Lecture notes on Abstract Algebra

Joel Antonio-Vásquez

Ica, Peru
E-mail address: hello@joelantonio.me
URL: http://joelantonio.me/

ABSTRACT. The intention to this lectures notes is present a lot of examples in basic abstract Algebra.

Contents

Preface

I must say that this notes are not finished at all, until now I only can say that this is a recompilation of many definitions of the books which are in the references, the first section has a different taste since Ive written my own examples and proofs, the rest is incomplete, you must to consider this. As soon as possible I will update this notes and I'll focus on examples and different proofs, please dont take this notes totally seriously yet, but if you have any suggestion or you see any typo, please send me a mail, thanks.

CHAPTER 1

Group Theory

First, we learn one of the most important structure on Abstract Algebra, namely **groups**.

Definition 1. Let G be a set with a function $* : G \times G \longrightarrow G$ such that for each $a, b \in G$ then $a * b \in G$. Further, G claims the following axioms:

G1. For all $a, b, c \in G$ then $a * (b * c) = (a * b) * c$, (**associativity**).
G2. There exists an element $e \in G$ such that $e * a = a * e = a$, (**identity**, denoted by 1_G).
G3. There exists an element $a' \in G$ such that $a * a' = a' * a = e$, where e is the identity element, (**inverse**, denoted by a^{-1}).

Then, G is called a group, denoted by $(G, *)$.

Proposition 1. $1_G \in G$ is unique in any group.

Proof: Let $1, 1'$ be identities of G. Then $1 = 1 * 1' = 1'$. □

Proposition 2. The inverse of any element $a \in G$ is unique.

Proof: Suppose that a', a'' are inverses of a. Then $a' * a = a' * a * a'' = a''$. □

Example. Let $\rho : y \longrightarrow \sin(y)$ be the sine curve map. Then its isometries forms a group.

$$\begin{bmatrix} 0 & v & -v \\ -v & 0 & v \\ v & -v & 0 \end{bmatrix}$$

The map ρ is only linear for this case, since $\sin(v + -v) = \sin(v) + \sin(-v) = 0$. Indeed, the identity element is 0 and asserts properties G1 and G2. Then, the isometries of the sine curve forms a group.

From here, we can define other kind of groups with additional axioms. Indeed, if we have a proper subset $G' \subset G$ such that G' asserts the axioms in definition 1 of G into G' (i.e., if $a, b \in G'$ so does $ab \in G$, $1_G \in G'$ and for every $a \in G$ so does $a^{-1} \in G$), then G' is called a **subgroup**, denoted by $G' < G$.

Example. The trivial subgroups (i.e. not proper subgroups) of a group G are itself and 1_G.

Example. $H_{i\in I}$ are subgroups of G, then so does $\bigcap_{i\in I} H_i$.
Proof: If $\bigcap_{i\in I} H_i = 1_G$ or G, then is trivially true. Let $G' \neq 1_G, G$, Then $1_G \in G'$ since every H_i must have the identity element. If $x \in G'$ so does $x^{-1} \in G'$ since every H_i have the inverses of elements. G' is associative for the above reasons. So, G' is a subgroup of G. □

Example. $H_{i\in I}$ are subgroups of G, then not necessarily does $\bigcup_{i\in I} H_i$.
Counterexample: $\mathbb{Q}[\sqrt[2]{5}] \cup \mathbb{Q}[\sqrt[3]{5}] \nless \mathbb{Q}[\sqrt[6]{5}]$.

Definition 2. Let G be a group in the sense of definition 1. Further, for all $a, b \in G$ asserts strictly that $a * b = b * a$. Then, G is called an **abelian group** (**commutative**).

Example (Dihedral group). The dihedral group, is the group of symmetries of a regular n-gon in the plane. It has the presentation

$$\langle x, a \mid a^n = x^2 = e, xax^{-1} = a^{-1} \rangle,$$

where e is the identity element.
The D_ns are nonabelian for $n \geqslant 3$, the elements a, x do not commute. But D_2 is, its elements are $\{1, p, r, pr\}$.

Definition 3. Let S be a set endowed with associative binary operation $* : S \times S \longrightarrow S$. Then S is called a **semigroup**.

We can say that a semigroup is called a **monoid** iff asserts the axiom G2. It's easy to see that a group is a monoid with the additional axiom G3.

Up to this point, we've seen basic and easy definitions related to groups, the main purpose now is to build several properties and operations around groups in the section 1. Before finished this little introduction, let's list some classic group examples.

Example.

- A symmetric $\mathbb{R}$-correlation;
- A skew $\mathbb{C}$-correlation;
- A skew $\widetilde{\mathbb{H}}$- or equivalently, $\overline{\mathbb{H}}$-correlation;
- Let $J = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}$;
- Let V be a vector space. Then $\mathrm{Aut}(V) := \{T : V \longrightarrow V | T \text{ a linear isomorphism}\}$.

Don't worry if you don't know at all the above examples, the idea of this is to start getting used of notation, in later sections we'll work on them.

1. Structure of a Group

Now, let's see what kind of operations we can do around groups.

1.1. Homomorphisms.

DEFINITION 4. A **homomorphism** of two groups G, G' is a function $f : G \longrightarrow G'$ such that $f(ab) = f(a)f(b)$ for every $a, b \in G$.

Actually, we can map the set of homomorphisms of two groups G, G' as

$$\operatorname{Hom}(G, G') = \{\text{homomorphisms } f : G \longrightarrow G'\}.$$

LEMMA 1. If $\varphi : A \longrightarrow B$ and $\rho : B \longrightarrow C$ are homomorphism groups. Then so is $\varphi \circ \rho : A \longrightarrow C$.

Proof: Let $a, b, c \in A, B, C$, respectively. $\varphi \circ \rho = \rho(\varphi(a)) = \rho(b) = c$. Moreover, $1_\varphi \circ 1_\rho = 1_{\varphi\circ\rho}$ and $\varphi^{-1} \circ \rho^{-1} = \varphi(\rho(c)^{-1})^{-1} = \varphi(b)^{-1} = a$. Indeed, homomorphisms preserve identity elements and inverses. □

A group homomorphism $\varphi : (G, \circ) \longrightarrow (G', *)$ sastifies the following properties:

1. $\varphi(1_G) = 1_{G'}$.
2. $\varphi(a^{-1}) = \varphi(a)^{-1}$ for all $a \in G$.
3. $\operatorname{Ker}\varphi \subset G$ and $\operatorname{Im}\varphi \subset G'$ are subgroups.

Proof:

(1). $1_{G'}\varphi(1_G) = \varphi(1_G) = \varphi(1_G 1_G) = \varphi(1_G)\varphi(1_G)$. Then $1_{G'} = \varphi(1_G)$.

(2). Since $1_{G'} = \varphi(1_G)$, then $1_{G'} = \varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1})$. Finally, $\varphi(a)^{-1} = \varphi(a^{-1})$.

(3). Let $x, y \in \operatorname{Ker}\varphi$, by (1) $\varphi(1_G) = 1_{G'}$ and $\varphi(x) = \varphi(y)$. Then,

$$\begin{aligned} &= \varphi(x^{-1} \circ y) = \varphi(x^{-1}) * \varphi(y) \\ &= (\varphi(x))^{-1} * \varphi(y) \\ &= 1_T^{-1} * 1_T \\ &= 1_T \end{aligned}$$

So, $x^{-1} \circ y \in \operatorname{Ker}\varphi$. Indeed, $\operatorname{Ker}\varphi$ is a subgroup. (Same to show that $\operatorname{Im}\varphi$ is a group). □

1.2. Cosets.

DEFINITION 5. Let $H < G$ be a subgroup of G of the form $gH = \{gh : h \in G\}$. Then the subset gH is called a **left coset** of a subgroup H (same apply to **right coset**, denoted by Hg).

A **coset** is left or right. Any element of a coset is called a **representative** of that coset.

Definition 6. A subgroup $H < G$ is called **normal** when the left cosets and the right cosets of the subgroup coincide (i.e., $gH = Hg$ for all $g \in G$), denoted by $H \trianglelefteq G$.

Proposition 3. All the subgroups of an abelian group are normal.

Proof: Let $H < G$ be a subgroup of any abelian group G. Let $h \in H$ be any element of H. Then for all $g \in G$ we have that $gh \in H$. Since G is commutative so is H, then $hg \in H$, so $gh = hg$. Indeed, $G \trianglelefteq H$. □

Example. Let 1_{S_2} be the identity of any subgroup of index 2, then to S_2 could be a group there exists another element v such that $v \cdot 1_{S_2} = v$ since the group has index 2, only left $v \cdot v = 1_{S_2}$. Now, $S_2 \leqslant G_n$ for a $n \geqslant 2$, since S_2 is a subgroup of G_n then $1_{S_2} = 1_{G_n}$ and for any $u \in G_n$ we have that $uS = Su$. Indeed, any subgroup of index 2 is normal. □

Example. D_n has normal subgroups, which consists of its rotations R and its reflections F subject to the relations $R^n = F^2 = 1_{D_n}$ and $(RF)^2 = 1_{D_n}$. For n odd the normal subgroups are $\{1_{D_n}\}$ and $\langle R^d \rangle$ (i.e., cyclic group) for all divisors $d|n$. If n is even, there are two more normal subgroups $\langle R^2, F \rangle$ and $\langle R^2, RF \rangle$.

Proposition 4. Let $A, B \leqslant G$ be subgroups of G. If $A \trianglelefteq B$ and $B \trianglelefteq G$ then not necessarilty $A \trianglelefteq G$.

Counterexample: Let $G = S_4$ (symmetry group), $A = \langle (12)(34) \rangle$ and $B = \{(12)(34), (13)(42), (23)(41), 1_B\}$. Clearly, $A \trianglelefteq B$, $B \trianglelefteq S_4$ but not $A \trianglelefteq S_4$. □

Proposition 5. Let $\varphi : A \longrightarrow B$ be an arbitrary homomorphism of groups, then $N \trianglelefteq A$ does not necessarily imply $\varphi(N) \trianglelefteq B$.

Counterexample: Let H be any non-normal subgroup of B. If $N = A = H$, then claim follows.

We need to notice that having a left or right coset H of a group G, then represents a **quotient** of G by H, denoted by G/H.

Definition 7. The **center** of a group G is

$$Z(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}.$$

$Z(G)$ is clearly a normal subgroup of G.

Example. Let $H \leqslant Z(G)$ and let $z \in Z(G)$, then $gzg^{-1} = z$ for all $g \in G$. Hence $gHg^{-1} = H$ for all H. Indeed, all subgroups of $Z(G)$ are normal subgroups of G.

1.3. Order.

Definition 8. The **order** of a group G is the cardinality $|G|$, which could be a positive integer or ∞.

Obviously, the order of a element g in a group G is infinite if $g^m \neq 1$ for all $m \neq 0$.

Example. Suppose that for any trivial group that $G = 1_G$, then its order is 1.

Theorem 1 (Lagrange's Theorem). If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.

Proof: Let H be a proper subset which is subgroup of G. We know that for all $g \in G$ then $|gH| = |H|$. So we define the *left translation map* $\varphi_g : H \longrightarrow Hg$ which is an onto map.

Lemma 2. φ_g is bijective.

Proof: Since φ_g is onto, only left to show that is also one-to-one map. If $gh = gh'$ where $h, h' \in G$ then implies that $h = h'$. Indeed, φ_g is bijective. □

By lemma 2, we have that exists a $\mathcal{H}$ left transversal for H in G, then

$$|G| = \sum_{\mathcal{H}} |gH| = \sum_{\mathcal{H}} |H| = |\mathcal{H}||H|$$

□

However, the converse of Lagrange's Theorem is false, let's see the following example.

Example. Let A_4 be the **alternating group** (i.e., group of even permutations of a finite set) of order 12, which has no subgroup of order 6.

Definition 9. The **order of an element** g in a finite group G is given by $g^m = 1_G$. By Theorem 1, m divides $|G|$.

Proposition 6. Any group of even order, has an element of order two.

Proof: Let G be a group and suppose that $|G| = 2m$, then one elemenet of G is obviously 1_G which left us $2m - 1$ elements. Apart of the elements paired with their inverses, there is an element $g \in G$ such that $g = g^{-1}$. Thus, g is an element of order two. □

Definition 10 (Cyclic group). Let C_n be a group which is generated by a single element c such that $C_n = \langle c \rangle$ where every element of C_n is a power of c.

Proposition 7. If m and n are relative primes, then $C_{mn} \cong C_m \times C_n$.

Proof: Let $C_{mn} = \langle c \rangle$ be cyclic of order mn. Let $M = \langle c^m \rangle \cong C_m$ and $N = \langle c^n \rangle \cong C_n$. $c^k \in M$ iff k divides m and $c^k \in N$ iff k divides n. Now, if $c^k \in M \cap N$, then k divides m and n, in fact k divides mn, thus $M \cap N = 1_{C_{mn}}$. Hence $MN = C_{mn}$, since m and n are relative primes. □

Definition 11 (Euler's ϕ function). Euler's function $\phi(n)$ is the number of integers $1 \leqslant k \leqslant n$ that are relatively prime to n. Where

$$\phi(n) = n \prod_{p \text{ prime}, \ p|n} (1 - 1/p).$$

Proposition 8. A cyclic group of order n, has exactly $\phi(n)$ elements order n.

Proof: Let $G = \langle c \rangle$ be cyclic of order n. Let $1 \leqslant k \leqslant n$ such that $(c^k)^n = 1_G$, then k has order n iff k and n are relatively prime. If $\gcd(k, n) = 1$, then c^k has order n. If $(c^k)^m = 1_G$, then n divides km and n divides m. □

Definition 12 (p-groups). Let p be a prime, then a p-group is a group of order power of p.

THEOREM 2 (Fundamental Theorem of Finite Abelian Groups). Let G be a finite additive group (i.e., $+ : G \times G \longrightarrow G$), let $p > 0$ be a prime number that divides G and let $G(p)$ be the unique p-subgroup of G of maximal order. Then,

$$G = \bigoplus_{p||G|} G(p),$$

where $G(p) = \{x \in G \mid x^{p^r} = 1_G, \text{ for some integer } r\} \trianglelefteq G$ and $|G(p)| = p^n$.

Futhermore, if $p| \ |G|$, then

$$G(p) \cong \bigtimes_{i=1}^{r} \mathbb{Z}/p^{p_{n_i}}\mathbb{Z},$$

where r is unique and $1 \leqslant n_1 \leqslant \cdots \leqslant n_r$ also unique relative to this ordering.

Proof: First, let's prove that $G \cong G(p_1) \times \cdots \times G(p_r)$. Clearly, $|G(p_1) \dots G(p_r)| = |G(p_1)| \dots |G(p_r)|$ since $G(p_1) \dots G(p_r)$ is a group, if $x_1 \dots x_r = 1_G$ with $x_i \in G(p_i)$ for $i = 1, \dots, r$, then $G(p_1) \times \cdots \times G(p_r) \longrightarrow G$ is a group homomorphism since $x_j^{n/p_i^{m_i}} = 1_G$ for all $j \neq i$. Thus, the map is clearly isomorphism. By the above, each $G(p)$ is isomorphic to product of clyclic p-groups, so now we need to show that

$$(*) \qquad \bigtimes_{i=1}^{r} \mathbb{Z}/p^{n_i}\mathbb{Z} \cong \bigtimes_{j=1}^{s} \mathbb{Z}/p^{m_j}\mathbb{Z},$$

with $n_1 \geqslant \cdots \geqslant n_r$ and $m_1 \geqslant \cdots \geqslant m_s$. Mutliplying (*) by p we get

$$\bigtimes_{i=1}^{r} \mathbb{Z}/p^{n_i-1}\mathbb{Z} \cong \bigtimes_{j=1}^{s} \mathbb{Z}/p^{m_j-1}\mathbb{Z}$$

as $p(\mathbb{Z}/p^k\mathbb{Z}) \cong \mathbb{Z}/p^{k-1}\mathbb{Z}$ for all k. Then $|G(p)| = \prod_{i=1}^{r} p^{n_i} = \prod_{i=1}^{s} p^{m_i}$, so we conclude that $r = s$ and $n_i = m_i$ for all i. □

As you can see, Theorem 2 generalizes to finitely generated abelian groups. Futhermore, an abelian group G is called:

i) *Torsion-free*, if every non-identity element in G has infinite order.
ii) *Torsion*, if every non-identity element in G has finite order.

1.4. Isomorphism.

1.4.1. *The first isomorphism theorem.*

THEOREM 3 (First Isomorphism Theorem). Let $\varphi : G \longrightarrow G'$ be a group homomorphism. Then $\operatorname{Ker}\varphi$ is a normal subgroup of G, and there is an isomorphism $\rho : G/\operatorname{Ker}\varphi \longrightarrow \operatorname{Im}\varphi$ given by $\rho(g\operatorname{Ker}\varphi) = \varphi(g)$. In fact, $G/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi$.

Proof: We need to prove that ρ is surjective and injective. Let $\psi : G \longrightarrow G/\operatorname{Ker}\varphi$, Since $\rho = \varphi \circ \psi$, then ρ is surjective. Now, let $x \in \operatorname{Ker}\rho$ such that x has the form $g\operatorname{Ker}\varphi$, then $\rho(x) = \varphi(g)$. Thus, $g \in \operatorname{Ker}\rho$. So ρ is injective and indeed is an isomorphism.

PROPOSITION 9. Any two cyclic groups of order n are isomorphic.

