MATH5031 Algebra

Albert Peng

February 2, 2024

FL2023 with Prof. Roya Beheshti Zavareh

Contents

1 Groups

Definition. G is a non-empty set with a binary associate operation $*$ is a **group** if

- There is an *identity element* e, $a * e = e * a = a \forall a \in G$
- Every element has an *inverse*. $\forall a \in G, \exists a^{-1} \in G such that a * a^{-1} = a^{-1} * a = e$

Note: Identity and inverse elements are unique.

If $n \geq 1, a^n = a * a * ... * a$ for n times. Similar follows for a^{-n}. Also $a^0 = e$.

Definition. G is called **abelian** if $ab = ba \forall a, b \in G$.

Example. Non Abelian Group: $GL(n, \mathbb{R})$ of $n \times n$ matrices with real entries with matrix multiplication.

A non-empty subset $H \subseteq G$ is a **subgroup** if it is itself a group with the induced operation.

- $e \in H$
- $a \in H \implies a^{-1} \in H$
- $a, b \in H \implies ab \in H$

Fact: A non-empty subset H is a subgroup iff $a, b \in H \implies ab^{-1} \in H$.

Notation: $H \leq G$.

If $X \subset G$ is a subset, the subgroup generated by X, $< X > := \bigcap_{H \leq G, X \subseteq H} H$

If $X = a, < a >= \{a^n \mid n \in \mathbb{Z}\}$

1.1 Cosets

Definition. Let $H \leq G, g \in G$. The **right coset** of H in G generated by g is : $Hg = \{hg \mid h \in H\}$. **Left cosets** are defined similarly, where $gH = \{gh \mid h \in H\}$.

Facts: $Hg_1 = Hg_2 \iff H = Hg_2g_1^{-1} \iff g_2g_1^{-1} \in H$. Similarly, $g_1H = g_2G \iff g_1^{-1}g_2H = H \iff g_1^{-1}g_2 \in H$.

Corollary. If $Hg_1 \neq Hg_2$, then $Hg_1 \cap Hg_2 = \emptyset$

Proof. Let $a = Hg_1 \cap Hg_2 \implies a = h_1g_2 = h_2g_2$. Then $h_2^{-1}h_1 = g_2g_1^{-1} \implies g_2g_1^{-1} \in H \implies Hg_1 = Hg_2$. ■

Similarly, if $g_1H \neq g_2H$, then $g_1H \cap g_2H = \emptyset$

Example. A right coset is not necessarily a left coset. One example would be S_n the group of permutation of $1, ..., n$.

Definition. An operation f is **injective**, or **one-to-one** on a set S if $\forall s_1, s_2 \in S, f(s_1) = f(s_2) \implies s_1 = s_2$.

Definition. An operation f is **surjective**, or **onto** on for $f : X \longrightarrow Y$ if $im(f) = Y$. In other words, $\forall y \in Y, \exists x \in X$ such that $f(x) = y$.

If X is a set and S_X is the set of **bijections** $f : X \to X$, then there is a group under composition of function, namely the group of permutations of X.

Fact: There is a bijection between the set of distinct left cosets of H and distinct right cosets of H: $aH \longleftrightarrow Ha^{-1}$.

Proof. $aH = bH \iff a^{-1}b \in H \iff (a^{-1}b)^{-1} \in H \iff b^{-1}a \in H \iff Ha^{-1} = Hb^{-1}$ ■

Definition. The **index** if H in G, $[G : H]$ is the number of distinct right (left) cosets of H in G.

If $|G| < \infty$, then $|G| = [G : H] \cdot |H|$. ($|Hg| = |H|$). In particular, $|H| \mid |G|$

If $K \leq H \leq G$ and if $[G : H], [H : K] < \infty$, then $[G : K] < \infty$ and $[G : K] = [H : K][G : H]$.

Exercise: Prove this. $a_iH, i \in I, b_jK, b_j \in H, j \in J \implies a_ib_jK$ give all the cosets of K in G. Hint: (Was in homework last semester)

Definition. For $g \in G$, g has **finite order** if $\exists n \geq 1$ such that $g^n = e$, and ord(g) is the smallest such n. So ord(g) means that $< g >$ is a subgroup of order n. And if $|G| < \infty$, then ord(g) $\mid |G|$.

Definition. G is **cyclic** if $\exists g \in G$ such that $G =< g >$.

If $|G| = p$, p prime, then G is cyclic: If $G \neq \{e\}$, then $e \neq g \in G$, then $< g > \leq G$, so $1 \neq |< g >| \mid p \implies |< g >| = p$.

If G is cyclic, then every subgroup H of G is cyclic

Proof. $H \leq G$, and let r be the minimum positive integer such that $g^r \in H$, then $H =< g^r >$, so for $g^m \in H, m = rq + r_0$. ■

Proposition. If G is a cyclic group of order n, then for any divies $d \mid n$, there is a unique subgroup of order d.

Remark: $|A_4| = 12$ has no subgroup of order 6.

1.2 Normal Subgroups

Definition. Let $H \leq G$ is **normal** if $\forall g \in G, gHg^{-1} \subseteq H$. Note that $gHg^{-1} = \{ghg^{-1} | h \in H\} \leq G$.

Proof. $ghg^{-1}(gh'g^{-1})^{-1} \in gHg^{-1}$ ■

Example.

- Every subgroup of an abelian group is normal
- $SL(n, \mathbb{R})$, real matrices with det=1, is a normal subgroup of $GL(n, \mathbb{R})$, invertible matrices.
-

Obviously for $A \in GL(n, \mathbb{R}), B \in SL(n, \mathbb{R})$, $det(ABA^{-1}) = det(A)det(B)det(A^{-1}) = 1$

We denote H normal in G as $H \trianglelefteq G$.

If $H \leq G$, then the following are equivalent.

1. $H \trianglelefteq G$
2. $gHg^{-1} = H \, \forall \, g \in G$

3. $gH = Hg \,\forall\, g \in G$
4. Every right coset of H is a left coset
5. Every left coset of H is a right coset

Proof of 4 implies 3: Suppose $Hg = aH$ for some a. But then $g \in Hg = aH$, and $g \in gH$. So $aH = gH \implies Hg = gH$.

Proof of 1 implies 2: $gHg^{-1} \subseteq H \,\forall g \in G$, so $(g^{-1}H(g^{-1}))^{-1} \subseteq H \implies g^{-1}Hg \subseteq H$. Multiply from left and right to cancel, so $H = \subseteq gHg^{-1}$. So $gHg^{-1} = H$

Corollary. Any subgroup of index 2 in any group G is normal.

Proof. $[G : H] = 2 \implies$ two distinct left cosets, H, aH where $a \notin H$. Similarly, H and Ha are distinct right cosets. This $H \cap aH = \emptyset, H \cap Ha = \emptyset$, so by 4, H is normal. ■

1.3 Quotient (Factor) Groups

If $N \trianglelefteq G$, then the set of cosets of N in G, G/N, form a group under $(aN)(bN) = abN$. We need to check that

- Well-defined: $aN = a'N$ and $bN = b'N \implies abN = a'b'N$.
- Group properties easily follow from the group properties of G

So $a^{-1}a', b^{-1}b' \in N$. (add from notes)

Notation: This group is denoted as G/N.

Example. $SL(n, \mathbb{R}) \trianglelefteq GL(n, \mathbb{R})$. Then $GL(n, \mathbb{R})/SL(n, \mathbb{R}) \longleftrightarrow \mathbb{R} - \{0\}$, and $A \cdot SL(n, \mathbb{R}) \to \det(A)$

1.4 Group Homomorphisms

Definition. Let G, G' be a group. $\phi : G \to G'$ is a **homomorphism** if $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$. f is an **isomorphism** if the homomorphism is injective and surjective.

<u>Facts:</u> If $\phi : G \to G'$ is a homomorphism, then

- $\phi(e_G) = e_{G'}$
- $\phi(a^{-1}) = (\phi(a))^{-1}$
- ker$(\phi) := \{a \in G | \phi(a) = e_{G'}\} \trianglelefteq G$
- im$(\phi) := \{\phi(a) | a \in G\} \leq G'$

Proof. From video ■

Example. Let $\mathbb{Z}_n$ be the group of integers $\mod n$. Then any cylic group of order n is isomorphic to $\mathbb{Z}_n$. In particular for $G =< g >$, we define $\phi : G \to \mathbb{Z}_n$, $\phi(g^i) = [i]$.

1.5 Isomorphism Theorems

1st IsomorphismTheorem. If $f : G \to G'$ is a group homomorphism, then

$$G/\ker(f) \simeq im(f)$$

Proof. Define $\phi : G/\ker(f) \to im(f)$ by $\phi(a\ker(f)) = f(a)$.

ϕ is well-defined and injective: $a\ker(f) = b\ker(f) \iff a^{-1}b \in \ker(f) \iff f(a^{-1}b) = e$. So $f(a^{-1})f(b) = e \implies f(b) = f(a)$.

ϕ homomorphism: .$\phi(a\ker(f)b\ker(f)) = \phi(ab\ker(f))$ since kernel is normal group and that is $f(ab)$. On the other side, $\phi(a\ker(f))\phi(b\ker(f)) = f(a)f(b)$, so this is homomorphism since f is homomorphism

ϕ surjective: If $b \in im(f)$, then $b = f(a)$ for some a. So $\phi(a\ker(f)) = b$. ■

Example. $SL(n, \mathbb{R}) \trianglelefteq GL(n, \mathbb{R})$. Then $GL(n, \mathbb{R})/SL(n, \mathbb{R}) \simeq (\mathbb{R} - \{0\}, \cdot)$

Proof. $f : GL(n, \mathbb{R}) \to \mathbb{R} - \{0\}, A \mapsto det(A)$. This is a group homomorphism, f is surjective, $\ker(f) = SL(n, \mathbb{R}) \implies GL(n, \mathbb{R})/SL(n, \mathbb{R}) \simeq \mathbb{R} - \{0\}$ ■

Remark: If $H, K \leq G, HK = \{hk | h \in H, k \in K\}$. HK is not necessarily a subgroup of G. For example, consider $G = S_3$.

Fact: If $N \trianglelefteq G$ and $H \leq G$, then $HN \leq G$, $HN = NH$, and HN is the subgroup of G generated by $H \cup N$.

Proof. $HN \leq G$: If $a = h_1n_1, b = h_2n_2$, then $ab^{-1} = h_1n_1n_2^{-1}h_2^{-1} = h_1h_2^{-1}h_2n_1n_2^{-1}h_2^{-1}$. Clearly, $n_1n_2^{-1} \in N$ so $h_2n_1n_2^{-1}h_2^{-1} \in N$. Thus, $ab^{-1} \in HN$.

$HN = NH$: We need to first show $HN \subseteq NH$. Let $hn \in HN \implies hnh^{-1} = n' \in N \implies hn = n'h \in NH$, so $HN \subseteq NH$. Similar for other direction.

Clearly, $H, N \subseteq HN \leq G$. And for any $K \leq G$, let $H, N \subseteq K$. Since K is a subgroup, $\forall n \in N, h \in H, hn \in K$. Thus $HN \leq K$ is the smallest subgroup. In particular, HN is the subgroup generated by $H \cup N$.

■

2nd Isomorphism Theorem. Let $H \leq G, N \trianglelefteq G$. Then $H \cap N \trianglelefteq H$ and

$$H/H \cap N \simeq HN/N$$

Proof. If $\phi : H \to HN/N$ is given by $\phi(h) = hN$.

$\ker(\phi) = \{h \in H | hN = N\} = H \cap N$.

ϕ is surjective (so the $im(\phi)$ =range): $hnN = hN = \phi(h)$.

ϕ is homomorphism.

Together by the first isomorphism theorem, the result follows. ■

3rd Isomorphism Theorem. Suppose $K \leq N \trianglelefteq G$ and $K \trianglelefteq G$. Then

$$N/K \trianglelefteq G/K \text{ and } (G/K)/(N/K) \simeq G/N$$

Proof. First part follows by definition.

Second part: Define $\phi : G/K \to G/N$, $\phi(gK) = gN$ and check well-defined, homomorphism, $\ker(\phi) = N/K$, and ϕ surjective.

Well defined: $gK = g'K \implies g^{-1}g \in K \implies g^{-1}g' \in N \implies gN = g'N$. Surjectivity is clear, the rest is left as *exercise.* ■

4th Isomorphism Theorem. (Correspondence Theorem)

Let $N \trianglelefteq G$, then $\phi : G \to G/N, \phi(g) = gN$ induces a 1-1 correspondence between subgroups of G which contain N and subgroups of G/N.

- $N \leq H_1 \leq H_2 \iff H_1/N \leq H_2/N$, and $[H_2 : H_1] = [H_2/N : H_1/N]$.
- $N \leq H_1 \trianglelefteq H_2 \iff H_1/N \trianglelefteq H_2/N$, and in this case, $H_2/H_1 \simeq (H_2/N)/(H_1/N)$.

1.6 Simple and Solvable Groups

Definition. A group G is called **simple** if it has no normal subgroup other than $\{e\}$ and G.

Example. If G is finite and abelian, then G is simple iff G is cyclic of prime order. (*proof later*).

Example. Consider A_n, the **alternating group** of n elements. For a $\sigma \in S_n$, σ is a product of transpositions, or cycles of length 2. We call σ odd or even if the number of transpositions is odd or even. $A_n \leq S_n$

Note that this is well-defined: Proved using determinant of matrices. σ matrix generated from identity matrix using series of corresponding row swaps, which just alternates the sign of determinants. Thus even/odd is defined by the number of swaps. In particlar, A_n defines the set of all even permutations.

Also, $A_n \longleftrightarrow B_n$, $\sigma \mapsto \sigma(1\,2)$. $[S_n : A_n] = 2 \implies A_n \trianglelefteq S_n$

Conclusion: $A_n, n \geq 5$ is simple. For $n = 2, A_2 = \{e\}$. For $n = 3, A_3 = \{e, (1\,2\,3), (1\,3\,2)\}$.

For $n = 4$, $|A_4| = 12.\sigma_1 = (1\,2)(3\,4), \sigma_2 = (1\,3)(2\,4), \sigma_3 = (1\,4)(2\,3)$. Here, $\{e, \sigma_1, \sigma_2, \sigma_3\} \leq A_4$

Theorem. A_n is simple if $n \geq 5$

Proof. (1) $A_n, n \geq 5$ is generated by 3 cycles, and (2) Every 2 3-cycles are conjugate in A_n: σ_1, σ_2 are 3-cycles, then $\exists \tau \in A_n : \tau\sigma_1\tau^{-1} = \sigma_2$., and (3) every normal subgroup $N \neq \{e\}$ in A_n has at least one 3-cycle. Together they prove the statement.

For (1), $T = \{(a\,b\,c) \mid 1 \leq a < b < c \leq n\} \subset A_n$, then $\langle T \rangle \subset A_n$. If

$$\sigma = (a\,b)(c\,d) = \begin{cases} e, & \text{if } \{a, b\} = \{c, d\} \\ (a\,c\,b)(a\,c\,d), & \text{if } a, b, c, d \text{ all distinct} \\ (a\,d\,b) & \text{if } a = c \end{cases}$$

For (2), if σ_1, σ_2 are 3 cycles, are conjugate in S_n ■

Theorem. Jordan-Holder Theorem. If G is any finite group, then there is a unique tower of subgroups

$$\{e\} = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_{k-1} \trianglelefteq N_k = G$$

such that N_i/N_{i-1} is simple.

Definition. A **tower of subgroups**, $G_m \leq G_{m-1} \leq \cdots \leq G_1 \leq G_0 = G$ is **normal** if $G_{i+1} \trianglelefteq G_i$, and it is **abelian** if G_i/G_{i+1} is abelian, and **solvable** if there is an abelian tower $\{e\} = G_m \leq G_{m-1} \leq \cdots \leq G_1 \leq G_0 = G$.

Example.

- Any abelian group is solvable.
- S_3 is solvable, $\{e\} \trianglelefteq \{e, \sigma_1, \sigma_1^2\} \trianglelefteq S_3$
- $S_n, n \geq 5$ is not solvable

Proof. If $N \trianglelefteq S_n$, then $N \cap A_n \trianglelefteq A_n$. But A_n simple, so $N \cap A_n = \{e\}$ or A_n.

If $N \cap A_n = A_n$, then $A_n \leq N \leq S_n \implies N = A_n$ or $N = S_n$ due to $[S_n : A_n] = 2$. If $N \cap A_n = \{e\}$ and $N \neq \{e\}$, then if $\sigma_1, \sigma_2 \neq e, \sigma_1, \sigma_2 \in N$, then $\sigma_1\sigma_2 \in N$ since they are even, so $\sigma_1\sigma_2 = e$.

But by parts 1 and 2 of previous theorem, $N = A_n$. Since $N = \{e\}, N$, or $S_n \implies S_n, n \geq 5$ is not solvable. ■

Definition. Let $x, y \in G$. The **commutator** of $x, y := xyx^{-1}y^{-1} = [x, y]$ Note that $[x, y] = e \iff xy = yx$, and $[x, y]^{-1} = [y, x]$. This gives us a notion of how far a group is from abelian.

Definition. G', the **commutator subgroup**, is the subgroup generated by all the commutators $[x, y]$, where $x, y \in G$. $G' = \{[x_1, y_1][x_2, y_2] \cdots [x_k, y_k] \bigm| x_i, y_i \in G\}$

Facts:

- $G' = \{e\} \iff G$ is ableian
- $G' \trianglelefteq G$
- G/G' is abelian

Proof. Insert gg^{-1} between the elements: $g[xy]g^{-1} = gxg^{-1}gyg^{-1}gx^{-1}g^{-1}gy^{-1}g^{-1} = [gxg^{-1}, gyg^{-1}] \in G'$.

