

Notes on Serge Lang's Algebra

Amanuel Tewodros

June 8, 2025

Contents

1	Groups	5
2	Rings	9
3	Modules	13

Chapter 1

Groups

Theorem 1 (Sylow Theorems). *Let G be a finite group with p divides $|G|$, where p is a prime. Then*

1. *There exists a Sylow p -subgroup of G .*
2. *The number of Sylow p -subgroups of G is congruent to 1 modulo p and divides $|G|$.*
3. *All Sylow p -subgroups of G are conjugate.*

Proof. If $H \leq G$ with $[G : H]$ coprime with p , then by induction H and therefore G contains a Sylow p -group. Otherwise, by the class equation,

$$|G| = |Z(G)| + \sum_x [G : N_x(G)],$$

it follows $Z(G)$ is divisible by p and thus $\langle g \rangle \leq Z(G)$ for some $g \in Z(G)$ with exponent $= p$. Inducting on the order of G , $G/\langle g \rangle$ contains a Sylow p -subgroup, say $S/\langle g \rangle$ that is the image of $S \leq G$ that is a Sylow p -subgroup of G .

Let $P, Q \in \text{Syl}_p(G)$. P does not normalize Q because otherwise $PQ \leq G$ and $p^m = |PQ| > |P|$, a contradiction. Let $S = \{P_1, \dots, P_k\}$ be the conjugates of P and let \mathcal{O}_i be the orbit of P_i by the action P on the set S by conjugation. Then $|\mathcal{O}_i| = [P : N_P(P_i)] = [P : N_G(P_i) \cap P] = [P : P_i \cap P] \implies k = 1 \pmod p$.

If $P, Q \in \text{Syl}_p(G)$ are not conjugates, then Q is not conjugate with conjugates of P . Consider the action of the elements of Q on the set $\{gPg^{-1} : g \in G\} = \{P_1, \dots, P_m\}$. Then

$$|\mathcal{O}_{P_i}| = [Q : N_Q(P_i)] = [Q : P_i \cap Q],$$

where the latter equality follows because $P_i(N_G(P_i) \cap Q)$ is a p -group that contains P_i with order $\leq |P_i|$ (a Sylow p -group) and thus $N_G(P_i) \cap Q \leq P_i$. Since Q is not a conjugate of P , $[Q : Q \cap P_i] = p^k, k > 0$ and \mathcal{O}_{P_i} is divisible by p and the number of conjugates of P which is $\sum_i |\mathcal{O}_{P_i}| = 0 \pmod p$, a contradiction. \square

Theorem 2. *If $|G| = pq$ for primes $p < q$, then $G = \mathbb{Z}/pq\mathbb{Z}$ if $p \nmid q-1$ else $G = \mathbb{Z}/pq\mathbb{Z}$ of $G = \mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$ for some non-trivial semi-direct product.*

Proof. If $q > p$, $n_q = 1$ and thus $Q \in \text{Syl}_q(G)$ is normal. $|\text{Aut}(\mathbb{Z}/q\mathbb{Z})| = q - 1$, therefore, there is a nontrivial map $\phi : \mathbb{Z}/p\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/q\mathbb{Z})$ if $p \mid q - 1$ \square

Theorem 3 (Fundamental Theorem of Finitely Generated Abelian Groups). *Let A be a finite abelian group and let $A(p)$ be the subgroup of all elements with order that is a power of p . Then*

$$\prod_{A(p) \neq \{1\}} A(p) = A.$$

Proof. Clearly the map $\phi : \prod_p A(p) \rightarrow A$ defined by $\phi((x_p)) = \prod_p x_p$ is an endomorphism. We show that ϕ is injective and surjective. Let $\phi((x_p)) = 1$ for some $x = (x_p) \in \prod_p A(p)$. Let q be a prime with $A(q) \neq \{1\}$. Then

$$x_q = \prod_{p \neq q} x_p^{-1}.$$

Let m be the least common multiple of the primes powers on the right hand side, i.e. powers of $p \neq q$. Then $x_q^m = 1$. But, $x_q^{q^r} = 1$ too. Consequently, $x_q^{(m, q^r)} = x_q^1 = x_q = 1$. Thus $\prod_p x_p = 1$ iff all $x_p = 1$ and $\ker \phi = \{1\}$.