Proof 1: Let $G_1 = \langle \mathrm{a} \rangle$ and $G_2 = \langle \mathrm{b} \rangle$ such that $|a| = |b| = n$. Then there is a map $\varphi : G_1 \longrightarrow G_2$ such that there is a bijection $\varphi(a^n) = b^n$ since that if $a^n = a^r$ and $b^r = b^n$ then $\varphi(a^n) = \varphi(a^r) = b^r = b^n$. Now, let $x = a^s, y = a^t \in G_1$ then

$$\varphi(xy) = \varphi(a^s a^t)$$

$$\begin{aligned} &= \varphi(a^{s+t}) \\ &= \varphi(b^{s+t}) \\ &= \varphi(b^s b^t) \\ &= \varphi(a^s)\varphi(a^t) \\ &= \varphi(x)\varphi(y) \end{aligned}$$

Thus, φ is homomorphism. Indeed, $G_1 \cong G_2$. □

Proof 2: There is a more abstract proof about proposition 9. Let G be a cyclic group with generator g, then there is a surjective homomorphism $(\mathbb{Z}, +) \longrightarrow G$ sending 1 to g. Let $H \leqslant \mathbb{Z}$ be a subgroup, by Theorem 3 $G \cong \mathbb{Z}/H$, thus we can generate the subgroups $0\mathbb{Z}, 1\mathbb{Z}, 2\mathbb{Z}, \dots$. The quotient group $\mathbb{Z}/n\mathbb{Z}$ has order n if $n \neq 0$ and order ∞ if $n = 0$, the order of G determines its isomorphism class. So, if $|G| = n$ is finite, then $G \cong \mathbb{Z}/n\mathbb{Z}$ and if $|G|$ is infinite, then $G \cong \mathbb{Z}$. □

1.4.2. *The second isomorphism theorem.*

Theorem 4 (Second Isomorphism Theorem). Let G be a group, $H < G$ be a subgroup and $N \lhd G$ be a normal subgroup. Then $HN \leqslant G$

is a subgroup, $N \trianglelefteq HN$ a normal subgroup, $H \cap N$ is a normal subgroup of H. In fact, there is a map isomorphism $\varphi : H/(H \cap N) \longrightarrow HN/N$.

Proof: First, we show that $HN \leqslant G$. Since $N \lhd G$, then $NH = HN$ and $1_G \in HN$. Let $h \in H$ and $n \in N$, then $hn \in HN$ and $(hn)^{-1} = n^{-1}h^{-1} \in HN = NH$. So, $HNHN = HHNN = HN$.

Now, as N is normal in G, it's certainly normal in HN, so we have a map

$$\rho : H \longrightarrow HN/N,$$

such that ρ sends h to hN. Suppose $x \in HN/N$, then $x = hnN = hN$, thus ρ is surjective. Suppose that $h \in \operatorname{Ker} \rho$, then $hN = N$ the identity coset, so that $h \in N$. Thus, $h \in H \cap N$. Then, $h \in \operatorname{Ker} \varphi$ and by Theorem 3 φ is isomorphic. □

1.4.3. *The third isomorphism theorem.*

THEOREM 5 (Third Isomorphism Theorem). Let G be a group and $N, M \trianglelefteq G$ be two normal subgroups such that $N \subset M$. Then

$$G/M \cong (G/N)(M/N).$$

Proof: Let $\rho : G \longrightarrow G/M$ be a map such that $N \subset \operatorname{Ker} \rho$, then there is a homomorphism $\phi : G/N \longrightarrow G/M$.

So, ϕ is surjective since ϕ sends gN to the left coset gM. Now, suppose that $gN \in \operatorname{Ker} \phi$, then the left coset gM is the identity coset, that is, $gM = M$, so that $g \in M$. Thus, the kernel consists of those left cosets of the form gN, for $g \in M$, that is, M/N. Indeed, by Theorem 3 then $G/M \cong (G/N)(M/N)$. □

1.5. Direct Products.

One way to construct groups from small groups is thought direct products.

DEFINITION 13. Let G_1, G_2 be two groups, then its direct product is denoted by $G_1 \oplus G_2$, which is in the end the cartesian product (i.e., $(x_1, x_2, \dots x_n)(y_1, y_2, \dots, y_n) = (x_1y_1, x_2y_2, \dots x_ny_n)$)

PROPOSITION 10. Let $G_1, G_2, \dots G_m$ be groups of order n. Then

$$G = \bigoplus_i G_i,$$

is in fact a group.

Proof: We have that $1_G = (1_{G_1} \dots 1_{G_m})$ is the identity element of G. Since we have a cartesian product of groups, then G is associative. Now, let g be any element of G, since $g = (g_1 \dots g_m)$ then its inverse is $g^{-1} = (g_1^{-1} \dots g_m^{-1})$. Indeed, G is a group. □

PROPOSITION 11. Let G_1, G_2 be groups, we say that a group G is isormorphic to the direct product $G_1 \oplus G_2$ iff there exists normal subgroups $A, B \lhd G$ such that $A \cong G_1$, $B \cong G_2$, $A \cap B = 1_G$ and $AB = G$.

Proof: Let $\varphi : G_1 \oplus G_2 \longrightarrow G_1$ and $\rho : G_1 \oplus G_2 \longrightarrow G_2$ be two projective maps then $\operatorname{Ker}\varphi$ and $\operatorname{Ker}\rho$ are two normal subgroups from $G_1 \oplus G_2$. We can see that $\operatorname{Ker}\varphi \cap \operatorname{Ker}\rho = 1_G$ and $\operatorname{Ker}\varphi \oplus \operatorname{Ker}\rho = G_1 \oplus G_2$ since $(x_1, x_2) = (x_1, 1)(1, x_2)$ for every $(x_1, x_2) \in G_1 \oplus G_2$ and every $(x_1, 1) \in \operatorname{Ker}\rho$ and $(1, x_2) \in \operatorname{Ker}\varphi$.

Suppose that the map : $G_1 \oplus G_2 \longrightarrow G$ be an isomorphism map, then $A = (\operatorname{Ker}\rho)$ and $B = (\operatorname{Ker}\varphi)$ are normal subgroups of G. Indeed, $A \cong \operatorname{Ker}\rho \cong G_1$, $B \cong \operatorname{Ker}\varphi \cong G_2$, $A \cap B = 1_G$ and $AB = G$. □

By proposition 11 we can define the **internal direct sum** as follows.

DEFINITION 14. Let G be a group, which is the internal direct sum of the groups $G_1 \oplus \cdots \oplus G_n$ when $G_i \trianglelefteq G$ for all $i = 1, \dots, n$, $\bigcap_i G_i = 1_G$ and $G_1 \dots G_n = G$.

EXAMPLE. Let $p_1, \dots, p_n$ be primes numbers. An abelian group of order $p_1^{k_1}, \dots, p_n^{k_n}$ is a direct sum of subgroups of order $p_1^{k_1}, \dots, p_n^{k_n}$.

About internal direct sums, we cay say that a group G is **indecomposable** when $G \neq 1$ and $G = M \oplus N$, that implies that $M = 1$ or $N = 1$. In this way, every finite group is a direct sum of indecomposable subgroups.

PROPOSITION 12. Every group of finite length is a direct sum of finitely indecomposable subgroups.

Proof: Let $G = A \oplus B$ and $M = C \oplus D$, then $G = A \oplus C \oplus D$ for some subgroup A, so $C, D \trianglelefteq G$. Then $C, D \subsetneq M$, so M is not indecomposable, but C and D are direct sums of indecomposable subgroups, the so is M, which is the required contradiction. □

We need to notice, that a simple group and indecomposable group are not equivalence. A simple group is indecomposable but an indecomposable group need not be simple.

EXAMPLE. $\mathbb{Z}/p^2\mathbb{Z}$ is indecomposable but not simple.

THEOREM 6 (Krull-Schmidt Theorem). Let G be a group of finite length such that is a direct sum

$$G = G_1 \oplus \cdots \oplus G_n = H_1 \oplus \cdots \oplus H_m$$

of indecomposable subgroups. Then $m = n$ and $G_i \cong H_i$. Hence,

$$G = G_1 \oplus \cdots \oplus G_k \oplus H_{k+1} \oplus \cdots \oplus H_n.$$

Proof: REMAINDER.

It's interesting see how in definition 14 is needed to keep both subgroups as normal subgroups. ***What would happen if only one of them would be normal?***

Well, supposing that G_1 is normal and G_2 is not, we can get the following interesting facts:

1. Since G_1 is normal, then for every $g_2 \in G_2$ we have $g_2 G_1 g_2^{-1} = G_1$, that means, each g_2 induces an automorphism of G_1. So, we can define a homomorphism map $\varphi : G_1 \longrightarrow \operatorname{Aut} G_2$, by letting g_2 map to the homomorphism $g_1 \mapsto g_2 g_1 g_2^{-1}$.

2. If G_1 and G_2 are abelian groups, that not mean that $G_1 \oplus G_2$ is necessarily abelian. By example, the symmetry group S_3 is a nonabelian group of order 6 viewed as the permutations of $\{1, 2, 3\}$, which is the cyclic group C_3 of order 3. If we letting $G_1 = C_3$ and $G_2 = C_2$ (i.e., cyclic group of order 2), then $G = \{I, (1, 2, 3), (1, 3, 2)\}$, which is not an abelian group.

3. If G_1 and G_2 have the same order k, that not mean that G should be of the same order (no as example 1.5). By example, letting $G_1 = C_2 \times C_2 = \{1, x\} \times \{1, x\}$ (which is of exponent 2), if we take $G_2 = \{1, n\} = C_2$, also of exponent 2, and let the nontrivial element of G_2 act on G_1 by the rule $n^{-1}(a, b)n = (b, a)$. Then, $(x, 1)n$ has order 4:

$$\begin{aligned}\big((x,1)n\big)^2 &= (x,1)n(x,1)n = (x,1)(n^{-1}(x,1)n) = (x,1)(1,x) = (x,x)\\ \big((x,1)n\big)^3 &= (x,x)(x,1)n = (1,x)n\\ \big((x,1)n\big)^4 &= (1,x)n(x,1)n = (1,x)(n^{-1}(x,1)n) = (1,x)(1,x) = (1,1).\end{aligned}$$

So far, we've seen interesting facts if only one of the groups is normal. So, let's make of this a defintion.

Definition 15 (Semidirect products). Let G be a group, which is isomorphic to the semidirect product of the groups G_1, G_2 iff there exist subgroups M and N of G such that $M \cong G_1$, $N \cong G_2$ where $M \lhd G$, $M \cap N = \{1_G\}$ and $MN = G$.

Perhaps, the notation for direct products and direct sums could be a little messy, however, we will specify which direct operation we are working on to be more precise. In the end, we will see what are the differents between these operations.

1.6. Conjugacy.

Definition 16. Conjugacy, is an equivalence relation on a group G such that $g, x \in G$, then ${}^{g}x = gxg^{-1}$, these equivalence classes are the **conjugacy classes** of G. So, any group G can be partitioned into conjugacy classes,

$$^{G}x = \{^{g}x : g \in G\}$$

for the conjugacy class of x in G.

Definition 17. The centralizer in G of an element x of a group G is

$$C_G(x) = \{g \in G \mid gx = xg\}.$$

We notice that the number of conjugates of an element of a group G is the index of its centralizer in G.

Definition 18. Let G be a group and $H < G$ be a subgroup. The **normalizer** of H in G is defined by

$$N_G(H) := \{g \in G \mid gHg^{-1} = H\}.$$

Proposition 13 (The Class Equation). In a finite group G,

$$|G| = \sum |C| = |Z(G)| + \sum_{|C|>1} |C|.$$

Proof: As the conjugacy classes constitute a partition of G, then $|G| = \sum |C|$. Iff $x \in Z(G)$, then the conjugacy class of x is trivial, this is $|C| = 1$.

Hence,

$$|G| = \sum |C| = \sum_{|C|=1} + \sum_{|C|>1} |C| = |Z(G)| + \sum_{|C|>1} |C|.$$

□

2. Groups Actions

Now that we know some basic structures about groups, let's see how a group G **acts** on a set X and which is the effect of this.

Definition 19. Let G be a group, let X be a set and let a homormorphism $* : G \longrightarrow S_X$ where S_X is the permutation set of X. We say that the pair $(X, *)$ is called a G-action.

Thus, in Definition 19 for each $g \in G$ gives a permutation $*_g$ of X, which sends any element $x \in X$ to an element $*(g)x$. We need to remark that if $* : G \times X \longrightarrow X$, then $(X, *)$ is called a left G-action and if $* : X \longrightarrow G \times X$, then is called a right G-action and X is a G-set.

Now, we can set up an equivalence relation. If X is a G-set, then we define the **stabilizer** of $x \in X$ by

$$\mathrm{Stab}(x) = G_x = \{g \in G \mid g * x = x\}.$$

Definition 20. The **orbit** of an element $x \in X$ is the subset given by

$$G \cdot x = \{g \cdot x : g \in G\} \subseteq X.$$

- The **kernel** of a group action $\varphi : G \longrightarrow S_X$ is the normal subgroup of G consisting of the elements acting trivially on X. Then,
$$\ker \varphi = \bigcap_{x \in X} G_x = \{g \in G : X^g = X\}.$$
- A G-action on X is **faithful** or **effective** if $\mathrm{Ker}\,\varphi$ is trivial. Equivalently, the action is faithful if no trivial element of G acts trivially on X. In other words, a group action is faithful iff the homomorphism to the group of transformation is an injection.

Now, it's necessary to prove that actually a G-action generates a bijection.

Proposition 14. Let X be a G-set, $x \in X$. Define

$$f_x : G/G_x \longrightarrow G * x \text{ by } gG_x \mapsto g * x.$$

Then, f_x is a well-defined bijection. In particular, if $|G : G_x|$ is finite, then

$$|G * x| = |G : G_x| \text{ and } |G * x| \text{ divides } |G|.$$

Proof: Let $g, g' \in G$, then $g * x = g' * x$

i. iff $g'^{-1} * (g * x) = x$,
ii. iff $(g'^{-1}g) * x = x$,
iii. iff $g'^{-1}g \in G_x$,
iv. iff $gG_x = g'G_x$.

Then, f_x is well-defined, one-to-one and surjective. So, claim follows. □

Example. Let X be a set, and define $\mathrm{Aut}_{\mathrm{Set}}(X)$ to be the set of automorphisms on X, which arises a group action.

Example. Let $G = X$ be a G-set by itself. The left action is given by

$$* : G \times X \longrightarrow X \text{ by } g * x = gxg^{-1}$$

called *conjugation* by G. The orbit of an element $a \in X = G$ is

$$C(a) := G * a = \{xax^{-1} \mid x \in G\},$$

called the *conjugacy class* of a, and the *stabilizer* of a is

$$\mathrm{Stab}(a) := G_a = \{x \in G \mid xax^{-1} = a\} = \{x \in G \mid xa = ax\}.$$

This subgroup of G, is called the *centralizer* of a. So, $Z_G(a)$ is the set of elements of G commuting with a. In particular, $\langle \mathrm{a} \rangle \subset Z_G(a)$. The set of fixed points of this action is

$$\begin{aligned} F_G(X) &= \{a \in X \mid xax^{-1} = a \text{ for all } x \in G\} \\ &= \{a \in G \mid xa = ax \text{ for all } x \in G\}, \end{aligned}$$

the *center* $Z(G)$ of G.

Definition 21. Let n be a positive integer and let

$$S_n \overset{\mathrm{def}}{=} \mathrm{Aut}_{\mathrm{Set}}(\{1, 2, \ldots, n\}).$$

We call this the **symmetry group** of n letters.

Theorem 7 (Cayley's Theorem). Every group G is isomorphic to a subgroup of the symmetric group S_G.

Proof: Let G be a group, and let S_G be the permutation group of G. For each $g \in G$, define $\rho_g : G \longrightarrow G$ by $\rho_g(g) = gh$. Then ρ_g is invertible with inverse $\rho_{g^{-1}}$, and so is the permutation of the set G.
Define $\phi : G \longrightarrow S_G$ by $\phi(g) = \rho_g$. Then ϕ is a homomorphism, since

$$(\phi(gh))(x) = \rho_{gh}(x) = ghx = \rho_g(hx) = (\rho_g \circ \rho_g)(x) = ((\phi(g))(\phi(h)))(x),$$

and ϕ is injective, since if $\phi(g) = \phi(h)$ then $\rho_g = \rho_h$, so $gx = hx$ for all $x \in X$, and so $g = h$ as required. So ϕ is an embedding of G into its own permutation group. If G is finite of order n, then simply numbering the element of G gives an embedding from G to S_n. □

Now, let's see a generalization of Cayley's Theorem given by Prof. Terence Tao (see), this generalization is about to have an index n subgroup that is isomorphic to a fixed group H.

THEOREM 8 (Cayley's Theorem for H-sets). Let H, G be groups such that G has index n and is isormorphic to H. Then, G is isomorphic to a subgroup $\tilde{G}$ of the semidirect product $S_n \ltimes H^n$, defined explicity as the set of tuples

$$(\phi, (h_i)_{i=1}^n)(\rho, (k_i)_{i=1}^n) := (\phi \circ \rho, (h_{\rho(i)} k_i)_{i=1}^n)$$

and inverse

$$(\phi, (h_i)_{i=1}^n)^{-1} := (\phi^{-1}, (h_{\phi(i)}^{-1})_{i=1}^n).$$

Proof: Let X, Y be H-sets and let a morphism $f : X \longrightarrow Y$ which respects the right action of H, thus $f(x)h = f(xh)$ for all $x \in X$ and $h \in H$. Suppose that $H \subset G$, then we can see G as an H-set, in this way, we notice that G is isomorphic to the H-set $\{1. \dots, n\} \times H$ with the right action of $H : (i, h)k := (i, hk)$ and identified with $S_n \ltimes H$, acting on the former H-set by the rule

$$(\phi, (h_i)_{i=1}^n)(i, h) := (\phi(i), h_i h).$$

□

2.1. Orbits. Now, let's extend the idea of equivalence relation introduced in Definition 20.

LEMMA 3. Let X be a G-set under $*$, then $\sim_G$ is an equivalence relation on X.

Proof: We need to prove three points:

1. **Reflexitivity:** For all $x \in X$, we see that $x = 1_G * x$, so $x \sim_G x$.
2. **Symmetry:** If $x_1 \sim_G x_2$, then there is a $g \in G$ such that $x_1 = g * x_2$, indeed
$$g^{-1} * x_1 = g^{-1} * (g * x_2) = 1_g * x_2 = x_2.$$
Of course, $x_1 = g * x_2$ iff $x_1 * g^{-1} = x_2$.
3. **Transitivity:** Suppose that $x_1 \sim_G x_2$ and $x_2 \sim_G x_3$. Let $g, g' \in G$ such that $x_1 = g * x_2$ and $x_2 = g' * x_3$. Then, $x_1 = g * x_2 = g * (g' * x_3) = (g.g') * x_3$, so $x_1 \sim_G x_3$.