Similarly, $g[x_1, y_1] \cdots [x_k, y_k]g^{-1} = (g[x_1, y_1]g^{-1}) \cdots (g[x_k y_k]g^{-1})$

G/G' abelian proof: Want $abG' = baG'$. $a^{-1}b^{-1}ab = [a^{-1}, b^{-1}] \in G'$. So it is true. ■

Proposition. If $N \trianglelefteq G$, then G/N is abelian $\iff G' \leq N$

Proof. $\implies: \forall a, b \in G, G/N$ abelian so $a^{-1}b^{-1}N = b^{-1}a^{-1}N$. Then $aba^{-1}b^{-1} \in N \implies [a, b] \in N \implies G' \leq N$

$\impliedby$: $a^{-1}b^{-1}ab = [a^{-1}, b^{-1}] \in G' \subseteq N \implies a^{-1}b^{-1}ab \in N$ ■

Example. $(S_n)' = A_n$. *Proof left as exercise*

Let $G^{(0)} := G, G^{(1)} = G', ..., G^{(i)} = (G^{(i-1)})'$. $G^{(i+1)} \trianglelefteq G^{(i)}$ and $G^{(i+1)}/G^{(i)}$ is abelian.

Proposition. G is solvable iff $G^{(m)} = \{e\}$ for some $m \geq 1$

Proof. $\Longleftarrow$: $\{e\} = G^{(m)} \trianglelefteq \cdots \trianglelefteq G^{(1)} \trianglelefteq G$ is an abelian tower.

$\Longrightarrow$: If $\{e\} = G_m \trianglelefteq \cdots \trianglelefteq G_1 \trianglelefteq G_0 = G$ is abelian, then $G_1 \trianglelefteq G_0, G_0/G_1$ abelian $\implies G' \leq G_1, G_2 \trianglelefteq G_1, G_1/G_2$ abelian $\implies (G_1)' \leq G_2$ implies together that $G^{(2)} \leq G_1' \leq G_2 \implies G^{(2)} \leq G_2$.

By induction, $G^{(i)} \leq G_i \forall i, G^{(m)} \leq G_m = \{e\}$.

■

Proposition. If $N \trianglelefteq G$, then $N, G/N$ are solvable $\iff G$ is solvable.

proof: exercise, use derivative as one, use tower definition.

1.7 Group Actions

Definition. For a group G acting on set X, an **action of** G **on** X is a function $\alpha : G \times X \to X, (g, x) \mapsto g \cdot x$ such that

- $e \cdot x = x, \forall x \in X$.
- $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x), \forall x_1, x_2 \in X, g \in G$

Note that $\forall g \in X, \phi_g : X \to X$ is a permutation, $x \mapsto g \cdot x$.

ϕ_g is bijective, where $g \cdot x = g \cdot x' \implies g^{-1} \cdot (g \cdot x) = g^{-1} \cdot (g \cdot x') \implies e \cdot x = e \cdot x'$.

Also $\forall x \in X, \phi_g^{-1}(g \cdot x) = g \cdot (g^{-1} \cdot x) = x$

So, $\psi : G \to S_X$, the group of permutations of X with composition of functions and $g \mapsto \phi_g$.

Thus ψ is a homomorphism (not necessarily injective), since $\psi(g_1 g_2)(x) = (g_1 g_2)x = g_1(g_2 x) = \psi(g_1) \circ \psi(g_2)(x)$.

Example.

1. Trivial action. $\forall g \in G, x \in X, g \cdot x = x$
2. Conjugation on elements of G. $X = G, g \cdot x = gxg^{-1}$
3. Conjugation on subgroups of G. Let X be set of subgroups of G, $g \in G, H \in X$. Then $g \cdot H = gHg^{-1} \leq G$, and $a, b \in gHg^{-1}$. Then $a = ghg^{-1}, b = gh'g^{-1} \implies ab = g(hh')g^{-1}$.
4. G acts on G by translation. $X = G, g \cdot x = gx$.

Definition. Suppose G acts on $X, x \in X$. Then the **stabilizer** is defined as

$$G_x := \{g \in G \mid gx = x\} \leq G$$

Definition. We also define an **orbit** of X that forms a partition in x.

$$O_x = \{gx \mid g \in G\} \subseteq X$$

Note: $x \sim y$ if $y \in O_x$, so $y = gx$ for some g. Thus, any two orbits are either *equal* or *disjoint.*

From the examples above, the stabilizer and orbit is

1. $G_x = G, O_x = \{x\}$
2. $G_x = \{g \in G \mid gx = xg\}$, $O_x = \{gxg^{-1} \mid g \in G\}$, the conjugacy class of x in G.
3. O_H = all subgroups conjugate to H, $G_H = \underbrace{\{g \in G \mid gHg^{-1} = H\}}_{\text{normalizer}} \leq H$
4. $G_x = \{g \in G \mid gx = x\} = \{e\}, O_x = \{gx \mid g \in G\} = G$

Definition. As mentioned above, the **normalizer** of H in G is the largest subgroup of G in which H is normal.

$$H \trianglelefteq N_G(H) = \{g \in G \mid gH = Hg\} \leq G$$

Definition. An action is **transitive** if there is only one orbit, $O_x = X$

Theorem. [Orbit Stabilizer Theorem]. Let X be a G-set, then $\forall x \in X$,

$$|O_x| = [G : G_x]$$

Proof. Define $\psi : O_x \to$ set of left cosets of G_x, $gx \mapsto gG_x$.

Well-defined (since we can't make sure $gx = gx' \implies x = x$): $gx = g'x \iff x = g^{-1}g'x \iff g^{-1}g' \in G \iff gG_x = g'G_x$.

Surjective: clear ■

Definition. For group G, the **center** of G, $Z(G)$, is defined as

$$Z(G) = \{g \in G \mid gg' = g'g \forall g' \in G\}$$

<u>Fact:</u>

- $Z(G) = G \iff G$ abelian
- $Z(G) \trianglelefteq G$

Proof. Exericse. (Check video 9/13) ■

Example. $Z(S_n) = \{e\}, n \geq 3$

Example. If G acts on its subgroups in conjugation, $H \leq G$,

$$|O_H| = [G : N_G(H)] \qquad N_G(H) = \{g \in G \mid gHg^{-1} = H\}$$

Theorem. Burnside's Lemma. If G, X finite, X is a G-set, then the number of orbits of the action is $\frac{1}{|G|}\sum_{g \in G} |F_g|$. where F_g is the set of elements of X fixed by g.

Proof. Consider $S = \{(g, x) \mid gx = x\} \subset G \times X$. We can count S in two different ways.

1. $\forall g \in G$, there are $|F_g|$ elements fixed by g so $|S| = \sum_{g \in G} |F_g|$.
2. $\forall x \in X$, there are $|G_x|$ elements of X fixed in x, which equals $|G|/[O_x]$.

So $\sum_{g \in G} |F_g| = \sum_{x \in X} \frac{|G|}{|O_x|} = |G| \sum_{\text{distinct orbits } O_x} \frac{1}{|O_x|} |O_x| = |G| \times$ num orbits in X ■

Corollary. If G acts transitively on X, and $|X| > 1$, then there is $g \in G$ such that $F_g = \emptyset$. In other words, $\forall x, y \in X, \exists g$ such that $gx = y$. Equivalently, X has 1 orbit.

Proof. Burnside's Lemma gives $|G| = \sum_{g \in G} |F_g| = F_e + \sum_{g \neq e} |F_g|$.

If $|F_g| \geq 1 \forall g$, then $|G| = |X| + \sum_{g \neq e} |F_g| \geq |X| + (|G| - 1) \implies |X| \leq 1$, a contradiction. ■

1.7.1 Class Formula

Class Formula is when G acts on G via conjugation. If $x \in G = X$,

$$G_x = \underbrace{\{g \in G \mid gx = xg\}}_{N(x)} \leq G, \quad O_x = \{gxg^{-1} \mid g \in G\}$$

O_x gives a partition of G. So $|G| = \sum_{\text{distinct orbits}} |O_x| = \sum_{\text{distinct orbits}} [G : G_x = N(x)]$

$|O_x| = 1 \iff x \in Z(G)$. So we can write that summing all distinct conjugacy class with more than 1 elements.

$$|G| = Z(G) + \sum [G : G_x]$$

Corollary. If $|G| = p^r$, p prime, then $Z(G) \neq \{e\}$.

Proof. Since $|G| = |Z(G)| = \sum [G : G_x]$, so if $Z(G) = \{e\}$, we get $p^r = 1 + \sum \frac{|G|}{|G_x|}$. where $|G|/|G_x| > 1$ and is a divisor of $|G| = p^r$. This implies that $p \mid 1$, a contradiction $\implies Z(G) \neq 1$ ■

Corollary. If $|G| = p^2$, then G is ableian.

Proof. If G is not abelian, then $|Z(G)| = p$, so $Z(G)$ is proper subgroup of G. Pick $a \in G - Z(G)$, then $N(a) = \{b \mid ab = ba\} \neq G$. However $Z(G)$ is proper subgroup of $N(a)$ and $N(a)$ proper subgroup of G, a contradiction (a in $N(a)$ but not in $Z(G)$). ■

Corollary. If $|G| = p^r$, then G is solvable.

Proof. Proof by induction on r, $r = 1$ true.

Suppose this holds for $1, ..., r - 1$. Consider $Z(G) \trianglelefteq G$ and $Z(G) \neq \{e\}$. Here $|Z(G)|$ and $|G/Z(G)|$ are powers of p. So by hypothesis, $Z(G)$ and $|G/Z(G)|$ solvable $\implies$ G also solvable. ■

1.8 Sylow Theorems

Theorem. Suppose $|G| = p^r m$, $\gcd(p, m) = 1$. Then $\forall 0 \leq s \leq r$, G has a subgroup of size p^s.

Proof idea: abelian case and non abelian case.

Lemma: If G is abelian and $p \mid |G|$, then G has a subgroup of order p.

Proof. Induction on order of G. If $|G| = p$, there is nothing to prove. Suppose $|G| > p$, Let $e \neq a \in G, t = ord(a)$. Then $H = \{e, a, ..., a^{t-1}\} \leq G$, and there are two cases:

1. If $p \mid t$, so $| < a^{\frac{t}{p}} > | = p$

2. Otherwise, let $n = |G|, n = tn'$ so $p \mid n' = |G/H| < n$. So, by induction hypothesis, G/H has subgroup of order p, so an order of order p. Let there be a surjective map $\phi : G \to G/H$, so if $\phi(b) = \bar{b}$, then $p \mid ord(b)$. So we can apply case 1 to b and get a subgroup of order p.

Remark: If $\phi : G \to G'$ is a group homomorphism and $g \in G$ and $ord(\phi(g)) \mid \underbrace{ord(g)}_{m}$, so $g^m = e \to \phi(g)^m = e$. ($a^k = e \implies ord(a) \mid k$) ■

Proof of theorem. Recall that class formula states that when G acts on G by conjugation, $|G| = |Z(G)| + \sum[G : G_x]$, summing over distinct orbits with more than 1 element.

Fix p induction on G. If $|G| = p$, we are done. Now, let's have two cases where (1) $p \mid |Z(G)|$ and (2) p doesn't divide $|Z(G)|$.

In case 1, by lemma, $Z(G)$ has subgroup H of order p. Since $H \leq Z(G)$ and $Z(G) \trianglelefteq G$, we get $H \trianglelefteq G$ so G/H is a group of size $p^{r-1}m$. So by induction hypothesis G/H has a subgroup of order s for all $0 \leq s \leq r-1$. Any subgroup of G/H is K/H for $H \leq K \leq G$. So $|H| = p, |K/H| = p^s \implies |K| = p^{s+1}$. So this holds for $1 \leq s+1 \leq r$.

In case 2, G is not abelian, and we make two subcases.

1. Suppose $\forall x \notin Z(G), p \mid [G : G_x]$. This case is not possible since $p \mid |G|$ and p doesn't divide $Z(G)$

2. $\exists x \in Z(G), p \nmid [G : G_x] = |G|/|G_x| \implies p^r \mid |G_x|$, and $|G_x| < |G|$. By induction hypothesis, G_x and therefore G has a subgroup of $p^s, 0 \leq s \leq r$.

■

Note: $H \trianglelefteq K \trianglelefteq G \;\not\Longrightarrow\; H \trianglelefteq G$. Look at $G = A_4$.

Definition. A group G is a **p-group** if $|G| = p^r$. So $\forall e \neq a \in G, p \mid ord(a)$. And if $|G| = p^r m, gcd(m,p) = 1$, $H \leq G$, then H is a **p-subgroup** if $|H| = p^s$, and H is a **p-sylow subgroup** if $|H| = p^r$.

Theorem. If $p \mid |G|$, then

1. Every p subgroup is contained in a $p-$sylow subgroup.
2. Any two $p-$sylow subgroups are conjugate.
3. If $r =$ number of p-sylow subgroups, then $r \mid |G|$ and $r \equiv 1 \mod p$

Proposition. If H is a p-subgroup and P is a sylow p-subgroup, then H is contained in a conjugate of P: $\exists g \in G, H \leq gP^{-1}g$

Implication: The proposition shows the first and second part of them.

Part 1. $|gPg^{-1}| = |P|$, so the conjugate is also a sylow P-sylow ■

Part 2. P, P' sylow, then $\exists g$ such that $P' \subseteq gPg^{-1}$. Then $|gPg^{-1}| = |P| = p^r$ and $|P'| = r \implies P' = gPg^{-1}$.

■

Proposition Proof. Let S be the set of conjugates of P and H acts on S by conjugation, so that $h \cdot gPg^{-1} := hgPg^{-1}h^{-1}$. Then $S = \sum_{\text{distinct orbits}} |O_s| = \text{number of fixed points} + \sum_{\text{distinct w/ size}>1} |O_s|$.

Now the goal is to show that there $\exists$ a fixed point. Since $|O_s| = [H : H_s]$ and $|H| = p^s$, then $p \,\big|\, |O_s|$.

Here, $|S| = [G : N_G(P)] \implies |S| = \frac{|G|}{|N_G(P)|}$. Since $P \trianglelefteq N_G(P) \leq G$ and $p^r \,\big|\, |N_G(P)|$, I get $p \nmid |S|$ and so $p^r \,\big|\, |N_G(P)|$.

Let gPg^{-1} be a fixed point. Then $\forall h \in H, hgPg^{-1}h^{-1} = gPg^{-1} \implies P = g^{-1}h^{-1}gPg^{-1}hg \implies P = g^{-1}h^{-1}gP(g^{-1}h^{-1}g)^{-1} \implies g^{-1}h^{-1}g \in N_G(P)$. So $\forall h \in H \implies g^{-1}Hg \subseteq N_G(P)$.

Let $K = g^{-1}Hg$, $K, P \leq N_G(P)$ and $P \trianglelefteq N_G(P)$.

So by the second isomorphism theorem, $KP/P \simeq K/K \cap P \implies |KP| = \frac{|P||K|}{|K \cap P|}$ and $|KP| \,\big|\, |G|$, and $|P||K|$ is a power of $p \implies \frac{|K|}{|K \cap P|} = 1 \implies K \subseteq P \implies g^{-1}Hg \subseteq P \implies H \subseteq gPg^{-1}$. ■

Part 3 Proof. By part 2, $r = \text{number of all conjugates of } P = [G : N_G(P)]$, and $[G : N_G(P)] \,\big|\, |G|$.

To show $r \equiv 1 \mod p$, let $H = P$ from proof of the proposition, so that $r = \text{number of fixed points + a multiple of } p$

If gPg^{-1} is a fixed point, then by the proof $P \subseteq gPg^{-1}$, but $|P| = |gPg^{-1}|$ so $P = gPg^{-1}$. So only one fixed point $\implies r \equiv 1 (mod\, p)$ ■

<u>Note</u>: $r = 1 \iff gPg^{-1} = P \, \forall g \in G \iff P \trianglelefteq G$

Corollary. If $|G| = pq$ where p, q are distinct primes and $p \not\equiv 1 \mod q$ and $q \not\equiv 1 \mod p$. Then G is cyclic.

Proof. Let r_1 be the number of sylow p-subgroups and r_2 be the number of sylow q-subgroups. Then $r_1 \,\big|\, pq, r_1 \equiv 1 \mod p \implies r_1 = 1$, and similarly $r_2 = 1$

If $H_1, H_2 \leq G$ with $|H_1| = p$ and $|H_2| = q$, then by the note, $H_1, H_2 \trianglelefteq G$.

$H_1 = \{e, a, ..., a^{p-1}\} =< a >, H_2 = \{e, b, ..., b^{q-1}\} =< b >$. For $aba^{-1} \in H_2$ and $ba^{-1}b^{-1} \in H_1$, $aba^{-1}b^{-1} \in H_1 \cap H_2 = \{e\} \implies ab = ba \implies ord(ab) \in \{1, p, q, pq\}$. So $(ab)^p = a^p b^p = b^p \neq e \implies ord(ab) = pq \implies G =< ab >$ ■

<u>Fact:</u> Group of order < 60 is solvable, since $N \trianglelefteq G, N, G/N$ solvable $\implies G$ solvable.

Example. If $|G| \leq 30$, and G is not of prime order, then G is not simple.

Corollary. If $|G| \leq 30$, then G is solvable.

Proposition. If $|G| = n$ and p is the smallest prime divisor of n and $H \leq G$ has index p, then $H \trianglelefteq G$

Proof. If $p = 2$, this is proved before.