To prove surjectivity, let $x \in A$ with $x^m = 1$ such that $m = \prod p_i^{r_i}$. By Euclidean algorithm, $1 = \sum_i u_i \prod_{j \neq i} p_j^{r_j}$ and thus $x = \prod_i x^{u_i \prod_{j \neq i} p_j^{r_j}}$ with $x^{u_i \prod_{j \neq i} p_j^{r_j}} \in A(p_i)$. \square

Why nilpotence and the existence of normal Sylow sub-groups are equivalent? If $P, Q \in \text{Syl}_p(G)$ then $N_P(Q) = P \cap Q < P, Q$ and thus $Z(G)$ is always $< G$. Thus $P = Q \iff G$ nilpotent.

The number of ways G acts on H : $= \#$ of homomorphisms from G to $\text{Aut}(H) = \#$ subgroups of order $|G|/|H^*|$.

Theorem 4. *If $n \geq 5$ then S_n is not solvable.*

Proof. Let S_n decompose as $S_n = H_m \supset \dots \supset H_0 = \{1\}$. Clearly, S_n contains all 3-cycles. We also know since H_n/H_{n-1} is abelian $(abc)(ade)(acb)(aed) = (adebc)(aedcb) = (abd) \in H_{m-1}$. By induction all 3 cycles are in $\{1\}$, a contradiction. \square

Theorem 5. *A_n is simple for all $n \geq 5$.*

A priori: A_n can be generated by 3-cycles and 3-cycles are conjugates.

Proof. Let $N \trianglelefteq A_n$. Let $\sigma \in N$. We show that σ is a 3-cycle or $\sigma = \text{id}$. The former implies $N = A_n$ and the latter implies N is the trivial subgroup. Let σ have the maximal number of fixed points in N .

Let σ 's orbits have size 2 and it does not fix elements i, j . If σ is (ijk) for some k , we are done. Otherwise, $\langle \sigma \rangle > \langle (ij)(rs) \rangle$ for some r, s because σ is an even permutation and not a 3-cycle. Let $\tau = (rsk)$ for some k . Then $\tau' = \tau \sigma \tau^{-1} \sigma^{-1} \in N$. But $\tau' = (i, j)\sigma$ contradicting σ fixes the maximal number of points. Thus at least one σ 's orbit has more than 2 elements.

Therefore, $\sigma = (ijk)(rs)\theta$ where θ is possible identity permutation. By similar argument as above picking $\tau' = (rsk)$, σ can not be the element of N with maximal fixed points unless it contains all of A_n . \square

Properties of Common Non-Abelian Groups

- *Dihedral Group*: D_{2n}
 - $\cong \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ acting by inversion
 - $= \{a, b \mid a^n, b^2, baba\}$
- *Binary Dihedral Group/ Dicyclic Group*: $\text{DiC}(4n)$
 - $\cong \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ acting by inversion
 - $= \{a, b \mid a^n, b^4, baba\}$
- *Generalized Quaternions*: $Q_{2^{n+2}}$
 - $\cong \mathbb{Z}/2^n\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ acting by inversion
 - $= \{a, b \mid a^{2^n}, b^4, baba\}$
- *Holomorph Group*: $\text{Hol}(G)$
 - $\cong G \rtimes \text{Aut}(G)$
 - if G is $\mathbb{Z}/p\mathbb{Z}$, p prime, $\text{Hol}(G)$ is isomorphic to the *generalized affine group*

Notes on Category Theory

- A category \mathcal{C} is a collection of **objects** $\text{Ob}(\mathcal{C})$, along with a set of maps, called **morphisms** between any two objects $A, B \in \text{Ob}(\mathcal{C})$ denoted by $\text{Mor}(A, B)$.
- Morphisms follow the law of composition.
- Three axioms
 1. **CAT 1** $\text{Mor}(A, B)$ and $\text{Mor}(A', B')$ are disjoint unless $(A, B) = (A', B')$, in which case they are equal.
 2. **CAT 2** For every $A \in \text{Ob}(\mathcal{C})$, there exists a morphism, id_A in $\text{Mor}(A, A)$ that acts as a left and right identity for the elements of $\text{Mor}(A, B)$ and $\text{Mor}(B, A)$ resp. for all B .
 3. **CAT 3** The law of composition of morphisms is associative.
- The **operation** of a group G on an object $A \in \text{Ob}(\mathcal{C})$ is a homomorphism from G to $\text{Aut}(A)$. It is also called a **representation**.

