$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A' & \longrightarrow & A & \longrightarrow & A'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & B' & \longrightarrow & B & \longrightarrow & B'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & C' & \longrightarrow & C & \longrightarrow & C'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & 0 & & \end{array}$$

with all columns being exacts.

1. If the bottom two rows are exact, then the top row is exact.
2. If the top two rows are exact, then the bottom row is exact.
3. If the top and bottom rows are exact and the middle row is a complex, then the middle row is exact.

Definition. A short sequence $0 \to A \xrightarrow{\psi} B \xrightarrow{\varphi} C \to 0$ is said to **split** if $B = \psi(A) \oplus C'$ for some $C' \leqslant B$ with $C' \cong C$ by φ, that is, $B \cong A \oplus C$.

- We say B is a **split extension of** C **by** A.

Lemma 4.1.28. Let R be a ring and M an R-module. If $\pi \in \operatorname{End}_R(M)$ is idempotent, i.e, $\pi^2 = \pi$, then $M \cong \ker \pi \oplus \operatorname{Im} \pi$.

Proof. Note that for all $m = \pi(m') \in \operatorname{Im}\pi$, we have $m - \pi(m) = \pi(m') - \pi^2(m') = 0$, since $\pi^2 = \pi$. Conversely, if $m \in \ker(\mathrm{id}_M - \pi)$, then $m = \pi(m) \in \operatorname{Im}\pi$. Hence, $\ker(\mathrm{id}_M - \pi) = \operatorname{Im}\pi$.

For each $m \in M$, we may write $m = \pi(m) + (\mathrm{id}_M - \pi)(m)$, so $M = \ker\pi + \operatorname{Im}\pi$. If $x \in \ker\pi \cap \operatorname{Im}\pi$, say $x = \pi(y)$, then $0 = \pi(x) = \pi^2(y) = \pi(y) = x$. Hence $M = \ker\pi \oplus \operatorname{Im}\pi$. □

Proposition 4.1.29. Let $0 \to A \xrightarrow{\psi} B \xrightarrow{\varphi} C \to 0$ be an exact sequence. TFAE:

1. It splits.
2. There exists a $\mu \in \mathrm{Hom}(C, B)$ such that $\varphi \circ \mu = \mathrm{id}_C$.
3. There exists a $\lambda \in \mathrm{Hom}(B, A)$ such that $\lambda \circ \psi = \mathrm{id}_A$.

If this is the case, we call μ a **splitting homomorphism**.

Proof. Assume 1, and let $B = \psi(A) \oplus C'$ with $C' \cong C$ by φ. Then pick $\mu = (\varphi|'_C)^{-1} : C \to C' \subseteq B$ and $\lambda : B \to \psi(A) \cong A$ be the projection.

Conversely, let $f = \mu \circ \varphi$ and $g = \psi \circ \lambda$. Both of them are idempotent endomorphisms on B, so by Lemma 4.1.29, $B \cong \ker f \oplus \operatorname{Im} f = \ker\varphi \oplus \operatorname{Im}\varphi \cong A \oplus C$, since μ is injective. Similarly, $B \cong \ker g \oplus \operatorname{Im} g \cong B/A \oplus A \cong C \oplus A$. □

Example 4.1.30. $0 \to \mathbb{Z} \xrightarrow{\times n} \mathbb{Z} \xrightarrow{\mathrm{mod}\ n} \mathbb{Z}/n\mathbb{Z} \to 0$ does not split since $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}) = 0$.

Projective modules

Proposition 4.1.31. Let R be a ring with 1 and A, B, C an R-module. TFAE:

1. $0 \to A \to B \to C$ is exact.
2. $0 \to \mathrm{Hom}_R(D, A) \to \mathrm{Hom}_R(D, B) \to \mathrm{Hom}_R(D, C)$ is exact for all R-modules D.

Proposition 4.1.32. Let R be a ring with 1 and P an R-module. TFAE:

1. $\mathrm{Hom}(P, -)$ is an exact functor.
2. $\mathrm{Hom}(P, -)$ is a right exact functor.
3. Every exact sequence $0 \to A \to B \to P \to 0$ splits.
4. P is a direct summand of some free module.

Definition. An R-module P satisfies any of the above equivalent conditions is called **projective**.

Corollary 4.1.32.1. Let R be a ring with 1.

1. Free R-modules are projective.
2. Every R-module is a quotient of some projective R-module.

Example 4.1.33.

1. If $R = F$ is a field, then any R-module is a F-vector space, which is free and thus projective.
2. If A is a nontrivial torsion abelian group, then it cannot be a projective $\mathbb{Z}$-module.
3. $\mathbb{Q}$ is not a projective $\mathbb{Z}$-module. In general, a divisible abelian group is not a projective $\mathbb{Z}$-module.

Theorem 4.1.34 (Dual basis lemma)**.** Let R be a ring and P be an R-module. TFAE:

1. P is projective.
2. There exist $\{a_i \mid i \in I\} \subseteq P$ and $\{f_i \mid i \in I\} \subseteq \mathrm{Hom}_R(P, R)$ such that for any $a \in P$, $f_i(a) = 0$ for all but finitely many i, and $a = \sum_i f_i(a)a_i$.

Proof.

2.⇒1. Let $F = \bigoplus_i Re_i$ and consider projection $g : F \to P$ given by $g(e_i) = a_i$. Also, consider $f : P \to F$ given by $f(a) = \sum f_i(a)e_i$. Then $g \circ f = \mathrm{id}_P$, and P is a direct summand of F.

1.⇒2. Let $F = \bigoplus_i Re_i$ be the free module and $g : F \to P$ be the projection. Let $a_i = g(e_i)$. Since P is projective, there exists $h : P \to F$ such that $a = \sum_i f_i(a)e_i$ and $h \circ g = \mathrm{id}_P$. Then $\{a_i\}$ and $\{f_i\}$ are the desired collection.

□

Definition. The associated right R-module $\mathrm{Hom}_R(M, R)$ of an R-module M is called the **dual module** of M, and is denoted by M^*.

- The R-action on M^* is given by $(\varphi r)(m) := \varphi(m)r$.
- If M is a finitely generated free left R-module, then M^* is a free right R-module of the same rank. In particular, if M is finitely generated projective, then M^* is projective.

Injective modules

Proposition 4.1.35. Let R be a ring with 1 and A, B, C be R-modules. TFAE:

1. $A \to B \to C \to 0$ is exact.
2. $0 \to \mathrm{Hom}_R(C, D) \to \mathrm{Hom}_R(B, D) \to \mathrm{Hom}_R(A, D)$ is exact for all R-modules D.

Proposition 4.1.36. Let R be a ring with 1 and J be an R-modules. TFAE:

1. $\mathrm{Hom}_R(-, J)$ is an exact functor.
2. $\mathrm{Hom}_R(-, J)$ is a right exact functor.
3. Every exact sequence $0 \to J \to B \to C \to 0$ splits.

Definition. An R-module P satisfies any of the above equivalent conditions is called **injective**.

Example 4.1.37. $\mathbb{Z}$ is not an injective $\mathbb{Z}$-module. Consider $\begin{array}{ccccc} 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{\times n} & \mathbb{Z} \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \\ & & \mathbb{Z} & & \end{array}$. If $n \neq \pm 1$, then id cannot be lifted to a homomorphism $n\mathbb{Z} \to \mathbb{Z}$.

Proposition 4.1.38 (Baer's criterion)**.** Let R a ring with 1 and J an R-module.

1. J is an injective R-modules $\Leftrightarrow$ for all left ideals $I \trianglelefteq R$, any R-module homomorphism $g : I \to J$ can be extended to some R-module homomorphism $f : R \to J$.
2. If R is a PID, then J is injective $\Leftrightarrow rJ = J$ for all $r \in R \backslash \{0\}$, i.e, J is a divisible R-module.

Proof.

1. Consider

$$\begin{array}{ccccc} 0 & \longrightarrow & A & \xrightarrow{\psi} & B \\ & & \downarrow{\scriptstyle g} & & \\ & & J & & \end{array}$$

and let $S := \{(B', g') \mid \mathrm{Im}\,\psi \subseteq B' \subseteq B \wedge g' \in \mathrm{Hom}_R(B', J) \text{ such that } g'\psi = g\}$; this is nonempty since $(\mathrm{Im}\,\psi, g\psi^{-1}) \in S$. Partially ordered S as usual and by Zorn's lemma, S admits a maximal element (B_0, f_0).

Suppose for contradiction that $B_0 \subsetneq B$, say $b \in B \backslash B_0$. Consider $I = (B_0 : b) \trianglelefteq R$ and define $f_1 : I \to J$ by $f'(r) := f_0(rb)$. By assumption, f_1 can be extended to some $f' : R \to J$. Put $B' = B_0 + Rb \supsetneq B_0$ and define $f' : B' \to J$ by $f'(b_0 + rb) = f_0(b_0) + f_1(r)$ for $b_0 \in B_0$, $r \in R$; this is well-defined and $(B', f') \in S$ is larger than (B_0, f_0), a contradiction.

2. Let $I = (r)$ be a nonzero ideal of R, and for each $q \in J$ define $g : I \to J$ such that $g(r) = q$; this is well-defined and unique. g can be extended to a homomorphism $G : R \to J$ if and only if there exists $q' \in J$ with $G(1) = q'$ such that $q'r = G(r) = g(r) = q$, if and only if $J = rJ$. The result follows from 1.

□

Corollary 4.1.38.1. A $\mathbb{Z}$-module is injective if and only if it's divisible.

Corollary 4.1.38.2. If R is a PID, then any quotient of an injective R-module is again injective.

Corollary 4.1.38.3. Every $\mathbb{Z}$-module is a submodule of some injective module.

Proof. Let A be a $\mathbb{Z}$-module and let $\varphi : \mathbb{Z}(A) \to A$ be the canonical projection. Consider $Q := \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}(A)$; this is an injective $\mathbb{Z}$-module since it's a direct sum of $\mathbb{Q}$ and thus divisible, Corollary 4.1.38.1 applies. Then $A \cong \mathbb{Z}(A)/\ker\varphi \leqslant Q/\ker\varphi$ and $Q/\ker\varphi$ is injective over $\mathbb{Z}$ by Corollary 4.1.38.2. □

Theorem 4.1.39. If R is a ring with 1, then every left R-module M is submodule of some injective module.

Proof.

1° Show that $\mathrm{Hom}_{\mathbb{Z}}(R, M)$ is a left R-module under the action $(r\varphi)(s) = \varphi(sr)$.

2° Show that if Q is an injective R-module then $\mathrm{Hom}_Z(R, Q)$ is also an injective R-module.

3° View M as an $\mathbb{Z}$-module any thus it's contained in some injective $\mathbb{Z}$-module Q.

4° Note that $\mathrm{Hom}_R(R, M) \subseteq \mathrm{Hom}_{\mathbb{Z}}(R, M) \subseteq \mathrm{Hom}_{\mathbb{Z}}(R, Q)$ and use the R-module isomorphism $M \cong \mathrm{Hom}_R(R, M)$ to conclude the theorem.

We elaborate on 2°. Given that $0 \longrightarrow A \xrightarrow{\varphi} B$ is an exact sequence of R-modules and now since Q is injective,

$$\mathrm{Hom}_{\mathbb{Z}}(B, Q) \xrightarrow{\varphi^*} \mathrm{Hom}_{\mathbb{Z}}(A, Q) \to 0$$

is exact. Given $f' \in \mathrm{Hom}_R(A, \mathrm{Hom}_{\mathbb{Z}}(R, Q))$, consider

$$\begin{array}{ccccc} 0 & \longrightarrow & A & \xrightarrow{\varphi} & B \\ & & \downarrow & & \\ & & \mathrm{Hom}_{\mathbb{Z}}(R, Q) & & \\ & & \downarrow & & \end{array} \qquad \begin{array}{c} a \\ \downarrow \\ f'(a) \\ \downarrow \\ f'(a)(1_R) \end{array}$$

$$M$$

Hence $f := f'(-)(1_R) \in \mathrm{Hom}_R(A, Q)$. By our assumption, there's a $g \in \mathrm{Hom}_{\mathbb{Z}}(B, Q)$ such that $f = g \circ \varphi$. Define $g'(b)(r) := g(rb)$ for $b \in B$ and $r \in R$; clearly $g'(b) \in \mathrm{Hom}_{\mathbb{Z}}(R, Q)$, and $g' \in \mathrm{Hom}_{\mathbb{Z}}(B, \mathrm{Hom}_{\mathbb{Z}}(R, Q))$. We contend $f' = g' \circ \varphi$. Indeed, for each $a \in A$ and $r \in R$,

$$g'(\varphi(a))(r) = g(r\varphi(a)) = g(\varphi(ra)) = f(ra) = f'(a)(r)$$

so $g' \circ \varphi = f'$. □

Remark 4.1.40. Among all injective modules containing M, a minimal one the called the **injective hull** E of M. "The" injective hull E has the universal property: if Q is an injective R-module such that $M \subseteq Q$, then $M \subseteq E \subseteq Q$.

For instance, $\mathbb{Q}$ is the injective hull of the $\mathbb{Z}$-module $\mathbb{Z}$ and any injective hull of a field F is F itself.

Flat modules

Proposition 4.1.41. Let R be a ring with 1 and A, B, C be R-modules. TFAE:

1. $A \to B \to C \to 0$ is exact.
2. $D \otimes_R A \to D \otimes_R B \to D \otimes_R C \to 0$ is exact for all R-modules D.

Definition. An R-module D is such that $D \otimes_R -$ is a left exact functor is called a **flat R-module**.

Proposition 4.1.42. Let R be a ring with 1. Then projective R-modules are flat.

Proof. Let P be a projective R-module and F a free R-module such that $F = P \oplus M$ for some R-module M. Let $\phi : A \to B$ be injective. Consider

$$(P \otimes A) \oplus (M \otimes A) \xrightarrow{\sim} (P \oplus M) \otimes A = F \otimes A \xrightarrow{\mathrm{id} \otimes \phi} F \otimes B \xrightarrow{\sim} (P \otimes B) \oplus (M \otimes B)$$

To show $P \otimes A \to P \otimes B$ is injective, it suffices to show $\mathrm{id} \otimes \phi$ is injective. Indeed, write $F = \bigoplus R$ and consider the commutative diagram

$$\begin{array}{ccccccc} \bigoplus (R \otimes A) & \xrightarrow{\sim} & (\bigoplus R) \otimes A & \longrightarrow & (\bigoplus R) \otimes B & \xrightarrow{\sim} & \bigoplus (R \otimes B) \\ \sim\uparrow & & & & & & \sim\uparrow \\ \bigoplus A & & & & \longrightarrow & & \bigoplus B \end{array}$$

The result follows once we note that the bottom arrow is injective. □

Proposition 4.1.43 (Flatness criterion)**.** Let R be a ring with 1 and D an R-module. TFAE:

1. D is flat.

2. For every finitely generated left ideal $I \trianglelefteq R$, the map $D \otimes_R I \to D \otimes_R R$ induced by the inclusion $I \subseteq R$ is injective.