Suppose $H \ntrianglelefteq G$. Then there is $g \in G$ such that $gHg^{-1} \neq H$. Let $K = gHg^{-1}$.

Since $|HK| = |H|\frac{|K|}{|H \cap K|}$, where $|H \cap K|$ which divides $|K|$ and so $|G|$. Then either $\frac{|K|}{|H \cap K|} = 1$ or $\frac{|K|}{|H \cap K|} \geq p$.

For the first case, $H \cap K = K \implies K \subseteq H \implies gHg^{-1} \subseteq H \implies gHg^{-1} = H$, not true.

For second case, $|HK| \geq p|H| = |G| \implies HK = G \implies g^{-1} \in HK = HgHg^{-1}$. So for some $h, h' \in H, hgh' = e \implies g = h^{-1}h'^{-1} \in H \implies gHg^{-1} = H$, a contradiction. So $H \trianglelefteq H$ ∎

Corollary. If $|G| = pq^r$, and p, q are distinct prime and $p < q$. Then G has a normal subgroup.

Proof. By Sylow Theorem, there is a sylow q-subgroup H, so $[G : H] = p$. H is normal from the previous corollary. ∎

Corollary. If $|G| = pq, p \neq q$, then G has a non-trivial normal subgroup.

Proposition. If $|G| = pq^2$, and p, q are distinct prime, then G is not simple.

Proof. If $p < q$, we are done by previous corollary.

So if $p > q$, let r be the number of sylow p-subgroups and s be number of sylow q subgroups.

Goal is to show that $r = 1$ or $s = 1$ since the only sylow subgroup is normal.

Since $r \equiv 1 \mod p, r \,\big|\, |G| = pq^2 \implies r \,\big|\, q^2$. So either $r = 1, r = q, r = q^2$. If $r = 1$, we are done. $r = q$ is impossible since $q \equiv 1 \mod p$ and $p \,\big|\, q - 1$ but $p > q$. So assume $r = q^2$.

So because $s \equiv 1 \mod q, s \,\big|\, |G| = pq^2$, then $s \,\big|\, p \implies s = 1$ or $s = q$. If $s = 1$, we are done. So assume $s = p$.

Then we have q^2 subgroups of order p and p subgroups of order q^2. Then $|G| \geq 1 + q^2(p-1) + q^2 - 1$, so there is only 1 q-sylow subgroup. So $s = 1$, and we are done. ∎

Corollary. Every group of size $\leq n$ which is not of prime is *not simple*.

[Check Video]

<u>Fact:</u> If $|G| = 24$, then G is not simple.

Proof. Let r be the number of sylow 2-subgroups and s be the number of sylow 3-subgroups.

$$\begin{cases} r \equiv 1 \mod 2 \\ r \,\big|\, 3 \end{cases} \implies \begin{cases} r = 1, \text{so we have normal subgroup} \\ r = 3 \end{cases}$$

So assume $r = 3$, and we have sylow 2-subgroups $H_1, H_2, H_3, |H_i| = 8$. Let $S = \{H_1, H_2, H_3\}$ and G acts on S by conjugation.

So there is a homomorphism $\phi : G \to S_3$, the group of permuations of S.

Use the fact that $\ker\phi \trianglelefteq G$ and we calim that $\ker\phi \neq \{e\}$ or G.

- $\ker\phi \neq \{e\} : |G| = 24, |S_3| = 6 \implies \phi$ not injective $\implies \ker\phi \neq \{e\}$
- $\ker\phi \neq G : H_1, H_2$ are conjugate by Sylow Theorem, so $\exists g \in G$ such that $gH_1g^{-1} = H_2 \implies g \cdot H_1 \neq H_1 \implies \phi(g) \neq e$.

$$\begin{cases} s \equiv 1 \mod 3 \\ s \,\big|\, 8 \end{cases} \implies \begin{cases} s = 1, \text{ so we have normal subgroup} \\ s = 4 \end{cases}$$

So assume $s = 4$ ∎

Fact: Any group of order < 60 is solvable. *Hint: 36 similar to 24, and 40 and 56 use counting of elements (union larger than elements?)*

1.9 Dihedral Group

Here, $|D_n| = 2n, D_n = \{e, x, .., x^{n-1}, y, yx, ..., yx^{n-1}\}$.

When $n = 3, D_3 = S_3$

Fact: D_n is solvable *(Homework exercise)*.

1.10 Direct Product of Groups

Let G_1, G_2 be groups. Then $G_1 \times G_2 = \{(g_1, g_2) \mid g_1 \in G_1, g_2 \in G_2\}$, and $(g_1, g_2)(g_1', g_2') = (g_1 g_1', g_2 g_2')$. The identity element is (e_1, e_2) and $(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1})$.

Let I be an index set $G_i, i \in I$. Then

$$\prod_{i \in I} G_i = \{(x_i)_{i \in I} \mid x_i \in G_i\}$$

are the **direct product** of G_i, where $(x_i)_{i \in I}(y_i)_{i \in I} = (x_i y_i)_{i \in I}$.

Then, the **direct sum** of *abelian groups* where A_i abelian, $\forall i \in I$.

$$\bigoplus_{i \in I} A_i \leq \prod_{i \in I} A_i, \quad \bigoplus_{i \in I} A_i = \{(a_i)_{i \in I} \mid \text{ there are only finitely many non-zero } a_i\}$$

Notice that if I is *finite*, then $\bigoplus_{i \in I} A_i = \prod_{i \in I} A_i$.

Definition. Let A be an ableian group. Then

- $a \in A$ is **torsion** if $\text{ord}(a)$ is finite: $\exists n > 0, na = 0$
- A_{tor} is the set of torsion elements in A, $A_{tor} \leq A$ since $na = 0, mb = 0 \implies nm(a+b) = 0$
- A is **torsion-free** if $A_{tor} = \{0\}$.
- A is **torsion** if $A_{tor} = A$

Example. $\mathbb{Z}$ is torsion-free. $\mathbb{Z}/m$ is torsion, and any finite abelian group is torsion.

Theorem. If A is a torsion abelian group, then $A \simeq \bigoplus_{p_i \text{ prime}} A(p)$, where $A(p)$ are elements a in A such that $ord(a)$ is a power of p, $p^r a = 0 \exists r \geq 1$.

Proof. Plan: We have $A \simeq A_{tor} \bigoplus A/A_{tor}$, where A/A_{tor} is torsion-free. Both parts are finitely generated. Then we show that A_{tor} is finite. Then since A/A_{tor} is finitely generated, and torsion free, $A/A_{tor} \simeq \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$. Then, show that A_{tor} finite is a direct sum of abelian p-groups, thus a direct sum of cyclic group.

Let $\phi : \oplus_{p \text{ prime}} A(p) \to A$ is homomorphism, $(x_p) \mapsto \sum x_p \in A$.

ϕ surjective: $a \in A, ord(a) = m = p_1^{r_1} \cdots p_n^{r_n}$, p_i distinct prime. Then proceed by induction on n. If $n = 1$, then $ord(a) = p_1^{r_1} \implies a \in A(p) \implies a \in im(\phi)$. Then for n, $ord(a) = p_1^{r_1} \cdots p_n^{r_n} \iff ap_1^{r_1} \cdots p_n^{r_n} = 0$. So since $p_1^n \cdots p_{n-1}^{r_{n-1}}$ and $p_n^{r_n}$ coprime, $\exists s, t \in \mathbb{Z}$ such that $sp_1^n \cdots p_{n-1}^{r_{n-1}} + tp_n^{r_n} = 1$, $asp_n^n \cdots p_{n-1}^{r_{n-1}} + atp_n^{r_n} = a$. Since the two numbers are in $im\phi$, their sum is in $im(\phi)$.

ϕ injective: Suppose $\phi((x_0)) = 0$, and $\exists q, x_q \neq 0$, then $\sum x_p = 0 \implies x_q = -\sum_{p\neq q} x_p \implies x_q = -x_{p_1} - ... - -x_{p_n}$. ord$(x_{p_i}) = p_i^{s_i} \implies p_1^{s_1} \cdots p_r^{s_r}(-x_{p_1} - ... - x_{p_r}) = 0 \iff q(p_1^{s_1} \cdots p_r^{s_r}) = 0 \implies ord(q) \mid p_1^{s_1} \cdots p_r^{s_r}$, a contradiction. ■

Example. $A = \mathbb{Q}/\mathbb{Z}$, where $A(p) = \{\frac{a}{b} + \mathbb{Z} \mid \frac{p^r a}{b} \in \mathbb{Z}\}$ for some r.Then $\frac{p^r a}{b} = c \implies \frac{a}{b} = \frac{c}{p^r}$, so $= \{\frac{c}{p^r} + \mathbb{Z} \mid c \in \mathbb{Z}, r \geq 0\}$

<u>*Lemma:*</u> Every finitely generated torsion abelian group is finite.

Proof. If $ord(a_i) = m_i$, and $A = \langle a_1, ..., a_k \rangle = \{n_1 a_1 + ... + n_k a_k \mid n_i \in \mathbb{Z}\} = \{n_1 a_1 + ... + n_k a_k \mid n_1 \in \mathbb{Z}, 0 \leq n_i < m_i\}$, which is finite. ■

Theorem. Every finite abelian p-group is a direct sum of cyclic groups.

<u>*Lemma:*</u> If A is a finite abelian p-group which is <u>not cyclic</u>, then A has at least 2 subgroups of order p.

Lemma Proof. See homework ■

Theorem Proof. Let $a \in A$ be an element of maximal order. We prove by induction on $|A|$ that there is a $B \leq A$ such that $A =< a > \oplus B$. This means that if $B_1, B_2 \leq A$ such that $B_1 \cap B_2 = \{0\}$.

If $|A| = p$, we are done.

Let $ord(a) = p^s$. Then $< a >$ has a unique subgroup of order p. Let $< b >$ be another subgroup of order p in A such that $\langle a \rangle \cap \langle b \rangle = \{0\}$, which exists due to the previous lemma.

Consider $\bar{A} = A/ < b >, |\bar{A}| = \frac{|A|}{p} < |A|$. Then there is $\bar{a} = a+ < b >$, an element of maximal order in $\bar{A}$.

By the induction hypothesis, there is a $\bar{B}$ such that $\bar{A} =< \bar{a} > \oplus \bar{B}$.

So $\bar{B} \leq \bar{A} = A/ < a > \implies \bar{B} = B/ < a >$ for $B \leq A$ with $< a > \subset B_0$. Then $A =< a > \oplus B$

■

Definition. A group A is **free** if A has a basis $\{a_i\}_{i \in I}$ such that $\forall a \in A, a = \sum_{i \in I} \lambda_i a_i$ in a unique way. So if A has a basis with n elements, $A \simeq \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{n \text{ elements}}$.

Proposition. Free abelian groups are torsion-free

Proof. $A =< a_i >$. Suppose $b \neq 0 \in A$ such that $mb = 0, b = \sum a_i \implies mb = \sum (m\lambda_i) a_i \implies m\lambda = 0 \forall i \implies b = 0$, a contradiction. ■

Example. Torsion-free abelian groups are not necessarily free. Consider $\mathbb{Q}$ as an example.

Proposition. Every *finitely-generated* torsion-free abelian group is free, $A \simeq \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$.

Proof. Let $A =< a_1, ..., a_n >$ and induct on n. If $n = 1, A =< a_1 >$ is torsion-free $\implies |A| = \infty \implies A \simeq \mathbb{Z}$.

$n-1 \implies n$: Let $B := \{a \in A \,\big|\, ma \in < a_1 > \exists m > 0\}$.

Claim: B is cyclic, $B \leq A \implies B$ finitely generated.

Let $B =< b_1, ..., b_l > \forall i \exists m_i, m_i b_i \in < a_1 >$. Let $m = m_1 \cdots m_l$. Then $mb \in < a_1 > \forall b \in B$.

Now look at $\phi : B \to < a >, b \mapsto mb$. Then $im(\phi) \leq < a_1 >$.

So $im(\phi)$ is cyclic: $im\phi =< \lambda a_1 >, \lambda \geq 1$. Let $b_1 \in B$ such that $\phi(b_1) = \lambda a_i$.

Then $B =< b_1 >$. If $b \in B, mb \in im\phi \implies mb = t\lambda = tmb_1$ for some $t \implies m(b - tb_1) = 0$. Since A torsion free, this means $b = tb_1 \implies b \in < b_1 >$.

A/B is generated by $a_2 + B, ..., a_n + b$ and is torsion-free, where if $m(a + B) = 0, ma \in B \implies \exists \lambda : \lambda ma \in < a_1 > \implies a \in B$.

By the induction hypothesis, A/B is free $\implies$ by proposition last time, $A = B \oplus C \simeq \mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$., so this is free. ■

Proposition. Every subgroup of a finitely generated abelian group is finitely generated.

Idea: This implies that A_{tor} is finitely generated. Combining with previous result that a finitely generated and torsion group is finite, I can then write $A_{tor} = \mathbb{Z}_{p_1^{r_1}} \oplus \cdots \oplus \mathbb{Z}_{p_m^{r_m}}$.

Proof. Let $H \leq A, A = \langle a_1, ..., a_n \rangle$, and proceed by induction on n. If $n = 1$, this is cyclic so clearly true.

$n-1 \implies n$: Let $B = \langle a_1, ..., a_{n-1} \rangle \leq A$. Then by induction hypothesis, $H \cap B = \langle h_1, ..., h_{n-1} \rangle$ generated by at most $n - 1$ elements.

Also, $A/B =< a_n + B >$.

Note that $\frac{H+B}{B} \simeq \frac{H}{H \cap B}$. Since $\frac{H+B}{B} \leq \frac{A}{B}$, it is also cyclic, so $\frac{H}{H \cap B}$ cyclic, generated by some $\langle h_n + (H \cap B) \rangle, h_n \in H$.

So $H =< h_1, .., h_n >$, I need to show that they actually generate H. If $h \in H$, then $h + (H \cap B) = \lambda_n h_n + (H \cap B) \implies h - \lambda_n h_n \in (H \cap B) \implies h - \lambda_n h_n = \sum_{i=1}^{n-1} \lambda_i h_i \implies h = \sum_{i=1}^{n} \lambda_i h_i$. ■

Proposition. If A is abelian and $B \subseteq A$ such that A/B is a free abelian group, then there is a subgroup $C \leq A$ such that $A = B \oplus C$.

Proof. Let $\{a_i + B\}_{i \in I}$ be a basis for A/B. Let $C =< a_i > \leq A$. We claim that $A = B \oplus C$.

First show $B \cap C = \{0\}$: Suppose $\sum_{i \in I} \lambda_i a_i \in B$, then $\sum_{i \in I} \lambda_i a_i + B = B$, so $\sum_{i \in I} \lambda_i (a_i + B) = B$, where B is the 0 of A/B. So, $\lambda_i = 0 \forall i$.

To show $A = B + C$: If $a \in A$, then $a + B = \sum_{i \in I} \lambda_i (a + B)$ in A/B, so $a + B = \sum_{i \in I} (\lambda_i a_i) + B$, so $a - \underbrace{\sum_{i \in I} \lambda_i a_i}_{\in C} \in B$. ■

Summary: Since A is finitely generated, A/A_{tor} is torsion-free, and A finitely generated $\implies$ A/A_{tor} is finitely generated. So, by previous proposition, A/A_{tor} is free.

Then by the other proposition, $\exists C \leq A, A = A_{tor} \oplus C$. So C is finitely generated, and can be written as $\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$

Definition. Let F be a group (not necessarily abelian) and $X \subset F$. Then F is a **free group** with basis X if it satisfies the following universal property:

- $\forall$ group G and every function $f : X \to G$, there is a *unique* homomorphism $\phi : F \to G$ extending f.

For a set X, the **free group generated** by $X = \{a_1 \cdots a_k \mid a_i \in \{e\} \cup X \cup X^{-1}\}$

Example. If $X = \{x\}$, the free group generated by $X = \{x^r \mid r \in \mathbb{Z}\} \simeq \mathbb{Z}$

Example. $X = \{x, y\}$, then $F = \{x^{k_1} y^{r_1} \cdots x^{k_n} y^{r_n} \mid r_n, k_n \in \mathbb{Z}, n > 0\}$.

Fact: Every group is a quotient of a free group. $G =< x_i >, i \in I$.

Let F be free group generated by $\{x_i\}_{i \in I}$. By the universal property, $\exists$ homomorphism $\phi : F \to G, \phi$ surjective. Let $N = \ker(\phi), N \trianglelefteq F$. Then $F/N \simeq G$.

If $N =< y_j >, j \in J$. Then $< x_i, i \in I \mid y_j = e, j \in J >$ is a presentation of G.

Example. $G = \mathbb{Z}_6, \mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$. Let $\phi : \mathbb{Z} \to \mathbb{Z}_6$, $1 \mapsto \bar{1}$. $N =< 6 >\subseteq \mathbb{Z}$. $Z_6 =< x \mid x^6 = e >$

Example. $S_3 = \{e, \underbrace{(1\,2)}_{x_1}, \underbrace{(1\,3)}_{x_2 x_1}, \underbrace{(2\,3)}_{x_2^2 x_1}, \underbrace{(1\,2\,3)}_{x_2}, \underbrace{(1\,3\,2)}_{x_2^2}\}$ Then $S_3 =< x_1, x_2 >$. So a *presentation* of $S_3 =< x_1, x_2 \mid x_1^2 = e, x_2^3 = e, x_2 x_1 = x_1 x_2^2 >$

Proposition. Let G be a free group generated by x, y. G is finitely generated, $H \leq G$ generated by $\{yxy^{-1}, y^2 x y^{-2}, y^3 x y^{-3}, ...\}$. Then H is not finitely generated.