- Given a category \mathcal{C} , we can construct a new category \mathcal{D} where the objects are the morphisms of \mathcal{C} and the morphisms between two objects f, f' are defined by a pair of morphisms (ϕ, ψ) that make the following diagram commute:

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \phi \downarrow & & \downarrow \psi \\ A' & \xrightarrow{f'} & B' \end{array}$$

- An object P of a category \mathcal{C} is called **universally attracting** (resp. **universally repelling**) if there exists a *unique* morphism from (resp. to) every object to (resp. from) P . If it is both, it is called **universal object**.

Chapter 2

Rings

Proposition 6. For two ideals $\mathfrak{a}, \mathfrak{b}$ of a ring A , if $\mathfrak{a} + \mathfrak{b} = A$, then $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$.

Proof. Clearly, $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$. Thus, it suffices to prove the contra-positive relation. Since $1 = a + b$ for some $a \in \mathfrak{a}, b \in \mathfrak{b}, c = c \cdot a + c \cdot b$ for all $c \in A$. Of course, if $c \in \mathfrak{a} \cap \mathfrak{b}$, $c \cdot a + c \cdot b \in \mathfrak{a}\mathfrak{b}$. \square

Let A be a ring and let $\lambda : \mathbb{Z} \rightarrow A$ given by

$$\lambda(n) = \underbrace{1_A + \cdots + 1_A}_{n \text{ times}}.$$

Then $\ker \lambda = \langle n \rangle$ for some $n \geq 0$. If $\langle n \rangle$ is a prime ideal, then we say A has characteristic n .

Proposition 7. If S is a set with more than two elements and A is a ring with $1_A \neq 0_A$, then $\text{Map}(S, A)$ is not an integral domain.

Proof. Let $\{\} \neq T \subset S$

$$f(x) = \begin{cases} 1_A & \text{if } x \in T \\ 0_A & \text{if } x \in S - T \end{cases} \quad \text{and } g(x) = 1_A - f(x).$$

$$fg = 0_{\text{Map}(S, A)}.$$

\square

If \mathfrak{p} is a prime ideal in a ring A , then it means

1. A/\mathfrak{p} is an integral domain.
2. $xy \in \mathfrak{p} \implies x \in \mathfrak{p} \text{ or } y \in \mathfrak{p}$.

The ideal $\{0_A\}$ is a prime ideal of A iff A is an integral domain.

Proof. (\implies) $A/\{0_A\} \cong A$, thus A should be an integral domain.

(\impliedby). If A is an integral domain, then $xy \in \{0_A\} \implies x = \{0_A\}$ or $y \in \{0_A\}$. \square

Theorem 8 (Chinese Remainder Theorem). *Let $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ be ideals of a ring A such that $\mathfrak{a}_i + \mathfrak{a}_j = A$ for any $i \neq j$. Let x_i be elements of A . Then there is an element $x \in A$ such that $x \equiv x_i \pmod{\mathfrak{a}_i}$.*

Proof. If $n = 2$, $A = \mathfrak{a}_1 + \mathfrak{a}_2$, and thus $1_A = a_1 + a_2$ for some $a_i \in \mathfrak{a}_i$. Then $x = x_1 a_1 + x_2 a_2$ satisfies the statement.

If $n > 2$, then $a_i + b_i = 1_A$ for some $a_i \in \mathfrak{a}_i$ and $b_i \in \mathfrak{a}_{j>1}$. Thus the product $\prod_i (a_i + b_i) = 1_A$. In other words,

$$A = \mathfrak{a}_1 + \prod_{i=2}^n \mathfrak{a}_i.$$

By the case for $n = 2$, there is an element y_1 such that,

$$y_1 \equiv 1_A \pmod{\mathfrak{a}_1} \text{ and } y_1 \equiv 0_A \pmod{\left(\prod_{i=2}^n \mathfrak{a}_i\right)}$$

Since $\prod_{i=2}^n \mathfrak{a}_i \subseteq \bigcap_{i=2}^n \mathfrak{a}_i$, it follows that $y_1 \in \mathfrak{a}_i$ for all $i > 1$ and therefore, $y \equiv 0_A \pmod{\mathfrak{a}_i}$ for $i > 1$. Carrying out the same procedure in similar fashion to obtain y_2, \dots, y_n such that

$$y_i \equiv 1_A \pmod{\mathfrak{a}_i} \text{ and } y_i \equiv 0_A \pmod{\mathfrak{a}_j, j \neq i},$$

we see that $x = \sum_{i=1}^n x_i y_i$ satisfies the statement of the theorem. \square