Proof. Let D be an R-module satisfying 2. We break our proof into some steps.

1° We show $D \otimes I \to D \otimes R$ is injective for every left ideal I of R. Indeed, every element in $D \otimes I$ is a finite sum of simple tensors, and hence is contained in some $D \otimes I'$ for some finitely generated left ideal I' of R. Hence if it's sent to zero, by our assumption it's itself zero in $D \otimes I'$ and thus in $D \otimes I$. This shows the injectivity.

2° We show if K is a submodule of some finitely generated free module F, then $M \otimes K \to M \otimes F$ is injective. Write $F = K + Rv_1 + \cdots + Rv_n$ and $F_i = K + Rv_1 + \cdots + Rv_n$. We show each step in

$$M \otimes K \longrightarrow M \otimes F_1 \longrightarrow M \otimes F_2 \longrightarrow \cdots \longrightarrow M \otimes F_n = M \otimes F$$

is injective. For convenience, put $K = F_0$. For $i = 0, 1, \ldots, n-1$, we have the short exact sequence

$$0 \longrightarrow F_i \longrightarrow F_{i+1} \longrightarrow F_{i+1}/F_i \cong R/I_i \longrightarrow 0$$

where $I_i := \{a \in R \mid av_{i+1} \in F_i\}$ and $\cong$ follows from some isomorphism theorem; I_i is an ideal of R since F_i is an R-module. Then we have the induced long exact sequence

$$\cdots \longrightarrow \operatorname{Tor}_1^R(M, R/I_i) \longrightarrow M \otimes F_i \longrightarrow M \otimes F_{i+1} \longrightarrow M \otimes R/I_i \longrightarrow 0$$

We contend $\operatorname{Tor}_1^R(M, R/I_i) = 0$. For each $i = 0, \ldots, n-1$, $0 \to I_i \to R \to R/I_i \to 0$ induces the exact sequence

$$0 = \operatorname{Tor}_1^R(M, R) \longrightarrow \operatorname{Tor}_1^R(M, R/I_i) \longrightarrow M \otimes I_i \longrightarrow M \longrightarrow M \otimes R/I_i \longrightarrow 0$$

By our assumption, $M \otimes I_i \to M \otimes R$ is injective, and thus $\operatorname{Tor}_1^R(M, R/I_i) = 0$. Hence

$$0 \longrightarrow M \otimes F_i \longrightarrow M \otimes F_{i+1} \longrightarrow M \otimes R/I_i \longrightarrow 0$$

and thus $M \otimes F_i \to M \otimes F_{i+1}$ is injective.

3° Now we show if K is a submodule of some free module F, then $M \otimes K \to M \otimes F$ is injective. Indeed, every element of $M \otimes K$ is a finite sum of simple tensors, and thus is contained in some finitely generated free submodule of F. Then this follows directly from 2°.

4° Let A, B be R-modules and $A \xrightarrow{g} B$ be injective. Write $B = F/Q$ for some free module F and submodule Q. Then we have a short exact sequence

$$0 \longrightarrow Q \longrightarrow F \xrightarrow{f} B \longrightarrow 0$$

Put $J = f^{-1}(g(A))$ and $\iota : J \to F$ to be the inclusion, then we have the commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & Q & \longrightarrow & J & \longrightarrow & A & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \iota} & & \downarrow{\scriptstyle g} & & \\ 0 & \longrightarrow & Q & \longrightarrow & F & \xrightarrow{f} & B & \longrightarrow & 0 \end{array}$$

Apply the functor $D \otimes -$, we obtain a commutative diagram with exact rows

$$\begin{array}{ccccccccc} D\otimes Q & \longrightarrow & D\otimes J & \longrightarrow & D\otimes A & \longrightarrow & 0 \\ \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \mathrm{id}\otimes\iota} & & \downarrow{\scriptstyle \mathrm{id}\otimes g} & & \\ D\otimes Q & \longrightarrow & D\otimes F & \xrightarrow{\mathrm{id}\otimes f} & D\otimes B & \longrightarrow & 0 \end{array}$$

By 2°, we know $\mathrm{id}\otimes\iota$ is injective, and by Proposition 4.1.24.1, $\mathrm{id}\otimes g$ is injective.

□

Proposition 4.1.44. Let R be a PID and D an R-module. Then D is flat $\Leftrightarrow$ D is torsion free.

Proof. ($\Leftarrow$) Let $I = (a) \neq 0$ be an ideal of R. Consider the composition of maps

$$\begin{array}{ccccccccc} D & \xrightarrow{\sim} & D\otimes_R R & \xrightarrow{\sim} & D\otimes_R I & \xrightarrow{\mathrm{id}\otimes\iota} & D\otimes_R R & \xrightarrow{\sim} & D \\ mr & \longmapsto & m\otimes r & \longmapsto & m\otimes ra & \longmapsto & m\otimes ra & \longmapsto & mra \end{array}$$

where $\iota : I \to R$ is the inclusion. Since D is torsion free, this composition is injective, and thus $\mathrm{id}\otimes\iota$ is injective. By flatness criterion, D is flat.

($\Rightarrow$) Let $a \in R\backslash\{0\}$ and consider the exact sequence $0 \longrightarrow R \xrightarrow{\times a} R$. Since N is flat, we have the exact sequence

$$\begin{array}{ccccc} 0 & \longrightarrow & D\otimes_R R & \xrightarrow{\mathrm{id}\times a} & D\otimes_R R \\ & & \downarrow{\scriptstyle\sim} & & \downarrow{\scriptstyle\sim} \\ & & D & \longrightarrow & D \\ & & m & \longmapsto & ma \end{array}$$

The injectivity gives $\mathrm{Ann}_M(a) = \{m \in M \mid ma = 0\} = 0$, and thus $\mathrm{Tor}(M) = \bigcup_{a\in R} \mathrm{Ann}_M(a) = 0$. □

We consider the following table. (HW. 6)

	Projective	Injective	Flat
submodule			
quotient			
finite direct sum			
direct sum			
direct product			
direct summand			
tensor product (assuming R is comm.)			
extension of scalars			

Each (i, j) blank corresponds to the question *whether any i of j module is j*. For instance, the $(1, 2)$ black corresponds to *whether any submodule of an injective modules is injective*. We will not complete this table, but we only discuss some of them.

submodules and quotients.

Definition. A ring R is **left hereditary** if all left ideal of R is a projective left R-modules.

Theorem 4.1.45. Let R be a hereditary ring. Then any submodule P of a free R-module $F = \bigoplus_{i\in I} Re_i$ is isomorphic to a direct sum of left ideals of R. In particular, P is projective over R.

Proof. By virtue of AC, let $<$ be a well-ordering on I. For each $i \in I$, let $F_i = \bigoplus_{j\leqslant i} Re_j$ and $G_i = \bigoplus_{j<i} Re_j$. Let $p_i : F \to R$ be the i-th projection. Put $J_i := p_i(P \cap F_i)$; this is a left ideal of R. Since J_i is projective over R, the exact sequence

$$0 \longrightarrow P \cap G_i \longrightarrow P \cap F_i \xrightarrow{p_i} J_i \longrightarrow 0$$

splits, and thus $P \cap F_i = (P \cap G_i) \oplus A_i$ for some submodule $A_i \cong J_i$ as R-modules. We contend $P = \bigoplus_{i\in I} A_i$.

Suppose $a_1 + \cdots + a_n = 0$ for some $a_i \in A_{\alpha_i}$; WLOG, say $\alpha_1 < \cdots < \alpha_n$. Then $a_n = -(a_1 + \cdots + a_{n-1}) \in G_{\alpha_n} \cap F_{\alpha_n} = 0$, so $a_n = 0$; by induction, $a_i = 0$. Finally, we show $P = \sum_{i\in I} A_i$. If not, then there would exist a smallest j (since $<$ is a well ordering) such that $P \cap F_j$ contains an element a that is not belonging to $\sum_{i\in I} A_i$. Write $a = b + c$ where $b \in P \cap G_j$ and $c \in A_j$. Then $b \in P \cap F_k$ for some $k < j$; the minimality of j shows $b \in \sum_{i\in I} A_i$. But $a = b + c \in \sum_{i\in I} A_i$, a contradiction. □

Corollary 4.1.45.1. A ring R is hereditary if and only if all R-submodules of a projective R-module are projective.

Proposition 4.1.46. Let R be a commutative ring. Then R is a PID $\Leftrightarrow$ all R-submodules of a free R-module are free.

Proof. ($\Leftarrow$) Let $a \in R\backslash\{0\}$. Then Ra is free, say ra is a basis, for some $r \neq 0$. If $ba = 0$ for some $b \in R$, then $b(ra) = 0$, hence $b = 0$. This shows R is an integral domain. On the other hand, any $x \neq y$ in $R\backslash\{0\}$ cannot be R-linearly independent since $yx + (-x)y = 0$. Hence if I is a nonzero ideal of R, since it's free, it must have a basis consisting of one element of I, and thus I is principal.
($\Rightarrow$) This follows from the fact that a PID is hereditary and Theorem 4.1.45. □

Proposition 4.1.47. A ring R is left hereditary $\Leftrightarrow$ all quotient of injective modules are injective.

direct sum.

Proposition 4.1.48. Let R be a ring and A, B be R-module. Then

$$A \oplus B \text{ is projective/injective/flat} \Leftrightarrow A, B \text{ are projective/injective/flat.}$$

This can be sharpen, for the flatness and projectivity.

Proposition 4.1.49. A direct sum of R-modules is flat/projective over R $\Leftrightarrow$ each direct summand is flat/projective over R.

4.2 Modules over PID

Definition. Let R be a ring and M be a left R-module. M is a **Noetherian module** if it satisfies any of the three equivalent conditions

1. Every submodule is finitely generated.
2. It satisfies the ascending chain condition on submodules.
3. Every nonempty set of submodules has a maximal element.

- A left Noetherian ring R is noetherian as left R-modules.

Example 4.2.1. Albeit $R = F[x_1, x_2, \ldots]$ is a finitely generated R-module, namely, generated by 1, $I = \{f \in R \mid f(0) = 0\}$ is not finitely generated as R-module.

Proposition 4.2.2. Let R be an integral domain and M be a free R-module of rank n. Then any $n+1$ element in M are R-linearly dependent.

Proof. Let $F = \operatorname{Frac} R$ and consider the embedding $M \hookrightarrow F \otimes_R M \cong F^n$. □

Definition. Let R be an integral domain. The **rank** of an R-module is defined to be the maximum number of R-linearly independent elements of M.

Theorem 4.2.3. Let R be a PID and M be an free R-module of rank n. Let $N \leqslant M$ be a submodule. Then

1. N is free of rank $m \leqslant n$.
2. There is an R-basis $y_1, \ldots, y_n$ for M and $a_j \in R\,(j = 1, \ldots, m)$ with $a_1 \mid a_2 \mid \cdots \mid a_m$ such that $a_1 y_1, \ldots, a_m y_m$ is an R-basis for N.

Proof.

1. This follows from Proposition 4.1.46 and 4.2.2.
2. Let $x_1, \ldots, x_n$ be a basis for M and pick $w_1, \ldots, w_k$ to be a generating set of N. Now we write

$$\begin{pmatrix} w_1 \\ \vdots \\ w_k \end{pmatrix} = \underbrace{\begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & & \vdots \\ b_{k1} & \cdots & b_{kn} \end{pmatrix}}_{:=B} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

   for some $B = (b_{ij}) \in M_{k\times n}(R)$.

Claim. We will show there exist $U \in \mathrm{GL}_k(R)$ and $V \in \mathrm{GL}_n(R)$ such that

$$UBV = \left(\begin{array}{ccc|c} a_1 & & & \\ & \ddots & & O \\ & & a_m & \\ \hline & O & & O \end{array}\right)$$

This means

$$U^{-1}\begin{pmatrix} w_1 \\ \vdots \\ w_k \end{pmatrix} = \left(\begin{array}{ccc|c} a_1 & & & \\ & \ddots & & O \\ & & a_m & \\ \hline & O & & O \end{array}\right)\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}, \text{where } \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = V\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

and implies N is a free module with basis $a_1y_1, \ldots, a_my_m$.

We devise an algorithm to construct what we desire. We set some global variables.
Let $m = 0$. For $i = 0, \ldots, \min(k, n) - 1$, let $d_i = 0$. For $i = 0, \ldots, k-1$, let $U_i = I_{k-i}$ and for $i = 0, \ldots, n-1$ let $V_i = I_{n-i}$. Let $k_0 = k$, $n_0 = n$ and for $1 \leqslant i \leqslant \min(k, n)$, let $k_i = n_i = 0$.

Algorithm.

1° Find j such that $b_{1j} \neq 0$. Let S be the matrix corresponding to swapping the 1-st column and the j-th column, and let $V_m = V_mS$, $B = BS$.

2° For $j = 2$ to k_m. Find α, β such that $\alpha b_{11} + \beta b_{j1} = \gcd(b_{11}, b_{j1})$. Put $\gamma = \dfrac{-b_{j1}}{\gcd(b_{11}, b_{j1})}$ and $\delta = \dfrac{b_{11}}{\gcd(b_{11}, b_{j1})}$. Let A be the matrix with

$$A_{11} = \alpha,\ A_{1j} = \beta,\ A_{j1} = \gamma,\ A_{jj} = \delta$$

$A_{ii} = 1$ for $i \neq 1, j$ and $A_{i\ell} = 0$ else. For example, when $j = 2$, we have

$$A = \left(\begin{array}{cc|c} \alpha & \beta & \\ \gamma & \delta & \\ \hline & & I \end{array}\right)$$

Now let $U_m = AU_m$ and $B = AB$. If $B_{i1} = 0$ for each $i = 2, \ldots, k_m$, go to 3°.

3° For $j = 2$ to n_m. Find α, β such that $\alpha b_{11} + \beta b_{1j} = \gcd(b_{11}, b_{1j})$. Put $\gamma = \dfrac{-b_{1j}}{\gcd(b_{11}, b_{1j})}$ and $\delta = \dfrac{b_{11}}{\gcd(b_{11}, b_{1j})}$. Let A be the matrix with

$$A_{11} = \alpha,\ A_{j1} = \beta,\ A_{1j} = \gamma,\ A_{jj} = \delta$$

$A_{ii} = 1$ for $i \neq 1, n$ and $A_{i\ell} = 0$ else. For example, when $j = 2$, we have

$$A = \left(\begin{array}{cc|c} \alpha & \gamma & \\ \beta & \delta & \\ \hline & & I \end{array}\right)$$

Now let $V_m = V_m A$ and $B = BA$. If $B_{1i} = 0$ for each $i = 2, \ldots, n_m$, go to 4°.

4° If $B_{i1} \neq 0$ for some $i = 2, \ldots, k_m$, go to 2°.
If $B_{1i} \neq 0$ for some $i = 2, \ldots, n_m$, go to 3°.