□

Thanks to Lemma 3, we can see that the equivalence class of x via $\sim_G$ is actually the set

$$\overline{x} = \{g * x \mid g \in G\}.$$

As we've seen in Definition 20, the set $\overline{x}$ is called the orbit of x under $*$, which gives a system of representatives $\mathcal{O}$ for the equivalence classes under $\sim_G$.

Definition 22 (Mantra of G-actions). Let X be a G-set and $\mathcal{O}$ a system of representatives. Then

$$X = \bigvee_{\mathcal{O}} G * x \text{ and if } |X| \text{ is finite, then } X = \sum_{\mathcal{O}} |G * x|.$$

Theorem 9 (Orbit Descomposition Theorem). Let X be a G-set. Then

$$X = F_G(X) \vee \bigvee_{\mathcal{O}*} G * x.$$

In particular, if X is a finite set, then

$$|X| = \sum_{\mathcal{O}} |G * x| = |F_G(X)| + \sum_{\mathcal{O}*} [G : G_x].$$

Proof: By Definition 22, $|G * x| = [G : G_x]$. So, claim follows. □

Example (A precise example). Let $G = D_3 = \{e, r, r^2, f, fr, rf\}$, with $|G| = 6$ and satisfying $r^3 = e = f^2$ and $frf^{-1} = r^{-1} = r^2$. We have $fr = r^2 f$ and $rf = fr^2$, so

$$\begin{aligned} C(e) &= \{e\} && \text{and} \quad 1|6 \\ C(r) &= \{r, r^2\} && \text{and} \quad 2|6 \\ C(f) &= \{f, fr, rf\} && \text{and} \quad 3|6 \end{aligned}$$

and

$$\begin{aligned} Z_G(e) &= G && \text{and} \quad |C(e)| = [G : Z_G(e)] = 1 \\ Z_G(r) &= \{e, r, r^2\} && \text{and} \quad |C(r)| = [G : Z_G(r)] = 2 \\ Z_G(f) &= \{e, f\} && \text{and} \quad |C(f)| = [G : Z_G(f)] = 3 \end{aligned}$$

with fixed points

$$Z(G) = \{e\},$$

so

$$\begin{array}{ccccccc} |G| & = & |Z(G)| & + & |C(r)| & + & |C(f)| \\ 6 & = & 1 & + & 2 & + & 3. \end{array}$$

Theorem 10 (Cauchy's Theorem). Let p be a prime number which divides the order of the finite group G. Then there exists an element of G of order p.

Proof: Let G be a finite group and p a prime number which divides the order of G. Set

$$X = \{(g_1, \dots, g_p) \in G^p \mid g_1 \dots g_p = e \text{ in } G\} \subset G^p,$$

where $G^p = G \times \cdots \times G$ (p times). Let $(\mathbb{Z}/p\mathbb{Z}, +)$ act on X. Applying Orbit Descomposition Theorem 9, we get

$$|G^p| = |X| = |F_{\mathbb{Z}/p\mathbb{Z}}(X)| + \sum_{\mathcal{O}*} [\mathbb{Z}/p\mathbb{Z} : (\mathbb{Z}/p\mathbb{Z})_x].$$

If $x \in \mathcal{O}^*$, then $(\mathbb{Z}/p\mathbb{Z})_x = 1$ as $\mathbb{Z}/p\mathbb{Z}$ has only the trivial subgroups. So,

$$0 \equiv |X| \equiv |F_{\mathbb{Z}/p\mathbb{Z}}(X)| \mod p.$$

Clearly, $e \neq g_1 = \cdots = g_p$. Then, $g^p = e$ as needed. □

PROPOSITION 15. The order of the orbit of an element is equation to the index of its stabilizer.

Proof: Let G act on X. Let $x \in X$, there is a surjection map $* : G \longrightarrow G \times X$ onto the orbit of x induces a injection correspondence between the elements of the orbit x and the classes of the equivalence relation induced on G by $*$. The latter are the left cosets of $\text{Stab}(x)$, since $g * x = h * x$ is equivalent to $x = g^{-1}h * xx$ and to $g^{-1}h \in \text{Stab}(x)$. Hence the order of the orbit of x equals the number of left cosets of $\text{Stab}(x)$. □

3. Simple Groups

Now that we know some facts about Definition 7, we can establish a relation between the center and simple groups. First, let's see what a simple group is.

DEFINITION 23. Let G be a group. We say that G is simple if G has no normal subgroups other than trivial ones (i.e., 1_G and G).

PROPOSITION 16. Every homomorphism from a simple group to another group is either injective or trivial.

Proof: Let $f : G \longrightarrow G'$ a nontrivial homomorphism from a simple group G into another group G', since $\text{Ker} f$ is a normal subgroup of G, then f is automatically injective and claim follows. □

By Proposition 16, if G is nonabelian simple, then the center $Z(G) = \{1_G\}$. By Lagrange's Theorem 1, any group of order prime is simple.

EXAMPLE. A_5 is the unique simple non-abelian group of smallest order.

Example. The $\mathrm{PSL}_n(K)$ for $n \geqslant 3$ and k has at least four elements, is simple.

Definition 24. Let G be a group and H a subgroup of G. We define the **core** of H in G by $\mathrm{Core}_G(H) := \bigcap_G xHx^{-1}$.

Lemma 4. Let H be a group, and suppose that HG is a subgroup with $|G : H| = n$. Then H contains a normal subgroup N of G such that $|G : N|$ divides $n!$.

Proof: Letting $N = \mathrm{Core}_G(H)$. Then G/N is isomorphic to a subgroup of the symmetric group S_n, and by Lagrange's Thereom 1, $|G/N|$ divides $|S_n| = n!$. □

Lemma 5. Let G be a simple group such G contains a subgroup of index $n > 1$. Then $|G|$ divides $n!$.

Proof: Taking N from Lemma 4, then it's proper in G because $n > 1$. Since G is simple, $N = 1$ and thus $|G| = |G/N|$ divides $n!$. □

4. Sylow's theorem

Let $p > 1$ and $m > 1$ be relatively primes. Let G be a group of order $p^r m$ where $r > 0$. We define the Sylow p-subgroup H of G by

$$\mathrm{Syl}_p(G) := \{H \mid H \text{ a Sylow } p\text{-subgroup of } G\}.$$

4.1. First Sylow Theorem.

Theorem 11 (First Sylow Theorem). Let p be a prime number. Let $k > 0$ such that p^k divides the order a group G, then G has a subgroup of order p^k.

Proof: By induction and assuming that $k \geqslant 2$, let T be a finite group such that $|T| < |G|$ and $p^k||T|$, then T contains a subgroup of order p^k. Now, we need to show that G actually contains a subgroup of order p^k.

Let H be a proper subset of G such that $H = \langle \mathrm{a} \rangle$ where $a \in G$. If $a \in Z(G)$, we see that $xa^ix^{-1} = a^i$ for all $x \in G$ and $i \in \mathbb{Z}$. Then $p \mid [G : Z_G(a)]$. In particular, $H \trianglelefteq G$ and G/H is a group of order $[H : H] = |G|/|H| = |G|/p < |G|$. Since $p^{k-1}||G/H|$, then there exists a subgroup $T \subset G/H$ of order p^{k-1}. Let $* : G \longrightarrow G/H$ be the canonical epimorphism. Then H is the kernel and there exists a subgroup $\tilde{T}$ of G containing G and satisfying $T = \tilde{T}/H$. Hence $|\tilde{T}| = |T||H| = p^m$, and claim follows. □

First Sylow Theorem can be viewed as a generalization of Cauchy's Theorem 10.

Lemma 6. Let P be a Sylow p-subgroup of a group G. Then every p-subgroup of the normalizer $N_G(P)$ is contained in P.

Proof: Let $H \leqslant N_G(P)$ be a p-subgroup. Since H normalizes P, the product HP is a subgroup of $N_G(P)$ and $P \trianglelefteq HP$. Since

$$HP/P \cong H/H \cap P$$

is a quotient of the p-group H, and P is a p-group, it follows that HP is a p-group. And $P \leqslant HP$. But P is maximal p-subgroup of G, by definition of Sylow p-subgroup. Hence $HP = P$, meaning that $H \leqslant P$. □

4.2. Second and Third Sylow Theorems.

Theorem 12 (Second Sylow Theorem). Let p be a prime number. The number of Sylow p-subgroups of a finite group G divides the order of G and is congruent to 1 module p.

Theorem 13 (Third Sylow Theorem). Let p be a primer number. All Sylow p-subgroups of a finite group are conjugate.

Proof: As Sylow did it, let's prove Theorem 12 and 13 together. Let S be a Sylow p-subgroup. A conjugate of a Sylow p-subgroup is a Sylow p-subgroup, therefore S acts on the set $\mathfrak{S}$ of all Sylow p-subgroups by inner automorphisms. Under this action, $\{S\}$ is an orbit, since $aSa^{-1} = S$ for all $a \in S$. Conservely, if $\{T\}$ is a trivial orbit, then $aTa^{-1} = T$ for all $a \in S$ and $s \subseteq N_G(T)$, then $T \trianglelefteq N_G(T)$ and yields $S = T$. Thus $\{S\}$ is the only trivial orbit. The orders of the other orbits are indexes in S of stabilizers and are multiples of p. Hence $|\mathfrak{S}| \equiv 1 \mod p$.

Suppose that $\mathfrak{S}$ contains two distinct conjugacy $\mathcal{C}$ and $\mathcal{C}'$ of subgroups. Any $S \in \mathcal{C}$ acts on $\mathcal{C}$ and $\mathcal{C}' \subseteq \mathfrak{S}$ by inner automorphisms. Then the trivial orbit $\{S\}$ is in $\mathcal{C}$, by the above, $|\mathcal{C}| \equiv 1$ and $|\mathcal{C}'| \equiv 0 \mod p$. But any $T \in \mathcal{C}'$ also acts on $\mathcal{C} \cup \mathcal{C}'$ by inner automorphisms, then the trivial orbit $\{T\}$ is in $\mathcal{C}'$, so that $|\mathcal{C}'| \equiv 1$ and $|\mathcal{C}| \equiv 0 \mod p$. This shows that $\mathfrak{S}$ cannot contain two distinct conjugacy classes of subgroups. Therefore $\mathfrak{S}$ is a conjugacy class and $|\mathfrak{S}|$ divides $|G|$. □

Proposition 17. In a finite group, every p-subgroup is contained in a Sylow p-subgroup.

Proof: As we seen, a p-subgroup H of a finite group G acts by inner automorphisms on the set $\mathfrak{S}$ of all Sylow p-subgroups. Since $|\mathfrak{S}| \equiv 1 \mod p$ there is a least one trivial orbit $\{S\}$. Then $hSh^{-1} = S$ for all $h \in H$ and $H \subseteq N_G(S)$. Now, S is a Sylow p-subgroup of $N_G(S)$, and $H \subseteq S$, so $S \trianglelefteq N_G(S)$. □

5. Series

Definition 25. Let G be a non-trivial group. A sequence of groups

$$N_0 \subset N_1 \subset \cdots \subset N_n = G,$$

is called *subnormal* if $N_i \trianglelefteq N_{i+1}$ and called *normal* if $N_i \trianglelefteq G$. The quotients $N_n/N_{n-1}, \ldots, N_1/N_0$ are called the *factors* of the series. Letting $N_0 = 1_G$ and $N_n = G$, then it's called

I. **Cyclic series**, if N_{i+1}/N_i is cyclic for all i.
II. **Abelian series**, if N_i/N_i is abelian for all i.
III. **Composition series**, if N_{i+1}/N_i is simple for all i.

Two normal series are equal if both of them have the same length, the same factors and up to isomorphism and indexing.

Example. Let $C = \langle \mathrm{c} \rangle$. Then, the series $1 \trianglelefteq \{1, c^3\} \trianglelefteq C$ and $1 \trianglelefteq \{1, c^2, c^4\} \trianglelefteq C$ are equal.

5.1. Normal series.

Definition 26. A *refinement* of a normal series $\mathcal{A}: 1_G = A_0, \trianglelefteq \ldots \trianglelefteq A_m = G$ is a normal series $\mathcal{B}: 1_G = B_0 \trianglelefteq \ldots \trianglelefteq B_n = G$ such that every A_i is one of the B_j's.

Theorem 14 (Schreier Refinement Theorem). Any two series of a group have equivalent refinements.

Proof: Let $\mathcal{A}: 1_G = A_0, \trianglelefteq \ldots \trianglelefteq A_m = G$ is a normal series $\mathcal{B}: 1_G = B_0 \trianglelefteq \ldots \trianglelefteq B_n = G$ two normal series of a group G. Let C_k, D_k where $0 \leqslant k \leqslant mn$, then we can write $k = ni + j$ for $0 \leqslant i < m$ and $0 \leqslant j < n$ as we can write $k = mj' + i'$ for $0 \leqslant i' < m$ and $0 \leqslant j' < n$. Then, there is a permutation $\phi : ni + j \longrightarrow mj + i$ of $\{0, 1, \ldots, mn - 1\}$.

By the above, we can see that $A_i = C_{ni} \subseteq \cdots \subseteq C_{ni+n} = A_{i+1}$ and $B_j = D_{mj} \subseteq \cdots \subseteq D_{mj+m} = B_{j+1}$, for all $0 \leqslant i < m$ and $0 \leqslant j < n$. Letting $A = A_i, A' = A_{i+1}$ and $B = B_j, B' = B_{j+1}$, then $C_{ni+j} = A(A' \cap B)$, $C_{ni+j+1} = A(A' \cap B')$, $D_{mj+i} = B(B' \cap A)$, $D_{mj+i+1} = B(B' \cap A')$ are subgroups of G, $C_{ni+j} \trianglelefteq C_{ni+j+1}$ and $D_{mj+i} \trianglelefteq D_{mj+i+1}$. So, they are normal series and refinements of $\mathcal{A}$ and $\mathcal{B}$. □

5.2. Composition series.

Proposition 18. Every finite group has a composition series.

Proof: Let $\mathcal{A} : \ 1_G = A_0 \ntrianglelefteq \ldots \ntrianglelefteq A_m = G$ has length $m \leqslant n$. Hence G has a strictly ascending normal series of maximal length. □

Theorem 15 (Jordan-Hölder Theorem). Any two composition series of a group are equivalent.

Proof: Let $\mathcal{A}$ and $\mathcal{B}$ be two compositions series from G. By Theorem 14, $\mathcal{A}$ and $\mathcal{B}$ have equivalent refinements $\mathcal{C}$ and $\mathcal{D}$, respectively. Let ϕ be a permutation such that $C_k/C_{k-1} \cong D_{\phi(k)}/D_{\phi(k-1)}$ for all $k > 0$ sends the nontrivial factors of $\mathcal{C}$ onto the nontrivial factors of $\mathcal{D}$, and sends the factors of $\mathcal{A}$ onto the factors of $\mathcal{B}$, therefore $\mathcal{A}$ and $\mathcal{B}$ are equivalent. □

Example. Let $m = a_1 \ldots a_n \in \mathbb{Z}$ where $a_i > 1$. Then we have a subnormal series

$$0 = a_1 \ldots a_n \mathbb{Z}/m\mathbb{Z} < \cdots < a_1\mathbb{Z}/m\mathbb{Z} < \mathbb{Z}/m\mathbb{Z}.$$

As $\mathbb{Z}/m\mathbb{Z}$ is finite group, by Proposition 18 it has a composition series.

6. Solvable Groups

Definition 27. A solvable group is a group with a normal series whose factors are abelian.

Example. Every abelian group is solvable.

Proof: Since any abelian group has a normal series $\mathcal{A}$, then for any two A_{i+1}/A_i where $A_{i+1}, A_i \in \mathcal{A}$ is actually a normal subgroup, then claim follows. □

Example. The dihedral group D_n is solvable for every $n \geqslant 2$ because it has a chain of subgroups $1 < C_n < G$ and $G/C_n = C_2$.

Definition 28. The *commutator* of two elements x, y is $xyx^{-1}y^{-1}$, the commutator subgroup of a group G is the subgroup G' of G generated by all commutators.

Proposition 19. G' is the smallest normal subgroup N of G such that G/N is abelian.

Proof: Since the inverse of a commutator is in fact a commutator, let $x \in G'$ b a product of commutators $x = c_1 \dots c_n$, then

$$axa^{-1} = ac_1a^{-1} \dots ac_na^{-1} \in G' \text{ for all } a \in G'.$$

Thus, $G' \trianglelefteq G$. If $N \trianglelefteq G$ and G/N is abelian, then $Nxy = Nyx$ and $xyx^{-1}y^{-1} \in N$ for all $x, y \in G$, and $G' \subseteq N$. □

Theorem 16. Let G be a group. Then G is solvable iff there exist an integer n such that $G^{(n)} = 1_G$.

Proof: It's known that $G^{(i)}/G^{(i+1)}$ is abelian, hence if $G^{(n)} = 1_G$ for some n, then G is solvable. Conversely, suppose that

$$1_G = N_n \subset N_{n-1} \subset \dots \subset N_1 \subset G$$

is an abelian series. By Proposition 19, $G' \subset N_1$. By induction, we suppose that $G^{(i-1)} \subset N_{n-1}$. Finally, $G^{(i)} = [G^{(i-1)}, G^{(i-1)}] \subset [N_{i-1}, N_{i-1}] \subset N_i$. □

Proposition 20. Every finite p-group is solvable.

Proof: As G has a subgroup N of order $p-1$, which is normal, then N and G/N are solvable. By induction, then G is in fact solvable. □

We can generalize Proposition 20 with the following proposition.

Proposition 21. Every group of order $p^m q^n$, where p and q are prime numbers, is solvable.

Proof: Since there are subgroups of order p^m and q^n, then by Proposition 20 are solvable. Then claim follows. □

Definition 29. A normal series $1_G = C_0 \trianglelefteq \dots \trianglelefteq C_m = G$ is **central normal series** when $C_i \trianglelefteq G$ and $C_{i+1}/C_i \subseteq Z(G/C_i)$ for all $0 \leqslant i < m$.

Definition 30. A group is **nilpotent** when it has a central normal series.

We can say that nilpotent groups are a kind of solvable groups with futher properties.

Proposition 22. Every finite p-group is nilpotent.