A non-zero polynomial f of degree d over a commutative ring A is homogenous iff for every set of $n + 1$ algebraically independent elements u, t_1, \dots, t_n over A ,

$$f(ut_1, \dots, ut_n) = u^d f(t_1, \dots, t_n).$$

Proof. Let $f(X) = \sum_{(v)} a_{(v)} X_1^{v_1} \cdots X_n^{v_n}$. If f is homogenous of degree d , $v_1 + \cdots + v_n = d$ for all $a_{(v)} \neq 0$. $f(ut_1, \dots, ut_n) = \sum_{(v)} a_{(v)} (ut_1)^{v_1} \cdots (ut_n)^{v_n}$. Since A is commutative, this is equal to $\sum_{(v)} a_{(v)} u^{v_1 + \cdots + v_n} t_1^{v_1} \cdots t_n^{v_n}$.

On the other hand, if $f(ut_1, \dots, ut_n) = u^d f(t_1, \dots, t_n)$, then $\sum_{(v)} a_{(v)} u^{v_1 + \cdots + v_n} = u^d \sum_{(v)} a_{(v)}$. This is a polynomial in u over A and equality is assured iff $u^d = u^{v_1 + \cdots + v_n}$. \square

Let G be a **monid** and let $A[G]$ be the set of all mappings $\alpha : G \rightarrow A$ such that $\alpha(x) = 0$ for almost all $x \in G$. Addition is defined ordinarily and multiplication is defined as

$$\alpha\beta(z) = \sum_{xy=z} \alpha(x)\beta(y).$$

Then $A[G]$ is a ring. A more convenient notation can be achieved if we define $a \cdot x$ as

$$a \cdot x(z) = \begin{cases} a & \text{if } z = x \\ 0 & \text{if otherwise.} \end{cases}$$

This way we can define, $\alpha = \sum_{x \in G} \alpha(x) \cdot x$, and

$$\left(\sum_{x \in G} a_x \cdot x \right) \left(\sum_{y \in G} b_y \cdot y \right) = \left(\sum_{x,y} a_x b_y \cdot xy \right)$$

$$\left(\sum_{x \in G} a_x \cdot x \right) + \left(\sum_{x \in G} b_x \cdot x \right) = \left(\sum_{x \in G} (a_x + b_x) \cdot x \right),$$

where $\{a_z\}_{z \in G}, \{b_z\}_{z \in G}$ are the elements of A , most of them equal to 0.

The injective homomorphisms $x \mapsto 1_A \cdot x$ and $a \mapsto a \cdot e$ show that G and A are embedded in $A[G]$.

Let A be a commutative ring and S be a multiplicative subset¹. For $a, a' \in A$ and $s, s' \in S$, we say

$$(a, s) \sim (a', s')$$

if there is $s_1 \in S$ such that

$$s_1(as' - sa') = 0.$$

\sim is an equivalence relation.

Proof. Symmetry and Reflexivity are trivial. Transitivity can be verified as follows. Let $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$. Then for some $s_1, s_2 \in S$, we have

$$s_1 ad = s_1 bc$$

$$s_2 de = s_2 cf$$

Multiplying both sides of first and the second equation by $s_2 f$ and $s_1 b$, it follows that $(s_1 s_2 d)(af - be) = 0$. \square

This construction of ring is called **ring of fraction of A by S** , $S^{-1}A$. The homomorphism $A \mapsto S^{-1}A$ defined by $a \mapsto a/1_A$ is a universal object (See 1). If A is an integral domain, then $S^{-1}A$ is the field of fractions.

If A has a unique maximal ideal, it is called a **local ring**. An interesting example is $A_{\mathfrak{p}} = S^{-1}A$, where S is the multiplicative subset $A - \mathfrak{p}$.

Principal Ideal Domains and Unique Factorization

Let A be a principal integral domain. We say a divides b if $b = ac$ for some $c \in A$

Definition 9. d is called the greatest common divisor of a and b if and only if $c|a$ and $c|b \implies c|d$.