- This terminates at a finite stage since R is Noetherian.

5° For $j = 2, \ldots, k_m$, let $D = \gcd\{b_{j2}, \ldots, d_{jn_m}\}$. If $b_{11} \nmid D$, let S the matrix corresponding to adding the j-th row to the 1-st row. Let $U_m = SU_m$, $B = SB$ and go to 3°.

- This terminates at a finite stage since R is Noetherian.

6° Let $d_m = B_{11}$ and let $B' \in M_{(k_m-1)\times(n_m-1)}$ be the submatrix in

$$B = \left(\begin{array}{c|c} d_m & O \\ \hline O & B' \end{array}\right)$$

If $B' = O$ or $\min\{k_m, n_m\} = 2$, break. Let $k_{m+1} = k_m - 1$, $n_{m+1} = n_M - 1$, $m = m + 1$ and $B = B'$. Go to 1°.

Now, let $U_0 = (I_m \oplus U_m) \cdots (I_0 \oplus U_0)$ and $V_0 = (I_0 \oplus V_0) \cdots (I_m \oplus V_m)$, where I_i is the $i \times i$ identity matrix. Hence, we have obtained that

$$U_0 B V_0 = \left(\begin{array}{ccc|c} d_0 & & & \\ & \ddots & & O \\ & & d_m & \\ \hline & O & & O \end{array}\right)$$

with $d_0 \mid d_1 \mid \cdots \mid d_m$ by 5°.

□

Definition. Let R be a PID and $A \in M_{n\times m}(R)$. A **smith normal form** of A is a diagonal matrix $D \in M_{n\times m}(R)$ of the form

$$\left(\begin{array}{ccc|c} a_1 & & & \\ & \ddots & & O \\ & & a_\ell & \\ \hline & O & & O \end{array}\right)$$

in which $a_1 \mid \cdots \mid a_\ell$ such that $D = UAV$ for some $U \in \mathrm{GL}_n(R)$, $V \in \mathrm{GL}_m(R)$.

- The diagonal element $a_1, \ldots, a_\ell$ are called the **invariant factors** of A.
- Note that ℓ is the rank of the matrix A.

Definition. Let A be a $n \times m$ matrix. For each $i \leqslant \min\{n, m\}$, an $i \times i$ **minor** of A is the determinant of a matrix obtaining by eliminating $n - i$ rows and $m - i$ columns of A.

- For each $i \leqslant \min\{n, m\}$, there are at most $\binom{m}{i}\binom{n}{i}$ $i \times i$ minors of A.

Corollary 4.2.3.1. Let R be a PID, $A \in M_{n\times m}(R)$ and r be the rank of A.

1. A admits a smith normal form, with invariant factors $d_1 \mid \cdots \mid d_r$.
2. For each $i \leqslant r$, let Δ_i be a GCD of all $i \times i$ minors of A. Then $d_1 = \Delta_1$ and $d_i = \Delta_i \Delta_{i-1}^{-1}$ for each $2 \leqslant i \leqslant r$, up to units.
3. The invariant factors of A are unique up to units.

Proof. It remains to show the second assertion. Let $Q \in M_n(R)$. Since the jk-entry of QA is a linear combination of entries of the j-column of A, this indicates that $i \times i$ minors of QA is a linear combination of those of A, and thus the GCD of $i \times i$ minors of A is a divisor of that of QA. Similar for the case AP when $P \in M_m(R)$. Hence, any two similar matrices have the same GCD of $i \times i$ minors. Now the second assertion is crystal clear. □

Theorem 4.2.4. Let R be a PID and M a finitely generated R-module. Then

$$M \cong R^r \oplus R/(a_1) \oplus \cdots \oplus R/(a_m)$$

in which $r \geqslant 0, a_j \in R$ with $a_1 \mid \cdots \mid a_m$.

Proof. Let $M = \sum_{i=1}^{n} Rx_i$ and let F be the free R-module on $\{e_1, \ldots, e_n\}$. Then we have the natural homomorphism

$$\varphi : F \longrightarrow M$$
$$e_i \longmapsto x_i$$

and thus $M \cong F/\ker\varphi$. By Theorem 4.2.3, there's a basis $\{y_1, \ldots, y_n\}$ for F and $a_j \in R$ with $a_1 \mid \cdots \mid a_m$ such that $a_1y_1, \ldots, a_my_m$ is a basis for $\ker\varphi$. Then

$$M \cong \frac{Ry_1 \oplus \cdots \oplus Ry_m \oplus \cdots \oplus Ry_m}{Ra_1y_1 \oplus \cdots \oplus Ra_my_m} \cong R^{n-m} \oplus R/(a_1) \oplus \cdots \oplus R/(a_m)$$

□

Example 4.2.5. Let $G = \mathbb{Z}^3$ and H be the subgroup of G generated by

$$w_1 = (12, 6, -6) \qquad w_2 = (-16, -4, 12) \qquad w_3 = (-24, -6, 18) \qquad w_4 = (4, 4, 6)$$

Let's find the structure of G/H. Put $\{e_1, e_2, e_3\}$ to be the standard basis of G. Then

$$\begin{pmatrix} w_1 \\ w_2 \\ w_3 \\ w_4 \end{pmatrix} = \begin{pmatrix} 12 & 6 & -6 \\ -16 & -4 & 12 \\ -24 & -6 & 18 \\ 4 & 4 & 6 \end{pmatrix} \begin{pmatrix} e_1 \\ e_2 \\ e_3 \end{pmatrix}$$

We apply our algorithm in Theorem 4.2.3 to find the basis for H.

$$\begin{pmatrix} 12 & 6 & -6 \\ -16 & -4 & 12 \\ -24 & -6 & 18 \\ 4 & 4 & 6 \end{pmatrix} \longrightarrow \begin{pmatrix} 4 & 4 & 6 \\ -16 & -4 & 12 \\ -24 & -6 & 18 \\ 12 & 6 & -6 \end{pmatrix} \longrightarrow \begin{pmatrix} 4 & 4 & 6 \\ 0 & 12 & 36 \\ 0 & 18 & 54 \\ 0 & -6 & -24 \end{pmatrix}$$

$$\longrightarrow \begin{pmatrix} 2 & 4 & 0 \\ 36 & 12 & 72 \\ 54 & 18 & 108 \\ -24 & -6 & -48 \end{pmatrix} \longrightarrow \begin{pmatrix} 2 & 0 & 0 \\ 36 & -60 & 72 \\ 54 & -90 & 108 \\ -24 & 42 & -48 \end{pmatrix} \longrightarrow \begin{pmatrix} 2 & 0 & 0 \\ 0 & -60 & 72 \\ 0 & -90 & 108 \\ 0 & 42 & -48 \end{pmatrix}$$

$$\longrightarrow \begin{pmatrix} 2 & 0 & 0 \\ 0 & -60 & 72 \\ 0 & 6 & -12 \\ 0 & 0 & -36 \end{pmatrix} \longrightarrow \begin{pmatrix} 2 & 0 & 0 \\ 0 & 6 & -12 \\ 0 & 0 & -48 \\ 0 & 0 & -36 \end{pmatrix} \longrightarrow \begin{pmatrix} 2 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & -48 \\ 0 & 0 & -36 \end{pmatrix}$$

$$\longrightarrow \begin{pmatrix} 2 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 12 \\ 0 & 0 & 0 \end{pmatrix}$$

Definition. Let the notation be as in Theorem 4.2.4.

1. The number r is called the **(free) rank** of M.
2. $a_1, \ldots, a_m$ are called the **invariant factors** of M.

- $r = \dim_F F \otimes_R M$, where $F = \operatorname{Frac} R$ is the fraction field of R.
- $\operatorname{Tor}(M) = R/(a_1) \oplus \cdots \oplus R/(a_m)$ called the **torsion part** of M.
- $\operatorname{Ann}_R(\operatorname{Tor}(M)) = (a_m) \subseteq R$.

Theorem 4.2.6. Let R be a PID and M a finitely generated R-module. Then

$$M \cong R^r \oplus R/(p_1^{e_1}) \oplus \cdots \oplus R/(p_k^{e_k})$$

for some prime powers $p_j^{e_j}$ (p_j may not be distinct).

Proof. Let $a \in R$ and let $a = up_1^{f_1} \cdots p_n^{f_n}$ be its prime factorization, where u is a unit and $p_1, \ldots, p_n$ are distinct primes. For $i \neq j$, $(p_i^{f_i}) + (p_j^{f_j}) = 1$; thus, by Chinese remainder theorem, we have

$$R/(a) \cong R/(p_1^{f_1}) \times \cdots \times R/(p_n^{f_n})$$

Now the theorem follows from Theorem 4.2.4. □

Definition. Let the notation be as in Theorem 4.2.6.

1. The prime power $p_j^{e_j}$ are called the **elementary divisors** of M.
2. Let
$$M_p := \{m \in M \mid p^k m = 0 \text{ for some } k \in \mathbb{N}\} = \bigoplus_{p_j = p} R/(p_j^{e_j})$$
We call M_p the **p-primary component** of M.

Theorem 4.2.7. Let R be a PID. Any two finitely generated R-modules are isomorphic $\Leftrightarrow$ they have the same rank and the same list of invariant factors / elementary divisors.

Proof. ($\Rightarrow$) Suppose $M_1 \cong M_2$. Note that an isomorphism must send p-primary components to p-primary components. Thus it suffices to show that the ranks are equal and the p-primary components have the same decomposition.

- $M_1/\mathrm{Tor}(M_1) \cong M_2/\mathrm{Tor}(M_2)$, so the ranks are equal.
- Let
$$M_{1p} = R/(p^{e_1}) \oplus \cdots \oplus R/(p^{e_m})$$
$$M_{2p} = R/(p^{f_1}) \oplus \cdots \oplus R/(p^{f_n})$$
be the p-primary component of M_1, M_2, respectively.

  Claim. For each $k \in \mathbb{N}$, $\#\{e_i \mid e_i \geqslant k\} = \#\{f_j \mid f_j \geqslant k\}$. ($\Rightarrow \{e_i\}_{1 \leqslant i \leqslant m} = \{f_i\}_{1 \leqslant i \leqslant n}$ as multisets.)

  Observe that $p^i(R/(p^j)) = \dfrac{(p^i) + (p^j)}{(p^j)} = \begin{cases} 0 & \text{, if } i \geqslant j \\ (p^i)/(p^j) & \text{, if } i \leqslant j \end{cases}$, so

$$\frac{p^{i-1}(R/(p^j))}{p^i(R/(p^j))} = \begin{cases} (p^{i-1})/(p^i) \cong R/(p) & \text{, if } i \leqslant j \\ 0 & \text{, if } i > j \end{cases}$$

  Since $M_{1p} \cong M_{2p}$,
$$\frac{p^{i-1}M_{1p}}{p^i M_{1p}} \cong \frac{p^{i-1}M_{2p}}{p^i M_{2p}}$$
as $R/(p)$-vector spaces, having dimension $\#\{e_k \mid e_k \geqslant i\} = \#\{f_k \mid f_k \geqslant i\}$.

□

4.2.1 Application to vector spaces

Rational canonical forms

In this subsection, unless otherwise stated, by F we always means a (fixed) field and by V we always means a (fixed) finite dimensional F-vector space.

As we've seen in Example 4.1.1.7, via an endomorphism $T \in \mathrm{End}_F(V)$ we may regard V as an $F[x]$-module, denoted as V_T, the action given by $x \cdot v := T(v)$ for each $v \in V$. Since $F[x]$ is a PID, the preceding fundamental theorem is available, i.e,

$$V \cong F[x]^r \oplus \mathrm{Tor}(V) \cong F[x]^r \oplus F[x]/(a_1) \oplus \cdots \oplus F[x]/(a_m)$$

where the $a_i \in F[x]$ are monic and have degree at least 1, such that $a_1(x) \mid \cdots \mid a_m(x)$ over $F[x]$. Since V is finite dimensional as F-vector space, it must be the case that $r = 0$, for $F[x]$ is an infinite dimensional F-vector space. Hence, V turns out to be torsion, i.e,

$$V = \mathrm{Tor}(V) \cong F[x]/(a_1) \oplus \cdots \oplus F[x]/(a_m)$$

Below we let $T \in \mathrm{End}_F(V)$ be a (fixed) endomorphism of V. Recall the **annihilators** of V

$$\mathrm{Ann}(V) := \{f \in F[x] \mid \forall\, v \in V\ [f \cdot v = 0]\}$$

This is an ideal of $F[x]$. Since $F[x]$ is a PID, there's a unique monic polynomial, denoted by $m_T(x)$, generates $\mathrm{Ann}(V)$.

Definition. The unique monic polynomial $m_T(x) \in F[x]$ is called the **minimal polynomial** of T.

A direct consequence of the fundamental theorem is that

Proposition 4.2.8. $m_T(x) = a_m(x)$ is the largest invariant factor of V.

For the completeness, we recall

Definition. $\mathrm{char}_T(x) := \det(xI - T)$ is called the **characteristic polynomial** of T.

Now consider $a(x) = x^k + b_{k-1}x^{k-1} + \cdots + b_1 x + b_0 \in F[x]$ and the F-vector space $F[x]/(a(x))$. Pick $\{1, \overline{x}, \cdots, \overline{x^{k-1}}\}$ as a basis for $F[x]/(a(x))$ over F, then the linear transformation $[v \mapsto x \cdot v]$ has the matrix representation

$$\mathcal{C}_{a(x)} := \begin{pmatrix} 0 & 0 & & 0 & -b_0 \\ 1 & 0 & \cdots & 0 & -b_1 \\ 0 & 1 & & 0 & -b_2 \\ & & \ddots & & \vdots \\ 0 & 0 & & 1 & -b_{k-1} \end{pmatrix} \in M_k(F)$$

This is called the **companion matrix** of $a(x)$.

Definition.

1. $\mathcal{C}_{a_1} \oplus \cdots \oplus \mathcal{C}_{a_m}$ is called the **rational (canonical) form** of T.
2. Let $A \in M_n(F)$. We say A is in **rational (canonical) form** if

$$A = \mathcal{C}_{b_1} \oplus \cdots \oplus \mathcal{C}_{b_k}$$

for some nonconstant monic polynomials $b_1, \ldots, b_k \in F[x]$ such that $b_1 \mid \cdots \mid b_k$ over $F[x]$.

Theorem 4.2.9.