Proof: The trivial case is when $p \leqslant 2$, then claim follows. Suppose that $n > 2$, then G has a nontrivial center, then $G/Z(G)$ is nilpotent and so does G. □

7. The Hall Theorems

The Hall Theorems can be viewed as stronger versions of Sylow's Theorem seen in Section 4. Futhermore, these theroems hold in Solvable groups.

Theorem 17. Let m and n be relative prime numbers. Every solvable of order mn contains a subgroup of order m.

Proof: The trivial case is when m is a power of any prime number, then claims follows by First Sylow Theorem 11. Otherwise, let G be a group and suppose that it has a normal subgroup N of order $p^k > 1$ for some prime p and $k \in \mathbb{Z}$. Then, p^k divides m or n.

If p^k divides m, then $|G/N| = (m/p^k)n$, where m/p^k and n are relatively prime and $|G/N| < |G|$. By induction, G/N has a subgroup H/N of order m/p^k, where $N \subset H \leqslant G$, then $|H| = m$.

If P^k divides n, then $|G/N| = (n/p^k)m$, where n/p^k and m are relatively prime and $|G/N| < |G|$. By induction, G/N has a subgroup H/N of order m when $N \subseteq H \leqslant G$. Then $|H| = mp^k$. Now, $N \trianglelefteq H$, N is abelian, and N has order p^k, which is relatively prime to m. Then H has a subgroup of order m, and then so does G. □

Theorem 18. In a solvable group of order mn, where m and n are relatively prime, all subgroups of order m are conjugate.

Proof: Let G be group of order mn, if m is a power of any prime number, then claim follows by Third Sylow Theorem 13. Otherwise, let G be a group and suppose that it has a normal subgroup N of order $p^k > 1$ for some prime p and $k \in \mathbb{Z}$. Let $A, B \leqslant G$ have order m.

Suppose that p^k divides m. By induction, A/N and B/N are conjugate in G/N, $G/N = (Nx)(A/N)(Nx)^{-1}$ for some $x \in G$. Then

$$\begin{aligned} B &= \bigcup_{b \in B} Nb = \bigcup_{a \in A} (Nx)(Na)(Nx)^{-1} \\ &= \bigcup_{a \in A} Nxax^{-1} = N(xAx^{-1}) = xAx^{-1}, \end{aligned}$$

since $N = xNx^{-1} \subseteq xA^{-1}$. Thus A and B are conjugate in G.

Now, suppose that p^k divides n. Then $A \cap N = B \cap N = 1$, hence $|NA| = |NB| = p^k m$, and the subgroups $NA/N \cong A/(A \cap N)$ and $NB/N \cong B/(b \cap N)$ of G/N have order m. By induction, NA/N and NB/N are conjugate in G/N. Therefore, A and B are conjugate in G. □

Theorem 19. In a solvable group of order mn, where m and n are relatively prime, every subgroup whose order divides m is contained in a subgroup of order m.

Proof: Let G be group of order mn, if m is a power of any prime number, then claim follows by Proposition 17. Otherwise, let G be a group and suppose that it has a normal subgroup N of order $p^k > 1$ for some prime p and $k \in \mathbb{Z}$. Let H be a subgroup of G whose order l divides m.

Suppose that p^k divides m. Then $|NH/N| = |H|/|H \cap N|$ divides m, is relatively prime to n, and divides $|G/N| = (m/p^k)n$. By induction, H/N is contained in a subgroup K/N of G/N of order m, where $N \subseteq K \leqslant G$, then $|K| = p^k m$ and $H \subseteq HN \subseteq K$. If $p^k < n$, then $|K| < |G|$ and H is contained in a subgroup of K of order m, by the induction.

Now, suppose that $p^k = n$. Let A be a subgroup of G of order m. Then $A \cap N = 1, |NA| = |N||A| = |G|$ and $NA = G$. Hence $|A \cap NH| = |A||NH|/|ANH| = mp^k l/mn = l$. Thus, H and $K = A \cap NH$ are subgroups of NH of order l. By Theorem 18, H and K are conjugate in $NH : H = xKx^{-1}$ for some $x \in NH$. Then H is contained in the subgroup xAx^{-1} of G, which has order m. □

CHAPTER 2

Ring Theory

Another structure and one of the most used and important in Abstract Algebra, are rings.

Definition 31. Let R be a a set. A ring is an ordere triple $(R, +, \cdot)$ where $+$ and $\cdot$ are binary operations, such that:

R1. $(R, +)$ is an abelian group.
R2. $(R, \cdot)$ is a semigroup. Futhermore, the multiplication is associative.
R3. The multiplication is distributive: $x(y+z) = xy + yz$ and $(y+z)x = yx + zx$ for all $x, y, z \in R$.

From the above definition, we can remark that if $(R, \cdot)$ has an identity element, then we say that $(R, +, \cdot)$ is a ring with identity (i.e., 1_R). Meanwhile, the identity from $(R, +)$ is denoted by 0_R.

Definition 32. A ring R is called commutative ring if for all $a, b \in R$, then

$$ab = ba.$$

Futhermore, a commutative ring R is called integral domain if $0_R \neq 1_R$ and if $ab = 0$, then either $a = 0$ or $b = 0$.

Definition 33. A **unit** in a ring is an invertible element.

Definition 34. A commutative division ring is called a **field**.

Example.

- $\mathbb{Z}$ is a domain.
- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields.
- Z/nZ, is a commutative ring for $n \in \mathbb{Z}^+$ and it's a domain iff n is a prime number.

Definition 35. Let R, S be rings. A map $\varphi : R \longrightarrow S$ is a ring homomorphism if for all $a, b \in R$, sastifies that:

1. $\varphi(0_R) = 0_S$.
2. $\varphi(a + b) = \varphi(a) + \varphi(b)$.
3. $\varphi(1_R) = 1_S$.
4. $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

By Definition 35, we can say that the map $\varphi : R \longrightarrow S$ is called

I. *Ring monomorphism* if φ is injective.

II. *Ring epiomorphism* if φ is surjective.
III. *Ring isomorphism* if φ is bijective with inverse ring homomorphism.
IV. *Ring automorphism* if $R = S$ and φ is a ring isomorphism.

Example (Polynomial rings). For any ring R, we have the ring

$$R[x] = \{a_0 + a_x x + \cdots + a_n x^n \mid a_1, \ldots, a_n \in R\},$$

called the *ring of polynomials with coefficients in* R, where x is the indeterminate.

Definition 36. Let R be a ring. A subring is a subset $S \subset R$ which sastifies the conditions of Definition 31.

Example. $\mathbb{Z} \subset \mathbb{Q}$ and $\mathbb{Z}, \mathbb{R}, \mathbb{Q} \subset \mathbb{C}$ are subrings.

Definition 37 (Binomial Theorem). In a commutative ring R,

$$(x+y)^n = \sum_{0 \leqslant i \leqslant n} \binom{n}{i} x^i y^{n-i}, \text{ where } \binom{x}{y} \frac{n!}{i!(n-i)!}.$$

The Definition 37 works perfectly for any ring, as long as $xy = yx$.

1. Ideals

Ideals can be viewed as the analogue in ring theory of a normal subgroup in group theory.

Definition 38. Let R be a ring. An ideal is a proper subset $I \subset (R, +)$ such that $x \in I$, then $xy \in I$ and $yx \in I$ for all $y \in R$.

Example. Let R, S be rings. A map $\varphi : R \longrightarrow S$ is a ring homomorphism, then the $\operatorname{Ker} \varphi$ is an ideal of R.

Proof: Clearly, $\operatorname{Ker} \varphi \subset R$. Let $x \in \operatorname{Ker} \varphi$ then $\varphi(x) = 0_S$. Now, for all $y \in R$

$$\begin{aligned} \varphi(y \cdot_R x) &= \varphi(y) \cdot_S \varphi(x) \\ &= \varphi(x) \cdot_S 0_S \\ &= 0_S \end{aligned}$$

Same for $\varphi(x \cdot_R y)$, then claim follows. □

Proposition 23. Let R be a ring. Let (I) be an ideal of R generated by the subset I. If R is commutative, then (I) is of all linar combinations of elements of I with coefficients in R.

Proof: If $I \in (I)$, then xiy must in (I) for any $i \in I$ and for all $x, y \in R$. If R is commutative, then $xiy = (xy)i$ and (I) is the set of all finite sums $x_1 i_1 + \cdots + x_n i_n$ with $n \geqslant 0, x_1, \ldots, x_n \in R$ and $i_1, \ldots, i_n \in I$. □

Definition 39. Let $a \in R$. Define

$$(a) = RaR := \{\sum_{i=1}^{n} x_i a y_i \mid n \in \mathbb{Z}^+, x_i, y_i \in R, 1 \leqslant i \leqslant n\},$$

an ideal of R called **principal ideal** generated by a. It's the smallest ideal in R containing a.

Proposition 1. Let R be a ring. The principal ideal generated by $a \in R$ is the set aR of all multiples of a.

Proof: By Proposition 23, a linear combination $x_1 a_1 + \cdots + x_n a_n$ of copies of a is a multiple $(x_1 + \cdots + x_n)a$ of a. Then, claim follows. □

Lemma 7. The intersection of two ideals is an ideal.

Counterexample: Let (2) and (3) be two ideals which are multiples of 2 and 3, respectively. So, $(2) \cap (3) = (6)$ but 6 is not a prime number as well as (6) is not a prime ideal. □

Definition 40. A **maximal ideal** of a ring R is an ideal $M \neq R$ of R such that there is no ideal $M \subsetneq I \subsetneq R$.

Proposition 24. Let R be a ring with identity. Every proper ideal is contained in a maximal ideal.

Proof: Since an ideal is proper iff not contains the identity element, then having an ideal $I \neq R$, we can apply Zorn's lemma to a chain of proper ideals of R. Then, by Zorn's lemma there is a maximal element M which is proper and claim follows. □

Definition 41. Let R be a commutative ring and let I be an ideal. We say that I is a prime ideal in R if

$$ab \in I \text{ implies that } a \in I \text{ or } b \in I.$$

Lemma 8. Every maximal ideal is a prime ideal.

Proof: Let M be a maximal ideal, by Definition 40 if $xy \in M$ then $x \in M$ or $y \in M$ since M is proper, clearly follows the Definition 41.

Example. Let p be a prime number, then $p\mathbb{Z} = (p)$ which is a maximal ideal and by Lemma 8 is also a prime ideal.

2. Homomorphism

Definition 42. Let R, S be rings. A map $\rho : R \longrightarrow S$ is a homomorphism of rings. Then image or range of ρ is

$$\operatorname{Im}\rho = \{\rho(x) \mid x \in R\}.$$

The kernel of ρ is

$$\operatorname{Ker}\rho = \{x \in R \mid \rho(x) = 0\}.$$

Definition 43. Let I be an ideal of a ring R. The ring of all cosets of I is the quotient ring R/I of R by I. The homomorphism $x \longmapsto x + 1$ is the canonical projection of R onto R/I.

Definition 44. Let n be an positive integer number. The ring $\mathbb{Z}_n$ of the integers modulo n is the quotient ring $\mathbb{Z}/\mathbb{Z}n$.

Theorem 20 (Factorization Theorem). Let I be an ideal of a ring R. Every homomorphism of ring $\rho : R \longrightarrow S$ whose kernel contains I factors uniquely through the canonical projection $\phi : R \longrightarrow R/I$, then there is homomorphism $\varphi : R/I \longrightarrow S$ unique such that $\rho = \phi \circ \varphi$.

Proof: $\phi((x+I)(y+U)) = \phi(xy+I) = \rho(xy) = \rho(x)\rho(y) = \varphi(x+I)\varphi(y+I)$ for all $x + I, y + I \in R/I$, and $\phi(1_R) = \phi(1_R + I) = \rho(1_R) = 1_R$. So, claim follows. □

Theorem 21 (Homomorphism Theorem). If $\rho : R \longrightarrow S$ is a homomorphism of rings, then

$$R/\operatorname{Ker}\rho \cong \operatorname{Im}\rho.$$

Indeed, there is an isomorphism $\theta : R/\operatorname{Ker} f \longrightarrow \operatorname{Im} f$ unique such that $\rho = \iota \circ \theta \circ \pi$ where $\iota : \operatorname{Im} f \longrightarrow S$ is the inclusion homomorphism and $\pi : R \longrightarrow R/\operatorname{Ker} f$ is the canonical projection.

Proof: Clearly, there is an isomorphism of abelian groups $\theta : (R/\operatorname{Ker} f, +) \longrightarrow (\operatorname{Im} f, +)$ unique such that $\rho = \iota \circ \theta \circ \pi$, equivalently , $\theta(x + \operatorname{Ker}\rho) = \rho(x)$ for all $x \in R$. Then ρ is homomorphism and an isomorphism. □

3. Noetherian Rings

Definition 45. Let R be a commutative ring, the ascending chain condition has three equivalent forms:

a. Every infinite ascending sequence $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots \subseteq \mathfrak{a}_n \subseteq \mathfrak{a}_{n+1} \subseteq \ldots$ of ideals of R terminates, then there exists $N > 0$ such that $\mathfrak{a}_n = \mathfrak{a}_N$ for all $n \geqslant N$,

b. there is no infinite strictly ascending sequence $\mathfrak{a}_1 \subsetneq \mathfrak{a}_2 \subsetneq \cdots \subsetneq \mathfrak{a}_n \subsetneq \mathfrak{a}_{n+1} \subsetneq \dots$ of ideals of R,

c. every nonempty set $\mathcal{S}$ of ideals of R has a maximal element (an element $\mathfrak{s}$ of $\mathcal{S}$, not necessarily a maximal ideal of R, such that there is no $\mathfrak{s} \subsetneq \mathfrak{a} \in \mathcal{S}$).

Definition 46. A commutative ring is Noetherian when its ideals satisfy the ascending chain condition in the sense of Definition 45.

Proposition 25. A commutative ring R is Noetherian iff every ideal of R is finitely generated (as an ideal).

Proof: Let $\mathfrak{a}$ be an ideal of R. Let $\mathcal{S}$ be the set of all finitely generated ideals of R contained in $\mathfrak{a}$. Then $\mathcal{S}$ contains principal ideals and is not empty. If R is Noetherian, then $\mathcal{S}$ has a maximal element $\mathfrak{s}$ by (c). Then $\mathfrak{s} \subseteq \mathfrak{s} + (a) \in \mathcal{S}$ for every $a \in \mathfrak{a}$, since $\mathfrak{s} + (a)$ is finitely generated, by a and the generators of $\mathfrak{s}$. Since $\mathfrak{s}$ is maximal in $\mathcal{S}$ it follows that $\mathfrak{s} = \mathfrak{s} + (a)$ and $a \in \mathfrak{s}$. Hence $\mathfrak{a} = \mathfrak{s}$ and $\mathfrak{a}$ is finitely generated.

Conversely, assume that every ideal of R is finitely generated. Let $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots \subseteq \mathfrak{a}_n \subseteq \mathfrak{a}_{n+1} \subseteq \dots$ be ideals of R. Then $\mathfrak{a} = \bigcup_{n>0} \mathfrak{a}_n$ is an ideal of R and is finitely generated, by, say $a_1, \dots, a_k$. Then $a_i \in \mathfrak{a}_{n_i}$ for some $n_i > 0$. If $N \geqslant n_1, \dots, n_k$, then a_N contains $a_1, \dots, a_k$. Hence $\mathfrak{a} \subseteq \mathfrak{a}_N$, and $\mathfrak{a} \subseteq \mathfrak{a}_N \subseteq \mathfrak{a}_n \subseteq \mathfrak{a}$ shows that $\mathfrak{a}_n = \mathfrak{a}_N$ for all $n \geqslant N$. □

Theorem 22 (Hilbert Basis Theorem). Let R be a commutative ring with identity. If R is Noetherian, then $R[X]$ is Noetherian.

Proof: Let $\mathfrak{U}$ be an udeal of $R[X]$. We construct a finite set of generators of $\mathfrak{U}$. For every $n \geqslant 0$ let

$$\mathfrak{a}_n = \{r \in R \mid rX^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathfrak{U} \text{ for some } a_{n-1}, \dots, a_0 \in R\}.$$

Then $\mathfrak{a}_n$ is an ideal of R, since $\mathfrak{U}$ is an ideal of $R[X]$, and $\mathfrak{a}_n \subseteq \mathfrak{a}_{n+1}$, since $f(x) \in \mathfrak{U}$ implies $Xf(X) \in \mathfrak{U}$. Since R is Noetherian, the ascending sequence $\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \cdots \subseteq \mathfrak{a}_n \subseteq \mathfrak{a}_{n+1} \subseteq \dots$ terminates at some $\mathfrak{a}_m(\mathfrak{a}_n = \mathfrak{a}_m$ for all $n \geqslant m)$. Also, each ideal $\mathfrak{a}_k$ has a finite generating set $\mathcal{S}_k$.

For each $s \in \mathcal{S}_K$ there exists $g_{\mathcal{S}} = sX^k + a_{k-1}X^{k-1} + \cdots + a_0 \in \mathfrak{U}$. We show that $\mathfrak{U}$ coincides with the ideal generated by all $g_{\mathcal{S}}$ with $s \in S_0 \cup S_1 \cup \cdots \cup S_m$. Hence $\mathfrak{U}$ is finitely generated, and $R[X]$ is Noetherian. Now let $f = a_nX^n + \cdots + a_0 \in \mathfrak{U}$ have degree $n \geqslant 0$. Then $a_n \in \mathfrak{a}_n$.

If $n \leqslant m$, then $a_n = r_1s_1 + \cdots + r_ks_k$ for some $r_1, \ldots, r_n \in R$ and $s_1, \ldots, s_k \in \mathcal{S}_n$, then $g = r_1g_{s_1} + \cdots + r_kg_{s_k} \in$ has degree at most n, and the coefficient of X^n in g is $r_1s_1 + \cdots + r_ks_k = a_n$. Hence $f - g \in \mathfrak{U}$ has degree less than n. Then $f - g \in$, by induction $f \in$.