Proposition 10. If $d = \gcd(a, b)$, then $ar + bs = d$ for some $r, s \in A$.

¹A subset containing 1_A and closed under multiplication

Proof. Let $a = dx$ and $b = dy$. Because d is a gcd of a and b , for $c \notin A^*c \mid x \implies c \nmid y$ and vice versa, thus $\gcd(x, y)$ is a unit in A .

Now, $A \subseteq \langle x, y \rangle$. To show that, let $\langle z \rangle = \langle x, y \rangle$. Since $x, y \in \langle x, y \rangle$, $x = w_1z$ and $y = w_2z$. But then z should be a unit in A and thus $1_A \in \langle x, y \rangle$. The proposition follows directly. \square

The proof also shows if $\langle a, b \rangle = \langle c \rangle$, then $c = \gcd(a, b)$.

Definition 11. We call $p \in A$ **irreducible** if $p = ab$ for some $a, b \in A$, then $\{a, b\} \cap A^* \neq \emptyset$. If $c \in A$ can be written as a product of a unit in A and a product of some irreducibles in A , we call the product **a factorization** of c . If every non-zero element of A has a unique factorization (upto commutativity) we call A a **unique factorization domain (UFD)** or **factorial ring**.

Theorem 12. If A is a principal ideal domain, then A is a UFD.

Proof. Existence: Let S be the set of ideals of A generated by elements a_i that don't have factorization. Let $S \neq \emptyset$. Then $\langle a_1 \rangle \in S$. Consider the chain,

$$\langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \cdots \subsetneq \langle a_n \rangle \subsetneq \cdots$$

Because, A is a principal ideal domain $\cup_i \langle a_i \rangle = \langle a \rangle$ for some $a \in A$. However, $\langle a_i \rangle \subsetneq \langle a_{i+1} \rangle$, $a \in \langle a_n \rangle$ for some n and the chain is finite. Thus if $\langle a \rangle \subsetneq \langle b \rangle$, then b admits factorization.

Remark 13. The fact that A is a principal ideal domain is important in constructing the chain. Consider the following chain if $A = \mathbb{Q}$, for example

$$\langle 1/2 \rangle \subsetneq \langle 1/4 \rangle \subsetneq \cdots \subsetneq \langle 1/2^n \rangle \subsetneq \cdots$$

The union of these ideals $= \mathbb{Q}$ which is not a principal ideal.

Now, consider a . Clearly, a is not an irreducible. Thus Assume $a = bc$. But $\langle a \rangle \subsetneq \langle b \rangle$. Thus b (and also c) admits factorization and by induction a does making S empty.

Uniqueness First, we prove that irreducibility implies primality. Let p be irreducible and let $p \mid ab$. If $p \nmid a$ then $\gcd(a, p) = 1_A$ and $1_A = ax + py \implies b = abx + pby = p(c'x + by)$ for some c .

If

$$a = up_1 \cdots p_r = vq_1 \cdots q_s,$$

$p_1 \mid q_1 \cdots q_s$ and WLOG, $q_1 = u_1 p_1$. Thus $up_2 \cdots p_r = vu_1 q_2 \cdots q_s$. The argument completes by induction. \square

Chapter 3

Modules

The concept of rings is motivated by the properties of a set of *endomorphisms* on an (additive) abelian group. Left R -modules are the abelian groups M such that there is a ring homomorphism $R \rightarrow \text{End}(M)$.

Example: If J is an ideal of a ring A , then we can define an operation of an element $a, b \in A$ on A/J as $a \cdot (x + J) \mapsto ax + J$. This mapping is an endomorphism of A/J because $a \cdot (x + y + J) = a \cdot (x + J) + a \cdot (y + J)$. We can define the a ring homomorphism from $A \rightarrow \text{End}(A/J)$ trivially. Therefore, A defines a module structure over A/J .

To show a group M is A -module, it suffices to show that for $a, b \in A, x, y \in M$

$$a(x + y) = ax + ay \text{ and } (a + b)x = ax + bx,$$

These conditions are equivalent to showing there is a ring homomorphism from the actions of elements of A on M to $\text{End}(M)$.

Some basic constructions from the companion. Let M be an A -module.