1. There exist a basis for V over F such that T is in rational form.
2. The rational form is unique.

Proof. Let $b_1, \ldots, b_t \in F[x]$ be nonconstant monic with $b_1 \mid \cdots \mid b_t$ over $F[x]$ such that there's an ordered basis β for V such that $[T]_\beta = \mathcal{C}_{b_1} \oplus \cdots \oplus \mathcal{C}_{b_t}$. Let $\beta_i \subseteq \beta$ be the corresponding ordered basis such that $[T|_{D_i}]_{\beta_i} = \mathcal{C}_{b_i}$, where D_i is the T-invariant subspace spanned by β_i. By definition, $\beta = \beta_1 \sqcup \cdots \sqcup \beta_t$, and

$$V = D_1 \oplus \cdots \oplus D_t$$

Let e_i be the first element in β_i. Clearly, D_i is a cyclic $F[x]$-module generated by e_i and has annihilator $(b_i(x))$. This means $D_i \cong F[x]/(b_i(x))$, and thus

$$V \cong F[x]/(b_1(x)) \oplus \cdots \oplus F[x]/(b_t(x))$$

with $b_1 \mid \cdots \mid b_t$. Hence $b_1, \ldots, b_t$ are the invariant factors of V as $F[x]$-modules, and Theorem 4.2.7 then shows $\{b_1, \ldots, b_t\} = \{a_1, \ldots, a_m\}$ as multisets. Therefore, the rational form is unique. □

Theorem 4.2.10. Let $S, T \in \mathrm{End}_F(V)$. TFAE:

1. $S \sim T$, i.e, $S = UTU^{-1}$ for some $U \in \mathrm{Aut}_F(V)$.
2. $V_S \cong V_T$ as $F[x]$-modules.
3. S, T have the same rational form.

Proof.

1. We claim that $U \in \mathrm{Hom}_{F[x]}(V_S, V_T)$. Indeed, $U(x \cdot v) = UT(v) = SU(v) = s \cdot U(v)$ for each $v \in V$. Hence $U : V_S \to V_T$ is an $F[x]$-module isomorphism.

2. The isomorphism guarantees that they have the same invariant factors, so they have the same rational form.

3. Let β, γ be the bases for V over F such that $[S]_\beta$, $[T]_\gamma$ are in rational form. Then

$$[S]_\beta = [\mathrm{id}]_\beta^\gamma [T]_\beta [\mathrm{id}]_\gamma^\beta$$

Let $U : V \to V$ be the linear transformation induced by $[\mathrm{id}]_\beta^\gamma$. Precisely, write $\beta = \{\beta_i\}$, $\gamma = \{\gamma_i\}$ and $v = a_1\gamma_1 + \cdots + a_k\gamma_k$; then

$$U(v) := \begin{pmatrix} \beta_1 & \cdots & \beta_k \end{pmatrix} [\mathrm{id}]_\beta^\gamma \begin{pmatrix} a_1 \\ \cdots \\ a_k \end{pmatrix}$$

Then $U \in \mathrm{Aut}_F(V)$ and $S = UTU^{-1}$.

□

Corollary 4.2.10.1. Let $A, B \in M_n(F)$. Then $A \sim B$ over F if and only if they have the same rational form over F.

Theorem 4.2.11. Let $A, B \in M_n(F)$ and $K \supseteq F$ be a field. Then

$$A \sim B \text{ in } F \Leftrightarrow A \sim B \text{ in } K.$$

Proof. Let M be the rational form of A computed over F. Since M is clearly satisfies the definition the rational form of A computed over K, the uniqueness shows that M is also the rational form of A over K, which implies the invariant factors of A are the same whether it's viewed over F or over K.

$A \sim B$ over K whenever $A \sim B$ over F. Now if $A \sim B$ over K, then they have the same invariant factors over K, thus over F, by the first paragraph. Hence $A \sim B$ over F. □

Corollary 4.2.11.1. Let $A \in M_n(F)$.

1. the minimal polynomial m_A is unchanged when A is viewed over a field extension of F.

2. $\mathrm{char}_A(x)$ equals the product of invariant factors of A.

3. $m_A(x) \mid \mathrm{char}_A(x)$ over $F[x]$.

4. m_A and char_A have the same roots, not counting multiplicities.

Assume that $\dim_F V = n$ and let $e = \{e_1, \ldots, e_n\}$ be an order basis of V over F. Consider the free $F[x]$-module $\bigoplus_{i=1}^{n} F[x]e_i$ on $\{e_1, \ldots, e_n\}$. Then we have the projection

$$\pi : F[x]^n \longrightarrow V$$
$$e_i \longmapsto e_i$$

The relations of e_i in V is that $x \cdot e_i = T(e_i)$, i.e, $(xI - T)e_i = 0$. Hence we have the exact sequence

$$F[x]^n \xrightarrow{xI-T} F[x]^n \xrightarrow{\pi} V \longrightarrow 0$$

We know $\operatorname{coker}(xI - T) = V \cong F[x]/(a_1) \oplus \cdots \oplus F[x]/(a_m)$, so $\ker \pi = F[x]^{n-m} \oplus (a_1) \oplus \cdots \oplus (a_m)$. Let $A = (a_{ij}) = [T]_e$ and put $v_j = (xI - T)e_j = x \cdot e_j - \sum_{i=1}^{n} a_{ij}e_i$. Then $v_1, \ldots, v_n$ generates $\ker(xI - T)$ and

$$\begin{pmatrix} v_1 & v_2 & \cdots & v_n \end{pmatrix} = \begin{pmatrix} e_1 & e_2 & \cdots & e_n \end{pmatrix} \begin{pmatrix} x - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & x - a_{22} & \cdots & -a_{2n} \\ \vdots & & \ddots & \\ -a_{n1} & -a_{n2} & \cdots & x - a_{nn} \end{pmatrix}$$

By Theorem 4.2.3 there are $P, Q \in \mathrm{GL}_n(F[x])$ such that

$$P(xI - T)Q = A = \left(\begin{array}{c|ccc} I & \multicolumn{3}{c}{O} \\ \hline & a_1 & & \\ O & & \ddots & \\ & & & a_m \end{array}\right)$$

Thus

$$\begin{pmatrix} v_1 & v_2 & \cdots & v_n \end{pmatrix} = \begin{pmatrix} e_1 & e_2 & \cdots & e_n \end{pmatrix} P^{-1}AQ^{-1}$$

Let

$$\begin{pmatrix} \xi_1 & \xi_2 & \cdots & \xi_n \end{pmatrix} = \begin{pmatrix} e_1 & e_2 & \cdots & e_n \end{pmatrix} P^{-1}$$

Now identifying e_i with $\pi(e_i) \in V$ gives $\xi_1 = \cdots = \xi_{n-m} = 0$. Put $f_j := \xi_{n-m+j}$ for $j = 1, \ldots, m$. From the matrix A we see

$$V \cong F[x]f_1 \oplus F[x]f_2 \oplus \cdots \oplus F[x]f_m$$

as $F[x]$-modules, with $F[x]f_i \cong F[x]/(a_i)$. Now put $\beta_i = \{f_i, Tf_i, T^2f_i, \ldots, T^{\deg a_i - 1}f_i\}$. Then $\beta := \beta_1 \sqcup \cdots \sqcup \beta_m$ is the desired basis for V over F such that

$$[T]_\beta = \begin{pmatrix} \mathcal{C}_{a_1} & & & \\ & \mathcal{C}_{a_2} & & \\ & & \ddots & \\ & & & \mathcal{C}_{a_m} \end{pmatrix}$$

Jordan canonical forms

Let the notation be as in the previous subsection. Assume that invariant factors $a_1, \ldots, a_m$ split completely in F, i.e, F contains all eigenvalues of T. Then each elementary divisor has the form $(x-\lambda)^k$. By Theorem 4.2.6, V is a direct sum of finitely many cyclic $F[x]$-modules of the form $F[x]/(x-\lambda)^k$, where $\lambda \in F$ is an eigenvalue of T.

Consider the elements $(\overline{x}-\lambda)^{k-1}, \ldots, \overline{x}-\lambda, 1$ in the quotient $F[x]/(x-\lambda)^k$; this is an F-basis for $F[x]/(x-\lambda)^k$. With respect to this basis, the linear transformation $[x \mapsto x \cdot v]$ has the matrix representation

$$\begin{pmatrix} \lambda & 1 & & & \\ & \lambda & \ddots & & \\ & & \ddots & 1 & \\ & & & \lambda & 1 \\ & & & & \lambda \end{pmatrix} \in M_k(F)$$

Such matrix is called a **Jordan block** corresponding to λ.

Definition.

1. A matrix is in **Jordan (canonical) form** if it's a block diagonal matrix with Jordan blocks along its diagonal.
2. A **Jordan (canonical) form** of the linear transformation T is a matrix representation of T that is in Jordan form.

- "The" Jordan form is unique up to permutation of the blocks along its diagonal by Theorem 4.2.7.

Theorem 4.2.12.

1. There's an F-basis for V such that T is in Jordan form.
2. The Jordan form of T is unique up to a permutation of the Jordan blocks along its diagonal.

Corollary 4.2.12.1. Let $A \in M_n(F)$ and F contain all eigenvalues of A. Then A is similar to a matrix J in Jordan form, i.e, $J = P^{-1}AP$ for some $P \in \mathrm{GL}_n(F)$.

Corollary 4.2.12.2. Let $A \in M_n(F)$ and F contain all eigenvalues of A.

1. A is similar to a diagonal matrix D, then D is its Jordan form.
2. Two diagonal matrices are similar if and only if their diagonal entries are the same up to a permutation.

3. A is diagonalizable if and only if its minimal polynomial m_A is separable over F.

We now convert a rational form to a Jordan form. For each invariant factor $a(x)$ of V_T, write $a(x) = (x-\lambda_1)^{\alpha_1} \cdots (x-\lambda_s)^{\alpha_s}$. By Chinese Remainder theorem, we have an isomorphism

$$F[x]/(a(x)) \longrightarrow F[x]/(x-\lambda_1)^{\alpha_1} \oplus \cdots \oplus F[x]/(x-\lambda_s)^{\alpha_s}$$

$$f \longmapsto (\, f \mod (x-\lambda_k)^{\alpha_k})_k$$

Let f be the $F[x]$-generator of the cyclic module $F[x]/(a(x))$. Then the elements

$$\frac{a(x)}{(x-\lambda_1)^{\alpha_1}} f,\ \frac{a(x)}{(x-\lambda_2)^{\alpha_2}} f,\ \ldots,\ \frac{a(x)}{(x-\lambda_s)^{\alpha_s}} f$$

are $F[x]$-generators of cyclic modules $F[x]/(x-\lambda_1)^{\alpha_1}$, $F[x]/(x-\lambda_2)^{\alpha_2}$, $\ldots$, $F[x]/(x-\lambda_s)^{\alpha_s}$, respectively. Put $g_i = \dfrac{a(x)}{(x-\lambda_j)^{\alpha_j}} f$. Then

$$(T-\lambda_j I)^{\alpha_j - 1} g_j,\ \ldots,\ (T-\lambda_j I) g_j,\ g_j$$

form an F-basis for $F[x]/(x-\lambda_j)^{\alpha_j}$, so that the restriction of T is in Jordan form with this basis.

4.3 Linear representations of finite groups

Definition. Let G be a group, F a field and V an F-vector space. A **(linear) representation** (ρ, V) **of** G **on** V is a group homomorphism $\rho : G \to \mathrm{GL}(V)$.

- $\dim_F V$ is called the **degree** of ρ.
- ρ is **faithful** if ρ is injective.
- If $W \subseteq V$ is an F-subspace such that for all $g \in W$ we have $\rho(g)W \subseteq W$, then we say W is a G**-invariant/stable subspace** of V, and $(\rho|_W, W)$ is a **subrepresentation** of (ρ, V).
- If an F-basis for V is chosen, we may realize ρ as a group homomorphism $\rho : G \to \mathrm{GL}_n(F)$.

Example 4.3.1.

1. If $V = F$ and $\rho(g) := \mathrm{id}_V$ for all $g \in G$, we say ρ is the **trivial representation**.
2. Define $\rho(h) : FG \to FG$ by $\rho(h)(\sum_{g\in G} c_g g) := \sum_{g\in G} c_g(hg)$ for all $h \in G$. Then $\rho : G \to \mathrm{GL}(FG)$ is a representation of G, called the **left regular representation**. Here FG is an F-algebra, called a **group algebra**.
3. Let $V := \bigoplus_{i=1}^{n} Fv_i$ and $G \leqslant S_n$. Define $\rho(\sigma)(v_i) := v_{\sigma(i)}$. Then $\rho : G \to \mathrm{GL}(V)$ is called a **permutation representation** of G
4. $G = D_8 = \langle \sigma, \tau \mid \sigma^4 = \tau^2 = 1,\ \tau\sigma\tau^{-1} = \sigma^{-1}\rangle$. Define
$$\rho : \sigma^i\tau^j \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^i \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}^j$$
One can check ρ is an representation of G. In general, for $G = D_{2n}$, the group homomorphism
$$\rho : \sigma^i\tau^j \mapsto \begin{pmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{pmatrix}^i \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}^j$$
is a faithful representation of D_{2n}.
5. For $G = Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, the map
$$\rho : i \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},\ j \mapsto \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}$$
is a representation of Q_8.

If $\rho : G \to \mathrm{GL}(V)$ is a representation of G, then V becomes an FG-module, on which FG acts by $(\sum_{g\in G} c_g g)v := \sum_{g\in G} c_g \rho(g)v \in V$. Conversely, if V is an FG-module, then we may define $\rho : G \to \mathrm{GL}(V)$ by $\rho(g)v := gv$. Thus, we obtain a bijection

$$\{\text{representations of } G \text{ over } F\} \longleftrightarrow \{FG\text{-modules}\}$$

Moreover, subrepresentations of a given representation correspond to FG-submodules of its corresponding FG-module. Via this connection, we say an FG-module is a **trivial/regular/permutation** FG-module if the corresponding representation is.

Example 4.3.2.

1. If $\#G < \infty$, $\{c \sum_{g\in G} g \mid c \in F\}$ is an FG-submodule of FG. In fact, this is a trivial FG-module.
2. The augmentation ideal $\{\sum_{g\in G} c_g g \mid \sum_{g\in G} c_g = 0 \in F\}$ is an FG-submodule of FG.
3. The group algebra FG, as FG-modules, corresponds to the left regular representation of G.

Definition. Let (ρ, V), (φ, W) be two representations of G. We say ρ and φ are **isomorphic/similar/equivalent** if there exists an F-vector space isomorphism $T : V \to W$ such that $\varphi(g)(Tv) = T(\rho(g)v)$ for all $g \in G$, $v \in V$, i.e, the diagram commutes for all $g \in G$:

$$\begin{array}{ccc} V & \xrightarrow{T} & W \\ {\scriptstyle \rho(g)}\downarrow & & \downarrow{\scriptstyle \varphi(g)} \\ V & \xrightarrow[T]{} & W \end{array}$$

Equivalently, ρ, φ are isomorphic if $V \cong W$ as FG-modules, i.e, there exists an FG-module isomorphism $T : V \to W$.

- A homomorphism $S : V \to W$ is said to **intertwine** ρ, φ if $\varphi(g)(Tv) = T(\rho(g)v)$ for all $g \in G$, $v \in V$, or equivalently, if it's also an FG-module homomorphism.

Definition. Let R be a ring and M a nonzero R-module.