If $n > m$ then $a_n \in \mathfrak{a}_n = \mathfrak{a}_m$ and $a_n = r_1s_1 + \cdots + r_ks_k$ for some $r_1, \ldots, r_n \in R$ and $s_1, \ldots, s_k \in S_m$, then $g = r_1g_{s_1} + \cdots + r_kg_{s_k} \in$ has degree at most m and the coefficient of X^m in g is $r_1s_1 + \cdots + r_ks_k = a_n$. Hence $X^{n-m}g \in$ has degree at most n, and the coefficient of X^n in g is a_n. As above, $f - X^{n-m}g \in$ by induction and $f \in$. □

4. Principal Ideal Domain

Definition 47. A principal ideal domain (or PID) is a domain (i.e., commutative ring with identity and no zero divisors) in which every ideal is principal.

Definition 48. An element p of a domain R is prime when p is not zero or a unit, and $p|a$ or $p|b$. An element q of a domain R is irreducible when q is not zero or a unit, and $q = ab$ implies that a is a unit or b is a unit.

Theorem 23. In a PID R, every element, other than 0 and units, is a nonempty product of irreducible elements. If futhermore two nonempty products $p_1p_2 \ldots p_m = q_1q_2 \ldots q_n$ of irreducible elements are equal, then $m = n$ and the terms can be indexed so that $Rp_i = Rq_i$ for all i.

Proof: Suppose that R has elements besides 0 and units that are not product of irreducible elements, the principal ideal generated by these elements, say $\mathfrak{I}$, consitute a set of ideals of R. Let's prove that $\mathfrak{I}$ has a maximal element Ri. Otherwise, let $Ri_1 \in IF$. Since Ri_1 is not maximal, there exists $Ri_1 \subsetneqq Ri_2 \in \mathfrak{I}$. By induction, $Ri_1 \subsetneqq Ri_2 \subsetneqq \cdots \subsetneqq Ri_n \subsetneqq Ri_{n+1} \subsetneqq \ldots$ Then $\mathfrak{i} = \bigcup_{n>0} Ri_n$ is an ideal of R. Since R is a PID, i is generated by some $i \in R$. Then $i \in Ri_n$ for some n, and $(i) \subseteq Ri_n \subsetneqq Ri_{n+1} \subsetneqq \mathfrak{i} = (i)$. This contradiction shows that $\mathfrak{I}$ has a maximal element Rm, where m is not 0, not unit and not irreducible.

Let $m = ab$ for some $a, b \in R$, neither of which is 0 or a unit. Then $Rm \subsetneqq Ra$ and $Rm \subsetneqq Rb$. Hence a and b cannot be neither 0 nor unit and are product of irreducible elements. But then so is $m = ab$. This contradiction shows that every element of R, other than 0 and unit, is a product of irreducible elements.

Now, suppose that $p_1p_2 \ldots p_m = q_1q_2 \ldots q_n$, where $m, n > 0$ and all p_i, q_j

are irreducible. Since q_k is irreducible, $q_k = up_m$ for some unit $u \in R$ and $Rq_k = Rp_m$. By induction, $m - 1 = n - 1$ and the remaining terms can be reindexed so that $Rp_1 = Ruq_q = Rq_1$ and $Rp_i = Rq_i$ for all $1 < i < m$. □

Theorem 24. Every nonzero element of R can be written as the product $p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}$ of a unit and of positive powers of distinct representative irreducible elements, which are unique up to the order of the terms.

Proof: Theorem 23 implies Theorem 24. So, claim follows. □

Definition 49. In a domain, an element m is a least common multiple (l.c.m.) of two elements a and b when m is a multiple of a and b.

Definition 50. In a domain, an element d is a greatest common divisor (g.c.d.) of two elements a and b when d divides a and b.

Proposition 26. In a PID R, every $a, b \in R$ have a least l.c.m and g.c.d. Moreover, $m = \text{lcm}(a, b)$ iff $Rm = Ra \cap Rb$, and $d = gcd(a, b)$ iff $Rd = Ra + Rb$. In particular, $d = gcd(a, b)$ implies $d = xa + yb$ for some $x, y \in R$.

Proof: By Definition 49, $m = \text{lcm}(a, b)$ iff $m \in Ra \cap Rb$, and $c \in Ra \cap Rb$ implies $c \in Rm$ iff $Rm = Ra \cap Rb$. As l.c.m exists then $Ra \cap Rb$ must be principal.

By Definition 50, $d = \text{gcd}(a, b)$ iff $a, b \in Rd$ and $a, b \in Rc$ implies $c \in Rd$, iff Rd is the smallest principal ideal of R contains both Ra and Rb. The latter is $Ra + Rb$, since every ideal of R is principal. Hence $d = \text{gcd}(a, b)$ iff $Rd = Ra + Rb$, and then $d = xa + yb$ for some $x, y \in R$. As g.c.d. exists then $Ra + Rb$ must be principal. □

4.1. Modules over a PID.

Theorem 25. Let M over a PID $\mathcal{R}$. There is a unique decresing sequence of proper ideals

$$d_1 \supseteq \cdots \supseteq d_n$$

such that M is isomorphic to the sum of cyclic modules

$$M \cong \bigoplus_i \mathcal{R}/(d_i).$$

The d_is are called invariant factors of M.

Proof: Let φ be a $\mathcal{R}$-linear map such that can be determined by $\varphi(e_1) = f_1, \ldots, \varphi(e_n) = f_n$ where $e_1, \ldots, e_n$ is the basis of n-dimensional $\mathcal{R}$. Then $\varphi(e_j) = \sum_{i=1}^{n} c_{ij} e_i$, such that (c_{ij}) is the matrix presentation of φ with respect to the basis. Then

$$\varphi(\mathcal{R}) = \mathcal{R}\varphi(e_1) \oplus \cdots \oplus \mathcal{R}\varphi(e_n) = \mathcal{R}f_1 \oplus \cdots \oplus \mathcal{R}f_n,$$

by aligned bases of $\mathcal{R}$ and its module $\varphi(\mathcal{R})$, we can say that

$$\mathcal{R} = \mathcal{R}v_1 \oplus \cdots \oplus \mathcal{R}v_n, \qquad \varphi(R) = \mathcal{R}a_1v_1 \oplus \cdots \oplus \mathcal{R}a_nv_n,$$

where a_is are nonzero integers. Then

$$\mathcal{R}/\varphi(R) \cong \bigoplus_i \mathcal{R}/a_i\mathcal{R}.$$

Obvioulsy, $\mathcal{R}/\varphi(R)$ is our M and claim follows. □

As an useful comment, we can calculate the invariant factors with the Smith Normal Form (SNF).

We need to remember that no every module has a basis, that's because we use free module here.

Definition 51. A free module is a module with a basis.

Lemma 9. Let $\mathcal{R}$ be a n-dimensional module over a PID, then every $\mathcal{R}$-submodule of $\mathcal{R}$ is an ideal.

Proof: Let $x \neq 0 \in \mathcal{R}$, then for $\mathcal{R}x$ since all ideals in $\mathcal{R}$ are principal, it's clearly that $\mathcal{R}x \cong \mathcal{R}$ as $\mathcal{R}$-modules. □

Lemma 10. Let $\mathcal{R}$ be a commutative ring and M be an R-module. Let f be an $\mathcal{R}$-linear and onto map such that $f : M \longrightarrow \mathcal{R}$, then there is an $\mathcal{R}$-module isomorphism $h : M \cong \mathcal{R}^n \oplus \operatorname{Ker} f$ where $h(m) = (f(m), *)$, making f the first component of h.

Proof: Let $\mathcal{R}^n = \mathcal{R}e_1 \oplus \cdots \oplus \mathcal{R}e_n$ where $e_1, \ldots, e_n$ is the basis of $\mathcal{R}$, let $m_i \in M$ such that $f(m_i) = e_i$ then there is a map $g : \mathcal{R}^n \longrightarrow M$ such that

$$g(c_1e_1 + \cdots + c_ne_n) = c_1m_1 + \cdots + c_nm_n,$$

Now, we define the function $h : M \longrightarrow \mathcal{R}^n \oplus \operatorname{Ker} f$ such that $h(m) = (f(m), m - g(f(m)))$. □

THEOREM 26. Let $M \subset \mathcal{R}$ be a free $\mathcal{R}$-module of rank n where $\mathcal{R}$ is a PID, then for any S submodule of M is free of rank $\leqslant n$.

Proof: The free $\mathcal{R}$-module is $\mathcal{R}^n$ by lemma 9. By induction on n, let $S \subset \mathcal{R}^{n+1}$ be a submodule. We gonna show that S is free of rak $\leqslant n+1$. The a projection of direct sum $\phi : \mathcal{R} \oplus \mathcal{R}^n \longrightarrow \mathcal{R}^n$ (i.e. $\mathcal{R}^{n+1} = \mathcal{R} \oplus \mathcal{R}^n$), then $N = \phi(S) \subset \mathcal{R}^n$ is free of rank $\leqslant n$. Now, by lemma 10

$$S \cong N \oplus \operatorname{Ker} \phi|_S,$$

so $N \oplus \operatorname{Ker} \phi|_S$ is free of rank $\leqslant n+1$, so S does. □

DEFINITION 52. Let $\mathcal{R}$ be a module and let $x \in \mathcal{R}$, which is called a torsion element if there exists a nonzero $r \in \mathcal{R}$ such that $rx = 0$. If $rx \neq 0$ for all $r \neq 0 \in R$, then the element x is called a torsion-free.

DEFINITION 53. Let T be a module, we say that T is called a torsion-free module, if every element of T is a torsion-free module.

DEFINITION 54. Let T be a finitely torsion module over the PID $\mathcal{R}$. By theorem 25, we write $T \cong R/(d_1) \oplus \cdots \oplus R/(d_m)$, then the $\mathcal{R}$-cardinality of T to be the ideal

$$\operatorname{card}_{\mathcal{R}}(T) = (d_1 d_2 \ldots d_m).$$

THEOREM 27. Let T_1 and T_2 be two finitely generated torsion $\mathcal{R}$-modules, then

$$\operatorname{card}_{\mathcal{R}}(T_1 \oplus T_2) = \operatorname{card}_{\mathcal{R}}(T_1)\operatorname{card}_{\mathcal{R}}(T_2).$$

Proof: We combine cyclic decompositions of T_1 and T_2 and then get $T_1 \oplus T_2$. □

If we pick $x_1, \ldots, x_n$ the generating set for a torsion-free module T as an $\mathcal{R}$-module, then we have a linear map $f : \mathcal{R}^n \longrightarrow T$ where $f(e_i) = x_i$ for the basis $e_1, \ldots, e_n$ of $\mathcal{R}^n$ such there exists a linearly indepedent sequence $y_1, \ldots, y_n$ of T such that $y_j = \sum_{i=1}^n a_{ij} x_i$ with $a_{ij} \in \mathcal{R}$. By zorn's lemma, there is a linearly independent subset of T with maximal size $t_1, \ldots, t_d$ such that $\sum_{j=1}^d A t_j \cong T^d$. Then we can get an isomorphism map

$$T \to aT \hookrightarrow \sum_{j=1}^d T t_j \to A^d,$$

for a linearly dependent set $x, t_1, \ldots, t_d$ and a nontrivial linear realtion $ax + \sum_{i=1}^d a_i t_i = 0$ with $a \neq 0$. Now, we can say the following

Lemma 11. Let T be a finitely generated torsion-free module over a PID $\mathcal{R}$ such that $T \neq 0$, then there is an embedding $T \hookrightarrow \mathcal{R}^d$ for some $d \geqslant 1$ such that the image of T intersects each standard coordinate axis of $\mathcal{R}^d$.

Now, we use the above lemma to formulate the next theorem

Theorem 28. Let $\mathcal{R}$ be a PID, then every finitely generated torsion-free $\mathcal{R}$-module is a free $\mathcal{R}$-module.

Proof: By lemma 11, there is a module that embeds a finite free $\mathcal{R}$-module, then it's finite free too by theorem 26. □

As last, we have the following theorem

Theorem 29. Let $\mathcal{R}$ be a PID, every finitely $\mathcal{R}$-module has the form $F \oplus T$ where F is a finite free $\mathcal{R}$-module and T is a finitely generated torsion $\mathcal{R}$-module. Moreover, $T \cong \bigoplus\limits_{j} \mathcal{R}/(a_j)$ with a nonzero a_j.

Proof: Let T be a finitely generated $\mathcal{R}$-module, with generators $x_1, \dots, x_n$. We define $f : \mathcal{R}^n \longrightarrow T$ by $f(e_i) = x_i$. We know that

$$\mathcal{R}^n/N \cong \left(\bigoplus_{j}^{m} \mathcal{R}/(a_j) \right) \oplus \mathcal{R}^{n-m},$$

for some $m \leqslant n$, a quotient $\mathcal{R}^n/N$ and nonzero a_js. The direct sum of the $A/(a_j)$'s is a torsion module and $\mathcal{R}^{n-m}$ is a finite free $\mathcal{R}$-module. □

Example. Describe, as a direct sum of cyclic groups, the cokernel of the map $\phi : \mathbb{Z}^3 \longrightarrow \mathbb{Z}^3$ given by left multiplication by the matrix

$$\begin{pmatrix} 15 & 6 & 9 \\ 6 & 6 & 6 \\ -3 & -12 & -12 \end{pmatrix}$$

Proof: Let ϕ be a $\mathbb{Z}$-linear map such that can be determined by $\phi(e_1) = f_1, \dots, \phi(e_n) = f_n$, where $e_1, \dots, e_n$ be the basis of $\mathbb{Z}^n$. Then $\phi(e_j) = \sum_{i=1}^{n} = c_{ij} e_i$ for $j = 1, \dots, n$, so (c_{ij}) is the matrix representation of ϕ with respect to the basis.

Then,

$$\phi(\mathbb{Z}^n) = \mathbb{Z}\phi(e_1) \oplus \cdots \oplus \mathbb{Z}\phi(e_n) = \mathbb{Z}f_1 \oplus \cdots \oplus \mathbb{Z}f_n,$$

by aligned bases for $\mathbb{Z}^n$ and its modulo $\phi(\mathbb{Z}^n)$, we can say that

$$\mathbb{Z}^n = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_n, \quad \phi(\mathbb{Z}^n) = \mathbb{Z}a_1v_1 \oplus \cdots \oplus \mathbb{Z}a_nv_n$$

where a_i's are nonzero integers. Then

$$\mathbb{Z}^n/\phi(\mathbb{Z}^n) \cong \bigoplus_{i=1}^{b} \mathbb{Z}/a_i\mathbb{Z}.$$

Now, for our solution we need to get the Smith Normal Form, since each a_i is the $M_{i,i}$ element of the matrix, the Smith Normal Form of the cokernel is:

$$\begin{pmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 18 \end{pmatrix}$$

So, we can describe the cokernel as the sum of cyclic groups:

$$\mathbb{Z}^3/\phi(\mathbb{Z}^3) \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/18\mathbb{Z}$$

□

5. Commutative Rings

In this Section, let's see many properties related this kind of rings that we haven't seen yet.

Definition 55. Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals of a commutative ring R and let S be a subset of R. The set

$$\mathfrak{a} : S = \{r \in R \mid rs \in \mathfrak{a} \text{ for all } s \in S\}$$

is an ideal and it's called the **transporter** of S into $\mathfrak{a}$.

Definition 56. Let R be a commutative ring. The radical $\operatorname{Rad}\mathfrak{a}$ of an ideal $\mathfrak{a}$ is the intersection of all primes ideals of R that contain $\mathfrak{a}$.

Proposition 27. $\operatorname{Rad}\mathfrak{a} = \{x \in R \mid x^n \in \mathfrak{a} \text{ for some } n > 0\}$.

Proof: Let $x \in R$ and let $\mathfrak{r}$ be the intersection of all prime ideals that contain $\mathfrak{a}$. If $x \in R/\mathfrak{r}$, then $x \notin \mathfrak{p}$ for some prime ideal $\mathfrak{p} \subset \mathfrak{a}$, $x^n \notin \mathfrak{p}$ for all $n > 0$ since $\mathfrak{p}$ is prime, and $x^n \notin \mathfrak{a}$ for all $n > 0$.

Suppose $x^n \notin \mathfrak{a}$ for all $n > 0$. By Zorn's lemma there is an ideal $\mathfrak{p}$ that contains $\mathfrak{a}$, and contains no x^n, and is maximal with thes properties. Let $a, b \in R/\mathfrak{p}$. By choice of $\mathfrak{p}, +(a)$ contains some x^m and $\mathfrak{p} + (b)$ contains some x^n. Then $x^m = p + ra, x^n = q + sb$ for some $p, q \in \mathfrak{p}$ and $r, s \in R$, $x^{m+n} = pq + psb + qra + rsab \in \mathfrak{p} + (ab) \subsetneq \mathfrak{p}$, and $ab \notin \mathfrak{p}$. Thus $\mathfrak{p}$ is a prime ideal, since $x \notin \mathfrak{p}$, it follows that $x \notin \mathfrak{r}$. □

Definition 57. An ideal $\mathfrak{a}$ of a commutative ring R is semiprime when it's an intersection of prime ideals.

Definition 58. Let R be a commutative ring and let $\mathfrak{r}$ be an ideal of R. We say that $\mathfrak{r}$ is **primary** when $\mathfrak{r} \neq R$ and, for all $x, y \in \mathfrak{r}$ implies $x \in \mathfrak{r}$ or $y^n \in \mathfrak{r}$ for some $n > 0$. An ideal $\mathfrak{r}$ of R is $\mathfrak{p}$-primary when $\mathfrak{r}$ is primary and $\operatorname{Rad} \mathfrak{r} = \mathfrak{p}$.

Lemma 12. Every ideal of a Noetherian ring R is the intersection of finitely many irreducible ideals of R.

Proof: Let $\mathfrak{b}$ be the ideal of a ring R. Suppose $\mathfrak{b}$ is not the intersection of finitely many irreducible ideals of R. Is this is false, then the set of such ideals of R is empty, since R is Noetherian, there is a maximal ideal $\mathfrak{p}$ which is not irreducible. Therefore, $\mathfrak{p} = \mathfrak{a} \cap \mathfrak{b}$ for some ideals $\mathfrak{a}, \mathfrak{b} \subsetneq \mathfrak{p}$. By the maximality of $\mathfrak{p}, \mathfrak{a}$ and $\mathfrak{b}$ are intersections of finetely many irreducible ideals, but then so is $\mathfrak{p}$, a contradiction. □

Theorem 30. In a Noetherian ring, every ideal is the intersection of finitely manu primary ideals.