1.11 Automorphisms

Definition. Let G be a group. If $\phi : G \to G$ is an *isomorphism*, then ϕ is an **automorphism** of G. $Aut(G)$ is the group of automorphisms of G under composition of function, $Aut(G) \leq S_G$.

Example. What is $Aut(G)$ if G is cylic of order m? Define $\phi : G \to G, \phi(x) = x^l, 0 \leq l \leq m-1$. This is always a homomorphism. In particular, ϕ isomorphism $\iff$ x^l has order m in $G \iff \frac{m}{gcd(m,l)} = m \iff gcd(m, l) = 1$.

Example. Let $\mathbb{Z}_m^\times$ be the group of units in $\mathbb{Z}_m$ under multiplication $= \{l \in \mathbb{Z}_m \mid gcd(l, m) = 1\}$. Then $Aut(G) \to \mathbb{Z}_m^\times$, $\phi \mapsto l$, $\phi(x) = x^l$ is an isomorphism.

$$\begin{cases} \phi \mapsto l_1 \implies \phi_1(x) = x^{l_1} \\ \phi_2 \mapsto l_2 \implies \phi_2(x) = x^{l_2} \end{cases} \implies \phi_2 \circ \phi(x) = \phi_1(x^{l_2}) = x^{l_1 l_2}$$

1.12 Semi-Direct Product of Groups

Previously for A abelian, $H, K \leq A, H \cap K = \{0\}, A = H + K$, we denote $A = H \oplus K$, where $H \times K \simeq A, (h, k) \mapsto h + k$.

More generally, if G is a group, $H, K \leq G$ such that $H \cap K = \{e\}, G = HK$ and $hk = kh \forall h \in H, k \in K$, then $H \times K \simeq G, (h,k) \mapsto hk$.

Proof. $(h,k) \mapsto hk, (h',k') \mapsto h'k', (hh',kk') \mapsto hh'kk' = hkh'k'$.

$(h,k) \mapsto e \implies hk = e \implies k = h^{-1} \implies k \in K \cap H \implies k, h = e$. ■

In particular if it is not the case that $hk = kh \forall h \in H, k \in K$, then $G \not\simeq H \times K$.

Example. $G = S_3$, $H = \{e, (1\,2\,3), (1\,3\,2)\}, K = \{e, (1\,2)\}$. $HK = S_3, H \cap K = \{e\}$. But $S_3 \not\simeq H \times K \simeq Z_3 \times \mathbb{Z}_2$.

If $K \leq G, H \trianglelefteq G$, then $HK \leq G$.

Example. Let K act on H (normal to G) by conjugation. Then $\phi : K \to Aut(H)$ is $k \mapsto \phi_k$, $\phi_k(h) = khk^{-1} \forall h$.

Definition. Let H and K be two groups and $\phi : K \to Aut(H)$ a homomorphism, $k \mapsto \phi_k$. Then $(H \times K)$ with operation $(h,k)(h',k') = (h\phi_k(h'), kk')$ is a group, denoted by $H \rtimes K$, the **semi-direct product** of H and K.

Proof of Group Properties. Identity: (e,e). $(e,e)(h,k) = (e\phi_e(h), k) = (h,k)$. $(h,k)(e,e) = (h, \phi_k(e), k) = (h,k)$.

Inverse of $(h,k) = (\phi_{k^{-1}}(h^{-1}), k^{-1})$. $(h,k)(\phi_{k^{-1}}(h^{-1}), k^{-1}) = (h\phi_k(\phi_{k^{-1}})(h^{-1}), e) = (e,e)$. ■

<u>Fact:</u> If ϕ is the identity homomorphism $\phi_k = e$ on H, then $H \rtimes K \simeq H \times K$.

$H \times K$ contains copies H and K as normal subgroup. $H \to H \times K$, $h \mapsto (h,e)$.

$(h',k')(h,e)(h',k^{-1}) = (h'hh^{-1}, e)$, and $H \trianglelefteq (H \rtimes K)$

Proposition. If $H, K \leq G, H \trianglelefteq G, H \cap K = \{e\}, G = HK$, then $G \simeq H \rtimes K$. $k \mapsto Aut(H), k \mapsto \phi_k$, $\phi_k(h) = khk^{-1}$.

Corollary. $S_3 \simeq \mathbb{Z}_3 \rtimes \mathbb{Z}_2$. Notice that this means that ϕ trivial or $\mathbb{Z}_3 \rtimes \mathbb{Z}_2 = \mathbb{Z}_2$ or $\phi_1(1) = 2$ which is S_3

Proposition Proof. $f : H \rtimes K \to G, (h,k) \mapsto hk$. To show f injective, $f(h,k) = e \implies hk = e \implies h, k = e$. ■

1.13 Classification of Small Groups

By order,

2. $\mathbb{Z}_2$
3. $\mathbb{Z}_3$
4. $\mathbb{Z}_2 \oplus \mathbb{Z}_2, \mathbb{Z}_4$
5. $\mathbb{Z}_5$
6. $\mathbb{Z}_2 \oplus \mathbb{Z}_3$. Non-abelian: S_3
7. $\mathbb{Z}_7$
8. $\mathbb{Z}_8, \mathbb{Z}_2 \oplus \mathbb{Z}_4, \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$. Non-abelian D_4, Q_8

9. $\mathbb{Z}_9, \mathbb{Z}_3 \oplus \mathbb{Z}_3$

10. $\mathbb{Z}_{10}, \mathbb{Z}_5 b \oplus \mathbb{Z}_2$. Non-abelian: D_5

11. $\mathbb{Z}_{11}$

12. $\mathbb{Z}_3 \oplus \mathbb{Z}_4, \mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$. Non-abelian: $D_6 (= \mathbb{Z}_2 \times S_3), A_4, \mathbb{Z}_3 \rtimes \mathbb{Z}_4,$

In particular, $\phi : \mathbb{Z}_4 \to Aut(\mathbb{Z}_3)$, which is $\mathbb{Z}_2$. $0 \mapsto 0, 1 \mapsto 1, 2 \mapsto 0, 3 \mapsto 1$

2 Rings

Definition. A non-empty set R is a **ring** if there are operations multiplication($\cdot$) and addition $(+)$ on R such that

- $(R,+)$ is an abelian group.
- $a\cdot(b\cdot c)=(a\cdot b)\cdot c$
- $a\cdot(b+c)=a\cdot b+a\cdot c,(b+c)\cdot a=b\cdot a+c\cdot a.$
- There is an element $1\in R$ such that $a\cdot 1=1\cdot a=a\forall a\in R$.

Properties:

- Unity is unique. $1=1\cdot 1'=1'$
- $0\cdot a=0,\forall a\in R:0a=(0+0)a=0a+0a\implies 0a=0$
- $(-a)b=a(-b)=-(ab).(-a)b+ab=(-a+a)b=0b=b\implies(-a)b=-(ab)$

Example. $(\mathbb{R},+,\cdot)$, $(M_n(\mathbb{R}),+,\cdot)$, $(\mathbb{R}[x],+,\cdot)$, $(\mathbb{R}[[x]],+,\cdot)$, which is the ring of formal power series. $\{a_0+a_1x+a_2x^2+...\,\big|\,a_i\in\mathbb{R}\}$.

Definition. Let R,S be rings, $f:R\to S$ is a **ring homomorphism** if

- $f(a+b)=f(a)+f(b)$
- $f(ab)=f(a)f(b)$
- $f(1_R)=f(1_S)$

Example. $f:\mathbb{R}\to M_2(\mathbb{R}),r\mapsto\begin{bmatrix}r&0\\0&0\end{bmatrix}$ satisfies 1 and 2 but not 3.

Definition. $S\subseteq R$ is a **subring** if $(S,+)\le(R,+)$ and $1\in S$ and S is closed under multiplication.

Definition. $I\subset R$ is a **left ideal** if

- $(I,+)\le(R,+)$
- $\forall r\in R,a\in I$, we have $ra\in I$.

A **right ideal** is similarly defined. In particular, $I\subset R$ is an **ideal** if *both right and left ideals*.

Fact: If $f:R\to S$ is a ring homomorphism, then

- $\ker(f)$ is an ideal of R
- $im(f)$ is a subring of S.

Definition. Let $I\subset R$ be an ideal

$$R/I:=\{r+I\,\big|\,r\in R\}$$

is a ring with $(r_1+I)(r_2+I):=r_1r_2+I$, $(r_1+I)(r_2+I):=(r_1+r_2)+I$

Definition.

- R is **commutative** if $ab=ba\forall a,b\in R$.
- R is a **division ring** if every $0\neq a\in R$ has a multiplicative inverse.

- A commutative division ring is a **field**.
- If $a, b \in R, a, b \neq 0$ but $ab = 0$, then a, b are called **zero devisors**.
- A *commutative ring* with no zero divisor is an **integral domain**.

Example.

- $\mathbb{Z}$ is an integral domain
- $\mathbb{Z}_n$ is a field $\iff$ n is prime.

2.1 Ideals and Quotient Rings

Let $I \subset R$ be an ideal, then we have $R/I = \{r + I \,|\, r \in R\}$, with $(r + I)(s + I) = rs + I$.

Proof of Well-defined Multiplication. Want to check that $r + I = r' + I$ and $s + I = s' + I \implies rs + I = r's' + I$.

$r - r', s - s' \in I$. On the other side, $rs - r's' = r(s - s') + (r - r')s' \in I$, which is true. ∎

R/I is a ring, with unity $1 + R$ and zero $0 + R$. The *canonical homomorphism* is given by

$$f : R \to R/I, \quad r \mapsto r + I$$

where f is clearly surjective and $ker(f) = I$.

2.1.1 Ring Isomorphism Theorems

First Isomorphism Theorem. If $f : R \to S$ is a ring homomorphism, then

$$R/ker(f) \simeq im(f)$$

[Second Isomorphism Theorem.] If $S \subseteq R$ is a subring and $I \subset R$ is an ideal, then $S \cap I$ is an ideal of S and I is an ideal in

$$S + I = \{s + i \,|\, s \in S, i \in I\} \leq R$$

and

$$S/S \cap I \simeq S + I/I$$

Ideal in $S + I$. $(s + i)(s' + i') = ss' + is' + si' + ii'$, with $is' + si' + ii' \in I$ ∎

[Third Isomorphism Theorem.] If $I \subset J \subseteq R, I, J$ ideals in R, then $J/I = \{j + I \,|\, j \in J\}$ is an ideal of R/I and

$$\frac{R/I}{J/I} \simeq R/J$$

[Fourth Isomorphism Theorem.] (Correspondance Theorem) Let $I \subset R$ be an ideal. There is a 1-1 correspondence between subrings of R/I and subrings of R containing I.

2.2 Maximal Ideals and Prime Ideals

Definition. An ideal $M \subsetneq R$ is called a **maximal ideal** if for any $I \subseteq R$ with $M \subseteq I \subseteq R$, then $I = M$ or $I = R$. Every **proper ideal** is contained in a maximal ideal by *Zorn's Lemma*.

[Zorn's Lemma] If S is a *partially ordered* set in which every *totally ordered subset* has an upper bound contains a maximal element. It is *Partially ordered* if

$$\begin{cases} a \leq a \\ a \leq b \text{ and } b \leq a \implies a = b \\ a \leq b \text{ and } b \leq c \implies a \leq c \end{cases}$$

So it follows that if $S' \subset S$ is totally ordered, then $\bigcup_{I \in S'} I$ is in S and an upper bound in S.

Proposition. I is maximal ideal $\iff$ R/I is a field

Proof. $\implies$: Assume $r + I \neq I$, so $r \notin I$. If R is a commutative ring, $X \subseteq R$, then the ideals generated by X, $\langle X \rangle = \{r_1 x_1 + \cdots r_k x_k \mid k \geq 1, r_i \in R, x_i \in X\}$.

Then let $J = \langle r, I \rangle \subseteq R$, then clearly $I \subseteq J \subseteq R$. Since J ideal and I maximal ideal, $I = J$ or $J = R$, but $r \in J - I$, so $J = R \implies 1 \in J = \langle i, J \rangle \implies 1 = r'r + i$. Thus $1 - rr' \in I \implies (1 + I) = (r + I)(r' + I)$, where $(r' + I)$ is the inverse of $(r + I)$.

$\impliedby$: If R/I is a field and $I \subseteq J \subseteq R$, then J/I is an ideal of R/I. The only proper ideals of a field is $\{0\}$ ∎

Definition. If $I \subsetneq R$ is an ideal, we say I is **prime** if $ab \in I \implies a \in I$ or $b \in I$ for $a, b \in R$.

Example. $R = \mathbb{Z}$, and let $m\mathbb{Z}$ be an ideal, $m \in \mathbb{Z}$. $m\mathbb{Z}$ is prime iff m is prime

Proof. $\implies$: If $m = ab$, and $a, b > 1$, then $ab = m \in m\mathbb{Z}$ but $a, b \notin m\mathbb{Z}$

$\impliedby$: If $ab \in m\mathbb{Z}$, then $m \mid ab \implies m \mid a$ or $m \mid$ ∎

Proposition.

1. Every maximal ideal is prime
2. $I \subsetneq R$ is prime $\iff$ R/I is an integral domain.
3. P is a prime ideal $\iff$ $IJ \subseteq P$ implies $I \subseteq P$ or $J \subseteq P$ for ideals $I, J \subseteq R$. In particular, $IJ := \{\sum_{i=1}^{n} a_i b_i \mid n \geq 1, a_i \in I, b_i \in J\}$ is an ideal of R and $IJ \subseteq I \cap J$.

Proof (1): If M is maximal and $ab \in M$ and $a \notin M$, then the ideal generated by a, M, $\langle a, M \rangle := \{ra + m, m \in M, r \in R\}$ is an ideal where $M \subsetneq \langle a, M \rangle \subset R$. Then $\langle a, M \rangle = R$ since M maximal, so $1 = ra + m$ for some $r \in R, m \in M \implies b = rab + mb$, so $b \in M$. ∎

Proof (2): $\implies$: If $(a + I)(b + I) = 0$, then $ab + I = 0$, so $ab \in I \implies a \in I$ or $b \in I$, so $a + I = \bar{0}$ or $b + I = \bar{0}$, where $\bar{0}$ is the zero of R/I.

$\impliedby$: If $ab \in I$, then $(a + I)(b + I) = \bar{0}$, so $a + I = \bar{0}$ or $b + I = \bar{0}$, so $a \in I$ or $b \in I$. ∎

Proof (3): If P is prime and $IJ \subseteq P$ but $I \subsetneq P$ and $J \subsetneq P$, then pick $a \in I \backslash P$ and $b \in J \backslash P$, then $ab \in IJ$ but $ab \notin P$, a contradiction

Conversely, assume $IJ \subseteq P$ implies $I \subseteq P$ or $J \subseteq P$ for ideals $I, J \subseteq R$. Let $I = \langle a \rangle = \{ra \,\big|\, r \in R\}$ and $J = \langle b \rangle = \{rb \,\big|\, r \in R\}$. Then $IJ = \langle ab \rangle$ (check this). So $IJ \subseteq P$, so $a \in I \subseteq P$ or $b \in J \subseteq P$, so $a \in P$ or $b \in P$. ■

Example. $m\mathbb{Z} \subseteq \mathbb{Z}$ is prime $\iff$ $m\mathbb{Z}$ is maximal $\iff$ m is prime.

Proof. $m\mathbb{Z} \subseteq n\mathbb{Z} \iff n \,\big|\, m$, so prime implies maximal ideal. Alternatively, consider proposition 2. ■

Example. $\{0\}$ is a prime ideal $\iff$ R is an integral domain. This also follows from proposition 2.

2.3 Chinese Remainder Theorem

For $0 < m_1, ..., m_n \in \mathbb{Z}, gcd(m_i, m_j) = 1$, then for any $r_1, ..., r_n \in \mathbb{Z}$, the system of equation

$$\begin{cases} x \equiv r_1 (\mod m_1) \\ \vdots \\ x \equiv r_n (\mod m_n) \end{cases} \qquad \text{has a solution}$$

In rings, I reformulate this problem for a commutative ring R, where $I_1, ..., I_n$, $n \geq 2$ are ideals in R such that $I_i + I_j = R$ for every $i, j, i \neq j$. Then for any $r_1, ..., r_n \in R$, there is $x \in R$ such that $x - r_i \in I_i \, \forall 1 \leq i \leq n$.

Proof. Proceed with induction on n: If $n = 2, I_1 + I_2 = R \implies \exists a_i \in I_i$ such that $a_1 + a_2 = 1$. Then let $x = r_1 a_1 + r_2 a_1$, then $x - r_1 = r_1(a_2 - 1) + r_2 a_1 = -r_1 a_1 + r_2 a_1 \in I_1$. Similar for $x - r_2$.

$2 \implies n$: For $I_1, ..., I_n$, let $J = I_2 \cdots I_n$. Claim: $I + J = R$.

So for $I_1 + I_i = R \forall i \geq 2, \exists a_i \in I_1, b_i \in I_i$ such that $a_i + b_i = 1 \implies 1 = \prod_{i=2}^{n}(a_i + b_i) = I_1 + J$. By case 2 of the theorem, $\exists y_1 \in R$ such that $y_1 - 1 \in I_1, y_1 - 0 \in J \implies y_1 \in I_2 \cdots I_n$. In a similar way, $\forall 1 \leq i \leq n$, we find $y_i \in R$ such that $y_i - 1 \in I_i$ and $y_i = I_1 \cdots \hat{I_i} \cdot I_n \subseteq I_j \forall j \neq i$. Note that $I \cap J \subseteq IJ$.