1. M is **simple/irreducible** if M has no proper nontrivial submodule.
2. M is **indecomposible** if M cannot be written as a direct sum of some proper nontrivial submodule of M. Otherwise, it's **decomposible**.
3. M is **semisimple/completely reducible** if it's a direct sum of irreducible submodules of M.

- We usually use the term "irreducible" when discussing FG-modules. In general, people tend to use "simple".
- An irreducible module is indecomposible and completely reducible.
- We say a representation is **irreducible/indecomposible/decomposible/completely reducible** if the corresponding FG-module is.

Example 4.3.3. $G = \mathbb{Z}/p\mathbb{Z}$, $F = \mathbb{F}_p$. Let $\rho : G \to \mathrm{GL}_2(F)$ defined by $\rho(k) = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$. Then ρ is reducible but indecomposible, and not completely reducible.

Theorem 4.3.4 (Maschke's)**.** Let $\#G < \infty$, $\mathrm{Char}\, F \nmid \#G$ and V be an FG-module. If U is an FG-module, then U is a direct summand of V.

Proof. We construct a $\pi \in \mathrm{Hom}_{FG}(V, V)$ such that $\mathrm{Im}\,\pi = U$ and $\pi^2 = \pi$. Then by Lemma 4.1.28, $V = U \oplus \ker \pi$ as FG-modules.

Let $\pi_0 \in \mathrm{Hom}_F(V, U)$ be the projection. Define $\pi : V \to U$ by

$$\pi(v) := \frac{1}{\#G} \sum_{g \in G} g^{-1} \pi_0(gv)$$

Then

- For $v \in V$, $\pi(v) \in U$ since $\mathrm{Im}\,\pi_0 = U$ and U is an FG-submodule.
- For $g' \in G$,
$$\pi(g'v) = \frac{1}{\#G} \sum_{g \in G} g^{-1} \pi_0(g'gv) = \frac{1}{\#G} \sum_{h \in G} g' h^{-1} \pi_0(hv) = g'\pi(v)$$
That is, $\pi \in \mathrm{Hom}_{FG}(V, V)$
- For $u \in U$,
$$\pi(u) = \frac{1}{\#G} \sum_{g \in G} g^{-1} \pi_0(gu) = \frac{1}{\#G} \sum_{g \in G} g^{-1} \cdot gu = u$$
This shows $\pi|_U = \mathrm{id}_U$, and thus $\pi^2 = \pi$.

□

Corollary 4.3.4.1. If $\#G < \infty$ and $\mathrm{Char}\, F \nmid \#G$, then any finite dimensional FG-module/representation is semisimple.

Below we assume all groups are finite and all FG-modules are finite dimensional.

Theorem 4.3.5 (Schur's lemma)**.** Let V, W be irreducible FG-modules.

1. If $\phi \in \mathrm{Hom}_{FG}(V, W)$, then either $\phi = 0$ or ϕ is an isomorphism.
2. If F is algebraically closed and $\phi \in \mathrm{End}_{FG}(V, V)$, then there exists $a \in F$ such that $\phi = a \cdot \mathrm{id}_V$.

Corollary 4.3.5.1. Let V, W be two non-isomorphic irreducible FG-submodules of FG. Then $vw = 0$ for all $v \in V$, $w \in W$.

Proof. For $w \in W$, the map $[v \mapsto vw]$ is an FG-modules homomorphism from V to W. By Schur's lemma, it's a zero map, since V, W are non-isomorphic by assumption. □

Theorem 4.3.6. Assume $\mathrm{Char}\, F \nmid \#G$. Then any irreducible FG-module is isomorphic to some irreducible submodule of FG.

Proof. Let V be an irreducible FG-module and let $v \neq 0$ in V. Define $\phi : FG \to V$ by $\phi(x) = xv$. Clearly, $\mathrm{Im}\, \phi \neq 0$, and by irreducibility it forces $\mathrm{Im}\, \phi = V$. Hence $V \cong FG/\ker \phi$. Since $FG = \ker \phi \oplus U$ for some $U \subseteq FG$, we conclude $U \cong V$. □

Proposition 4.3.7. Assume F is algebraically closed. Given two irreducible FG-modules V, W, we have

$$\dim_F \mathrm{Hom}_{FG}(V, W) = \begin{cases} 1 & \text{, if } V \cong W \\ 0 & \text{, if } V \ncong W \end{cases}$$

Proof. By Schur's lemma, $\dim_F \mathrm{Hom}_{FG}(V, W) = 0$ when $V \ncong W$. If $\phi : V \to W$ is an isomorphism and $\psi : V \to W$ is another, then $\psi^{-1} \circ \phi \in \mathrm{Aut}_{FG}(V)$, and by Schur's lemma again, $\psi^{-1} \circ \phi = a \cdot \mathrm{id}_V$, i.e, $\phi = a\psi$ for some $a \in F$. Hence $\dim_F \mathrm{Hom}_{FG}(V, W) = 1$ when $V \cong W$. □

Proposition 4.3.8. Assume $V = U_1 \oplus \cdots \oplus U_n$ is a decomposition of V into a direct sum of irreducible FG-modules. If U is an irreducible FG-submodules of V, then $U \cong U_i$ for some i.

Proof. The composition $U \hookrightarrow V \twoheadrightarrow U_i$ is nonzero for some i, and the irreducibility shows it's an isomorphism. □

Corollary 4.3.8.1. Assume F is algebraically closed and suppose $V = U_1 \oplus \cdots \oplus U_n$ is a decomposition of V into a direct sum of irreducible FG-modules. Let U be an irreducible FG-module. Then

$$\#\{U_i \mid U_i \cong U\} = \dim_F \mathrm{Hom}_{FG}(V, U) = \dim_F \mathrm{Hom}_{FG}(U, V)$$

Proof. This follows from Proposition 4.3.7, 4.3.8 and the universal property of finite direct sum of modules. □

Corollary 4.3.8.2. If $\operatorname{Char} F \nmid \#G$ and F is algebraically closed, then the number of irreducible FG-modules, up to isomorphisms, is finite.

Proof. This follows from Proposition 4.3.6, 4.3.8 and 4.3.7. □

Corollary 4.3.8.3. Assume $\operatorname{Char} F \nmid \#G$ and F is algebraically closed. Let $FG = U_1 \oplus \cdots \oplus U_n$ be a decomposition of V into a direct sum of irreducible FG-modules, and $\{V_1, \ldots, V_k\}$ is a complete set of irreducible FG-modules. Then

$$\#\{U_i \mid U_i \cong V_j\} = \dim_F V_j$$

In particular, $\#G = \sum_{j=1}^{k} (\dim_F V_j)^2$.

Proof. By Corollary above, $\#\{U_i \mid U_i \cong V_j\} = \dim_F \operatorname{Hom}_{FG}(FG, V_j) = \dim_F V_j$. The second assertion follows by observing $\#G = \dim_F FG = \sum_{i=1}^{n} \dim_F U_i$. □

4.3.1 Characters

Definition. Let $\rho : G \to \mathrm{GL}(V)$ be a representation. The **character** $\chi : G \to F$ is defined by $\chi(g) := \operatorname{tr}(\rho(g))$.

- We call χ is **trivial/regular/irreducible** if its representation is.
- We say χ is **linear** if its representation is one dimensional.
- The character χ of an FG-module V is defined by

$$\chi(\sum_{g \in G} c_g g) := \sum_{g \in G} c_g \operatorname{tr}(\rho(g))$$

  where ρ is the associated representation on V.

Example 4.3.9.

1. For the trivial character χ, we have $\chi(g) = 1$ for all $g \in G$.
2. For the regular character χ_{reg}, we have $\chi_{reg}(g) = \begin{cases} \#G & \text{, if } g = 1 \\ 0 & \text{, if } g \neq 1 \end{cases}$
3. Let $G \leqslant S_n$ and $\rho : G \to \mathrm{GL}(V)$ be the permutation representation. Then its character χ satisfies $\chi(\sigma) = \operatorname{fix}(\sigma) := \#\{i \in \{1, \ldots, n\} \mid \sigma(i) = i\}$.

4. Let G, V be as above. Say $V = \bigoplus_{i=1}^{n} Fv_i$. V has a submodule $U = FG(v_1 + \cdots + v_n)$, which is the trivial FG-module. By Maschke's theorem, $V = W \oplus U$ for some submodule W. Then the character of W is $[\sigma \mapsto \mathrm{fix}(\sigma) - 1]$.

5. Let $G = D_8 = \langle \sigma, \tau \mid \sigma^4 = \tau^2 = 1,\ \tau\sigma\tau^{-1} = \sigma^{-1} \rangle$ and

$$\rho : \sigma^i \tau^j \mapsto \begin{pmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{pmatrix}^i \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}^j$$

   Then its character χ satisfies $\chi(g) = \begin{cases} 2 & , \text{if } g = 1 \\ -2 & , \text{if } g = \sigma^2 \\ 0 & , \text{else} \end{cases}$

6. Let $G \leqslant S_n$. Then $\chi : \sigma \mapsto \begin{cases} 1 & , \text{if } \sigma \in A_n \\ -1 & , \text{if } \sigma \notin A_n \end{cases}$ is a character.

Proposition 4.3.10. Let V, V_1, V_2 be FG-modules and χ, χ_1, χ_2 be their characters.

1. $V_1 \cong V_2 \Rightarrow \chi_1 = \chi_2$.
2. $g_1, g_2 \in G$ are conjugates $\Rightarrow \chi(g_1) = \chi(g_2)$.
3. $V = V_1 \oplus V_2 \Rightarrow \chi = \chi_1 + \chi_2$

Proof. For $1, 2$, one note that $\mathrm{tr}(AB) = \mathrm{tr}(BA)$ for $A, B \in M_n(F)$. □

Definition. We say $f : G \to F$ is a **class function** if $f(g) = f(hgh^{-1})$ for each $g, h \in G$.

- For $g \in G$, we denote by g^G the conjugacy class of g in G.

Below we assume $F = \mathbb{C}$, for the sake of algebraically closedness, characteristic 0 and the existence of inner product.

Proposition 4.3.11. Let $\rho : G \to \mathrm{GL}(V)$ be a representation and χ its character.

1. $\chi(1) = \dim_{\mathbb{C}} V$
2. $\mathrm{ord}\, g = m \in \mathbb{N} \Rightarrow \chi(g)$ is a sum of some m-th roots of unity.
3. $\chi(g^{-1}) = \overline{\chi(g)}$.
4. $g^{-1} \in g^G \Rightarrow \chi(g) \in \mathbb{R}$.

Proof.

2. Note that $\rho(g)^m = I$ implies the minimal polynomial of $\rho(g)$ divides $x^m - 1$, which is separable. This means $\rho(g)$ is diagonalizable, and all eigenvalues are distinct m-th roots of unity.

3. Let β be a basis for V such that

$$[\rho(g)]_\beta = \begin{pmatrix} \omega^{k_1} & & \\ & \ddots & \\ & & \omega^{k_n} \end{pmatrix}$$

where $\omega = e^{2\pi i/m}$ and $k_i \in \mathbb{Z}$. Then

$$[\rho(g^{-1})]_\beta = \begin{pmatrix} \omega^{-k_1} & & \\ & \ddots & \\ & & \omega^{-k_n} \end{pmatrix} = \overline{[\rho(g)]_\beta}$$

so that $\chi(g^{-1}) = \overline{\chi(g)}$.

□

Corollary 4.3.11.1. Let G be a finite group. Then there are finitely many irreducible characters of G over $\mathbb{C}$, and they satisfy $\sum_{\chi:\text{ irr.}} \chi(1)^2 = \#G$.

Proof. This is a reformulation of Corollary 4.3.8.3. □

Proposition 4.3.12. Let $\rho : G \to \mathrm{GL}(V)$ be a representation of G and χ its character.

1. $|\chi(g)| \leqslant \chi(1)$, and the equality holds $\Leftrightarrow \rho(g) = a \cdot \mathrm{id}_V$ for some $a \in \mathbb{C}$.

2. $\ker \rho = \{g \in G \mid \chi(g) = \chi(1)\}$.

Proof.

1. Assume $g \in G$ has order m and put $\omega = e^{2\pi i/m}$. Then $\rho(g)$ has eigenvalue $\omega^{a_1}, \ldots, \omega^{a_n}$ for some $0 \leqslant a_1 \leqslant m-1$, so

$$|\chi(g)| = |\omega^{a_1} + \cdots + \omega^{a_n}| \leqslant |\omega^{a_1}| + \cdots + |\omega^{a_n}| = n = \chi(1)$$

The equality holds iff $\omega^{a_1} = \lambda_i \omega^{a_i}$ for some $\lambda_i > 0$. Since each of them has norm 1, $\lambda_i = 1$ for each i, and thus $\rho(g) = \omega^{a_1} \cdot \mathrm{id}_V$.

2. If $\chi(g) = \chi(1)$, by 1 we obtain $\rho(g) = \mathrm{id}_V$, and thus $g \in \ker \rho$.

□

Definition. We define the **kernel of a character** to be the kernel of its representation.

4.3.2 Orthogonality relations

Definition. Let $\theta, \varphi : G \to \mathbb{C}$ be two functions. Define their **inner product** to be

$$\langle \theta, \varphi \rangle = \frac{1}{\#G} \sum_{g \in G} \theta(g)\overline{\varphi(g)}$$

- If χ_1, χ_2 are characters of G, then

$$\langle \chi_1, \chi_2 \rangle = \frac{1}{\#G} \sum_{g \in G} \chi_1(g)\chi_2(g^{-1}) = \frac{1}{\#G} \sum_{g \in G} \chi_1(g^{-1})\chi_2(g) = \langle \chi_2, \chi_1 \rangle$$

  so $\langle \chi_1, \chi_2 \rangle \in \mathbb{R}$.

Definition. Let V be an FG-module. The **composition factor** of U is an irreducible FG-module V that is isomorphic to some submodule of V.

Proposition 4.3.13. Let $\mathbb{C}G = V_1 \oplus V_2$ and V_1, V_2 have no common composition factor. Write $1_G = e_1 + e_2$ with $e_i \in V_i$, $i = 1, 2$. Then

1. $e_i v_j = \delta_{ij} v_j$, $i, j = 1, 2$. In particular, $e_i^2 = e_i$, i.e, e_i is idempotent.
2. Let χ_1 be the character of V_1. We have

$$e_1 = \frac{1}{\#G} \sum_{g \in G} \chi_1(g^{-1})g$$

Proof.

1. This follows from Corollary 4.3.5.1.
2. Put $e_1 = \sum_{g \in G} c_g g$ and let χ_{reg} be the regular character of G. For $h \in G$, consider the left translation $\phi_h : x \mapsto h^{-1}e_1 x$ on $\mathbb{C}G$. Then

$$\mathrm{tr}(\phi_h) = \chi_{reg}(\sum_{g \in G} c_g h^{-1} g) = c_h \cdot \#G$$

   Here recall the corresponding representation of $\mathbb{C}G$ is the regular representation.