1. For $N \subseteq M$, $\{r \in A : rN = 0\}$ forms an left ideal in A .
2. For $N \subseteq M$, $\{r \in A : rM \subseteq N\}$ forms a right ideal of A .
3. For $N \subseteq M$, $\{r \in A : rN \subseteq N\}$ forms a subring.
4. If N is a submodule, then the ideals in 1 and 2 are 2-sided. Here, it is important to point out that when N is a submodule, then closure of the actions of A on N is maintained.

If $x \in M$, then $Rx \cong R/I$, where I is the annihilator ideal of $\{x\}$ as in 1.

Every ideal (left, right and 2-sided) and subring of A can be constructed in the above way

Definition 14. A **module-homomorphism** is an additive group homomorphism $f : M \rightarrow M'$ from modules M to module M' and such that $f(ax) = af(x)$.

If f is module-homomorphism from M to M' then the kernel and the image of f are submodules of M and M' respectively.

Proof. Clearly, $\ker f \leq M$ because f is a group homomorphism. Let $a \in A$ and $x \in \ker f$. $f(ax) = af(x) = 0$. Hence, the kernel of f is a submodule of M .

Again, $\text{Im } f \leq M'$. $af(x) = f(ax) \in \text{Im } f$.

□

$M' / f(M)$ is a universal (initial) among the modules N with homomorphism $g : M' \rightarrow N$ such that $g \circ f = 0$. That is the following diagram commutes and \hat{g} is unique:

$$\begin{array}{ccccc}
 M & \xrightarrow{\quad f \quad} & M' & \xrightarrow{\quad g \quad} & N \\
 & & \downarrow c & \nearrow \hat{g} & \\
 & & M' / f(M) & &
 \end{array}$$

This is dual with the kernel of f which is a terminal object among modules N with homomorphism $g : N \rightarrow M$ such that $f \circ g = 0$. Thus, it is called the **cokernel** of f .

Definition 15. A **monomorphism** is a module-homomorphism $u : N \rightarrow M$ characterized by the exact sequence $0 \rightarrow N \xrightarrow{u} M$. Similarly, an **epimorphism** is characterized by dual exact sequence $N \xrightarrow{u} M \rightarrow 0$.

These definitions coincide with the definitions of one-to-one homomorphisms and surjective homomorphism in the category of modules over a ring R .

Definition 16. For a commutative¹ ring A , we say K is an A -algebra, if K is a module with E a **A -bilinear map** $g : E \times E \rightarrow E$.

In the companion, the following remark is left.

Let A be a commutative ring. Then

associative, unital A -algebra $R \equiv \text{Ring } R \text{ with a homomorphism } f : A \rightarrow Z(R)$.

f is a way of encoding the bilinear operator, and why it's into the center of R is mainly because we require $a \cdot xy = (a \cdot x)y = x(a \cdot y) := f(a)xy = (f(a)x)y = xf(a)y$

¹ the concept of algebras does not make much sense with non-commutative rings

Another interesting remark is that algebras are abstractions of the natural structure of A -module-endomorphisms of a module M , $\text{End}_A(M)$, just like rings abstract the endomorphisms of an abelian group.

A sequence $\cdots \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow \cdots$ is called exact if $\text{Im } f = \ker g$. We denote the group of A -homomorphisms from A -module X to Y by $\text{Hom}_A(X, Y)$.

Proposition 17. *Let X, X', X'' and Y be A -modules. Then the short sequence*

$$X' \xrightarrow{\lambda} X \xrightarrow{\mu} X'' \rightarrow 0$$

is exact if and only if

$$\text{Hom}_A(X', Y) \xleftarrow{\lambda'} \text{Hom}_A(X, Y) \xleftarrow{\mu'} \text{Hom}_A(X'', Y) \leftarrow 0$$

is exact for all Y .

Remark 18. This proposition is analogous to the duality of linear maps in vector spaces.

Proof. Suppose the first sequence is exact. Then the following statements hold:

- (i) $\text{Im } \lambda = \ker \mu$
- (ii) $\text{Im } \mu = X''$.

Let $g \mapsto g \circ \lambda = 0$. Since $\text{Im } \lambda \subseteq \ker g$, g factors through $X/\text{Im } \lambda$. By **i** and **ii**, $X/\text{Im } \lambda \cong \text{Im } \mu = X''$ which implies $g = f \circ \mu$ for some $f \in \text{Hom}(X'', Y)$. This shows $\ker \lambda' \subseteq \text{Im } \mu'$. Similarly, let $h \circ \mu \in \text{Im } \mu'$. By **i**, the composition of this with λ , $h \circ \mu \circ \lambda = 0$, implying $\text{Im } \mu' \subseteq \ker \lambda'$ (thus $\text{Im } \mu' = \ker \lambda'$). The first implication of the proposition follows from the fact that if $f \mapsto f \circ \mu = 0$ for some $f : X'' \rightarrow Y$, then $f = 0$ by **ii**.