Let $x = r_1 y_1 + ... + r_n y_n$. Then $x - r_i = r_1 y_1 + \cdots r_i(y_i - 1) + \cdots r_n y_n$. Every y_i is in I_i, so this entire expression is in I_i. ■

2.4 Product of Rings

Let R, S be rings, then

$$R \times S = \{(r, s) \,\big|\, r \in R < s \in S\}$$

where $(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$. and $(r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1, s_2)$

Corollary. If $I_1, ..., I_n$ are ideals of R such that $I_i + I_j = R$ for $i \neq j$. Then

$$\frac{R}{\bigcap_{i=1}^{n} I_n} \simeq \prod_{i=1}^{n} R/I_i$$

Proof. Define $\phi : R \to \prod_{i=1}^n R/I_i$ by $\phi(r) = (r + I_1, ..., r + I_n)$, and ϕ is a ring homomorphism. $\ker(\phi) = \cap_{i=1}^n I_i$.

ϕ surjective: $\forall (r_1 + I_1, ..., r_n + I_n) \in \prod_{i=1}^n R/I_i$, by the chinese remainder theorem, $\exists x \in R$ such that $x + I_i = r_i + I_i$, so by the first isomorphism theorem, we get the result. ■

Example. If $R = \mathbb{Z}$, and prime factorization $m = p_1^{r_1} \cdots p_n^{r_n}, I_i = p_i^{r_i}\mathbb{Z}$. Then note that $I_i = p_i^{r_i}\mathbb{Z}, I_i + I_j = \mathbb{Z}$, and $\cap_{i=1}^n I_i = m\mathbb{Z}$. So,

$$\mathbb{Z}/m\mathbb{Z} \simeq \prod_{i=1}^n \mathbb{Z}/p_i^{r_i}\mathbb{Z}$$

as rings. Also,

$$\mathbb{Z}_m \simeq \prod_{i=1}^n \mathbb{Z}_{p_i}^{r_i}$$

as rings.

2.5 Localization

Suppose R is an integral domain. Consider the equivalence relation $\frac{a}{b} \sim \frac{c}{d} \iff ad = bc$. Then, we can mod out by equivalence relationship.

$$\{\frac{a}{b} \,\big|\, a, b \in R, b \neq 0\}/\sim$$

Then we define the ring structure such that for $b, d \neq 0, \frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}, \frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$. There are well-defined. The unity is $\frac{1}{1}$, and the zero is $\frac{0}{1}$. This is a commutative ring, and any non-zero element $\frac{a}{b}, a, b \neq 0$ has a multiplicative inverse $\frac{b}{a}$. Thus we get a field, namely the <u>field of fraction</u> of R (Quotient field).

Definition. Suppose R is a commutative ring. Then $S \subset R$ is a **multiplicative subset**, where $1 \in S$ and $a, b \in S \implies ab \in S$, and $0 \notin S$

Example.

- For $0 \neq r \in R,\ S = \{1, r, r^2, ...\}$
- $P \subsetneq R$ be a prime ideal and $S = R \backslash P$. Then $a, b \notin P \implies ab \notin P$.

Define $S^{-1}R = \{(r, s) \,\big|\, r \in R, s \in S\}/\sim$. Then consider the equivalence relationship $(r, s) \simeq (r', s') \iff \exists s'' \in S$ such that $s''(rs' - sr') = 0$.

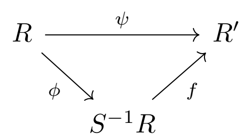
If $0 \in S$, then $(r, s) \simeq (0, 0)$, and everything is 1 equivalence relationship. So from now on, we assume $0 \notin S$. Then we have ring structure on $S^{-1}R$, $\frac{r}{s} + \frac{r'}{s'} = \frac{rs'+r's}{ss'}$, and $\frac{r}{s}\frac{r'}{s'} = \frac{rr'}{ss'}$.

Operations are well-defined: If $\frac{r}{s} = \frac{r_0}{s_0}$, then $\exists s'', s''(rs_0 - r_0 s) = 0$. Then I want to check that $\frac{r}{s} + \frac{r'}{s'} = \frac{r_0}{s_0} + \frac{r'}{s'} \iff \frac{rs'+r's}{ss'} = \frac{r_0 s'+r' s_0}{s_0 s'} \iff \cdots = 0$. Last step consists of annoying factorization.

There is a natural ring homomorphism defined by $\phi : R \to S^{-1}R, \phi(r) = \frac{r}{1}$.

In particular if R is an integral domain (so $rs' = r's$), $S^{-1}R$ is a subring of the field of fractions of R, which we can write as $R \subset S^{-1}R \subset K$, where K is the field of fractions.

Note that $\phi : R \to S^{-1}R$ has the property that $\phi(s)$ is invertible. Namely $\forall s \in S, \phi(s) = \frac{s}{1}$, so $\frac{s}{1}\frac{1}{s} = \frac{1}{1}$. And if $\psi : R \to R'$ is a ring homomorphism such that $\psi(s)$ invertible in R', then $\exists! f : S^{-1}R \to R'$ such that $f \circ \phi = \psi$ [Check video for graph]



Proposition. Assume R is an integral domain

- If $S = R \setminus \{0\}$, then $S^{-1}R$ is the field of fractions of R.
- If $S = \{1, f, f^2, ..., \}$ where $f \in R$ such that $f^n \neq 0 \forall n$, $R_f = S^{-1}R = \{\frac{a}{f^r} \,\big|\, a \in R, r \geq 0\}$.
- If $P \subset R$ is a prime ideal and $S = R \setminus P$, $R_P = S^{-1}R = \{\frac{a}{b} \,\big|\, a, b \in R, b \notin P\}$
- If $P \subsetneq R$ is a prime ideal, then R_p is a **local ring**. i.e. it has a *unique* maximal ideal. This unique maximal ideal is defined as $\{\frac{a}{b} \,\big|\, a, b \in R, b \notin P, a \in P\}$. If $b \notin P$, then there is an inverse which is not possible since $P \subsetneq R$.

2.6 Principal Ideal Domains (PIDs)

Definition. For *integral domain R*, an ideal $I \subseteq R$ is **principal** if it is generated by one element $I = \langle a \rangle = \{ra \,\big|\, r \in R\}$. Then R is **PID** if every ideal is *principal*.

Example.

- $\mathbb{Z}$ is PID. Every ideal generated by some n.
- $\mathbb{R}[x]$ is a PID. If $I \neq \{0\}$ is an ideal and $0 \neq f(x) \in I$ has the smallest degree, then $I = \langle f(x) \rangle$. If $g \in I$, dividing g by f means that $g(x) = q(x)f(x) + r(x)$. So $r(x)$ or $deg(r) < deg(f)$. By $r(x) = g(x) - q(x)f(x) \in I$, by $degr(x) \geq degf(x) \implies r = 0 \implies g \in \langle f \rangle$.
- $\mathbb{R}[x, y]$ is not a PID. $\langle x, y \rangle = \{f(x, y) \,\big|\, f(0, 0) = 0\}$ not principal.
- $\mathbb{Z}[x]$ is not a PID. $\langle x, y \rangle = \{f(x) \,\big|\, f(0) \text{ is even}\}$ not principal.

Definition.

- For an integral domain R, $a \in R$ is **prime** if $\langle a \rangle$ is a prime ideal. Equivalently, $a \,\big|\, bc \implies a \,\big|\, b$ or $a \,\big|\, c$.
- $0 \neq a \in R$ is **irreducible** if it is not a unit and if $a = xy$, then x is a unit or y is a unit.

Proposition. A *prime* element is *irreducible*.

Proof. If a is prime and $a = xy$, then $a \,\big|\, x$ or $a \,\big|\, y$, so $x = ax'$ or $y = ay'$, so $a = ax'y$ or $a = xay' \implies a(1 - x'y) = 0$ or $a(1 - xy') = 0 \implies 1 = x'y$ or xy', so y is a unit or x is a unit. ■

Example. Let $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \,\big|\, a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$.

It is clear to see that this is closed under multiplication. We claim that $3 \in R$ is irreducible but not prime. We let $3 = (a + b\sqrt{-5})(c + d\sqrt{-5})$, and define the norm as $|a + \sqrt{-5}| := \sqrt{a^2 + 5b^2}$.

Then squaring, $9 = (a^2+5b^2)(c^2+5d^2)$. Clearly neither of the values can be 3. so $a^2+5b^2 = 1$ or $c^2+5d^2 = 1$. Thus $(a,b) = (\pm 1, 0) \implies (a+b\sqrt{-5})$ is a unit, or $c+d\sqrt{-5}$ is a unit. Thus 3 is irreducible.

But $3^2 \bigm| (2+\sqrt{-5})(2-\sqrt{-5}) \implies 3 \bigm| (2+\sqrt{-5})(2-\sqrt{-5})$. and $3 \nmid (2+\sqrt{-5})$ and $3 \nmid 2-\sqrt{-5}$ since $2+\sqrt{5} \neq 3(a+b\sqrt{-5})$, for $a,b \in \mathbb{Z}$.

Proposition. If R is a PID, then irreducible $\implies$ prime.

Proof. Suppose $a \in R$ is irreducible, then it suffices to show that a is a prime ideal. Then the ideal generated by a, $(a) \neq R$ since a is not a unit. So there is a maximal ideal M where $(a) \subseteq M \subsetneq R$.

Since R is a PID, $M = (b)$ for some $b \implies (a) \subseteq (b) \implies a = bc$ for some c. $(b) \neq R$ so b is not a unit. Since a irredcible, c has to be a unit. So $b = c^{-1}a \implies b \in (a) \implies (b) \subseteq (a)$, so $(a) = (b)$, so (a) maximal and therefore prime. ■

Proposition. Every prime ideal is maximal in a PID.

Proof. If $I = (a)$ prime, then $(a) \subseteq M \subsetneq R$ where M is maximal, then let $M = (b) \implies a \in (b) \implies a = bc$. a is prime so it is irredcible, so c is a unit. So $b \in (a) \implies (a) = (b) \implies (a)$ maximal. ■

2.7 Unique Factorization Domains (UFDs)

Definition. Let R be an integral domain. For $a,b \in R$, we say a,b **associates** if $(a) = (b)$. Note: $(a) = (b) \iff a = bu$.

Proof. $\impliedby$: $(a) \subseteq (b)$ and $b = u^{-1}a \implies (b) \subseteq (a)$.

$\implies$: $a = bx$ and $b = ay \implies a = axy \implies a(1-xy) - 0 \implies (1-xy) = 0 \implies x$ is a unit. ■

Definition. If R is an integral domain, then R is a **unique factorization domain** (UFD) if every non-zero $x \in R$ can be written as a unique product of irreducible elements (up to associates and reordering).

Example. If $x = a_1 \cdots a_r = b_1 \cdots b_m$. Then a_i, b_j all irreducible, and $r = m$ and after reordering, a_i and b_j are associate.

Example. For $\mathbb{Z}$, the units are ± 1. Prime elements are $\{\pm p \bigm| p \text{ prime}\}$. $\mathbb{Z}$ is UFD.

Example. $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

Proposition. Integral Domain R is a UFD $\iff$

1. Every irreducible element is prime.
2. R satisfies the ascending chain condition for principle ideals. Namely, $(a_1) \subseteq (a_2) \subseteq \cdots \subseteq (a_m) \subseteq \cdots$, and $\exists (a_n) = (a_{n+1}) = \cdots$

Proof. $\implies$: First assume R is a UFD.

(1). If $a \in R$ irreducible and $a \mid bc$, so for $bc = ax$, write b, c, x as a product of irreducible elements, where $b = q_1 \cdots q_l, c = y_1 \cdots y_t, x = x_1 \cdots x_k$. So $bc = ax \implies q_1 \cdots q_l y_1 \cdots y_t = ax_1 \cdots x_k$. Since R UFD, $\exists q_i$ or y_i associate to a. Assume WLOG $uq_i = a$ for a unit a, so $u^{-1}a = q_i \mid b \implies b = b'u'a \implies a \mid b$

(2). $(a) \subseteq (b) \iff b \mid a$. If $(a) \subsetneq (b)$, then $a = bc$, where c is a non-unit. So the number of irreducible factors of b <number of irreducible factors of a, so there can't be infinitely many strict inclusion in the chain.

Conversely, assume (1) and (2) holds. To show the existnece of factorization, let for a not unit and cannot be written as product of irreducible elements, let $S = \{(a)\}$. We want to show that S is empty using Zorn's lemma. Since S is a partially ordered set (by inclusion), every ascending chain has an upper bound, so by Zorn's lemma, S has a maximal element (a).

Then when a is not a unit and not irreducible (and since $(a) \in S$), so $a = bc$), where $a = bc, b, c$ not unit. Thus $(a) \subsetneq (b)$ and $(a) \subsetneq (c) \implies (b), (c) \notin S$. So b and c are products of irreducible elements, so a is a product of irredcible elements, which is a contradiction.

Uniqueness: Suppose $a = x_1 \cdots x_n = y_1 \cdots y_m$, where x_i, y_j irreducible. Then $y_1 \mid x_1 \cdots x_n$ and y_i prime $\implies y_1 \mid x_i$ for some i. So, $x_i = uy_1$ and x_i irreducible $\implies u$ is a unit, so y_1, x_i associates.

■

Theorem. Every PID is a UFD.

Proof. (1) It is proved that every irreducible element is prime.

(2) If $(a_1) \subset (a_2) \subset \cdots$. Let $I = \bigcup (a_i)$, then I is an ideal. Since R is a PID, we want $I = (b)$. Since $b \in I, \exists i$ such that $b \in (a_i)$, so $(b) \subseteq (a_i)$. But $(a_i) \subseteq (b)$, so $(a_i) = (b)$, so $(a_i) = (a_{i+1}) = (a_{i+1}) = ...$ ■

<u>Remark:</u> Fields $\subset$ Euclidean Rings $\subset$ PIDs $\subsetneq$ UFDs $\subsetneq$ integral domains $\subset$ rings.

Definition. If R is an integral domain and $a, b \in R$. Then d is the **greatest common divisor** of a, b if

- $d \mid a$ and $d \mid b$.
- If $d' \mid a$ and $d' \mid b$, then $d' \mid d$

<u>Fact:</u> In a UFD, gcd exists.

For $a = a_1 \cdots a_t a_{t+1} \cdots a_n, b = b_1 \cdots b_t b_{t+1} \cdots m$, a_i, b_j irreducible, we can rearrage it so that a_i, b_i associates for $1 \leq i \leq t$, and otherwise they don't associate. So $\gcd(a, b) = a_1 \cdots a_t$.

<u>Remark:</u> In $\mathbb{Z}[\sqrt{5}]$, the gcd does not exist.

<u>Fact:</u> In a PID, $\gcd(a, b)$ is a "linear combination" of a, b.

If $(a, b) = (d)$, then $d \mid a$ and $d \mid b$ and if $d' \mid a$ and $d' \mid b$, then $(a, b) \subseteq (d') \implies (d) \subseteq (d') \implies d' \mid d$

2.8 Euclidean Domains

Definition. An *integral domain* R is a **Euclidean domain** if there is a map $d : R \setminus \{0\} \longrightarrow \mathbb{Z}_+$ such that

- if $a, b \in R$, $b \mid a$, then $d(b) \leq d(a)$
- If $a, b \in R \setminus \{0\}, \exists t, r \in R$ such that $a = tb + r$, where $r = 0$ or $d(r) < d(b)$

Example.

- $R = \mathbb{Z}, d(a) = |a|$.
- If $\mathbb{R} = F[x]$ where f is a field, then $d(f(x))$= deg(f).
- For any field F, $d(a) = 0 \, \forall a \in F \setminus \{0\}$.

Proposition. Euclidean domains are PIDs

Proof. If $\{0\} \notin I \subsetneq R$ is an ideal, then let $a \in I$ be a non-zero element with the smallest degree. We want to claim that $I = (a)$.

If $0 \leq b \in I$, we write $b = at + r, r = 0$ or $d(r) < d(a)$. But $r = b - at \in I$, so $d(r) \geq d(a)$, so it has to be that $r = 0$, so $b \in (a)$. ■

Example. $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ is an Euclidean domain.

Proof. Let $d : \mathbb{Z}[i] - \{0\} \longrightarrow \mathbb{Z}_+$ be $d(a + bi) = a^2 + b^2$.

d is multiplicative: $d((a + bi)(a' + b'i)) = d((aa' - bb') + (ab' + a'b)i) = (a^2 + b^2)(a'^2 + b'^2) = d(a + bi)d(a' + b'i)$.

(1): If $a = bc$, where $a, b, c \neq 0$, then $d(a) = d(b)d(c) \geq d(b)$.

(2): Suppose $x, y \in \mathbb{Z}[i]$ and we want to divide x by y. If $y = n \in \mathbb{Z}_+$, $x = a + bi$ and I write $a = nq + r, r = 0$ or $|r| < n$ and $b = nq' + r, r' = 0$ or $|r'| < \frac{n}{2}$. This is possible since if $a = nq + r$, $\frac{n}{2} \leq r < n$, then $a = n(q + 1) + (r - n), |r - n| < \frac{n}{2}$.

Then $x = a + bi = (nq + r) + i(nq' + r') = n(q + iq') + (r + ir')$, and $d(r + ir') = r^2 + r'^2 < \frac{n^2}{4} + \frac{n^2}{4} = \frac{n^2}{2} < n^2 = d(n)$.