Proof: By Lemma 12, we only need to show that every irreducible ideal $\mathfrak{r}$ of a Noetherian ring R is primary. Suppose that $ab \in \mathfrak{r}$ and $b \notin \operatorname{Rad} \mathfrak{r}$. Let $\mathfrak{a}_n = \mathfrak{r} : b^n$. Then $a \in \mathfrak{a}_1$, $\mathfrak{r} \subset \mathfrak{a}_n$, $\mathfrak{a}_n$ is an ideal, and $\mathfrak{a}_n \subseteq \mathfrak{a}_{n+1}$, since $xb^n \in \mathfrak{r}$ implies $xb^{n+1} \in \mathfrak{r}$. Since R is Noetherian, the ascending sequence $(\mathfrak{a}_n)_{n>0}$ terminates, hence $\mathfrak{a}_{2n} = \mathfrak{a}_n$ if n is large enough. Let $\mathfrak{b} = \mathfrak{r} + Rb^n$. If $x \in \mathfrak{a}_n \cap \mathfrak{b}$, then $xb^n \in \mathfrak{r}$ and $x = t + yb^n$ for some $t \in \mathfrak{r}$ and $y \in R$, whence $tb^n + yb^{2n} \in \mathfrak{r}$, $yb^{2n} \in \mathfrak{r}$, $y \in \mathfrak{a}_{2n} = \mathfrak{a}_n$, $yb^n \in \mathfrak{r}$, and $x = t + yb^n \in \mathfrak{r}$. Hence $\mathfrak{a}_n \cap \mathfrak{b} = \mathfrak{r}$. Now, $\mathfrak{b} \subsetneq \mathfrak{r}$, since $b^n \notin \mathfrak{r}$. Therefore $\mathfrak{a}_n = \mathfrak{r}$, hence $\mathfrak{a}_1 = \mathfrak{r}$ and $a \in \mathfrak{r}$. □

Definition 59. A ring extension of a commutative ring R is a commutative ring E of which R is a subring.

Definition 60. Let R be a ring. A R-module is an abelian group M together with an action $(r, x) \longmapsto rx$ of R on M such that $r(x + y) = rx + ry, (r + s)x = rx + sx, r(sx) = (rs)x$ and $1_R x = x$, for all $r, s \in R$ and $x, y \in M$. A submodule R-module M is additive msubgroup N of M such that $x \in N$ implies $rx \in N$ for every $r \in R$.

Definition 61. An element α of a ring extension E of R is integral over R when it sastifies the following conditions:

- $f(\alpha) = 0$ for some monic polynomial $f \in R[X]$,

- $R[\alpha]$ is a finetely generated submodule of E,
- α belongs to a subring of E that is a finitely generated R-module.

5.1. Integral Extension.

Definition 62. A ring extension $R \subset E$ is integral, and E is integral over R, when every element of E is integral over R.

Definition 63. A ring extension E of R, an ideal $\mathfrak{U}$ of E lies over an ideal $\mathfrak{a}$ of R when $\mathfrak{U} \cap R = \mathfrak{a}$.

Proposition 28. If E is an ring extension of R and $\mathfrak{U} \subset E$ lies over $\mathfrak{a} \subset R$, then $\mathfrak{a}/R$ may be identified with a subring of $E/\mathfrak{U}$, if E is integral over R, then $E/\mathfrak{U}$ is integral over $R/\mathfrak{a}$.

The inclusion homomorphism $R \longrightarrow E$ induces a homomorphism $R \longrightarrow E/\mathfrak{U}$ whose kernel is $\mathfrak{U} \cap R = \mathfrak{a}$, and in injective homomorphism $R/\mathfrak{a} \longrightarrow E/\mathfrak{U}$, $r + \mathfrak{a} \longmapsto r + \mathfrak{U}$. Hence $R/\mathfrak{a}$ may be identified with a subring of $E/\mathfrak{U}$. If $\alpha \in E$ is integral over R, then $\alpha + \mathfrak{U}$, then $\alpha + \mathfrak{U} \in E/\mathfrak{U}$ is integral over $R/\mathfrak{a}$. □

Definition 64. The integral closure of a ring R in a ring extension E of R is the subgring $\overline{R}$ of E of all elements of E that are integral over R. The elements of $\overline{R} \subseteq E$ are the algebraic integerss of E (over R).

Definition 65. A domain R is integrally closed when its integral closure in its quotient field $Q(R)$ is R itself (when no $\alpha \in Q(R)\backslash R$ is integral over R).

Proposition 29. Let R be a domain and let E be an algebraic extension of its quotient field. The integral closure $\overline{R}$ of R in E is an integrally closed domain whose quotient field is E.

Proof: Every $\alpha \in E$ is algebraic over $Q(R)$, $r\alpha$ is integral over R for some $r \in R$, hence $E = Q(\overline{R})$. If $\alpha \in E$ is integral over $\overline{R}$, then α is integral over R and $\alpha \in \overline{R}$, so $\overline{R}$ is integrally closed. □

5.2. Localization.

Definition 66. A multiplicative subset of a commutative ring R is a subset S of R that contain the identity element of R and is closed under multiplication. A multiplicative subset S is proper when $0 \notin S$.

Definition 67. If S is a proper multiplicative subset of a commmutative ring R, then $S^{-1}R$ is the ring of faction of R with denominators in S.

If R is a domain, then $S = R\backslash\{0\}$ is a proper multiplicative subset and $S^{-1}R$ is the field of fractions or quotient fild $Q(R)$ of R.

Definition 68. Let S be a proper multiplicative subset of R. The contraction of an ideal $\mathfrak{U}$ of $S^{-1}R$ is $\mathfrak{U}^C = \{a \in R \mid a/1 \in \mathfrak{U}\}$. The expansion of an ideal $\mathfrak{a}$ of R is $\mathfrak{a}^E = \{a/s \in S^{-1}R \mid a \in \mathfrak{a}, s \in S\}$.

Definition 69. The localization of a commutative ring R at a prime ideal p is the ring of fractions $R_p = (R)^{-1}R$.

Definition 70. A commutative ring is local when it has only one maximal ideal.

We need to remark that Localization tranfers properties from local rings to more general rings.

Theorem 31. Every homomorphism of a ring R into an algbraically closed field L can be extended to every integral extension E of R.

Proof: If R is a field, then E is a field and E is an algebraic extension of R.
Now, let R be local and let $\varphi : R \longrightarrow L$ be a homomorphism whose kernel is the maximal ideal $\mathfrak{m}$ of R. Then φ factors through the projection $R \longrightarrow R/\mathfrak{m}$ and induces a homomorphism $\phi : R/\mathfrak{m} \longrightarrow L$. There is a maximal ideal $\mathfrak{M}$ of E that lies over $\mathfrak{m}$. The field $R/\mathfrak{m}$ may be identified with a subfield of $E/\mathfrak{M}$. Then $E/\mathfrak{M}$ is algebraic over $R/\mathfrak{m}$ and $\pi : R/\mathfrak{m} \longrightarrow L$ can be extended to $E/\mathfrak{M}$. Hence φ can be extended to E.

Finally, let $\varphi : R \longrightarrow L$ be any homomorphism. Then $\mathfrak{p} = \operatorname{Ker}\varphi$ is a prime ideal of R and $S = R/\mathfrak{p}$ is a proper multiplicative subset of R and of E. Therefore ϕ extends to $S^{-1}E$, which is integral over $S^{-1}R$, hence φ extends to E. □

5.3. Dedekind Domains.

Definition 71. A fractional ideal of a domain R is a subset of its quotient field Q of the form $\mathfrak{a}/c = \{a/c \in Q \mid a \in \mathfrak{a}\}$, where $\mathfrak{a}$ is an ideal of R and $c \in R$, $c \neq 0$.

Proposition 30. Let R be a domain and let Q be its quotient field. Every finitely generated submodule of Q is a fractional ideal of R. If R is Noetherian, then every fractional ideal of R is finetely generated as a submodule.

Proof: If $n > 0$ and $q_1 = a_1/c_1, \dots, q_n = a_n/c_n \in Q$, then

$$Rq_1 + \cdots + Rq_n = Rb_1/c + \cdots + Rb_n/c = (Rb_1 + \cdots + Rb_n)/c,$$

where $c = c_1 \dots c_n$, hence $Rq_1 + \cdots + Rq$ is a fractional ideal of R. Conversely, if every ideal $\mathfrak{a}$ is finetely generated, $\mathfrak{a} = Rb_1 + \cdots + Rb_n$ for some $b_1, \dots, b_n \in R$ then every fractional ideal $\mathfrak{a}/c = Rb_1/c + \cdots + Rb_n/c$ is a finetely generated submodule of Q.

Definition 72. A Dedekind domain is a domain that satisfies the equivalent condition:

1. Every nonzero ideal of R is invertible (as a fractional ideal),
2. every nonzero fractional ideal of R is invertible,
3. every nonzero ideal of R is a product of prime ideals of R,
4. every nonzero ideal of R can be written uniquely as a product of positive powers of distinct prime ideals of R.

Futhermore, R is Noetherian and every prime ideal of R is maximal.

Theorem 32 (Krull Intersection Theorem). Let $\mathfrak{a} \neq R$ be an ideal of a Noetherian ring R and let $\mathfrak{r} = \bigcap_{n>0} \mathfrak{a}^n$. Then $\mathfrak{a}\mathfrak{r} = \mathfrak{r}$ and $(1-a)\mathfrak{r} = 0$ for some $a \in \mathfrak{a}$. If R is a domain, or if R is local, then $\mathfrak{r} = 0$.

Proof: Let $\mathfrak{q}$ be a primary ideal that contains $\mathfrak{a}\mathfrak{i}$ and let $\mathfrak{p}$ be its radical. Then $\mathfrak{p}^n \subset \mathfrak{q}$ for some n and $\mathfrak{i} \subset \mathfrak{q}$, otherwise $\mathfrak{a} \subset \mathfrak{q}$, since $\mathfrak{q}$ is primary and $\mathfrak{i} \subset \mathfrak{a}^n \subset \mathfrak{q}$ anyway. Since $\mathfrak{i}$ is an intersection of primary ideals, this implies $\mathfrak{i} \subset \mathfrak{a}\mathfrak{i}$ and $\mathfrak{i} = \mathfrak{a}\mathfrak{i}$. Suppose that $(1-a)\mathfrak{i} = 0$ for some $a \in \mathfrak{a}$. Then $1 - a \neq 0$. If R is a domain, then $(1-a)\mathfrak{i} = 0$ for some $a \in \mathfrak{a}$. Then $1 - a \neq 0$. If R is a domain, then $(1-a)\mathfrak{i} = 0$ implies $\mathfrak{i} = 0$. If R is local, then $1 - a$ is a unit and again $(1-a)\mathfrak{i} = 0$ implies $\mathfrak{i} = 0$. □

5.4. Krull Dimension.

Definition 73. In a commutative ring R, the height $\operatorname{hgt}\mathfrak{p}$ of a prime ideal $\mathfrak{p}$ is the least upper bound of the lengths of strictly descending sequences $\mathfrak{p} = \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_m$ of prime ideals of R.

Definition 74. The **spectrum** of a commutative ring is the set of its prime ideals, partially ordered by inclusion. The Krull dimension or dimension $\dim R$ of R is the least upper bound of the heights of the prime ideals of R.

Lemma 13. Let R be a domain and let $\mathfrak{P}$ be a prime ideal of $R[X]$. If $\mathfrak{P} \cap R = 0$, then $\mathfrak{P}$ has height at most 1.

Proof: Let Q be the quotient field of R and let $S = R\backslash\{0\}$, so that $S^{-1}R = Q$. Since every $r \in R\backslash 0$ is a unit in Q and in $Q[X]$. There is a homomorphism $\theta : S^{-1}(R[X]) \longrightarrow Q[X]$, which sends $(a_0 + \cdots + a_nX^n)/r \in S^{-1}(R[X])$ to $(a_0/r) + \cdots + (a_n/r)X^n \in Q[X]$. If $g(X) = q_0 + q_1X + \cdots + q_nX^n \in Q[X]$, then rewriting $q_0, q_1, \ldots, q_n$ with a common denominator puts g in the form $g = f/r$ for some $f \in R[X]$ and $r \in R$, hence θ is an isomorphism. Thus $S^{-1}(R[X]) \cong Q[X]$ is a PID.

Now, let $\mathfrak{P} \cap R = 0$ and let $0 \neq \mathfrak{Q} \subset \mathfrak{P}$ be a prime ideal of $R[X]$. Then $\mathfrak{Q} \cap R = 0$, and $\mathfrak{Q}^E \subseteq \mathfrak{P}^E$ are nonzero prime ideals of the PID $S^{-1}(R[X])$. Hence $\mathfrak{Q}^E$ is a maximal ideal. $\mathfrak{Q}^E = \mathfrak{P}^E$, and $\mathfrak{Q} = \mathfrak{P}$. □

Theorem 33. If R is Noetherian domain, then $\dim R[X] = 1 + \dim R$.

Proof: Let (X) be a prime ideal of $R[X]$ and $R[X]/(X) \cong R$. In particular, $\dim R[X]$ is infinite when $\dim R$ is infinite, and we may assume that $n = \dim R$ is finite. We prove by induction on n that $\dim R[X] \leqslant n + 1$. If $n = 0$, then 0 is a maximal ideal of R, R is a field, $R[X]$ is a PID, and $\dim R[X] = 1$. Now, let $n > 0$ and

$$\mathfrak{P}_0 \subsetneq \mathfrak{P}_1 \subsetneq \cdots \subsetneq \mathfrak{P}_m$$

be prime ideals of $R[X]$. We want to show that $m \leqslant n + 1$. Since $n \leqslant 1$ we suppose that $m \leqslant 2$ and $\mathfrak{P}_{m-1} \cap R \neq 0$. Indeed, suppose that $\mathfrak{P} \cap R = 0$. Then $\mathfrak{P}_2 \cap R \neq 0$ and there exists $0 \neq a \in \mathfrak{P}_{m-2} \cap R$. Now, $\mathfrak{P}_{m-2}$ has height at least 2 and is not minimal over (a).

Now, $\mathfrak{p} = \mathfrak{P}_{m-1} \cap R$ is a nonzero prime ideal of R. Then $\dim R/\mathfrak{p} \leqslant \dim R - 1 = n - 1$. By induction, $\dim(R/\mathfrak{p})[X] \leqslant n$. The projection $R \longrightarrow R/\mathfrak{p}$ induces a surjective homomorphism $R[X] \longrightarrow (R/\mathfrak{p})[X]$ whose kernel is a nonzero prime ideal $\mathfrak{P}$ of $R[X]$, which consists of all $f \in R[X]$ with coefficients in $\mathfrak{p}$. Then $\mathfrak{P} \subset \mathfrak{P}_{m-1}$, since $\mathfrak{p} \subset \mathfrak{P}_{m-1}$, $\dim R[X]/\mathfrak{P} = \dim(R/\mathfrak{p})[X] \leqslant n$, and the sequence

$$\mathfrak{P}_0/\mathfrak{P} \subsetneq \mathfrak{P}_1/\mathfrak{P} \subsetneq \cdots \subsetneq \mathfrak{P}_{m-1}/\mathfrak{P}$$

has length $m - 1 \leqslant n$, so that $m \leqslant n + 1$. □

6. Rational Fraction

Definition 75. Let K be a field. A **partial fraction** is a rational fration $f/q^r \in K(X)$ in which q is monic and irreducible, $r \geqslant 1$, and $\deg f < \deg q$. Then f, q, and r are unique.

LEMMA 14. Every rational fraction can be written uniquely in reduced form.

Proof: Given f/g, divide f and g by the leading coefficient of g and then by a monic g.c.d. of f and g, the result is in reduced form.

Let $f/g = p/q, fq = gp$, with g, q monic and $\gcd(f, g) = \gcd(p, q) = 1$. Then q divides gp, since $\gcd(p, q) = 1$, q divides g. Similarly, g divides q. Since q and g are monic, $q = g$. Then $p = f$. □

LEMMA 15. Every rational fraction can be written uniquely as the sum of a polynomial and a polynomial-free fraction in reduced form.

Proof: By Lemma 14, we start with a rational fraction f/g in reduced form. Polynomial division yields $f = gq + r$ with $q, r \in K[X]$ and $\deg r < \deg g$. Then $f/g = q + r/g$, r/g is polynomial-free and is in reduced form, since g is monic and $\gcd(r, g) = \gcd(f, g) = 1$. Conversely let $f/g = p + s/h$, with $p \in K[X]$, $\deg s < \deg h$, h monic, and $\gcd(s, h) = 1$. Then $f/g = (ph+s)/h$. Both fractions are in reduced form, hence $g = h$ and $f = ph + s = pg + s$, by Lemma 14. Uniqueness in polynomial division then yields $p = q$ and $s = r$. □

7. Unique Factorization Domains

DEFINITION 76. A unique factorization domain (or UFD) is a domain R (i.e., a commutative ring with identity and no zero divisors) in which

1. Every element, other than 0 and units, is a nonempty product of irreducible elements of R, and
2. if two nonempty products $p_1 p_2 \dots p_m = q_1 q_2 \dots q_n$ of irreducible elements of R are equal, then $m = n$ and the terms can be indexed so that $Rp_i = Rq_i$ for all i.

DEFINITION 77. A polynomial p over a UFD R is primitive when no irreducible element of R divides all the coefficients of p.

LEMMA 16. Every nonzero polynomial $f(X) = Q(X)$ can be written in the form $f(X) = tf^*(X)$, where $t \in Q, t \neq 0$, and $f^*(X) \in R[X]$ is primitive. Moreover, t and f^* are unique up to multiplication by units of R.

Proof: We have $f(X) = (a_0/b_0) + (a_1/b_1)X + \cdots + (a_n/b_n)X^n$, where $a_i, b_i \in R$ and $b_i \neq 0$. Let b be a common denominator (for instance, $b = b_0 b_1 \dots b_n$). Then $f(X) = (1/b)(c + c_1 X + \cdots + c_n X^n)$ for some $c_i \in R$. Factoring out $a = \gcd(c_0, c_1, \dots, c_n)$ yields $f(X) = (a/b) f^*(X)$, where f^* is primitive.