The proof of the converse is an easy application of the following common technique:
To study the consequences of a condition holding for all morphisms of a given sort, consider a universal example.

Suppose the second sequence is exact, i.e.,

- (i) $\ker \lambda' = \text{Im } \mu'$
- (ii) $\ker \mu' = 0$.

By **i**, $\ker \lambda' \supseteq \text{Im } \mu'$. That is, for every Y and $f : X'' \rightarrow Y$ $f \circ \mu \circ \lambda = 0$. Now, consider the universal example for all f s, i.e., the category of morphisms from X'' which is id , the identity morphisms. $\text{id} \circ \mu \circ \lambda = \mu \circ \lambda = 0$ implies $\ker \mu \supseteq \text{Im } \lambda$.

Similarly, the condition $\ker \lambda' \subseteq \text{Im } \mu'$ implies for every Y , a map $g : X \rightarrow Y$ such that $g \circ \lambda = 0$ can be factored through X'' . The universal object of all morphisms from $X \rightarrow Y$ which are 0 at $\text{Im } \lambda$ is the canonical homomorphism $q : X \rightarrow X/\text{Im } \lambda$. Hence $q = f \circ \mu$ which is obviously 0 on $\text{Im } \lambda$ and thus $\ker q = \text{Im } \lambda \supseteq \ker \mu$.

Finally, the universal object of morphisms from $X'' \rightarrow Y$ annihilated by $\text{Im } \mu$ is the canonical morphism $p : X'' \rightarrow X''/\text{Im } \mu$. However, **ii** implies $p = 0$ and $X'' \cong \text{Im } \mu$ which completes the proof. \square

Let $\{M_i\}_{i \in I}$ be a family of submodules of M . Then we have the induced homomorphism

$$\lambda_* : \bigoplus_{i \in I} M_i \rightarrow M$$

defined by $\lambda_*((x_i)) = \sum x_i$. If λ_* is isomorphism, then we call the family $\{M_i\}_{i \in I}$, **direct sum decomposition** of M as we have

$$\bigoplus M_i = M.$$

Otherwise, if λ_* is only surjective, we can write

$$M = \sum M_i$$

Remark 19. This notion is analogous to linear independence and direct sums in linear algebra.

Let M_1, M_2, N be modules. Then we have the following isomorphism of abelian groups

$$\text{Hom}(M_1 \oplus M_2, N) \cong \text{Hom}(M_1, N) \times \text{Hom}(M_2, N)$$

$$\text{Hom}(N, M_1 \times M_2) \cong \text{Hom}(N, M_1) \times \text{Hom}(N, M_2)$$

The first isomorphism follows from the association $f \mapsto (f_1, f_2)$ where f is an element of the LHS group and $f_i : M_i \rightarrow N$ are the homomorphisms defined by $f_i = f \circ I_i$. The second one follows with similar associations.

Proposition 20. *Let the following sequence of modules be exact:*

$$0 \rightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \rightarrow 0$$

The following conditions are equivalent

1. *There is a homomorphism $\varphi : M'' \rightarrow M$ such that $\text{id} = g \circ \varphi$.*
2. *There is a homomorphism $\psi : M \rightarrow M'$ such that $\text{id} = \psi \circ f$.*

If these conditions are satisfied, then we have the following isomorphisms:

$$M = \ker g \oplus \text{Im } \varphi = \ker \psi \oplus \text{Im } f \cong M' \oplus M''.$$

The general idea is the exactness of the sequence makes M factorize into $M' \times M/M'$ in group theory terms.

Proof. Let $x \in M$. Then $x - \varphi(g(x)) \in \ker g$ by definition. Thus $x = (x - \varphi(g(x))) + \varphi(g(x)) \in \ker g + \text{Im } \varphi$. This sum is direct because $\ker g \cap \text{Im } \varphi = 0$. The others isomorphisms follow immediately. \square

Definition 21. A **free module** is an A -module that admits a basis.