Now suppose we are dividing x by an arbitary y, and we use the previous result by letting $n = y\bar{y} = d(y) > 0$. So we can divide $x\bar{y}$ by n where

$$x\bar{y} = qn + r, \qquad d(r) < d(n) \implies x\bar{y} = q\bar{y}y + r$$

Then claim that $x = qy + (x - qy)$, where $d(x - qy) < d(y)$. Notice that

$$d(x - qy)d(\bar{y}) = d(x\bar{y} - qy\bar{y}) = d(r) < d(n) = d(y)^2 \implies d(x - qy) < d(y)$$

Thus, this result holds. ■

Example. This is not unique. $3 = (1 + i)(1 - i) + 1, d(1) < d(1 - i)$. Also $3 = (2 - i)(1 - i) - i$, $d(-i) < d(1 - i)$

Remember that gcd exists in any UFD. So if $d = gcd(a, b)$, then $d \mid a, d \mid b$ and $d' \mid a, d' \mid b \implies d' \mid d$.

IF R is a PID, $\exists x, y \in R, d = ax + by$.

If R is a Euclidean Domain, and $a, b \in R \neq 0$, I can find the gcd using the following algorithm

$$\begin{aligned}
a &= bq_0r_0 && \implies gcd(a,b) = gcd(b, r_0) \\
b_0 &= r_0q_1 + r_1 && \implies gcd(b, r_0) = gcd(r_0, r_1) \\
&\vdots \\
r_{n+1} &= r_{n+2}q_{n+3} + 0 && \implies gcd = r_{n+2}
\end{aligned}$$

2.9 Polynomial Rings

Definition. For any commutative ring R, we define a **polynomial ring**

$$R[x] = \{a_0 + ... + a_nx^n \mid a_i \in R\}$$

If $f(x) = a_nx^n + ... + a_1x + a_0$, where a_n is the **leading coefficient**, n is the **degree** of $f(x)$, and a_0 is the **constant term**. If $a_n = 1$, then $f(x)$ is **monic**.

Division Algorithm: If R is an integral domain and non-zero $f(x), g(x)$ with $g(x)$ monic, then there are unique polynomials $q(x), r(x) \in R[x]$ such that $f(x) = g(x)q(x) + r(x)$, where $r = 0$ or $deg(r) < deg(g)$.

Proof. For existence, let n be degree of f and m be degree of g, proceed by induction on n.

If $n = 0$, then $f(x) = g(x) \times 0 + f(x)$. $deg(f) = 0 < deg(g)$ if g is non-constant. If g is a constant $= b_0 \neq 0$, then $a_0 = b_0\frac{a_0}{b_0} + 0$, so still $deg(r) < deg(g)$. Note that $b_0 = 1$ since g monic.

If the statement holds for $deg(f) < n$, I can write $f(x) = a_nx^n + ... + a_0, g(x) = x^m + ... + b_0$. Let $f_1(x) = f(x) - a_nx^{n-m}g(x)$. Clearly, since $deg(f_1) < n$, by induction hypothesis, I can write $f_1(x) = g(x)q_1(x) + r_1(x)$, with $r_1 = 0$ or $deg(r_1) < deg(g)$. So rewriting,

$$\begin{aligned}
f(x) &= f_1(x) + a_nx^{n-m}g(x) \\
&= g(x)q_1(x) + r_1(x) + a_nx^{n-m}g(x) \\
&= g(x)\underbrace{q_1 + a_nx^{n-m}}_{q(x)} + r_1(x)
\end{aligned}$$

Uniqueness: $f = gp_q + r_1 = gq_2 + r_2 \implies g(q_1 - q_2) = r_2 - r_1$. Suppose they are not equal. Clearlyt $deg(r_1 - r_2) < deg(g)$. Also, $deg(g(q_1 - q_2) \geq deg(g)$ since R is a UFD (so $deg(f) + deg(g) = deg(fg)$). This is a contradiction unless both sides are 0, so $q_1 = q_2$ and $r_1 = r_2$

■

Remark: If F is a field, the same argument shows for any non-zero $f(x), g(x) \in F[x]$.

Corollary. If R is an integral domain, $f(x) \in R[x]$ and $a \in R$. Then $f(a) = 0 \iff x - a \mid f(x)$

Proof. Suppose $f(a) = 0$. Write $f(x) = (x - a)q(x) + r(x)$, where $r = 0$ or $deg(r) \leq 0 \implies f(a) = r$. So $f(a) = 0 \iff r = 0$ ■

Corollary. If R is an integral domain and $f(x) \in R[x]$ has degree n, then $f(x)$ has $\leq n$ zeros.

Example. It is important for this to satisfy integral domain property. In $\mathbb{Z}_8$, $f(x) = x^2 - 1$ has roots $1, 3, 5, 7$

Corollary. If F is a field, $F[x]$ is a Euclidean domain.: $d(f(x)) = deg(f)$. So $F[x]$ is a UFD.

Definition. Let R be a UFD. For non-zero $a_1, ..., a_n \in R$, $d = \gcd(a_1, ..., a_n)$ exists, where a_n is unique up to associates. Then for $f(x) = a_n x^n + ... + a_1 x + a_0 \in R[x]$, the **content** of $f(x), c(x) := \gcd(a_n, ..., a_1, a_0)$. And f is **primitive** if $c(f)$ is a unit.

Lemma. $c(fg) = c(f)c(g)$ up to units.

Proof. Case I: Suppose f, g primitive, want to show that fg is primitive. If $f = a_n x^n + ... + a_1 x + a_0, g = b_m x^m + ... + b_1 x b_0$, then $fg = c_{n+m} x^{n+m} + ... + c_1 x + c_0$. If fg is not primitive, $\exists$ prime $p \in R$ such that $p \mid c_i \forall i$. However, f, g primitive. Suppose i_0 is the smallest i such that $p \nmid a_i$ and j_0 be the smallest j such that $p \nmid b_j$. Then $p \nmid c_{i_0+j_0}$, where $c_{i_0+j_0} = a_0 b_{i_0+j_0} + ... + a_{i_0-1} b_{j_0+1} + a_{i_0} b_{j_0} + ... + a_{i_0+j_0} b_0$. This is a contradiction.

Case II: Let f, g be arbitrary. Let $f = c(f) f_1, g = c(g) g_1$, with f_1, g_1 primitive so $f_1 g_1$ primitive. So $fg = c(f)c(g) f_1 g_1 \implies c(fg) = c(f)c(g)$ ■

Lemma. If F is the quotient field of R and $f(x) \in R[x]$ is primitive, then $f(x)$ irreducible in $R[x] \iff f(x)$ irreducible in $F[x]$

Proof. $\Longleftarrow$: Suppose $f(x)$ not irreducible in $R[x]$, then $f(x) = f_1(x) f_2(x)$ for f_1, f_2 non-units in $R[x]$. If $deg(f_1) = 0$, then it is a constant $c \implies f = c f_2 \implies c \mid f \implies c$ unit since f primitive, a contradiction.

Then suppose $deg(f_2), deg(f_1) \geq 1$. Since units of $F[x]$ are non-zero constants, $f(x)$ not irreducible.

$\Longrightarrow$: Suppose $f(x) \in R[x]$ can be written as $f = f_1 f_2, f_1, f_2 \in F[x], deg(f_1, f_2) \geq 1$. Write $f_1 = \frac{b_n}{c_n} x^n + ... + b_0 c_0, \quad b_i, c_i \in R$. So if $r_1 = c_1 \cdots c_n \in R$, then $r_1 f_1 \in R[x]$. Let $g = c f_1$. Similarly there is $r_2 \in R$ such that $g_2 = r_2 f_2 \in R[x] \implies g_1 g_2 = r_1 r_2 f_1 f_2$. So $g_1 = c(g_1) h_1, g_2 = c(g_2) h_2$ with $h_1, h_2 \in R[x]$ primitive. So $c(g_1) c(g_2) h_1 h_2 = r_1 r_2 f \implies$ taking contents, $c(g_1) c(g_2) = r_1 r_2$ up to units.

So $ucc(g_1) c(g_2) = r_1 r_2$ for unit u, so $u h_1 h_2 = f \implies (u h_1) h_2 = f$. Combining with $deg(h_1) = deg(g_1) = deg(g_1) \geq 1$, we have f irreducible in $R[x]$. ■

Example. $f(x) = 2x + 2 \in F[x]$ is irreducible in $\mathbb{Q}[x]$ but not in $F[x]$

Theorem. If R is a UFD, then $R[x]$ is a UFD.

Proof. Case 1: If $f(x)$ primitive, then $f(x) \in F[x]$ can be written as $f(x) = f_1(x) \cdots f_n(x)$, where $f_i(x)$ irreducible in $F[x]$. $\exists b_i \in R$ such that $b_i f_i(x) = g_i(x) \in R[x]$.

Then, let $c_i = c(g_i) \implies c_i h_i(x) = b_i f_i(x)$ for some $h_i(x)$ primitive in $R[x]$. Write this as $f_i = \frac{c_i h_i}{b_i}$, so $b_1 \cdots b_n f(x) = c_1 \cdots c_n h_1(x) \cdots h(x)$. Therefore, $b_1 \cdots b_n = c_1 \cdots c_n$ up to units, so $c_1 \cdots c_n = u b_1 \cdots b_n$, so $f(x) = u h_1(x) \cdots h_n(x)$

Uniqueness: If $f(x) = p_1 \cdots p_n(x) = q_1(x) \cdots q_m(x)$, where p_i, q_j irreducible in $R[x]$. Then $f(x)$ primitive $\implies p_i, q_j$ primitive $\forall j \implies$ by the lemma, p_i, q_j irreducible in $F[x] \forall i, j$. Since $F[x]$ is a UFD, $n = m$, $p_{-} = q_j$ up to reordering and multiplying So $p_i = \frac{a_i}{b_i} q_i$, $a, b \in R \implies$

$b_i p_i(x) = a_i q_i(x) \implies$ by p_i, q_i primitive that $b_i = a_i$ up to a unit, $b_i = u_i a_i \implies u_i p_i = q_i \implies p_i = q_i$ up to unit.

Case 2: Let $f(x) \in R[x]$ be arbitrary, let $c = c(f) \implies f(x) = cg(x)$, where $g(x)$ is primitive. From case 1, we can write $g(x) = g_1(x) \cdots g_n(x)$, where $g_i \in R[x]$ irreducible. Then $f(x) = cg_1(x) \cdots g_n(x)$.

When we factor c in R, $c = c_1 \cdots c_m \implies f(x) = c_1 \cdots c_m g_1(x) \cdots g_n(x)$, all irreducible in $R[x]$.

Uniqueness: Suppose $f(x) = f_1 \cdots f_n = g_1 \cdots g_m$, where $f_i, g_j \in R[x]$ irreducible. Consider cases when their degree is 0 and greater than 0. ■

Corollary. If R UFD, then $R[x_1, ..., x_n]$ is a UFD for $n \geq 1$.

2.10 Eisenstein Criterion for Irreducibility

Let R be UFD, $f(x) = a_n x^n \cdots + a_1 x + a_0 \in R[x]$, $n \geq 0, a_n \neq 0$.

Theorem. If p is a prime element in R such that

- $p \mid a_i, 0 \leq i < n$
- $p \nmid a_n$
- $p^2 \nmid a_0$

Then, $f(x)$ is irreducible.

Example. $x^2 + y^2 + 1 \in \mathbb{C}[x, y]$ is irredcible

Proof. Consider $R = \mathbb{C}[x]$ as a UFD and $\mathbb{C}[x, y] = \mathbb{C}[x][y]$. Rewrite as $y^2 + (x+1)(x-i)$, where $(x+1)(x-i)$ irreducible in $R = \mathbb{C}[x]$. We have $x + i \mid x^2 + 1, x + i \nmid 1, (x^2+1)^2 \nmid x^2 + 1 \implies x^2 + y^2 + 1$ irreducible. ■

Example. $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 \in \mathbb{Z}[x]$ is irreducible for p prime.

Proof. Consider $f(x+1) = (x+1)^p + (x+1)^{p-2} + ... + (x+1) + 1$.

$$\begin{aligned} f(x+1) &= \sum_{i=0}^{p} (x+1)^i \\ &= \sum_{i=0}^{p-1} \sum_{j=0}^{i} \binom{i}{j} x^j, \qquad 0 \leq i \leq p-1, 0 \leq j \leq i \\ &= \sum_{j=0}^{p-1} \left(\sum_{i=j}^{p-1} \binom{i}{j} \right) x^j \end{aligned}$$

Set $c_j = \sum_{i=j}^{p} \binom{i}{j}$, and I claim that $p \mid c_j, c_{p-1} = \binom{p-1}{p-1} = 1$. Using the identity $\binom{j}{j} + \cdots + \binom{m}{j} = \binom{m+1}{j+1}$, $c_j = \binom{p}{j+1} = \frac{p!}{(j+1)!(p-j-1)!}$. Also $c_0 = \binom{p}{1} = 1$, so $p^2 \nmid c_0$. Therefore by eisenstein criterion, $f(x+1)$ irreducible, so $f(x)$ irreducible. ■

Proof of Eisenstein Criterion. If $f(x) = g(x)h(x)$ non-units with $g(x) = b_r x^r + \cdots b_1 x + b_0, h(x) = c_k x^k + \cdots c_1 x + c_0$. If $deg(g) = 0, g(x) = b_0$ and $b_0 \mid a_i \forall i \implies$ since f primitive, b_0 is a unit, a contradiction.

So assume $r \geq 1$. Then $p \mid a_0 = b_0 c_0, p^2 \nmid b_0 c_0 \implies$ either $p \mid b_0, p \nmid c_0$ or $p \nmid b_0, p \mid c_0$. Also, $p \nmid a_n = b_r c_k \implies p \nmid b_r$

Now, let $i \geq 1$ be the smallest number such that $p \nmid b_i$, and we have $i \leq r > n$. Then $a_i = b_0 c_i + b_i c_{i-1} + ... + b_{i-1} c_1 + b_i c_0$. However, $p \mid a_i$ and $p \mid b_0 c_i + b_i c_{i-1} + ... + b_{i-1} c_1 \implies p \mid b_i c_0 \implies p \mid b_i$ or $p \mid c_0$, both not true. Therefore contradiction. ■

3 Modules

Definition. Suppose we have arbitrary ring R and abelian group M such that there is $R \times M \to M$, $(r, m) \mapsto rm$ with distributivity. This is a **left module**, and satisfies the distributivity below:

- $(r + s)m = rm + sm$
- $r(m_1 + m_2) = rm_1 + rm_2$
- $(rs)m = r(sm)$
- $1_R m = m$

Fact: If R is a field, then this is a vector space.

Modules also satisfy the following properties:

- $r0_M = 0_M$
- $0_R m = 0_M$
- $(-r)m = -(rm)$

Definition. If $\emptyset \neq N \subset M$, then N is a **submodule** if it is a subspace of M and $r \in R, n \in N \implies rn \in N$.

Example.

- Let R be a ring and R be a module over R. Submodules are (left) ideals in this case.
- Every abelian group is a module over $\mathbb{Z}$. Then submodules correspond to subgroups.

Definition. If M, N are R modules, then $f : M \to N$ is a R-**homomorphism** if f is a group homomorphism and $f(rm) = rf(m) \forall r \in R, m \in M$. Note that $ker(f) \subset M$ as a submodule, and $im(f) \subseteq N$ as a submodule.

Remark: If f is an isomorphism, $f^{-1} : N \to M$ is also a R-homomorphism.

3.1 Isomorphism Theorems

If $N \subseteq M$ is a submodule, then M/N has the structure of a R-module.

$$r(m + N) := rm + N$$

well-defined: Does $m + N = m' + N \implies r(m + N) = r(m' + N)$?. yes, because $m - m' \in N$ and $r(m - m') \in N$

Isomorphism Theorem 1: If $f : M \to N$ is a R-homomorphism, then

$$M/\ker(f) \simeq im(f) \text{ as } R\text{-modules}$$

Theorem 2: If N_1, N_2 are submodules of M, then $N_1 + N_2 := \{x + y \mid x \in N_1, y \in N_2\}$ is a submodule of M, and $N_1 \cap N_2$ is also a submodule of M, and

$$\frac{N_2}{N_1 \cap N_2} \simeq \frac{N_1 + N_2}{N_1}, \quad f : N_2 \to \frac{N_1 + N_2}{N_1},\ f(n_2) = n_2 + N_1$$

Theorem 3: If $N \subseteq M$ and $K \subseteq N$ are submodules, then N/K is a submodule of M/K, and

$$\frac{M/K}{N/K} \simeq M/N$$

Theorem 4: If $N \subseteq M$ is a submodule, the canonical map $M \to M/N, m \mapsto m + N$ induces a 1-1 correspondence between submodules of M/N and submodules of M containing N

3.2 Direct Product and Sum of Modules

Let R be an arbitray ring and $\{M_i\}_{i\in\mathcal{I}}$ be a family of R-modules. The **direct product** is defined as

$$\prod_{i\in\mathcal{I}} M_i = \{(x_i)_{i\in\mathcal{I}} \mid x_i \in M_1\},\ r(x_i)_{i\in\mathcal{I}} = (rx_i)_{i\in\mathcal{I}}$$

Direct Sum is defined $\bigoplus_{i\in\mathcal{I}} M_i = \{(x_i)_{i\in I} \mid x_i \in M_i, \text{all but finitely zero}\}$

Remark: If M is a module and $N_1, N_2 \subseteq M$ are submodules such that

- $M_1 \cap M_2 = \{0\}$
- $M_1 + M_2 = M$

Then $M \simeq M_1 \oplus M_2 \simeq M, (m_1, m_2) \mapsto m_1 + m_2$.

3.3 Exact Sequences

Definition. Let R be a ring and M, M', M'' be R-modules. A sequence of R-homomorphism $M' \xrightarrow{f} M \xrightarrow{g} M''$ is called **exact** if $im(f) = ker(g)$. More generally, sequence $M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3$ is **exact** if $im(f_i) = ker(f_{i+1})$.