Suppose that $(a/b)\ g(X) = (c/d)\ h(X)$, where g, h are primitive. Since g and h are primitive, ad is a g.c.d. of the coefficients of $ad\ g(X)$, and bc is a g.c.d, of the coefficients of $bc\ h(X)$. Hence, $bc = adu$ for some unit u of R, so that $g(X) = uh(X)$ and $(a/b)u = c/d$ in Q. □

Proposition 31 (Eisenstein's Criterion). Let R be a UFD and let $f(X) = a_0 + a_1 X + \cdots + a_n X^n \in R[X]$. If f is primitive and there exists an irreducible element p of R such that p divides a_i for all $i < n$, p does not divide a_n, and p^2 does not divide a_0, then f is irreducible.

Proof: Suppose that $f = gh$, let $g(X) = b_0 + b_1 X + \cdots + b_r X^r$ and $h(X) = c_0 + c_1 X + \cdots + c_s X^s \in R[X]$, where $r = \deg g$ and $s = \deg h$. Then $a_k = \sum_{i+j=k} b_i c_j$ for all k. In particular, $a_0 = b_0 c_0$. Since p^2 does not divide a_0, p does not divide both b_0 and c_0. But p divides a_0, so p divides, say, b_0, but not c_0. Also, p does not divide b_r, since p does not divide $a_n = b_r c_s$. Hence there is a least $k \leqslant r$ such that p does not divide b_k, and then p divides b_i for all $i < k$. Now p divides every term of $\sum_{i+j=k} b_i c_j$ except for $b_k c_0$. Hence p does not divide a_k. Therefore $k = n$, since $k \leqslant r \leqslant r + s = n$ this implies $r = n$, and h is contant. □

Example. Let $f = 3X^3 + 4X - 6 \in \mathbb{Z}[X]$ is irreducible in $\mathbb{Z}[X]$. Indeed, f is primitive, 2 divides all the coefficients of f except the leading coefficient, and 4 does not divide the constant coefficient. Futhermore, f is also irreducible in $\mathbb{Q}[X]$, and so is $\frac{5}{6} f = \frac{5}{2} X^3 - \frac{5}{3} X - 5$.

CHAPTER 3

Module Theory

Already we have seen some introduction to modules on the Sub-Section 4.1. In this chapter, let's expand the theory about modules. We can see modules as a generalization of abelian groups, which sastifies all the axioms of a vector space (except for scalars, which can come from another ring or field). From now, let R be a fixed ring.

Definition 78. A (left) R-module is an additive group M together with a map $\cdot : R \times M \longrightarrow M$ (the R-action) called *scalar multiplication*, which sastifies for all $r, s \in R$ and $x, y \in M$ the following properties:

1. $r \cdot (x + y) = r \cdot x + r \cdot y$,
2. $(r + s) \cdot x = r \cdot x + s \cdot x$,
3. $r \cdot (s \cdot x) = (r \cdot s) \cdot x$,
4. $1 \cdot x = x$.

Example. Let K be a field. A K-module is a vector space over K with scalars on the left.

Example. Every abelian group A is a unital $\mathbb{Z}$-module, in which nx is the usual integer multiple (i.e., $nx = x + x + \cdots + x$, when $n > 0$).

Example. Let $\mathfrak{U}$ be a left ideal in R. Then $\mathfrak{U} + \mathfrak{U} \subset \mathfrak{U}$ and $R\mathfrak{U} \subset \mathfrak{U}$, so $\mathfrak{U}$ is a submodule of R. In this way, an R-module generalizes the notion of left ideal.

Now, let M be a R-module and $N \subset M$, the **factor group** M/N becomes an R-modules by

$$\cdot : R \times M/N \longrightarrow M/N \text{ defined by } r(m + N) = rm + N,$$

for all $r \in R, m \in M$. Then, it's called the **quotient** or **factor module** of M by N.

Definition 79. A submodule of a left R-module M is an additive subgroup A of M such that $x \in A$ implies $ax \in A$ for all $r \in R$.

Definition 80. A map $f : M \longrightarrow N$ of R-modules is called an R-homomorphism if f is R-linear (i.e., $f(rx + y) = rf(x) + f(y)$ for all $r \in R$ and $x, y \in M$).

Example. Let M be a R-module where R is a commutative ring in the sense of Definition 32 and $r \in R$. Then

$$\lambda_r : M \longrightarrow M \text{ by } x \mapsto rx$$

is an R-homomorphism.

EXAMPLE. Let R be a commutative ring and M, N are R-modules, then

$$\mathrm{Hom}_R(M, N) = \{f : M \longrightarrow N \mid f \text{ an } R\text{-homomorphism}\}$$

is an R-module with the usual $+$ for functions and the R-action $\cdot$ given by $r \cdot f : x \mapsto rf(x)$.

DEFINITION 81. The **Annihilator** of a left R-module M is the ideal $\mathrm{Ann}(M) = \{r \in R \mid rx = 0 \text{ for all } x \in M\}$ of R.

We need to remark that a left R-module is *faithful* when its annihilator is 0.

LEMMA 17. Let M be an R-module and m, m' elements in M. Then

(i) $\mathrm{Ann}_R(m) \subset R$ is a left ideal.

(ii) $\rho_m : R \longrightarrow M$ given by $r \mapsto rm$ is an R-homomorphism and satifies $\mathrm{Ker}\, \rho_m = \mathrm{Ann}_R(m)$.

(iii) If ρ_m is the homomorphism in (ii), then ρ_m induces an R-isomorphism $\overline{\rho_m} : R/\,\mathrm{Ann}_R(m) \longrightarrow Rm$.

(iv) If R is a commutative ring and $Rm \subset Rm'$, then $\mathrm{Ann}_R(m) \subset \mathrm{Ann}_R(m')$.

Proof: (i) and (ii) are trivial. For (iii), we can use First Isomorphism Theorem 3 for modules and claim follows. For (iv), suppose that $m = am'$ for some $a \in R$. If $rm' = 0$, then $ram' = arm' = 0$. □

PROPOSITION 32. Let M be an R-module. Then M is a cyclic R-module iff there exists a left ideal $\mathfrak{U}$ in R sastifying $M \cong R/\mathfrak{U}$.

Proof: $R/\mathfrak{U} = \langle 1 + \mathfrak{U} \rangle = R(1 + \mathfrak{U})$ is cylcic and claim follows by Lemma 17.

DEFINITION 82. The direct product of a family $(A_i)_{i \in I}$ of left R-modules is their cartesian product $\prod_{i \in I} A_i$ in the sense of Definition 13 with componentwise addition and action of R:

$$(x_i)_{i \in I} + (y_i)_{i \in I} = (x_i + y_i)_{i \in I}, r(x_i)_{i \in I} = (rx_i)_{i \in I}.$$

DEFINITION 83. The sum direct product (or external sum) of a family $(A_i)_{i \in I}$ of left R-modules is the submodule of $\prod_{i \in I} A_i$:

$$\bigoplus_{i \in I} A_i = \{(x)_{i \in I} \in \prod_{i \in I} A_i \mid x_i = 0 \text{ for almost all } i \in I\}.$$

DEFINITION 84. A left R-module M is the internal direct sum $M = \bigoplus_{i \in I} A_i$ of submodules $(A_i)_{i \in I}$ when every element of M can be written uniquely as a sum $\sum_{i\in I} a_i$, where $a_i \in A_i$ for all i and $a_i = 0$ for almost all i.

We need to remark that a nonzero R-module is **descomposable** if it's isomorphic to the direct sum of two nonzero submodules. Otherwise is **indecomposable**.

Proposition 33. Let $(M_i)_{i\in I}$ be left R-modules. For a left R-module M the following conditions are equivalent:

(1) $M \cong \bigoplus_{i\in I} M_i$,

(2) M contains submodules $(A_i)_{i\in I}$ such that $A_i \cong M_i$ for all i and every element of M can be written uniquely as a sum $\sum_{i\in I} a_i$, where $a_i \in A_i$ for all i and $a_i = 0$ for almost all i,

(3) M contains submodules $(A_i)_{i\in I}$ such that $A_i \cong M_i$ for all i, $M = \sum_{i\in I} A_i$, and $A_j \cap (\sum_{i\neq j} A_i) = 0$ for all j.

Proof: (1) implies (2). Since $\bigoplus_{i\in I} M_i$ contains submodules $M_i' = \iota(M_i) \cong M_i'$ such that every element of $\bigoplus_{i\in I} M_i$ can be written uniquely as a sum $\sum_{i\in I} a_i$, where $a_i \in M_i'$ for all i and $a_i = 0$ for almost all i. If $\theta : \bigoplus_{i\in I} M_i \longrightarrow M$ is an isomorphism, then the submodules $A_i = \theta(M_i')$ of M have similar properties.

(2) implies (3). By (2), $M = \sum_{i\in I} A_i$, moreover, if $x \in A_j \cap (\sum_{i\neq k} A_i)$, then x is a sum $x = \sum_{i\in A} a_i'$ in which $a_j' = x, a_i' = 0$ for all $i \neq j$, and a sum $x = \sum_{i\in I} a_i''$ in which $a_j'' = 0 \in A_j, a_i'' \in A_i$ for all i, $a_i'' = 0$ for almost all i, by (2), $x = a_j' = a_j'' = 0$.

(3) implies (2). By (3), $M = \sum_{i\in I} A_i$, so that every element of M is a sum $\sum_{i\in I} a_i$, where $a_i \in A_i$ for all i and $a_i = 0$ for almost all i. If $\sum_{i\in I} a_i' = \sum_{i\in I} a_i''$ where $a_i', a_i'' \in A_i$, then for every $j \in I$, $a_j'' - a_j' = \sum_{i\neq j}(a_i' - a_i'') \in A_i \cap (\sum_{i\neq j} A_i)$ and $a_j'' = a_j'$.

(2) implies (1). The inclusion homomorphism $A_i \longrightarrow M$ induce a module homomorphism $\theta : \bigoplus_{i\in I} A_i \longrightarrow M$, namely $\theta((a_i)_{i\in I}) = \sum_{i\in I} a_i$. Then θ is bijective by (2). The isomorphisms $M_i \cong A_i$, then induce an isomorphism $\bigoplus_{i\in I} M_i \cong \bigoplus_{i\in I} A_i \cong M$. □

We need to remark that by Proposition 33, internal and external sums differ only by isomorphisms, that is, if M is an external sum of modules $(A_i)_{i\in I}$, then M is an internal direct sum of submodules $A_i \cong M_i$, if M is an internal direct sum of submodules $(A_i)_{i\in I}$, then M is isomorphic to the external direct sum $\bigoplus_{i\in I} A_i$.

Example. Let $R = K[x]$. For $n \geqslant 1$, $\langle x^n\rangle$ is an ideal, and therefore $M = R/\langle x^n\rangle$ is a module which is indecomposable.

Proof: From the internal characterisation of direct product groups, we need only show that any two submodules intersect nontrivially. We show indeed that any nonzero $N \leqslant M$ contains $x^{n-1} + \langle x^n \rangle$. We suppose that

$$N \in \alpha_j x^j + \cdots + \alpha_{n-1} x^{n-1} + \langle x^n \rangle, \alpha_j \neq 0 := n.$$

Then, $n\alpha_j^{-1} x^{n-1-j} = x^{n-1} + \langle x^n \rangle$. □

1. Free Modules

We expand the Definition 51 in the following way.

Definition 85. A nonzero R-module M is called a free R-module if there exists a basis for M, that is, a subset $\mathcal{B}$ of M satisfying:

(i) $M = \langle \mathcal{B} \rangle$ (i.e., $\mathcal{B}$ generates or spans M).

(ii) $\mathcal{B}$ is linearly independent (i.e., $\sum_{\mathcal{B}} r_x x = 0$ for all $x \in \mathcal{B}, r \in R$).

Example. Let M be a R-cyclic. Then M is a free R-module if there exists an $x \in M$ satisfying $M = Rx$ and $\mathrm{Ann}_R(x) = 0$. It follows that M is a free R-module iff $M \cong R$.

Example. $\mathbb{Q}$ is not a free $\mathbb{Z}$-module.

Theorem 34 (Universal Property of Free Modules). Let $\mathcal{B} = \{x_i\}_I$ be a basis for a free R-module M. If N is an R-module and $y_i, i \in I$, elements in N, then there exists a unique R-homomorphism $f : M \longrightarrow N$ such that $x_i \mapsto y_i$, for all $i \in I$.

Proof: If $z \in M$, there exists a unique $r_i \in R$, almost all $r_i = 0$ such that $z = \sum_I r_i x_i$. In particular, the uniqueness of the r_i implies that $f : M \longrightarrow N$ given by $z \mapsto \sum_I r_i y_i$ is well-defined. Clearly, f is uniquely determined by $x_i \mapsto y_i$ and f is an R-homomorphism. □

Lemma 18. Let M and N be free R-modules on bases $\mathcal{B}$ and $\mathcal{C}$, respectively. If there exists a bijection $g : \mathcal{B} \longrightarrow \mathcal{C}$ (i.e., $|\mathcal{B}| = |\mathcal{C}|$), then $M \cong N$.

Proof: The maps g and g^{-1} of sets induce inverse R-isomorphisms $M \longrightarrow N$ and $N \longrightarrow M$. □

2. Noetherian Modules

Definition 86 (The Maximum Principle). If S is a non-empty set of submodules of M, then S contains a maximal element, that is a module $M_0 \in S$ such that if $M_0 \in N$ with $N \in S$, then $N = M_0$.

Proposition 34. Let M be a R-module. Then the following are equivalent:

(1) Every submodule of M is finetely generated,

(2) M satifies the ascending chain condition, that is, if $M_i \subset M$ are submodules and

$$M_1 \subset M_2 \subset \cdots \subset M_n \subset \ldots,$$

then there exists a positive integer N such that $M_N = M_{N+i}$ for all $i \geqslant 0$. We say every ascending chain of submodules of M stabilizes. Equivalently, ther exists no infinite chain

$$M_1 < M_2 < \ldots M_n < \ldots,$$

(3) M satifies *The Maximum Principle* in the sense of Definition 86.

Proof: (1) implies (2). Let

$$\mathcal{C} : M_1 \subset M_2 \subset \cdots \subset M_n \subset \ldots$$

be a chain of submodules of M. It follows that the subset $M' = \bigcup_{i=1}^{\infty} M_i \subset M$ is a submodule. By (1), it's finitely generated, so we can write $M' = \sum_{i=1}^{n} Rx_i$ for some $x_i \in M'$. By definition, $x_i \in M_{j_i}$ some j_i. Let s be the maximum of the finitely many j_i's. Then $M' = M_S$. It follows that $M_s = M' = M_{s+i}$ for all $i \geqslant 0$.

(2) implies (3). Suppose that S is a non-empty set of submodules of M. Let M_1 lie in S. If M_1 is not maximal, there exists an $M_2 \in S$ with $M_1 < M_2$. Inductively, if M_i is not maximal, there exist an M_{i+1} in S with $M_i < M_{i+1}$. By the a.c.c., the sequence

$$M_1 < M_2 < \ldots M_i < \ldots$$

must terminate.

(3) implies (1). Let $M \subset N$ be a submodule and set

$$S = \{M_i \mid M_i \subset N \text{ is a finitely generated submodule}\}.$$

Then $(0) \in S$ so $S \neq \varnothing$. By assumption, there exists a maximal element $M' \in S$. If $N \neq M'$, then there exists $x \in N \backslash M'$. But M' finitely generated means that $M' + Rx \subset N$ is also finitely generated, so the submodule $M' + Rx$ of N lies in S. This contradicts the maximality of M'. Hence $N = M'$ is finitely generated. □

Definition 87. Let R be a commutative ring. We say that R is a Noethereian ring if R is a Noetherian R-module.

Definition 87 coincides with the Definition 46.

Proposition 35. Let M be an R-module and N a submodule of M. Then M is R-Noetherian iff N and M/N are R-Noetherian. In particular, if

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

is an exact sequence of R-modules with two of the modules M, M', M'' being R-Noetherian, then they all are R-Noetherian.

Proof: Since $N_0 \subset N$ is a submodule, then $N_0 \subset M$ is a submodule hence finitely generated – or any ascending chain in N is an ascending chain in M. Thus N is R-Noetherian. By the Correspondence Principle, a (countable) chain of submodules in M/N has the form $M_1/N \subset M_2/N \subset \dots$ where $N \subset M_1 \subset M_2 \subset \dots$ chain of submodules of M. Thus there exists an r such that $M_r = M_{r+j}$ for all $j \geqslant 0$ and hence $M_r/N = M_{r+j}/N$ for all $j \geqslant 0$. □

Theorem 35. Let R be Noetherian ring. If M is a finitely generated R-module, then M is R-Noetherian.

Proof: Suppose $M = \sum_{i=1}^{n} Rx_i$. Let $f : R^r \longrightarrow M$ be the R-epimorphism given by $e_i \mapsto x_i$, where $\{e_1, \dots, e_n\}$ is the standard basis for R^n. Since R-Noetherian sinc $M \amalg N$ is R-module because $(M \amalg N)/N \cong M$ where N, M are Noetherian R-modules. Hence, so is $M \cong R/\operatorname{Ker} f$ by Proposition 35.

3. Hilbert's Theorems

Theorem 36 (Hilbert Basis Theorem). If R is a Noetherian ring so is the ring $R[t_1, \dots, t_n]$.

Proof: By induction on n, it suffices to show that $R[t]$ is Noetherian. Let $\mathcal{B} \subset R[t]$ be an ideal. We must show that $\mathcal{B}$ is finitely generated. Let

$$\mathfrak{U} = \{r \in R \mid r = \text{ lead } f, f \in \mathcal{B}\}.$$

First, let's show that $\mathfrak{U}$ is an ideal. Let $a, b \in \mathfrak{U}$ and $r \in R$ with $ra+b$ nonzero. Choose $f, g \in \mathcal{B}$ say of degrees m and n respectively, satisfying lead $f = a$ and lead $g = b$. Set $h = rt^n f + t^m g$ in $\mathcal{B}$. Then $ra + b =$ lead h proving $\mathfrak{U}$ is an ideal. As R is Noetherian, $\mathfrak{U} = (a_1, \dots, a_n)$ for some $a_1, \dots, a_n \in \mathfrak{U}$ with $n \in \mathbb{Z}^+$. Choose f_{id_i} in $\mathcal{B}$ such that $a_i =$ lead f_{id_i} and $\deg f_{id_i} = d_i$. Let $\mathcal{B}_0 = (f_{1d_1}, \dots, f_{nd_n})$, and ideal in $R[t]$, and $N = \max\{d_1, \dots, d_n\}$.