   On the other hand, $\mathrm{tr}(\phi_h) = \mathrm{tr}(\phi_h|_{V_1}) + \mathrm{tr}(\phi_h|_{V_2})$.

   - For all $v_1 \in V_1$, $h^{-1}e_1 v_1 = h^{-1}v_1$, so $\mathrm{tr}(\phi_h|_{V_1}) = \chi_1(h^{-1})$.
   - For all $v_2 \in V_2$, $h^{-1}e_1 v_2 = 0$, so $\mathrm{tr}(\phi_h|_{V_2}) = 0$.

Thus $c_h \cdot \#G = \chi_1(h^{-1})$, i.e, $c_h = \dfrac{1}{\#G}\chi_1(h^{-1})$ for each $h \in G$.

□

Theorem 4.3.14 (Orthogonality relations)**.** Let V_1 and V_2 be two irreducible $\mathbb{C}G$-modules and χ_1, χ_2 be their characters, respectively. Then $\langle \chi_1, \chi_2 \rangle = \begin{cases} 1 & \text{, if } V_1 \cong V_2 \\ 0 & \text{, if } V_1 \ncong V_2 \end{cases}$

Proof. WLOG, we assume $V_1, V_2 \subseteq \mathbb{C}G$. (Theorem 4.3.6.) Let $\mathbb{C}G = U_1 \oplus \cdots \oplus U_k$ be a decomposition of $\mathbb{C}G$ into a direct sum of irreducible submodules. Let

$$W_1 = \bigoplus_{j:\, U_j \cong V_1} U_j, \qquad W_2 = \bigoplus_{j:\, U_j \cong V_2} U_j$$

and let ϕ_1, ϕ_2 be the characters of V_1, V_2, respectively; note that $\phi_i = (\dim V_i)\chi_i$, $i = 1, 2$.

Write $1_G = e_1 + e_2$ with $e_i \in W_i$, $i = 1, 2$. By Proposition 4.3.13, $e_1 = \dfrac{1}{\#G} \sum\limits_{g \in G} \phi_1(g^{-1})g$. Then

$$(\dim V_1)^2 \langle \chi_1, \chi_1 \rangle = \langle \phi_1, \phi_1 \rangle = \frac{1}{\#G} \sum_{g \in G} \phi_1(g^{-1})\phi_1(g) = \phi_1(e_1)$$

On the other hand, $e_1 w_1 = w_1$ for all $w_1 \in W_1$. Thus

$$\phi_1(e_1) = \operatorname{tr}(W_1 \ni w_1 \mapsto e_1 w_1) = \dim W_1 = (\dim V_1)^2$$

Hence $\langle \chi_1, \chi_1 \rangle = 1$. Similarly,

$$0 = \operatorname{tr}(W_2 \ni w_2 \mapsto e_1 w_2) = \phi_2(e_1) = \dim V_1 \dim V_2 \langle \chi_1, \chi_2 \rangle$$

and thus $\langle \chi_1, \chi_2 \rangle = 0$. □

Example 4.3.15. $G = S_3$. Let χ_1 be the trivial character, $\chi_2 : \sigma \mapsto \begin{cases} 1 & \text{, if } \sigma \text{ is even} \\ -1 & \text{, if } \sigma \text{ is odd} \end{cases}$. Since S_3 has three conjugacy classes and $6 = 1^2 + 1^2 + 2^2$, there is a 2-dimensional irreducible character, denoted by χ_3. By orthogonality relations, we may complete the following table

	e	$(1\,2)$	$(1\,2\,3)$
$\lvert g^{S_n} \rvert$	1	3	2
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

- $\chi_3(e) = 2$ since χ_3 has dimension 2.
- $\chi_1(e)\overline{\chi_1((1\,2))} + \chi_2(e)\overline{\chi_2((1\,2))} + \chi_3(e)\overline{\chi_3((1\,2))} = 0$, so $\chi_3((1\,2)) = 0$.
- $\chi_1(e)\overline{\chi_1((1\,2\,3))} + \chi_2(e)\overline{\chi_2((1\,2\,3)))} + \chi_3(e)\overline{\chi_3((1\,2\,3)))} = 0$, so $\chi_3((1\,2\,3))) = -1$.
- $\langle \chi_3, \chi_3 \rangle = \frac{1}{6}[1 \times 2^2 + 3 \times 0^2 + 2 \times (-1)^2] = 1$, which demonstrates the irreducibility of χ_3.

Corollary 4.3.14.1. Let $\{V_1, \ldots, V_n\}$ be a complete set of irreducible $\mathbb{C}G$-modules up to isomorphisms and $\chi_1, \ldots, \chi_n$ be their characters, respectively.

1. Let V be a $\mathbb{C}G$-module and $V = \bigoplus_{i=1}^{n} V_i^{d_i}$ be its decomposition into irreducible $\mathbb{C}G$-modules. Let θ be its characters. Then $\theta = \sum_{i=1}^{n} \langle \chi_i, \theta \rangle \chi_i$, i.e, $d_i = \langle \chi_i, \theta \rangle$ for each i, and $\langle \theta, \theta \rangle = \sum_{i=1}^{n} d_i^2$. If $\theta' = e_1\chi_1 + \cdots + e_n\chi_n$, then $\langle \theta, \theta' \rangle = \sum_{i=1}^{n} d_i e_i$.
2. A character χ is irreducible if and only if $\langle \chi, \chi \rangle = 1$.
3. $\chi_1, \ldots, \chi_n$ are $\mathbb{C}$-linearly independent.

Corollary 4.3.14.2. Let V_1 and V_2 be two $\mathbb{C}G$-modules and χ_1, χ_2 be their characters, respectively.

1. $\dim_{\mathbb{C}} \mathrm{Hom}_{\mathbb{C}G}(V_1, V_2) = \langle \chi_1, \chi_2 \rangle$.
2. $V_1 \cong V_2 \Leftrightarrow \chi_1 = \chi_2$.

Proposition 4.3.16. For each conjugacy class C of G, define $e_C = \sum_{g \in C} g$. Then $\{e_C\}_C$ form $\mathbb{C}$-basis of $Z(\mathbb{C}G)$, the center of $\mathbb{C}G$.

Proof.

$$\begin{aligned} x = \sum c_g g \in Z(\mathbb{C}G) &\Leftrightarrow \forall\, h \in G\, [] h(\sum c_g g)h^{-1} = \sum c_g g] \\ &\Leftrightarrow \forall\, h, g, g' \in G\, [g' = hgh^{-1} \Rightarrow c_g = c'_g] \\ &\Leftrightarrow c_g = c'_g \text{ if } g, g' \text{ are conjugates.} \\ &\Leftrightarrow x \in \mathrm{span}\{e_C\} \end{aligned}$$

□

Theorem 4.3.17. #{irreducible characters of $\mathbb{C}G$} = #{conjugacy classes of G}.

Proof. Let $\chi_1, \ldots, \chi_n$ be distinct irreducible characters of G and $C_1, \ldots, C_m$ be distinct conjugacy classes of G. We must show $m = n$.

1° Since the χ_j are linearly independent class functions, they are linearly independent elements in $\mathrm{Hom}_{\mathbb{C}}(Z(\mathbb{C}G), \mathbb{C})$, and hence $n \leqslant m$.

2° Let $V_1, \ldots, V_n$ be $\mathbb{C}G$-modules corresponding to $\chi_1, \ldots, \chi_n$, respectively. Write $\mathbb{C}G = U_1 \oplus \cdots \oplus U_k$ be a decomposition of $\mathbb{C}G$ into a direct sum of irreducible submodules and put $W_i = \bigoplus_{j:\, U_j \cong V_i} U_j$ for each i. Write $e = e_1 + \cdots + e_n$ with $e_i \in W_i$ for each i.

Claim. $Z(\mathbb{C}G) \subseteq \mathrm{span}\{e_1, \ldots, e_n\}$ $(\Rightarrow m \leqslant n)$

Since the V_i are irreducible, for all $x \in Z(\mathbb{C}G)$, there exists $a_i \in \mathbb{C}$ such that for all $v_i \in V_i$, we have $xv_i = a_i v_i$. In fact, for all $w_i \in W_i$, we have $xw_i = a_i w_i$ (explicitly, $a_i = \chi_i(x)/\chi_i(e)$). Consequently

$$x = xe = x(e_1 + \cdots + e_n) = a_1 e_1 + \cdots + a_n e_n$$

□

Corollary 4.3.17.1. Let G be a finite group. Then G is abelian if and only if every complex irreducible character of G is linear.

Character tables

Definition. Let $\chi_1, \ldots, \chi_n$ be the irreducible characters of G and $g_1, \ldots, g_n$ be the representatives of conjugacy classes of G. The $n \times n$ matrix $(\chi_i(g_j))_{ij}$ is called a **character table** of G.

- Non-isomorphic groups may have the same character table, as shown in the following example.

Example 4.3.18.

(i) $D_8 = \langle \sigma, \tau \mid \sigma^4 = \tau^2 = 1, \tau\sigma\tau^{-1} = \sigma^{-1} \rangle$: Let χ_1 be the trivial character. Let

$$H_1 = \langle \sigma \rangle, \qquad H_2 = \langle \sigma^2, \tau \rangle, \qquad H_3 = \langle \sigma^2, \sigma\tau \rangle$$

these are the subgroups of index 2. For $i = 1, 2, 3$, define $\chi_{i+1} : g \mapsto \begin{cases} 1 & , \text{if } g \in H_i \\ -1 & , \text{else} \end{cases}$. Also, define

$$\rho_5 : \sigma \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \tau \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

and let χ_5 be its character.

	e	$\{\sigma^2\}$	$\{\sigma, \sigma^2\}$	$\{\tau, \sigma^2\tau\}$	$\{\sigma\tau, \sigma^3\tau\}$
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	1	1	-1	1	-1
χ_4	1	1	-1	-1	1
χ_5	2	-2	0	0	0

Since $\langle \chi_5, \chi_5 \rangle = \dfrac{1 \times 2^2 + 1 \times 2^2}{8} = 1$, χ_5 is irreducible.

(ii) $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$: define $\chi_1, \ldots \chi_4$ in a similar way as above and define

$$\rho_5 : i \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \; j \mapsto \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}$$

and χ_5 be its character; it's irreducible by a direct computation of its inner product. Then

	$\{1\}$	$\{-1\}$	$\{\pm i\}$	$\{\pm j\}$	$\{\pm k\}$
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	1	1	-1	1	-1
χ_4	1	1	-1	-1	1
χ_5	2	-2	0	0	0

Theorem 4.3.19 (Orthogonality relations)**.** Let $\chi_1, \ldots, \chi_n$ and $g_1, \ldots, g_n$ be as usual. Then

1. $\displaystyle\sum_{k=1}^{n} \frac{\chi(g_k)\overline{\chi_j(g_k)}}{\#C_G(g_k)} = \begin{cases} 1 & \text{, if } i = j \\ 0 & \text{, else} \end{cases}$

2. $\displaystyle\sum_{k=1}^{n} \chi_k(g)\overline{\chi_k(h)} = \begin{cases} \#C_G(g) & \text{, if } h \in g^G \\ 0 & \text{, else} \end{cases}$

Sometimes 1. is referred to as the **row orthogonality relations** and 2. is referred to as the **column orthogonality relations** for the irreducible characters.

Proof. This is a reformulation of Theorem 4.3.14. □

Example 4.3.20. $G = S_4$.

	1	2	3	22	4
$\#g^G$	1	6	8	3	6
$\#C_G(g)$	24	4	3	8	4
χ_1	1	1	1	1	1
χ_2	1	-1	1	1	-1
χ_3	3	1	0	-1	-1
χ_4	3	-1	0	-1	1
χ_5	2	0	-1	2	0

- Note $\ker \chi_5 = \{1, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$, which implies that it's a normal subgroup of S_4.

4.3.3 Galois property of characters

Let $\rho : G \to \mathrm{GL}(V)$ be a complex representation. Assume that $g \in G$ has order m. Then there's a basis for V such that $\rho(g)$ is diagonal with respect to this basis, and all diagonal entries are m-th roots of unity, say

$$\rho(g) = \begin{pmatrix} \omega^{i_1} & & \\ & \ddots & \\ & & \omega^{i_n} \end{pmatrix}$$

where $\omega = e^{2\pi i/m}$ and $i_1, \ldots, i_n \in \mathbb{N} \cup \{0\}$. Then $\chi(g) = \omega^{i_1} + \cdots + \omega^{i_n}$. Now for j with $(j, m) = 1$, let $\sigma_j \in \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ such that $\omega \mapsto \omega^j$. Then

$$\sigma_j(\chi(g)) = \omega^{i_1 j} + \cdots + \omega^{i_n j} = \mathrm{tr} \begin{pmatrix} \omega^{i_1} & & \\ & \ddots & \\ & & \omega^{i_n} \end{pmatrix}^j = \chi(g^j)$$

Lemma 4.3.21. For j with $(j, m) = 1$, $\sigma_j(\chi(g)) = \chi(g^j)$.

Corollary 4.3.21.1. Suppose $g \in G$ has order m. If $g^j \in g^G$ for all j with $(j, m) = 1$, then $\chi(g) \in \mathbb{Z}$ for all characters χ.

Proof. By Lemma, we have $\sigma_j(\chi(g)) = \chi(g^j) = \chi(g)$ for all j with $(j, m) = 1$. By Galois theory, $\chi(g) \in \mathbb{Q}$. Since $\chi(g)$ is an algebraic integer, $\chi(g) \in \mathbb{Z}$. □

Example 4.3.22. When $G = S_n$, the hypothesis of Corollary above is satisfied so that $\chi(g) \in \mathbb{Z}$ for all $g \in S_n$ and characters χ.

Theorem 4.3.23. Let χ be an irreducible character and V a $\mathbb{C}G$-module corresponding to χ. Then $\chi(1) \mid \#G$.

Proof. Let $g_1, \dots, g_n \in G$ be the representatives of conjugacy classes of G. For each j, define

$$e_j := \sum_{g \in g_j^G} g \in \mathbb{C}G$$

Recall, in fact, $e_j \in Z(\mathbb{Z}G)$ (Proposition 4.3.16), so there exists $a_j \in \mathbb{C}$ such that $e_j v = a_j v$ for all $v \in V$, and thus $\chi(e_j) = a_j \chi(1)$.

Claim. a_j is an algebraic integer.

Note that a_j is an eigenvalue of the linear map $\mathbb{C}G \ni x \mapsto e_j x$. Now with respect to its standard basis $\{g \mid g \in G\}$, the entries of its matrix are all integers, which precisely shows that a_j is an algebraic integer.