Proposition 22. *Let M be a free module with basis $\{x_i\}_{i \in I}$ and let \mathfrak{a} be a two-sided ideal of A . Then*

1. $\mathfrak{a}M$ is also a submodule of M that is also \mathfrak{a} -module.
2. Each $\mathfrak{a}x_i$ is a submodule of Ax_i .
3. We have the module isomorphism

$$M/\mathfrak{a}M \cong \bigoplus_{i \in I} Ax_i/\mathfrak{a}x_i.$$

4. $Ax_i/\mathfrak{a}x_i$ is isomorphic to A/\mathfrak{a} as A -module
5. Suppose A is commutative. Then A/\mathfrak{a} is a ring. Furthermore $M/\mathfrak{a}M$ is a free over A/\mathfrak{a} and $Ax_i/\mathfrak{a}x_i$ is a free over A/\mathfrak{a} . If \bar{x}_i is the image of x_i under the canonical homomorphism $Ax_i \rightarrow Ax_i/\mathfrak{a}x_i$, then \bar{x}_i is the basis of $Ax_i/\mathfrak{a}x_i$.

Proof. We go through the statements one by one:

1. Let $x \in M$. Then $x = \sum_{i \in I} a_i x_i$ uniquely for $\{a_i\}_{i \in I} \subseteq A$. By definition, $\mathfrak{a}M = \{\sum yx : y \in \mathfrak{a}, x \in M\}$. But $yx = \sum_i y a_i x_i = \sum_i y_i x_i \in M$ where $y_i \in \mathfrak{a}$ because \mathfrak{a} is two-sided ideal.
2. Clearly, $\mathfrak{a}x_i \subseteq Ax_i$. Let $a', b' \in \mathfrak{a}$ and $a, b, c \in A$. Ax_i is a A -module because $(a+b)cx_i = (ac+bc)x_i = acx_i + bcx_i$ and $c(a'x_i + b'x_i) = c(a+b)x_i = (ca+cb)x_i = cax_i + cbx_i$. The statement follows from $Aax_i \subseteq \mathfrak{a}x_i$.
3. By definition, $M = \bigoplus_{i \in I} Ax_i$. Consider the isomorphism

$$\sum_{i \in I} a_i x_i \mapsto (a_i x_i)_{i \in I}$$

which induces the isomorphism

$$\sum_{i \in I} a_i x_i + \mathfrak{a}M \mapsto (a_i x_i + \mathfrak{a}M)_{i \in I}.$$

Since $\mathfrak{a}M$ is a \mathfrak{a} -module and $a_i x_i + \mathfrak{a}M = a_i x_i + \mathfrak{a}x_i$, and $Ax_i/\mathfrak{a}x_i$ is an A/\mathfrak{a} -module, the statement is true.

4. Consider the isomorphism $1_A \mapsto x_i$.
5. A/\mathfrak{a} is a ring of cosets of \mathfrak{a} . $M/\mathfrak{a}M$ is free as the basis $\{x_i\}_{i \in I}$ serves as a basis for $M/\mathfrak{a}M$ over A/\mathfrak{a} .

□

We say an exact sequence of abelian groups

$$0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$$

splits if $B \cong A \oplus C$.

For Example: The sequence

$$0 \rightarrow \mathbb{Z}/2\mathbb{Z} \xrightarrow{x \mapsto x} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \xrightarrow{-1} \mathbb{Z}/2\mathbb{Z} \rightarrow 0$$

splits but

$$0 \rightarrow \mathbb{Z}/2\mathbb{Z} \xrightarrow{x \mapsto 2x} \mathbb{Z}/4\mathbb{Z} \xrightarrow{\text{mod } 2} \mathbb{Z}/2\mathbb{Z} \rightarrow 0$$

does not split.

Proposition 23. *Every surjective module-homomorphism from a A -module, M to a **free** A -module F splits.*

Proof. Let $\phi : M \rightarrow F$ be a surjective homomorphism. By the first isomorphism theorem, $F \cong M/\ker \phi$. Let $\{x_i + \ker \phi\}_{i \in I}$ form the basis of $M/\ker \phi$. Define $\psi : M/\ker \phi \rightarrow M$ as

$$\psi\left(\sum_{i \in I} a_i x_i + \ker \phi\right) = \sum_{i \in I} a_i x_i.$$

Clearly $\phi \circ \psi = \text{id}$

□