Example. The sequence $0 \to M' \xrightarrow{f} M$, is *exact* if and only if f is injective.

Example. The sequence $M \xrightarrow{g} M'' \to 0$ is *exact* if and only if g is surjective

Definition. If $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ is an exact sequence, then it is called a **short exact sequence**

Example. If $N \subseteq M$ is a submodule, $0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0$.

Proposition. Let $0 \longrightarrow M' \underset{\psi}{\overset{f}{\rightleftarrows}} M \underset{\phi}{\overset{g}{\rightleftarrows}} M'' \longrightarrow 0$ be a short exact sequence of R-modules. Then the following conditions are equivalent.

1. $\exists$ R-homomorphism $\phi : M'' \to M$ such that $g \circ \phi = id_{M''}$
2. $\exists$ R-homomorphism $\psi : M \to M'$ such that $\psi \circ f = id_{M'}$

and they imply $M \simeq M' \oplus M''$. In this case, we say the sequence **splits**

Example. $R = \mathbb{Z}_4, M = \mathbb{Z}_4, N = \{0, 2\}$. Then $0 \to N \to \mathbb{Z}_4 \to \mathbb{Z}_4/N \to 0$. Notice that $\psi(1) = 0 \implies \psi(2) = 0$ and $\psi(1) = 2 \implies \psi(2) = 0$. Therefore this does not split.

Proof of Proposition. $(1) \implies (2)$: If $m \in M$, then $g(\phi(g(m))) = g(m) \implies g(m - \phi(g(m))) = 0 \implies m - \phi(g(m)) \in ker(g) = im(f) \implies \exists! x \in M'$ such that $f(x) = m - \phi(g(m))$.

Let $\psi(m) = x$. We need to check that ψ is a R-homomorphism (exercise), and $\psi \circ f = id_{M'}$: if $y \in M'$, let $m = f(y)$. Then $m - \phi(g(m)) = f(y) - \phi(\underbrace{g(f(y))}_{=0}) = f(y)$. By definition of $\psi : \psi(m) = y \implies \psi(f(y)) = y \, \forall y$

$(2) \implies (1)$: Suppose $x \in M''$, then $\exists y \in M$ such that $g(y) = x$. Then let $\phi(x) = y - f(\psi(y))$.

This is well-defined: If $y' \in M$ such that $g(y') = x$. I want to check that $y - f(\psi(y)) = y' - f(\psi(y'))$, or $y - y' = f(\psi(y - y'))$. But $g(y - y') = 0$. Since $\ker(g) = im(f)$, $\exists z \in M'$ such that $y - y' = f(z) \implies f(\psi(y - y')) = f(\psi(f(z))) = f(z) = y - y'$. So ϕ well-defined.

Also $g \circ \phi = id_{M''}$: If $x \in M''$, $\phi(x) = y - f(\psi(y))$ for some $y \in M$ with $g(y) = x$, so $g(\phi(x)) = g(y) - g(f(\psi(y))) = g(y) = x$, since $g \circ f = 0$. Also ϕ is a R-homomorphism, since $\forall r, s \in R, x_1, x_2 \in M'', \phi(rx_1 + sx_2) = r\phi(x_1 + s\phi(x_2))$.

Direct Sum: Define

$$M' \oplus M'' \xrightarrow{\alpha} M, (x, y) \mapsto f(x) + \phi(x)$$

$$M \xrightarrow{\beta} M' \oplus M'', m \mapsto (\psi(m), g(m))$$

Then $\beta \circ \alpha(x, y) = \beta(f(x) + \phi(y)) = (x, y)$, since $\psi \circ \phi = 0$ (Show this as an exercise:) ■

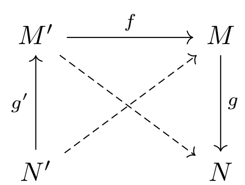
3.4 Module Homomorphism

Definition. Let M, N be R-module, with $Hom_R(M, N)$ being the **set of R-homomorphism** $f : M \longrightarrow N$, and $Hom_R(M, N)$ has the structure of an R-module.

Let $f, g \in Hom_R(M, N)$ if $f + g \in Hom_R(M, N)$. Note $(rf)(m) = rf(m), (f + g)(m) = f(m) + g(m)$. We have

$$Hom_R(M, N) \xrightarrow{- \circ f} Hom_R(M', N)$$

$$Hom_R(N, M') \xrightarrow{f \circ -} Hom_R(N, M)$$

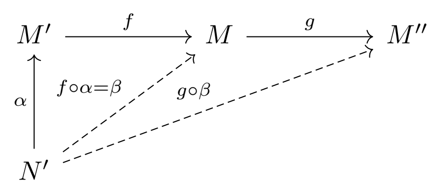


Lemma. If $0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ is a short exact sequence of R-modules and N is a R-module, then

(1). $0 \to Hom_R(N, M') \xrightarrow{\psi} Hom_R(N, M) \xrightarrow{\phi} Hom_R(N, M'')$ exact

(2). $0 \longrightarrow Hom_R(M'', N) \longrightarrow Hom(M, N) \longrightarrow Hom(M', N)$ exact

Proof.



$Hom_R(N, M') \to_R Hom(N, M)$ injective: If $f \circ \alpha = 0$ for some $\alpha \in Hom_R(N, M')$, then since f injective, $\alpha = 0$.

$\phi \circ \psi = 0(\implies im(\psi) \subset ker(\phi))$: If $\alpha \in Hom_R(N, M')$, then $\phi \circ \psi(\alpha) = g \circ f \circ \alpha = 0$, where $g \circ f = 0$ since it is exact.

If $\beta \in \ker(\phi)$, then $g \circ \beta = 0$, so for any $x \in N, g(\beta(x)) = 0$, so $\beta(x) \in im(f) \implies$ there is a unique $y \in M'$ such that $f(y) = \beta(x)$. Let $\alpha : N \to M'$ be defined by $\alpha(x) = y$, then α is a R-homomorphism (Exercise). And clearly $\beta = f \circ \alpha$, so $\beta \in im(\psi)$ ■

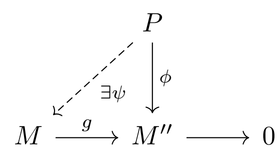
Remark: If $M' \subseteq M$ is a submodule, then $0 \to M' \to M \to M/M'$ is a short exact sequence. If $g : M \to M''$ is a surjective R homomorphism, then $0 \to ker(g) \to M \to M'' \to 0$ is a short exact sequence.

3.5 Free Module

Definition. If M is a R-module, and $S \subset M$ is a **basis** if $\forall m \in M, m = r_1 s_1 + ... + r_k s_k$ in a *unique* way with $r \in R, s \in S$. Equivalently, if $0 = r_1 s_1 + ... + r_k s_k$, then $r_1 = ... = r_k = 0$. If $\{s_i\}_{i \in \mathcal{I}}$ is a basis for M, then $M \simeq \bigoplus_{i \in \mathcal{I}} R$. Then, M is **free** is it has a *basis*.

Definition. If R is a ring and P is a R-module, then P is a **projective module** if it satisfies the following:

1. If g, ϕ are R homomorphism, $\exists \psi : P \to M$, R-homomorphism such that $g \circ \psi = \phi$

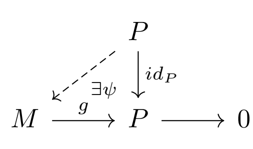


2. If $0 \to M' \to M \to P \to 0$ is exact, then it splits.
3. There is a R-module N such that $N \oplus P$ is a *free module*.
4. If $0 \to M' \to M \to M''$ is exact, then

$$0 \to Hom(P, M') \to Hom(P, M) \to Hom(P, M'') \to 0$$

is exact.

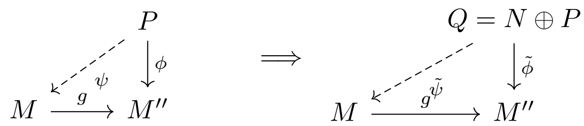
(1) $\implies$ (2). If $0 \to M' \to M \to P \to 0$ is exact, then by (1) $\exists \psi : P \to M$ such that $g \circ \psi = id_P$, so the sequence splits



■

(2) $\implies$ (3). Let $\{x_i\}_{i \in \mathcal{I}}$ be a generating subset of P as a R-module. Then, $g : \bigoplus_{i \in I} R \to P, (r_i)_{i \in I} \mapsto \sum_{i \in I} r_i x_i$. is surjective. Then, $0 \to ker(g) \to \bigoplus_{i \in I} R \to P \to 0$ is a short exact sequence. By (2) this splits, so free R-module $\bigoplus_{i \in I} R \simeq ker(g) \oplus P$. ■

(3) $\implies$ (4). It is enough to show that $Hom(P, M) \to Hom(P, M'')$ is surjective. If P is free and $(x_i)_{i \in I}$ is a basis for P and let $y_i = \phi(x_i)$ and $z_i \in m$ such that $g(z_i) = y_i$. Then let $\psi(x_i) = z_i$ and $\psi(\sum r_i x_i) = \sum r_i z_i$. Then $g \circ \psi = \phi$. If $N \bigoplus P$ is free, then $\tilde{\phi}(r, p) = \phi(p)$ is a R homomorphism, $\exists \tilde{\psi} : N \oplus P \to M$ such that $g \circ \tilde{\psi} = \tilde{\phi}$. Define $\psi : P \to M, \psi(p) = \tilde{\psi}(n, p)$, then $g \circ \psi = \phi$.



■

(4) $\implies$ (1). The surjective map $g : M \to M'$ gives a short exact sequence $0 \to ker(g) \to M \to M'' \to 0$. So by (4) there is a surjective map $Hom(P, M'') \to Hom(P, M)$. This is exactly 1. ■

Example. $R = \mathbb{Z}_6$. Let $\mathbb{Z}_6$ be a $\mathbb{Z}_6$-module and $I_1 = \{0, 3\}, I_2 = \{0, 2, 4\}$. Then $I_1 \cap I_2 = \{0\}$ and $I_1 + I_2 = \mathbb{Z}_6 \implies \mathbb{Z}_6 = I_1 + I_3$. So by 3, I_1, I_2 are projective modules but not free.

3.6 Finitely Generated Modules over PIDs

Theorem. If R is a PID and M is a finitely generated module over R, then

$$M \simeq R \oplus \cdots \oplus R \oplus \frac{R}{p_1^{n_1}} \oplus \cdots \oplus \frac{R}{p_k^{n_k}}$$

where $p_1, ..., p_k$ are irredcible (prime) elements of R. In particular, finitely generated projective modules are free over R.

Let R be an integral domain and M be a R-module, $m \in M$. m is torsion if there is $0 \neq r \in R$ such that $rm = 0$. So let M_{tor} be set of torsion elements in M, so M_{tor} is a submodule, where $m_1, m_2 \in M_{tor} \implies m_1 + m_2 \in M_{tor}$. M is torsion if $M = M_{tor}$, and if torsion-free if $M_{tor} = \{0\}$. Free modules are torsion-free.

Recall that for abelian groups, torsion free does not imply free, take $\mathbb{Q}$ as example. Meanwhile, torsion free and finitely generated implies free group.

However in arbitrary integral domain, torsion free and finitely generated does *not* imply free group. One example would be $R = \mathbb{C}[x, y], M = (x, y)$ [proof of example not written down]

Fact: Suppose R is a PID

- A submodule of a finitely generated R-module is finitely generated
- If M is finitely generated R-module, then $M \simeq M_{tor} \oplus N$ for a free R-module N.

Note, making it a PID makes everything similar to $\mathbb{Z}$

3.7 Tensor Products

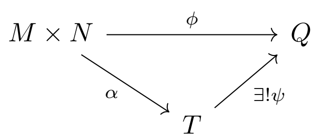
Let R be a ring and M, N be R-modules. Let F be a free module generated by elements $(m, n), m \in M, n \in N$. $F = \{r_1(m_1, n_1) + ... + r_k(m_k, n_k) \,|\, r_i \in R, m_i \in M, n_i \in N\}$. D is the submodule of F generated by elements of the forms below

- $(m_1 + m_2, n) - (m_1, n) - (m_2, n)$,
- $(m, n_1 + n_2) - (m, n_1) - (m, n_2)$
- $(rm, n) - r(m, n)$
- $(m, rn) - r(m, n)$

with $r \in R, m, m_1, m_2 \in M, n, n_1, n_2 \in N$.

Let $T := F/D$ be an R-module. Note there is a map $\alpha : M \times N \longrightarrow T, \alpha(m, n) = (m, n) + D$. This map is bilinear: $\alpha(r_1 m_1 + r_2 m_2, n) = r_1 \alpha(m_1, n) + r_2 \alpha(m_2, n)$ and $\alpha(m, r_1 n_1 + r_2 n_2) = r_1 \alpha(m, n_1) + r_2 \alpha(m, n_2)$

Proof of above requires us to show $(r_1 m_1 + r_2 m_2, n) - r_1(m_1, n) - r_2(m_2, n) \in D$. Rewrite expression into $((r_1 m_1 + r_2 m_2, n) - (r_1 m_1, n) - (r_2 m_2, n)) + ((r_1 m_1, n) - r_1(m_1, n)) + ((r_2 m_2, n) - r_2(m_2, n))$



T has the following *universal property*: If Q is a R-module and $\phi : M \times N \longrightarrow Q$ is a bilinear map, then there is a unique R-homomorphism $\psi : T \to \mathbb{Q}$ with $\phi = \psi \circ \alpha$, and define $\psi((r_1(m_1, n_1) + ... + r_k(m_k, n_k)) + D) = r_1 \phi(m_1, n_1) + ... + r_k \phi(m_k, n_k)$.

We need to check that ψ is well-defined and is a R-homomorphism. For well-defined, it suffices to show that elements $\in D$.

We denote **tensor product** of M and N as $M \otimes_R N = T = F/D$. Any element is of the form

$$r_1(m_1, n_1) + ... + r_k(m_k, n_k) + D = \underbrace{(r_1 m_1, n_1) + ... + (r_k m_k, n_k) + D}_{:= r_1 m_1 \otimes n_1 + ... + r_k m_k \otimes n_k}$$

Proposition. The following properties are satisfied:

1. $m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2$
2. $(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n$
3. $(rm) \otimes n = r(m \otimes n) = m \otimes (rn)$
4. $0 \otimes n = 0 = m \otimes 0$

Example.

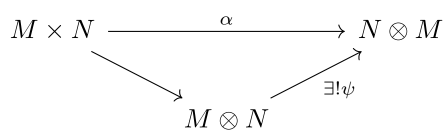
- $\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathbb{Q} = \{0\}$: $a \otimes \frac{b}{c} = a \otimes \frac{bp}{cp} = pa \otimes \frac{b}{cp} = 0 \otimes \frac{b}{cp} = 0$.
- $\mathbb{Z}_2 \otimes \mathbb{Z}_3 = \{0\} : 0 \otimes x = 0, 1 \otimes 0, 2 = 0$. Finally $1 \otimes 1 = 1 \otimes (2+2) = 2 \otimes 1 + 2 \otimes 1 = 0 + 0 = 0$.
- $gcd(m, n) = 1, \mathbb{Z}_m \otimes_{\mathbb{Z}} \mathbb{Z}_n = \{0\}$

Proposition. If M, N, P are R-modules, then

- $M \otimes_R N \simeq N \otimes_R M$
- $(M \otimes_R N) \otimes_R P \simeq M \otimes_R (N \otimes_R P)$

- $M \otimes_R (N \oplus P) \simeq M \otimes_R N \bigoplus M \otimes_R P$
- $M \otimes_R R \simeq R \otimes_R M \simeq M$

Proposition 1 Proof. $M \times N \xrightarrow{\alpha} N \otimes M$ is clearly bilinear, $(m, n) \mapsto n \otimes m$



By the universal property, we have R-homomorphism $\psi(m \otimes n) = \alpha(m, n) = n \otimes m$. Conversely, $\exists R$-homomorphism $\phi : N \otimes M \to M \otimes N$, and $n \otimes m \mapsto m \otimes n$, and $\phi \circ \psi$ and $\psi \circ \phi$ are identity maps. ■

Proposition 2 Proof. Fix $m \in M$ and define $\alpha_m : N \times P \to (M \otimes N) \otimes P, (n, p) \mapsto (m \otimes n) \otimes p$. Then, α_m is bilinear: $\alpha_m(n, p_1 + p_2) = \alpha_m(n, p_1) + \alpha_m(n, p_2)$. $\alpha_m(n_1 + n_2, p) = \alpha_m(n_1, p) + \alpha_m(n_2, p)$. $\alpha_m(m, p) = r\alpha_m(n, p)$. $\alpha_m(n, rp) - r\alpha_m(n, p)$. Together, this implies that $\exists R$-homomorphism $\psi_m : N \otimes P \longrightarrow (M \otimes N) \otimes P$.

Now, we have a bilinear map $\psi : M \times (N \otimes P) \to (M \otimes N) \otimes P, \psi(m, x) = \psi_m(x)$ and show that this is bilinear.

- $\psi(m, x_1 + x_2) = \psi(m, x_1) + \psi(m, x_2)$
- $\psi(m, rx) = r\psi(m, x)$

So ψ_m is a R-homomorphism. Also $\psi(m_1 + m_2, x) = \psi(m_1, x) + \psi(m_2, x)$ and $\psi(rm, x) = r\psi(m, x)$ so $\psi_{m_1 + m_2} = \psi_{m_1} + \psi_{m_2}$.

Since there is a bilinear map, $\exists R$-homomorphism $\gamma : M \otimes (N \otimes P) \to (M \otimes N) \otimes P, m \otimes (n \otimes p) = (m \otimes n) \otimes p$.