We resume our proof. Since

$$1 = \langle \chi, \chi \rangle = \frac{1}{\#G} \sum_{j=1}^{n} \#g_j^G \chi(g_j) \overline{\chi(g_j)}$$

and

$$\chi(e_j) = \sum_{g \in g_j^G} \chi(g) = \#g_j^G \chi(g_j)$$

we have

$$1 = \frac{\chi(1)}{\#G} \sum_{j=1}^{n} \frac{\#g_j^G}{\chi(1)} \chi(g_j) \overline{\chi(g_j)} = \frac{\chi(1)}{\#G} \sum_{j=1}^{n} a_j \overline{\chi(g_j)}$$

i.e,

$$\frac{\#G}{\chi(1)} = \sum_{j=1}^{n} a_j \overline{\chi(g_j)}$$

Since the RHS is an algebraic integer, so is the LHS; since the LHS is also a rational number, it's an integer, i.e, $\chi(1) \mid \#G$. □

Example 4.3.24. $G = S_5$.

	1	2	22	23	3	4	5
$\#g^G$	1	10	15	20	20	30	24
$\#C_G(g)$	120	12	8	6	6	4	5
χ_1	1	1	1	1	1	1	1
χ_2	1	−1	1	−1	1	−1	1
χ_3	4	2	0	−1	1	0	−1
χ_4	4	−2	0	1	1	0	−1
χ_5	5	1	1	1	−1	−1	0
χ_6	5	−1	1	−1	−1	1	0
χ_7	6	0	−2	0	0	0	1

- $\chi_3 = \mathrm{fix}(\sigma) - 1$. Check it's irreducible.
- The values of χ_5, χ_6, χ_7 are determined by orthogonality relations, Theorem 4.3.23 and Example 4.3.22.
- $\chi_4 = \chi_2\chi_3$ and $\chi_6 = \chi_2\chi_5$. These will be shown to be representations of G by Proposition 4.3.31.
- $2\chi_5(1)^2 + \chi_7(1)^2 = 86$ and $\chi_5(1), \chi_7(1) \mid 120$, so that $\chi_5(1) = \chi_6(1) = 5$ and $\chi_7(1) = 6$.

4.3.4 Method of constructing characters

Lifts

Assume $N \trianglelefteq G$ and $\rho : G/N \to \mathrm{GL}(V)$ is a representation. By the universal property of quotient group, ρ lifts to a unique homomorphism $\tilde{\rho} : G \to \mathrm{GL}(V)$, defined by $g \mapsto \rho(gN)$. $\tilde{\rho}$ is a representation of G, called the **lift** of ρ.

Proposition 4.3.25. If ρ is irreducible, then so is $\tilde{\rho}$.

Proof. Let χ be the character of ρ. Then χ is also the character of $\tilde{\rho}$. Since ρ is irreducible, we have

$$1 = \frac{\#N}{\#G} \sum_{g \in G/N} \chi(g)\overline{\chi(g)} = \frac{1}{\#G} \sum_{g \in G} \chi(g)\overline{\chi(g)}$$

so that χ is an irreducible character of G, i.e, $\tilde{\rho}$ is irreducible. □

Corollary 4.3.25.1. The number of the distinct linear characters of G equals $\#(G/[G,G])$.

Example 4.3.26. $G = A_4$, $[G,G] = \{1, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$ so that $G/[G,G] = C_3$. Put $\zeta = e^{2\pi i/3}$.

	1	$(1\,2\,3)$	$(1\,3\,2)$	$(1\,2)(3\,4)$
$\#g^G$	1	4	4	3
$\#C_G(g)$	12	3	3	4
χ_1	1	1	1	1
χ_2	1	ζ	ζ^2	1
χ_3	1	ζ^2	ζ	1
χ_4	3	0	0	-1

- The up-left 3×3 matrix is the character table of C_3. The values of χ_1, χ_2, χ_3 for $(1\,2)(3\,4)$ are 1 since $(1\,2)(3\,4) \in [G,G]$.

- $\chi_4 = \mathrm{fix}(\sigma) - 1$. Check it's irreducible.

Proposition 4.3.27. A group G is simple $\Leftrightarrow \ker\chi = 1$ for all nontrivial irreducible characters χ.

Proof. The only if part is clear since $\ker\chi \trianglelefteq G$. For the if part, suppose G is not simple, say N is a nontrivial proper normal subgroup of G. Consider the quotient group G/N. Since $G/N \neq 1$, G/N has a conjugacy class other than $\{1\}$, so G/N admits a nontrivial irreducible representation, and by Proposition 4.3.25 it lifts to a nontrivial irreducible representation of G whose kernel contains N. □

Galois conjugates

Proposition 4.3.28. Let N be a positive integer such that $g^N = 1$ for all $g \in G$. Let χ be a character. For $\sigma \in \mathrm{Gal}(\mathbb{Q}(e^{2\pi i/N})/\mathbb{Q})$, define $\chi^\sigma : g \mapsto \sigma(\chi(g))$. Then χ^σ is also a character. Moreover, χ^σ is irreducible whenever χ is irreducible.

Proof. Let $\rho : G \to \mathrm{GL}(V)$ be a complex representation of G with character χ.

Method I. By Proposition 3.3.23, σ extends to an automorphism σ' on $\mathbb{C}$. Then $\sigma' \circ \rho : G \to \mathrm{GL}(V)$ is a representation of G with character being χ^σ. The moreover part holds by a direct computation.

Method II. Note that the complex irreducible characters of G are exactly the $\overline{\mathbb{Q}}$ irreducible characters of G, so every complex representation is isomorphic to some $\overline{\mathbb{Q}}$-representation. Hence we may regard ρ as a $\overline{\mathbb{Q}}$-representation. Now extend σ to an automorphism σ' on $\overline{\mathbb{Q}}$. Then $\sigma' \circ \rho$ is a representation with character χ^σ. □

Proposition 4.3.29. Assume $g \in G$ has order m. For j with $(j, m) = 1$, let σ_j be the element of $\mathrm{Gal}(\mathbb{Q}(e^{2\pi i/m})/\mathbb{Q})$ that maps $e^{2\pi i/m}$ to $e^{2\pi ij/m}$.

1. The set $\{j \in (\mathbb{Z}/m\mathbb{Z})^\times \mid g^j \in g^G\}$ is a subgroup of $(\mathbb{Z}/m\mathbb{Z})^\times$.
2. Let K be the fixed field of $\{\sigma_j \mid j \in A\}$. Then $\chi(g) \in K$ for all characters χ of G.
3. Let $B \leqslant (\mathbb{Z}/m\mathbb{Z})^\times$ and L the fixed field of $\{\sigma_j \mid j \in B\}$. If $\chi(g) \in L$ for all characters χ of G, then $g^j \in g^G$ for all $j \in B$.

Proof.

1. Let $j, k \in A$, $\ell = k^{-1} \in (\mathbb{Z}/m\mathbb{Z})^\times$ and $h, h' \in G$ such that $g^j = hgh^{-1}$, $g^\ell = h'gh'^{-1}$. Then
$$g^{j\ell} = h^\ell g^k g^{-\ell} = h^\ell h' g h'^{-1} h^{-\ell} = h^\ell h' g (h^\ell h')^{-1} \in g^G$$
so that $j\ell \in A$. Hence $A \leqslant (\mathbb{Z}/m\mathbb{Z})^\times$.

2. It suffices to show $\sigma_j\chi(g) = \chi(g)$ for each $j \in A$. Recall we have $\sigma_j\chi(g) = \chi(g^j)$, and since characters are class functions and $j \in A$, we have $\chi(g^j) = \chi(g)$, as wanted.

3. We prove a stronger result:

   Lemma 4.3.30. $g, g' \in G$ are conjugates if and only if $\chi(g) = \chi(g')$ for all characters χ of G.

   Proof. The only if part holds since each character is a class function. For the if part, recall the orthogonality relations

   $$\sum_\chi \chi(g)\overline{\chi(g')} = \begin{cases} \#C_G(g) & \text{, if } g' \in g^G \\ 0 & \text{, else} \end{cases}$$

   To show g, g' are conjugates, it suffices to show $\sum_\chi \chi(g)\overline{\chi(g')} \neq 0$. This holds since $\sum_\chi \chi(g)\overline{\chi(g')} = \sum_\chi \chi(g)^2 > 0$. □

   Since $\chi(g) \in L$, $\chi(g) = \sigma_j\chi(g) = \chi(g^j)$ for all $j \in B$ and χ. Hence, it follows from Lemma that $g^j \in g^G$, as desired.

   □

Tensor products

Proposition 4.3.31. Let V, W be two $\mathbb{C}G$-module. Let G act on $V \otimes_\mathbb{C} W$ by $g(v \otimes w) := gv \otimes gw$. Then $V \otimes_\mathbb{C} W$ is a $\mathbb{C}G$-module, and its character is the product of those of V and W.

Consider $V \otimes_\mathbb{C} V$. We have an involution $T \in \mathrm{End}_\mathbb{C}(V \otimes_\mathbb{C} V)$ (i.e, $T^2 = \mathrm{id}$) given by $T(v_1 \otimes v_2) = v_2 \otimes v_1$. Since $T^2 = \mathrm{id}$, $V \otimes_\mathbb{C} V$ is the direct sum of 2 eigenspaces corresponding to eigenvalues 1 and -1. One corresponding to 1 is called the **symmetric square** $S(V \otimes_\mathbb{C} V)$ of V and to -1 is called the **alternating square** $A(V \otimes_\mathbb{C} V)$ of V.

Proposition 4.3.32. $S(V \otimes V)$ and $A(V \otimes V)$ are $\mathbb{C}G$-modules. Let χ, χ_S, χ_A be the characters of V, $S(V \otimes V)$, $A(V \otimes V)$, respectively. Then

$$\chi_S(g) = \frac{1}{2}(\chi(g)^2 + \chi(g^2))$$

$$\chi_A(g) = \frac{1}{2}(\chi(g)^2 - \chi(g^2))$$

Proof. That they're $\mathbb{C}G$-modules is clear. For the rest part, let $g \in G$ and pick a basis $\{v_1, \ldots, v_n\}$ for V so that the matrix of $[v \mapsto gv]$ is $\mathrm{diag}(\lambda_1, \ldots, \lambda_n)$. Note that $\{v_i \otimes v_j + v_j \otimes v_i \mid 1 \leqslant i \leqslant j \leqslant n\}$ is a basis for $S(V \otimes V)$ and $\{v_i \otimes v_j - v_j \otimes v_i \mid 1 \leqslant i < j \leqslant n\}$ is that for $A(V \otimes V)$. We have

$$g(v_i \otimes v_j + v_j \otimes v_i) = \lambda_i \lambda_j (v_i \otimes v_j + v_j \otimes v_i)$$

$$g(v_i \otimes v_j - v_j \otimes v_i) = \lambda_i \lambda_j (v_i \otimes v_j - v_j \otimes v_i)$$

and hence

$$\begin{aligned}
\chi_S(g) &= \sum_{1 \leqslant i \leqslant j \leqslant n} \lambda_i \lambda_j = \sum_{1 \leqslant i \leqslant n} \lambda_i^2 + \sum_{1 \leqslant i < j \leqslant n} \lambda_i \lambda_j \\
&= \sum_{1 \leqslant i \leqslant n} \lambda_i^2 + \frac{1}{2}((\sum_i \lambda_i)^2 - \sum_i \lambda_i^2) \\
&= \frac{1}{2}((\sum_i \lambda_i)^2 - \sum_i \lambda_i^2) = \frac{1}{2}(\chi(g)^2 + \chi(g^2))
\end{aligned}$$

$$\chi_A(g) = \sum_{1 \leqslant i < j \leqslant n} \lambda_i \lambda_j = \frac{1}{2}((\sum_i \lambda_i)^2 - \sum_i \lambda_i^2) = \frac{1}{2}(\chi(g)^2 - \chi(g^2))$$

□

Example 4.3.33. $G = S_5$.

	1	2	3	22	4	23	5	Inner product
$\#g^G$	1	10	20	15	30	20	24	
$\#C_G(g)$	120	12	6	8	4	6	5	
g^G	1	1	3	1	22	3	5	
χ_1	1	1	1	1	1	1	1	1
χ_2	1	−1	1	1	−1	−1	1	1
χ_3=fix$(g) - 1$	4	2	1	0	0	−1	−1	1
$\chi_4 = \chi_2\chi_3$	4	−2	1	0	0	1	−1	1
$\chi_{3,S}$	10	4	1	2	0	1	0	3
$\chi_{3,A}$	6	0	0	−2	0	0	1	1
$\chi_{3,S} - \chi_1 - \chi_3$	5	1	−1	1	−1	1	0	1
$\chi_2(\chi_{3,S} - \chi_1 - \chi_3)$	5	−1	−1	1	1	−1	0	1

- $\chi_{3,S}$ and $\chi_{3,A}$ are the symmetric square and the alternating square induces by χ_3.
- $\langle \chi_{3,S}, \chi_1 \rangle = 1 = \langle \chi_{3,S}, \chi_3 \rangle$ so $\chi_{3,S} - \chi_1 - \chi_3$ is irreducible.

Remark 4.3.34. Note that

$$\chi(5) \equiv \chi(1) \pmod 5$$
$$\chi(3) \equiv \chi(1) \pmod 3$$
$$\chi(2), \chi(4) \equiv \chi(1) \pmod 2$$

In general, when the order of $g \in G$ is a prime power p^k, if $\chi(g) \in \mathbb{Z}$, we must have $\chi(g) \equiv \chi(1) \pmod p$.

Proof. Pick a basis such that the matrix of $\rho(g)$ is diagonal, say

$$\rho(g) = \begin{pmatrix} \omega^{i_1} & & \\ & \ddots & \\ & & \omega^{i_n} \end{pmatrix}$$

where $\omega = e^{2\pi i/p^k}$, i_j are integers. Then $\chi(g) - \chi(1) = \sum(\omega^{i_j} - 1) \in (1-\omega)\mathbb{Z}[\omega]$. By algebraic number theory, $(1-\omega)\mathbb{Z}[\omega]$ is a prime ideal of $\mathbb{Z}[\omega]$ and $(1-\omega)\mathbb{Z}[\omega] \cap \mathbb{Z} = p\mathbb{Z}$, so $\chi(g) \equiv \chi(1) \pmod p$. □

Restriction

If $H \leqslant G$ and $\rho : G \to \mathrm{GL}(V)$ is a representation of G, then $\rho|_H : H \to \mathrm{GL}(V)$ is a representation of H. If χ is the character of ρ, we denote by $\mathrm{Res}^G_H \chi$ the character of $\rho|_H$.

Proposition 4.3.35. Let H be a subgroup of G. Let χ be an irreducible character of G and $\psi_1, \ldots, \psi_k$ be irreducible characters of H. Decompose $\mathrm{Res}^G_H \chi$ as $\mathrm{Res}^G_H \chi = d_1\psi_1 + \cdots + d_k\psi_k$. Then

$$\sum_{i=1}^{k} d_i^2 \leqslant [G : H]$$

and the equality holds if and only if $\chi(g) = 0$ for all $g \notin H$.