Let $f \in \mathcal{B}$ with lead $f = a$ and $\deg f = d$. Suppose that $d > N$. There exist $r_i \in R$ satisfying $a = \sum_{i=1}^{n} r_i a_i$, hence $f - \sum_{i=1}^{n} r_i t^{d-d_i} f_{i,d_i}$ lies in $\mathcal{B}$ and has degree less than d. It follows by induction that there exists a $g \in \mathcal{B}_0$ such that $f - g$ lies $\mathcal{B}$ with $\deg(f - g) \leqslant N$. As the R-module $M = \sum_{i=0}^{n} Rt^i$ is finitely generated and R is Noetherian, M is a Noetherian R-module. In particular, the submodule $M_0 = \{f \in \mathcal{B} \mid \deg f \leqslant N\}$ is finitely generated. If $M_0 = \sum_{i=0}^{m} R[t]g_i$, then $\mathcal{B} = \mathcal{B} + \sum_{i=0}^{m} R[t]g_i$ is finitely generated. □

Definition 88. Let $R \subset S$ be commutative rings. We say that S is a finitely generated commutative R-algebra (or an affine R-algebra when R is a field) if there exists $x_1, \dots, x_n$ in S satisfying $S = R[x_1, \dots, x_n]$ as rings.

Proposition 36. Let R be a commutative ring and S a finitely generated commutative R-algebra. If R is Noetherian so is S.

Proof: Let $S = R[x_1, \dots, x_n]$. Since $R[t_1, \dots, t_n]$ is Noetherian and we have a ring epimorphism $R[t_1, \dots, t_n] \longrightarrow R[x_1, \dots, x_n]$ via $f(t_1, \dots, t_n) \mapsto f(x_1, \dots, x_n)$, all ideals of S are finitely generated by the Correspondence Principle. □

Theorem 37 (Hilbert Nullstellensatz, Strong Form). Suppose that F be an algebraically closed field and $R = F[t_1, \dots, t_n]$. Let $f, f_1, \dots, f_r$ be elements in R and $\mathfrak{U} = (f_1, \dots, f_r) \subset R$. Suppose that $f(a) = 0$ for all $a \in Z_F(\mathfrak{U})$. Then there exists an integer m such that $f^m \in \mathfrak{U}$ (i.e., f $\in \sqrt{U}$). In particular, if $\mathfrak{U}$ is a prime ideal, then $f \in \mathfrak{U}$.

Proof: We may assume that f is nonzero. Let $S = R[t]$. Define the ideal $\mathcal{B}$ in S by $\mathcal{B} = (f_1, \dots, f_r, 1 - tf) \subset S$. If $\mathcal{B} < S$, then there exists a point $(a_1, \dots, a_{n+1}) \in Z_F(\mathcal{B})$. Thus $f_i(a_1, \dots, a_n) = 0$ for all i and $1 - a_{n+1} f(a_1, \dots, a_{n+1}) = 0$. In particular, $(a_1, \dots, a_n)$ lies in $Z_F(\mathfrak{U})$. By hypothesis, this means that $(a_1. \dots, a_n) = 0$ which in turn implies that $1 = 0$, a contradiction. Thus $\mathcal{B} = S$. So we can write

$$1 = \sum_{i=1}^{r} g_i f_i + g \cdot (1 - tf)$$

for some $g, g_i \in S$. Substituting $1/f$ for t and clearing denominators yields the result. □

CHAPTER 4

Field Theory

Definition 89. A field is a commutative ring (necessarily a domain) whose nonzero elements constitute a group under multiplication.

Definition 90. A subfield of a field F is a subset K of F such that K is an additive subgroup of F on $K\backslash\{0\}$ is a multiplicative subgroup of $F\backslash\{0\}$.

Equivalently to Definition 90, K is a subfield of F iff

I. $0, 1 \in K$,
II. $x, y \in K$ implies $x - y \in K$,
III. $x, y \in K, y \neq 0$ implies $xy^{-1} \in K$.

Then $x, y \in K$ implies $x + y \in K$ and $xy \in K$, so that K inherits an addition and a multiplication from F, and K is a field under these inherited operations, this field K is also called a subfield of F.

Example. $\mathbb{Q}$ is a subfield of $\mathbb{R}$, and $\mathbb{R}$ is a subfield of $\mathbb{C}$.

Definition 91. A homomorphism of a field K into a field L is a mapping $\varphi : K \longrightarrow L$ such that $\varphi(1) = 1, \varphi(x + y) = \varphi(x) + \varphi(y)$ and $\varphi(xy) = \varphi(x)\varphi(y)$ for all $x, y \in K$.

Proposition 37. The characteristic of a field is either 0 or a prime number.

Proof: REIMAINDER

Proposition 38. Every field K has a smallest subfield, which is isomorphic to $\mathbb{Q}$ if K has characteristic 0, to $\mathbb{Z}_p$ if K has characteristic $p \neq 0$.

Proof: REIMAINDER

Definition 92. An element r of a field K is an nth root of unity when $r^n = 1$.

1. Extensions

Definition 93. A field extension of a field K is a field E of which K is a subfield.

Definition 94. Let $K \subseteq E$ and $K \subseteq F$ be field extensions of K. A K-homomorphism of E into F is a field homomorphism $\varphi : E \longrightarrow F$ that is the identity on $K(\varphi(x) = x$ for all $x \in K)$.

Definition 95. The degree $[E : K]$ of a field extension $K \subseteq E$ is its dimension as a vector space over K. A field extension $K \subseteq E$ is finite when it has finite degree and is finite otherwise.

Example. $[\mathbb{C} : \mathbb{R}] = 2$.

Proposition 39. If $K \subseteq E \subseteq F$, then $[F : K] = [F : E][E : K]$.

Proof: Let $(\alpha_i)_{i\in I}$ be a basis of E over K and let $(\beta_j)_{j\in J}$ be a basis of F over E. Every element of F is a linear combination of β_j's with coefficients in E, which are themselves linear combinations of α_i's with coefficints in K.

Hence every element of F is a linear combination of $\alpha_i\beta_j$'s with coefficients in K. Moreover, $(\alpha_i\beta_j)_{(i,j)\in I\times J}$ is a linearly independent family in F, viewed as a vector space over K : if $\sum_{(i,j)\in I\times J} x_{i,j}\alpha_i\beta_j = 0$ (with $x_{i,j} = 0$ for almost all (i, j)), then $\sum_{j\in J}\left(\sum_{i\in I} x_{i,j}\alpha_i\right)\beta_j = 0$, $\sum_{i\in I} x_{i,j}\alpha_i = 0$ for all j, and $x_{i,j} = 0$ for all i, j. Thus $(\alpha_i\beta_j)_{(i,j)\in I\times J}$ is a basis of F over K and $[F : K] = |IJ| = |I||J| = [F : E][E : K]$. □

Definition 96. Let $K \subset E$ be a field extension. An element of E is **algebraic** over K when $f(x) = 0$ for some nonzero polynomial $f(X) \in K[X]$. Otherwise, α is **transcendental** over K.

Definition 97. Let α be algebraic over K. The unique monic irreducible polynomial $q = \mathrm{Irr}(\alpha : K) \in K[X]$ such that $q(\alpha) = 0$ is the irreducible polynomial of α over K, the degree of α over K is the degree of $\mathrm{Irr}(\alpha : K)$.

Definition 98. A field extension $K \subseteq E$ is algebraic, and E is algebraic over K, when every element of E is algebraic over K. A field extension $K \subseteq E$ is transcendental over K, when some element of E is transcendental over K.

Example. $\mathbb{C}$ is algebraic extension of $\mathbb{R}$ and $\mathbb{R}$ is a transcendental extension of $\mathbb{Q}$.

1.1. The Algebraic Closure.

Definition 99. A field is algebraically closed when it satisfies the following equivalent conditions:

1. The only algebraic extension of K is K itself.
2. In $K[X]$, every irreducible polynomial has degree 1.
3. Every nonconstant polynomial in $K[X]$ has a root in K.

Example. $\mathbb{C}$ is algebraically closed.

Theorem 38. Every homomorphism of a field K into a algebraically closed field can be extended to every algebraic extension of K.

Proof: Let E be an algebraic extension of K and let α be an homomorphism of K into an algebraically closed field L. If $E = K(\alpha)$ is simple extension of K, and $q = \operatorname{Irr}(\alpha : K)$, then ${}^{\varphi}q \in L[X]$ has a root in L, since L is algebraically closed and φ can be extended to E. □

We need to remark that K can be embedded into an algebraically closed field $\overline{K}$ that is algebraic over K, and then every algebraic extension of K can be embedded in $\overline{K}$, by Theorem 38.

Definition 100. An algebraic closure of a field K is an algebraic extension $\overline{K}$ of K that is algebraically closed.

Definition 101. An algebraic extension $K \subseteq E$ is separable when the irreducible polynomial of its elements are separable (have no multiple roots).

Example. $f(X) = X^4 + 2X^2 + 1 \in \mathbb{R}[X]$ factors as $f(X) = (X^2+1)^2 = (X-i)^2(X+i)^2$ in $\mathbb{C}[X]$ and has two multiples roots in $\overline{\mathbb{R}} = \mathbb{C}$, it is not separable. But $X^2 + 1 \in \mathbb{R}[X]$ is separable.

Definition 102. An element α is separable over K when α is algebraic over K and $\operatorname{Irr}(\alpha : K)$ is separable. An algebraic extension E of K is separable, and E is separable over K, when every element of E is separable over K.

Definition 103. An algebraic extension $K \subseteq E$ is purely inseparable, and E is purely inseparable over K, when no element of $E\backslash K$ ise separable over K.

Proposition 40. For every algebraic extension E of K, $S = \{\alpha \in E \mid \ \alpha \text{ is separable over } K\}$ is a subfield of E, S is separable over K, and E is purely inseparable over S.

Proof: First, 0 and $1 \in K$ are separable over K. If $\alpha, \beta \in E$ are separable over K, then $K(\alpha, \beta)$ is separable over K and $\alpha - \beta, \alpha\beta^{-1} \in K(\alpha, \beta)$ are separable over K. Thus S is a subfield of E. Clearly S is separable over K. If $\alpha \in E$ is separable over S, then $S(\alpha)$ is separable over K and $\alpha \in S$. □

Definition 104. A field extension $K \subseteq E$ is totally transcendental, and E is transcendental over K, when every element of $E \backslash K$ is transcendental over K.

Proposition 2. For every field $K, K((X_i)_{i \in I})$ is totally transcendental over K.

Proof: First, we show that $K(X)$ is totally transcendental over K. For clarity's sake we prove the equivalent result that $K(\gamma) \cong K(X)$ is totally transcendental over K when γ is transcendental over K. Let $\alpha \in K(\gamma)$, so that $\alpha = f(\gamma)/g(\gamma)$ for some $f, g \in K[X], g \neq 0$. If $\alpha \notin K$, then $\alpha g(X) \notin K[X], \alpha g(X) \neq f(X)$, and $\alpha g(X) - f(X) \neq 0$ in $K(\alpha)[X]$. But $\alpha g() - f(\gamma) = 0$, so γ is algebraic over $K(\alpha)$. Hence $K(\gamma) = K(\alpha)(\gamma)$ is finite over $K(\alpha)$. Therefore $[K(\alpha) : K]$ is infinite. Otherwise, $[K(\gamma) : K]$ would be finite. Hence α is transcendental over K.

That $K[X_1, \ldots, X_n]$ is totally transcendental over K now follows by induction on n. Let $\alpha \in K(X_1, \ldots, X_n)$ be algebraic over K. Then $\alpha \in K(X_1, \ldots, X_{n-1})(X_n)$ is algebraic over $K(X_1, \ldots, X_{n-1})$. By the case, $n = 1, \alpha \in K(X_1, \ldots, X_{n-1})$, and the induction hypothesis yields $\alpha \in K$.

Finally, let $\alpha = f/g \in K((X_i)_{i \in I})$ be algebraic over K. The polynomials f and g have only finitely many nonzero terms. Hence $\alpha \in K((X_i)_{i \in J})$ for some finite subset J of I. Therefore $\alpha \in K$. □

2. Separability

Definition 105. Two field extension $K \subseteq E \subseteq L$, $K \subseteq F \subseteq L$ are linearly disjoint over K when they satisfy the following equivalent conditions:

1. .$(\alpha_i)_{i \in I} \in E$ linearly independent over K implies $(\alpha_i)_{i \in I}$ linearly independent over F.
2. $(\beta_j)_{j \in J} \in F$ linearly independent over K implies $(\beta_i)_{i \in I}$ linearly independent over E.
3. $(\alpha_i)_{i \in I} \in E$ and $(\beta_j)_{j \in J} \in F$ linearly independent over K implies $(\alpha_i \beta_j)_{(i,j) \in I \times J} \in L$ linearly independent over K.

Definition 106. A transcendence base B of a field extension $K \subset E$ is separating when E is separable (algebraic) over $K(B)$.

Definition 107. A field extension E of K is separable, and E is separable over K, when every finitely generated subfield $K \subseteq F$ of E has a separating transcendental base.

3. Galois Theory

DEFINITION 108. A polynomial $f \in K[X]$ splits in a field extension E of K when it has a factorization $f(X) = a(X - \alpha_1)(X - \alpha_2)\dots(X -{}_n)$ in $E[X]$.

DEFINITION 109. Let K be a field. A splitting field over K of a polynomial $f \in K[X]$ is a field extension E of K such that f splits in E and E is generated over K by the roots of f. A splitting field over K of a set $\mathcal{S} \subseteq K[X]$ of polynomials is a field extension E of K such that every $f \in \mathcal{S}$ splits in E and E is generated over K by the roots of all $f \in \mathcal{S}$.

LEMMA 19. If E and F are splitting fields of $\mathcal{S} \subseteq K[X]$ over K, and $F \subseteq \overline{K}$, then $\varphi E = F$ for every K homomorphism $\varphi : E \longrightarrow \overline{K}$.

Proof: Every $f \in \mathcal{S}$ has unique factorizations $f(X) = a(X - \alpha_1)\dots(X - \alpha_n)$ in $F[X] \subseteq \overline{K}[X]$. Since φ is the identity on K, $f,^{\varphi} f = a(X - \varphi\alpha_1)\dots(X - \varphi\alpha_n)$ in $\overline{K}[X]$, therefore $\{\alpha_{1,\dots,\alpha_n}\} = \{\beta_1, \dots, \beta_n\}$. Thus φ sends the set R of all roots $f \in \mathcal{S}$ in E onto the set $\mathcal{S}$ of all roots $f \in \mathcal{S}$ in F. Then, φ sends $E = K(R)$ onto $K(S) = F$. □

DEFINITION 110. A normal extension of a field K is an algebraic extension of K that satisfies the following equivalent conditions:

1. E is the splitting field over K of a set of polynomials,
2. $\varphi E = E$ for every K-homomorphism $\varphi : E \longrightarrow \overline{K}$,
3. $\varphi E \subseteq E$ for every K-homomorphism $\varphi : E \longrightarrow \overline{K}$,
4. $\rho E = E$ for every K-automorphism $\rho :$ of $\overline{K}$,
5. $\rho E \subseteq E$ for every K-automorphism $\rho :$ of $\overline{K}$,
6. every irreducible polynomial $q \in K[X]$ with a root in E splits in E.

DEFINITION 111. A Galois extension of a field K is a normal and separable extension E of K, then E is Galois over K.

DEFINITION 112. The **Galois group** $\mathrm{Gal}(E : K)$ of a Galois extension E of a field K, also called the Galois group of E over K, is the group of all K-automorphisms of E.

EXAMPLE. The Galois group $\mathbb{C} = \overline{\mathbb{R}}$ over $\mathbb{R}$ has two extensions, the identity on $\mathbb{C}$ and the complex conjugation.

PROPOSITION 41. If E is Galois over K, then $|\mathrm{Gal}(E : K)| = [E : K]$.

Proof: If $E \subseteq \overline{K}$ is normal over K, then every K-homomorphism of E into $\overline{K}$ sends E and is (as a set of ordered pairs) a K-automorphism of E. Hence $|\mathrm{Gal}(E : K)| = [E : K]_s = [E : K$ when E is separable over K. □

Definition 113. Let E be a field and let G be a group of automorphisms of E. The fixed field of G if $\mathrm{Fix}_E(G) = \{\alpha \in E \mid \varphi\alpha = \alpha \text{ for all } \varphi \in G\}$.

Theorem 39 (Fundamental Theorem of Galois Theory). Let E be a finite Galois extension of a field K.

If F is a subfield of E that contains K, then E is a finite Galois extension of F and F is the fixed field of $\mathrm{Gal}(E : F)$.

If H is a subgroup of $\mathrm{Gal}(E : K)$, then $F = \mathrm{Fix}_E(H)$ is a subfield of E that contains K , and $\mathrm{Gal}(E : F) = H$.

This defines a one-to-one correspondence between intermediate fields $K \subseteq F \subseteq E$ and subgroups of $\mathrm{Gal}(E : K)$.

Bibliography

[Gr] P. A. Grillet, *Abstract Algebra (Graduate Texts in Mathematics), Second Edition.* Springer New York, 2007.

[La] Serge Lang, *Algebra (Graduate Texts in Mathematics), Third Edition.* Springer Science & Business Media, 2005.

[Ro] J. J. Rotman, *Advanced Modern Algebra (Graduate Texts in Mathematics), Third Edition, Part I.* American Mathematical Soc., 2015.

[Ed] H. M. Edwards, *Galois Theory (Graduate Texts in Mathematics).* Springer New York, 1997.

[El] Richard Elman, *Lectures on Abstract Algebra (Preliminary Version).* http://www.math.ucla.edu/~rse/algebra_book.pdf .

[Ch] Evan Chen, *Math 55a Lecture Notes.* Harvard, Fall 2014 http://www.mit.edu/~evanchen/notes/Harvard-55a.pdf .

[Re] Mark Reeder, *Notes on Group Theory.* Boston College, 2015 https://www2.bc.edu/mark-reeder/Groups.pdf .