Similarly, there is a $R-$homomorphism $\beta : (M \otimes N) \otimes P = M \otimes (N \otimes P), (m \otimes n) \otimes p \mapsto m \otimes (n \otimes p)$. γ, β are inverse maps, so they are isomorphisms. ■

Proposition 4 Proof. There is a binear map $M \times R \xrightarrow{\alpha} M, (m, r) \mapsto rm$ bilinear. So there is an R-homomorphism $\psi : M \otimes R \to M, m \otimes r \mapsto rm$. Also there is an R-homomorphism $\phi : M \to M \otimes R, m \mapsto m \otimes 1$. $\psi \circ \phi = id, \phi \circ \psi(m \otimes r) = \phi(rm) = rm \otimes 1 = m \otimes r \implies \phi \circ \psi = id \implies \phi$ isomorphism. ■

Example. Consider $R[x] \otimes_R R[x]$, where R is a commutative ring, we claim that $R[x] \otimes R[x] \simeq R[x, y]$.

Let $\phi : R[x] \otimes_R r[x] \to R[x, y]$ be the R-homomorphism induced by the bilinear map $R[x] \times R[x] \longrightarrow R[x, y], (f(x), g(x)) \mapsto f(x)g(y)$.

To define ψ, note that $R[x, y]$ is a free module over R with basis $x^i y^j, 0 \le i, j$. Let $\psi : R[x, y] \to R[x] \otimes_R R[x]$ be such that $\psi(x^i y^j) = x^i \otimes x^j$.

ϕ, ψ are inverse maps: $x^i y^j \xrightarrow{\psi} x^i \otimes x^j \xrightarrow{\phi} x^i y^j$, $f(x) \otimes g(x) = \sum_{i,j} c_{i,j} x^i \otimes x^j, x^i \otimes x^j \xrightarrow{\phi} x^i y^j \xrightarrow{\psi} x^i \otimes x^j$.

Proposition. Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence of R-modules, and let N be an R module, then

$$M' \otimes_R N \to M \otimes_R N \to M'' \otimes_R N \to 0$$

is exact. Here, $M' \xrightarrow{f} M$ induces $M' \otimes N \xrightarrow{f \otimes id} M \otimes N$, $\sum m_i' \otimes n_i \mapsto \sum f(m_i') \otimes n_i$.

Lemma. Let M, N, Q be R modules, then $Hom_R(M \otimes_R N, Q) \simeq Hom_R(M, Hom_R(N, Q))$.

Corollary. If $Q = R$, $(M \otimes_R N)^\vee \simeq Hom_R(M, N^\vee)$.

Example. Let k be a field, $R = k[x,y]/(x,y), M = R/(x), N = R/(y)$. Then, $M \otimes_R N = R/(x) \otimes R(y) \simeq R/(x,y)$. Also, $(M \otimes_R N)^\vee \simeq (R/(x,y))^\vee = Hom_R(R/(x,y), R) = \{0\}$.

Also, $M^\vee = Hom(R/(x), R) \simeq M, N^\vee = Hom(R/(y), R) \simeq N$. Consider $\phi : R/(x) \to R, 1 \mapsto \bar{f}, 0 = \bar{x} \mapsto \overline{xf} = 0, f \in k[x,y] \implies xf \in (xy) \implies f \in (y)$.

So $M^\vee \otimes N^\vee \simeq M \otimes N \simeq R/(x,y) \neq \{0\}$.

Proposition Proof using Lemma. If $M' \to M \to M'' \to 0$ is exact, then let Q be an arbitrary R-module and take $Hom(-, Hom_R(N,Q))$. Then we have exact sequence

$$0 \to Hom(M'', Hom_R(M'', Q)) \to Hom_R(M, Hom_R(N,Q)) \to Hom_R(M'_, Hom(N,Q))$$

So we have an exact sequence

$$0 \to Hom_R(M'' \otimes N, Q) \to Hom_R(M \otimes N, Q) \to Hom_R(M' \otimes N, Q)$$

So by homework 9 question, $M' \otimes_R N \to M \otimes_R N \to M'' \otimes_R N \to 0$ is exact. ■

Example. Let $0 \to \mathbb{Z} \xrightarrow{f} \mathbb{Z} \to Z_2$ be a short exact sequence of $\mathbb{Z}$-modules and tensored with $\mathbb{Z}_2$, where $f : a \mapsto 2a$.

Then, $\underbrace{\mathbb{Z} \otimes \mathbb{Z}_2}_{\simeq \mathbb{Z}_2} \to \mathbb{Z} \otimes \mathbb{Z}_2$. [fill in from notes]

Proof of Lemma. Define $\phi : Hom_R(M \otimes_R N, Q) \to Hom_R(M, Hom_R(N,Q))$, where $(\alpha : M \otimes N \to P) \mapsto (\beta : M \to Hom_R(N,Q))$. $\beta : m \mapsto \beta_m, \beta(n) = \alpha(m \otimes n) \in Q$.

I need to show that β is R-homomorphism, ϕ is R-homomorphism.

β homomorphism: $\beta \in Hom_R(M, Hom_R(N,Q))$: Show that $\beta_{r_1 m_1 + r_2 m_2} = r_1 \beta_{m_1} + r_2 \beta_{m_2}$. So, $\beta_{r_1 m_1 + r_2 m_2}(n) = \alpha((r_1 m_1 + r_2 m_2) \otimes n) = \alpha(r_1(m_1 \otimes n) + r_2(m_2 \otimes n))$, and $(r_1 \beta_{m_1} + r_2 \beta_{m_2})(n) = r_1 \alpha(m_1 \otimes n) + r_2 \alpha(m_2 \otimes n)$, which is true

ϕ homomorphism shown similarly.

Also define $\psi : Hom_R(M, Hom_R(N,Q)) \to Hom_R(M \otimes_R N, Q)$ with $\beta : M \to Hom_R(N,Q)$ given. Define bilinear map $M \times N \to Q, (m,n) \mapsto \beta(m)(n)$, this gives a map $\alpha : M \otimes_R N \to Q$.

So ϕ, ψ are inverse maps. ■

Definition. A module F is **flat** if for any short exact sequence $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$, the following sequence is exact:

$$0 \to M' \otimes F \xrightarrow{f \otimes id} M \otimes F \xrightarrow{g \otimes id} M'' \otimes F \to 0$$

Equivalently, F is **flat** if for any R-homomorphism $f : M' \to M, M' \otimes F \to M \otimes N$ is injective.

Example. $\mathbb{Z}_2$ is not a flat $\mathbb{Z}$-module. Consider $\mathbb{Z} \to \mathbb{Z}, n \mapsto 2n$. $\mathbb{Z} \otimes \mathbb{Z}_2 \to \mathbb{Z} \otimes \mathbb{Z}_2, a \otimes b \mapsto 2a \otimes b = a \otimes 2b = 0$. Not injective, so this is not flat.

Example. Suppose R is an integral domain:

- Free modules are flat. If F is a free R-module, $F \simeq \bigoplus_{i\in I} R, f : M' \to M$ is an injective map that gives the following injectvitiy.

$$\begin{array}{ccccccc} M' \otimes F & & M' \otimes (\bigoplus_i R) & & \bigoplus_i M' \otimes R & & \bigoplus_i M' \\ \big\downarrow{\scriptstyle f\otimes id} & \simeq & \big\downarrow{\scriptstyle f\otimes id} & \simeq & \big\downarrow{\scriptstyle \bigoplus f\otimes id} & \simeq & \big\downarrow{\scriptstyle \oplus f} \\ M \otimes F & & M \otimes (\bigoplus_i R) & & \bigoplus_i M \otimes R & & \bigoplus_i M \end{array}$$

- More generally, projective modules are flat. If P is projective, $\exists P'$ such that for a free module F, $F = P \oplus P'$. Then if $M' \to M$ is injective, then $M' \otimes F \to M \otimes F$ by the previous example. So $M' \otimes P \bigoplus M' \otimes P' \longrightarrow M \otimes P \bigoplus M \otimes P'$ is an injective map $\implies M' \otimes P \to M \otimes P$ is injective.
- Flat module does not necessarily imply projective modules. $\mathbb{Q}$ as a $\mathbb{Z}$-module is flat. [Check 11/29 minute 30 for proof] But $\mathbb{Q}$ is not projective. Suppose $\mathbb{Q} \oplus P'$ is free, then pick a basis and write $(1, 0) = \lambda_1 x_1 + ... + \lambda_n x_n$, $x_1, ..., x_n$ part of a basis and $\lambda_1, ..., \lambda_n \in \mathbb{Z}$. Pick N where $N > |\lambda_1|, ..., |\lambda_n|$. Then write $(\frac{1}{N}, 0)$ as a combination of basis elements, where $(\frac{1}{N}, 0) = c_1 x_1 + ... + c_n x_n$, where $c_1, ..., c_n \in \mathbb{Z}$ may be 0. So $(1, 0) = N c_1 x_1 + ... + N c_n x_n$. If $c_i \neq 0$, then $|N c_i| > |\lambda_i|$, so they cannot be equal.
- If F is a flat R-module, then it is torsion-free. We need to show that if $0 \neq x \in F$ and $0 \neq r \in R$, then $rx \neq 0$. Let $R \xrightarrow{f} R$, $s \mapsto rs$ be multiplication by r. Then f is injective since R is an integral domain. So, $R \otimes F \xrightarrow{f\otimes id} R \otimes F$ is injective. $0 \neq 1 \otimes x \mapsto r \otimes x = 1 \otimes rx$. So $1 \otimes rx \neq 0, rx \neq 0$

Note: Free $\implies$ Projective $\implies$ Flat $\implies$ Torsion-free

Let $R \xrightarrow{f} S$ be a ring homomorphism.

- Any S-module M has the structure of an R-module, $rm : f(r)m$
- Now, suppose N is a module over R. $N \otimes_R S$ is a R-module which has the structure of S-module, $s(n_1 \otimes s_1) := n_1 \otimes s s_1$

If $\phi : N_1 \to N_2$ is a R-homomorphism, $\phi \otimes id : N_1 \otimes S \to N_2 \otimes_R S$ is a S-homomorphism.

4 Category Theory

Definition. A category $\mathcal{C}$ consists of a collection (class) of objects $Obj(\mathcal{C})$. For any two objects A, B of $\mathcal{C}$, a set of morphisms $Hom_{\mathcal{C}}(A, B)$ satisfies for any object $A \subset Obj(\mathcal{C})$, there is a morphism $1_A \in Hom_{\mathcal{C}}(A, A)$ and a composition function $Hom_{\mathcal{C}}(A, B) \times Hom_{\mathcal{C}}(B, C) \longrightarrow Hom_{\mathcal{C}}(A, C), (f, g) \mapsto gf$. which is associative: $(hg)f = h(gf), f1_A = f, 1_B f = f$.

$$A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$$

Example.

- $\mathcal{C}$ is a category of sets $Obj(\text{set})$, and $Hom_{\text{set}}(A, B)$ are functions from A to B.
- Let S be a set with a relation $\sim$ that is reflexive and transitive, and $\mathcal{C}$ is a category $obj(\mathcal{C})$. $Hom_{\mathcal{C}}(a, b) = \phi$ if $a \not\sim b$ and $\{(a, b)\}$ if $a \sim b$.

  $a \in obj(\mathcal{C}), 1_a = (a, a)$ with composition $(a, b) \in Hom(a, b), (b, c) \in Hom(b, c)$ therefore $(b, c)(a, b) = (a, c)$.
- Let $\mathcal{C}$ be a category, $A \in Obj(\mathcal{C})$ and $\mathcal{C}_A$ be a new catory, where objects are morphism from any object of $\mathcal{C}$ to A.

  $$Hom_{\mathcal{C}_A}(f, g) = \{\sigma \in Hom_{\mathcal{C}}(B, C) \mid g\sigma = f\}$$

  and $Hom_{\mathcal{C}_A}(f, g) \times Hom_{\mathcal{C}_A}(g, h) \to Hom_{\mathcal{C}_A}(f, h), (\sigma, \alpha) \mapsto \alpha\sigma$. So $h(\alpha\sigma) = (h\alpha)\sigma = g\sigma = f$, and $1_B f = f$.

4.1 Morphisms

Definition. Let $\mathcal{C}$ be a category, $f \in Hom_{\mathcal{C}}(A, B)$. Then f is an **isomorphism** if it has a two-sided inverse under composition with $g \in Hom(B, A)$ so that $gf = 1_A, fg = 1_B$. This inverse is unique, and is denoted by f^{-1}.

This has the properties that

- $(1_A)^{-1} = 1_A$
- $(fg)^{-1} = g^{-1} f^{-1}$
- $(f^{-1})^{-1} = f$

Example.

- If $\mathcal{C}$ is a set, then isomorphism are bijections.
- $\sim$ on S: (a, b) is an isomorphism $\iff b \sim a$

Definition. $f \in Hom_{\mathcal{C}}(A, B)$ is a **monomorphism** if $\forall C \in Obj(\mathcal{C})$ and $g_1, g_2 \in Hom_{\mathcal{C}}(A, C)$ with fg_1, fg_1, we have $g_1 = g_2$.

Definition. f is an **epimorophism** if $\forall C \in Obj(\mathcal{C}), h_1, h_2 \in Hom_{\mathcal{C}}(B, C)$ with $h_1 f = h_2 f$, we have $h_1 = h_2$

Example.

- For $\mathcal{C}$ a set, a monomorphism is injective and epimorphism is surjective.
- For $S, \sim$, all morphisms are monomorphism and epimorphism.

4.2 Initial and Final Objects

Definition. For category $\mathcal{C}, I \in Obj(\mathcal{C})$ is **initial** if for any $A \in Obj(\mathcal{C}), Hom_{\mathcal{C}}(I, A)$ has one element. $F \in Obj(\mathcal{C})$ is **final** if for any $A \in Obj(\mathcal{C})$, then $Hom_{\mathcal{C}}(A, F)$ has one element.

Example.

- For $\mathcal{C}$ a set, $\emptyset$ is the initial object, any singleton set is a final object.
- For $(S, \sim)$ with $(\mathbb{Z}, \leq)$, there is no initial or final object.

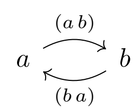
Note: Initial and final objects are unique up to isomorphism.

Example.

- For category of sets, initial object is $\emptyset$ and final object is singleton set.
- For category of groups, initial object is $\{e\}$ and final is also $\{e\}$.
- For category of rings, intial object is $\mathbb{Z}$, final object is $\{0\}$.
- For category of R-modules, initial element is $\{0\}$ and final is $\{0\}$.
- For category of fields, there are no initial and final objects

Definition. A category $\mathcal{C}$ is a **groupoid** if every morphism is an isomorphism.

Example. If $\sim$ on S is an equivalence relation,

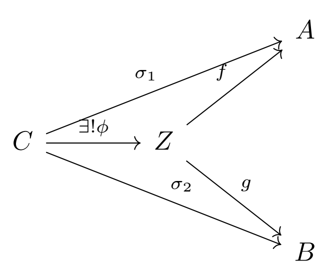


Definition. If $A \in Obj(\mathcal{C})$ isomorphisms $\in Hom(A, A)$ are **automorphism**, they form a group denoted by $Aut(A)$

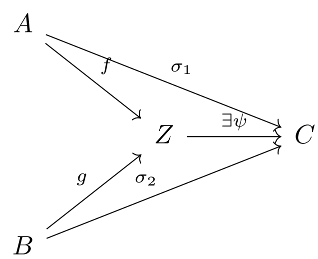
Fact: A *group* is a *groupoid* of 1 object!

4.3 Product and Coproduct

Definition. Let $\mathcal{C}$ be a category with $A, B \in Obj(\mathcal{C})$. Z is a **product** of A, B if $\exists f \in Hom(Z, A), g \in Hom(Z, B)$ such that $\forall C \in Obj(\mathcal{C})$, $\sigma_1 \in Hom(C, A), \sigma_2 \in Hom(C, D), \exists! \phi \in Hom(C, Z)$ such that $f \circ \phi = \sigma_1, g \circ \phi = \sigma_2$



Definition. It is a coproduct is the following diagram commutes:



If product (coproduct) of A, B then it is unique up to isomorphism. If Z, Z' coproduct $\psi : Z \to Z', \phi : \mathbb{Z} \to Z$ (replace C with Z' from above). Then $\phi \circ \sigma_2 = g, \psi \circ g = \sigma_2$.

Example. For set A, B, $A \times B$ is the product and the coproduct is the disjoint union $A \sqcup B$. By definition, $\{1, 2\} \sqcup \{2, 3\} = \{1, 2, 2', 3\}$.

Example. For groups G_1, G_2, the product is $G_1 \times G_2$ and the coproduct is free product $G_1 * G_2$ (Note that $G_1 \times G_2$ is only coproduct when it is abelian.)

fill in examples from written notes

4.4 Functors

Definition. Suppose $\mathcal{C}$ and $\mathcal{D}$ are categories and $F : \mathcal{C} \to \mathcal{D}$ is a **covariant functor** if $\forall A \in Obj(\mathcal{C})$, $F(A) \in Obj(\mathcal{C})$ and a function $Hom_{\mathcal{C}}(A, B) \to Hom_{\mathcal{D}}(F(A), F(B))$ such that

- $F(1_A) = 1_{F(A)}$. $A \xrightarrow{\beta} B \xrightarrow{\alpha} Z$
- $F(\alpha\beta) = F(\alpha)F(\beta)$. $F(A) \xrightarrow{F(\beta)} F(B) \xrightarrow{F(\alpha)} F(Z)$