Proof.

$$\begin{aligned} 1 = \langle \chi, \chi \rangle_G &= \frac{1}{\#G} \sum_{g \in G} \chi(g)\overline{\chi(g)} = \frac{1}{\#G} \sum_{h \in H} \chi(h)\overline{\chi(h)} + \frac{1}{\#G} \sum_{g \in G \setminus H} \chi(g)\overline{\chi(g)} \\ &= \frac{\#H}{\#G} \sum_{i=1}^{k} d_i^2 + \frac{1}{\#G} \sum_{g \in G \setminus H} \chi(g)\overline{\chi(g)} \\ &\geqslant \frac{1}{[G : H]} \sum_{i=1}^{k} d_i^2 \end{aligned}$$

Since $\chi(g)\overline{\chi(g)} > 0$ for each $g \in G \setminus H$, we may easily see the equality holds if and only if $\chi(g) = 0$ for each $g \in G \setminus H$. □

Example 4.3.36. $G = S_5$, $H = A_5$.

	1	2	3	22	4	23	5
$\#g^G$	1	10	20	15	30	20	24
$\#C_G(g)$	120	12	6	8	4	6	5
χ_1	1	1	1	1	1	1	1
χ_2	1	-1	1	1	-1	-1	1
χ_3	4	2	1	0	0	-1	-1
χ_4	4	-2	1	0	0	1	-1
χ_5	5	1	-1	1	-1	1	0
χ_6	5	-1	-1	1	1	-1	0
χ_7	6	0	0	-2	0	0	1

$\rightsquigarrow$

	1	3	22	5_1	5_2
$\#g^G$	1	20	15	12	12
$\#C_G(g)$	60	3	4	5	5
$\mathrm{Res}^G_H \chi_1$	1	1	1	1	1
$\mathrm{Res}^G_H \chi_3$	4	1	0	-1	-1
$\mathrm{Res}^G_H \chi_5$	5	-1	1	0	0
ψ_1	3	0	-1	$\frac{1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$
ψ_2	3	0	-1	$\frac{1-\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$

- For $\chi_1, \ldots, \chi_6$, there are odd permutations on which characters do not vanish. By Proposition above, $\langle \mathrm{Res}^G_H \chi_i, \mathrm{Res}^G_H \chi_i \rangle_H < [G : H] = 2$, i.e, $\langle \mathrm{Res}^G_H \chi_i, \mathrm{Res}^G_H \chi_i \rangle_H = 1$ so that the $\mathrm{Res}^G_H \chi_i$ are irreducible for $i = 1, \ldots, 6$.
- For χ_7, $\langle \mathrm{Res}^G_H \chi_7, \mathrm{Res}^G_H \chi_7 \rangle_H = 2$ and $\langle \mathrm{Res}^G_H \chi_7, \mathrm{Res}^G_H \chi_i \rangle_H = 0$ for $i = 1, \ldots, 6$.
- $\psi_1(1)^2 + \psi_2(1)^2 = 18 = 9 + 9$ so that $\psi_1(1) = \psi_2(1) = 3$.
- By column orthogonality relations we have

$$\begin{cases} \psi_1^2(22) + \psi_2^2(22) & = 2 \\ \psi_1(22) + \psi_2(22) & = -2 \end{cases}$$

  so $\psi_1(22) = \psi_2(22) = -1$.
- By column orthogonality relations again we have

$$\begin{cases} \psi_1^2(3) + \psi_2^2(3) & = 0 \\ \psi_1(3) + \psi_2(3) & = 0 \end{cases}$$

  so $\psi_1(3) = \psi_2(3) = 0$.
- The down-right block can be filled in the same manner as above.
- The down-right block gives an example of the Galois property. Since $(1\,2\,3\,4\,5)$ is conjugate to $(1\,5\,4\,3\,2) = (1\,2\,3\,4\,5)^{-1}$ in H, by Proposition 4.3.29, the value of $(1\,2\,3\,4\,5)$ must lie in the fixed field of $\langle \sigma : e^{2\pi i/5} \mapsto e^{-2\pi i/5} \rangle$, i.e, $\mathbb{Q}(\sqrt{5})$.

- $\operatorname{Res}_H^G \chi_7 = \psi_1 + \psi_2$.
- By Proposition 4.3.27, A_5 is simple.

Proposition 4.3.37. Let N be a normal subgroup of G. Let V be an irreducible $\mathbb{C}G$-module. Assume that U is an irreducible $\mathbb{C}N$-submodule of $\operatorname{Res}_N^G V$. Then

1. for all $g \in G$, the set gU is an irreducible $\mathbb{C}N$-submodule of V.
2. V is a direct sum of some gU (as $\mathbb{C}N$-modules), and
3. if g_1U and g_2U are isomorphic $\mathbb{C}N$-modules, then gg_1U and gg_2U are isomorphic $\mathbb{C}N$-modules.

In particular, every irreducible $\mathbb{C}N$-submodule of V has the same degree as U and every $\mathbb{C}N$-composition factor has the same multiplicity.

Proof.

1. Let $n \in N$; since $N \trianglelefteq G$, $ng = gn'$ for some $n \in N$. For each $u \in U$, $ngu = gn'u \in gU$ since U is a $\mathbb{C}N$-module. gU is clearly a $\mathbb{C}$-vector subspace of V, so gU is thus a $\mathbb{C}N$-submodule of V. Now if W is a $\mathbb{C}N$-submodule of gU, then $g^{-1}U$ is a $\mathbb{C}N$-submodule of U. Since U is irreducible, $g^{-1}W = 0$ or $g^{-1}W = U$, and thus $W = 0$ or $W = gU$; this shows gU is irreducible.

2. We have $V = \sum_{g \in G} gU$. The results follows from the general fact below.

   Lemma 4.3.38. Let $\{N_i\}_{i \in I}$ be a family of simple modules. If $M = \sum_{i \in I} N_i$, then $M = \bigoplus_{i \in I'} N_i$ for some subset $I' \subseteq I$.

3. Let $\phi : g_1U \to g_2U$ be a $\mathbb{C}N$-module isomorphism. We show $g\phi g^{-1} : gg_1U \to gg_2U$ is a $\mathbb{C}N$-module homomorphism with inverse $g\phi^{-1}g^{-1}$, and hence an isomorphism. It's clear a $\mathbb{C}$-linear transformation, so it remains to show it's an N-homomorphism. Let $n \in N$ and $u \in U$. Then

   $$(g\phi g^{-1})(ngg_1u) = g\phi(g^{-1}ngg_1u) = gg^{-1}ng\phi(g_1u) = n(g\phi g^{-1})(gg_1u)$$

   showing that $g\phi g^{-1}$ is an N-homomorphism. That $g\phi^{-1}g^{-1}$ and $g\phi g^{-1}$ are mutually inverses is clear, and the proof is completed.

□

Example 4.3.39. In the above example, since $A_5 \trianglelefteq S_5$, we see $\operatorname{Res}_H^G \chi_7 = \psi_1 + \psi_2$ and $\psi_1(1) = \psi_2(1)$.

Induction

Definition. Let $H \leqslant G$ and U a FH-module. The FG-module $FG \otimes_{FH} U$ is called the **induced FG-module** of U, denoted by $\operatorname{Ind}_H^G U$. If χ is the character of U, denote by $\operatorname{Ind}_H^G \chi$ the character of $\operatorname{Ind}_H^G U$.

- Let $g_1, \ldots, g_m$ be representatives of left cosets of H in G. Then

$$FG \otimes_{FH} U = (g_1 \otimes U) \oplus \cdots \oplus (g_m \otimes U)$$

as F-vector spaces.

- For each i, there exists a unique i' and $h_i \in J$ such that $gg_i = g_{i'}h_i$. Then for all $u \in U$,

$$gg_i \otimes u = g_{i'}h_i \otimes u = g_{i'} \otimes h_i u$$

Let $u_1, \ldots, u_n$ be a basis of U. Then

$$\{g_1u_1, \ldots, g_1u_n, g_2u_1, \ldots, g_2u_2, \ldots, g_mu_n\}$$

is a basis for $FG \otimes_{FH} U$. Then the matrix of g with respect to this basis if

$$\begin{pmatrix} A_{11} & \cdots & A_{m1} \\ \vdots & & \vdots \\ A_{m1} & & A_{mm} \end{pmatrix}$$

where $A_{ij} \in M_n(F)$ such that $A_{ij} = \delta_{i'j}H_i$ and H_i is the matrix of h_i with respect to $\{u_1, \ldots, u_n\}$. Thus

$$(\operatorname{Ind}_H^G \chi)(g) = \sum_{i:i=i'} \operatorname{tr} H_i = \sum_{i:i=i'} \chi(h_i) = \sum_{i:i=i'} \chi(g_i^{-1}gg_i) = \sum_{i:g_i^{-1}gg_i \in H} \chi(g_i^{-1}gg_i)$$

Proposition 4.3.40.

$$(\operatorname{Ind}_H^G \chi)(g) = \sum_{i:g_i^{-1}gg_i \in H} \chi(g_i^{-1}gg_i) = \frac{1}{\#H} \sum_{x \in G: x^{-1}gx \in H} \chi(x^{-1}gx)$$

Example 4.3.41. $H = S_4$, $G = S_5$, $g_i = (1\,2\,3\,4\,5)^i$.

	1	2	3	22	4
χ_1	1	1	1	1	1
χ_2	1	−1	1	1	−1
χ_3	3	1	0	−1	−1
χ_4	3	−1	0	−1	1
χ_5	2	0	−1	2	0

- For 2, say $(1\,2)$, we need to count how many g_i are there such that $(g_i(1)\,g_i(2)) = g_i(1\,2)g_i^{-1} \in S_4$, i.e, $g_i(1), g_i(2) \neq 5$. We have

$$\#\{g \in S_5 \mid g(1\,2)g^{-1} \in S_4\} = (4 \times 3) \times 3 \times 2 \times 1 = 72$$

so that

$$(\mathrm{Ind}_H^G \chi)((1\,2)) = \frac{1}{24} \times 72 \times \chi((1\,2)) = 3\chi((1\,2))$$

- Similarly,

$$\begin{aligned}(\mathrm{Ind}_H^G \chi)((1\,2\,3)) &= \frac{\chi((1\,2\,3))}{24} \times \#\{g \in S_5 \mid g(1\,2\,3)g^{-1} \in S_5\} \\ &= \frac{\chi((1\,2\,3))}{24} \times 4 \times 3 \times 2 \times 2 \times 1 = 2\chi((1\,2\,3))\end{aligned}$$

- In general, for $g \in S_{n-1}$, we have

$$(\mathrm{Ind}_{S_{n-1}}^{S_n} \chi)(g) = \chi(g)\frac{\#\{\sigma \in S_n \mid \sigma g \sigma^{-1} \in S_{n-1}\}}{\#S_{n-1}} = \chi(g)\mathrm{fix}(g)$$

where $\mathrm{fix}(g) = \#\{i \in \{1, \ldots, n\} \mid gi = i\}$. Note that $g \in S_n \backslash S_{n-1}$ makes no sense for the RHS, but $\mathrm{fix}(g) = 0$ in this situation. Then

	1	2	3	22	4	23	5
$\mathrm{Ind}_H^G \chi_1$	5	3	2	1	1	0	0
$\mathrm{Ind}_H^G \chi_2$	5	-3	2	1	-1	0	0
$\mathrm{Ind}_H^G \chi_3$	15	3	0	-1	-1	0	0
$\mathrm{Ind}_H^G \chi_4$	15	-3	0	-1	1	0	0
$\mathrm{Ind}_H^G \chi_5$	10	0	-2	2	0	0	0

One can check they're linear sums of irreducible characters of S_5 with non-negative integral coefficients.

Example 4.3.42. $G = \mathrm{PSL}_2(\mathbb{F}_7) = \mathrm{SL}_2(\mathbb{F}_7)/\mathrm{center} = \mathrm{SL}_2(\mathbb{F}_7)/\{2\text{-th roots of unity}\}$

4.3.5 An application to group theory

Theorem 4.3.43 (Burnside's)**.** Let p, q be two primes. Then any group of order $p^a q^b$, $a, b \geqslant 0$ is solvable.

Proof.

1. Reduction : It suffices to show that the only simple group of order p^aq^b are cyclic.
2. Let G be a simple group of order p^aq^b. Then G has either a nontrivial center or has a conjugacy class of size p^r, $1 \leqslant r \leqslant a$.
3. If G has a nontrivial center, then G is simple abelian, i.e, G is cyclic.
4. If G has a conjugacy class of size p^r, show that there exists a nontrivial irreducible character χ such that $|\chi(g)| = \chi(1)$ for some nonidentity element $g \in G$.
5. Let ρ be a representation with character χ. Since G is simple, ρ is injective. Also, by Proposition 4.3.12, $|\chi(g)| = \chi(1)$ implies $\rho(g)$ is a scalar matrix, i.e, $\rho(g) \in Z(\operatorname{Im}\rho)$, and thus $g \in Z(G)$. So $Z(G)$ is nontrivial center, reducing to 3.

1. Recall if $N \trianglelefteq G$ is a normal subgroup, then G is solvable if and only if both G/N and N are solvable.
2. If $b = 0$, then G is a p-group, so by class equation it must have a nontrivial center. If $b \neq 0$, let $Q \in \operatorname{Syl}_q(G)$ and $g \in Z(Q)\backslash\{1\}$. We have $C_G(g) \supseteq Q$, so
$$\#g^G = \frac{\#G}{\#C_G(g)} = \frac{p^aq^b}{p^xq^b} = p^{q-x}$$
for some x. If $x = a$, i.e, $C_G(g) = G$, then $g \in Z(G)$. If $x < a$, then good!
3. Let $\chi_1, \ldots, \chi_n$ be the irreducible characters of G, with χ_1 being the trivial character. Let $g \in G$ be in the conjugacy class of size p^r mentioned. By column orthogonality,
$$1 + \sum_{i=1}^{n} \chi_i(1)\overline{\chi(g)} = 0$$
so there exists χ_j such that $p \nmid \chi_j(1)$ and $\chi_j(g) \neq 0$ (if not, then $1 + p(\text{algebraic integers}) = 0$, a contradiction.) Since $p \nmid \chi_j(1)$, we have $\gcd(\#g^G, \chi_j(1)) = 1$, i.e, $a\#g^G + b\chi_j(1) = 1$ for some $a, b \in \mathbb{Z}$. Then
$$a\#g^G\frac{\chi_j(g)}{\chi_g(1)} + b\chi_j(g) = \frac{\chi_j(g)}{\chi_j(1)}$$
so that $\dfrac{\chi_j(g)}{\chi_j(1)}$ is an algebraic integer (Proposition 4.3.23) with absolute value $\leqslant 1$. Let $m = \operatorname{ord} g$ and $\zeta = e^{2\pi i/m}$. We have $\mathrm{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}\left(\dfrac{\chi_j(g)}{\chi_j(1)}\right) \in \mathbb{Q} \cap \{\text{algebraic numbers}\} = \mathbb{Z}$. Since it also has absolute value $\leqslant 1$, we conclude $\chi_j(g) = 0$ or $|\chi_j(g)| = \chi_j(1)$.

□