Algebra

this is my notes for Dummit Foote - Abstract Algebra. Despiting hating math and algebra in my secondary school, high school, university. Turn out algebra is the discipline that inspires me the most. Hopefully can be an algebraist or algebraic geometer/topologist someday. There is another book from Paolo Aluffi, will start that one after this

Part 1: Group Theory - Dec 2023

Part 2: Ring Theory and Module Theory - Dec 2024

Nguyen Ngoc Khanh

May 20, 2025

Chapter 1

GROUP THEORY

1.1 INTRODUCTION TO GROUPS

1.1.1 BASIC AXIOMS

Definition 1.1.1 (Group)

A group is an ordered pair $(G, \cdot)$ where G is a set and $\cdot$ is a binary operation on G such that

- There exists an element $e \in G$, namely identity, such that $ae = ea = e$ for each $a \in G$
- For each $a \in G$, there exists an element a^{-1}, namely inverse, such that $aa^{-1} = a^{-1}a = e$
- $\cdot$ is associative, that is, $(ab)c = a(bc)$ for all $a, b, c \in G$

A group $(G, \cdot)$ is said to be abelian if $\cdot$ is commutative, that is, $ab = ba$ for all $a, b \in G$

Definition 1.1.2 (Direct Product)

If $(A, \star), (B, \diamond)$ are groups, the direct product $(A, \star) \times (B, \diamond)$ is a group of $A \times B$ under $\cdot$ defined as

$$A \times B = \{(a, b) : a \in A, b \in B\}$$

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 \star a_2, b_1 \diamond b_2)$$

Proposition 1.1.3 (Basic Properties)

If G is a group under $\cdot$, then

1. The identity of G is unique
2. The inverse is unique for each $a \in G$
3. $(a^{-1})^{-1} = a$ for each $a \in G$
4. $(ab)^{-1} = b^{-1}a^{-1}$

Proposition 1.1.4 (Cancellation Laws)

Let G be a group and $a, b \in G$. The two equations below have unique solutions

- $ax = b$
- $ya = b$

That is, $x = a^{-1}b$, $y = ba^{-1}$

Definition 1.1.5 (Order of An Element)

Let G be a group and $x \in G$. Let n be the smallest positive integer such that $x^n = 1$. n, denoted by $|x|$, is said to be the order of x. If there is no positive integer n satisfying $x^n = 1$, the order of x is said to be infinity.

1.1.2 DIHEDRAL GROUP

Definition 1.1.6 (D_{2n} - Dihedral Group of Order $2n$)

The symmetry group of a regular n-polygon. Let r be the rotation clockwise about the origin through $2\pi/n$ radian and s be the reflection about the line of symmetry through vertex 1 and the origin. The following are true

1. $1, r, r^2, ..., r^{n-1}$ are distinct and $r^n = 1$, so $|r| = n$
2. $|s| = 2$
3. $D_{2n} = \{1, r, r^2, ..., r^{n-1}, s, sr, sr^2, ..., sr^{n-1}\}$, $|D_{2n}| = 2n$
4. $rs = sr^{-1}$, more generally, $r^i s - sr^{-i}$ for all $i \in \mathbb{Z}$

Generators and Relations

Definition 1.1.7 (Generators and Relations)

A subset S of a group G is said to be the set of generators of G if every element of G can be written as a finite product of elements of S, denoted by $G = \langle S \rangle$. Furthermore, the equations that elements of S satisfy are said to be relations, denoted by $R_1, R_2, ..., R_m$. We write

$$G = \langle S | R_1, R_2, ..., R_m \rangle$$

The dihedral group D_{2n} can be written as

$$D_{2n} = \langle r, s | r^n = s^2 = 1, rs = sr^{-1} \rangle$$

1.1.3 SYMMETRIC GROUP

Definition 1.1.8 (Symmetric Group)

Let Ω be a nonempty set and S_Ω be the set of all bijections from Ω onto itself (i.e the set of all permutations of Ω). S_Ω is a group under function composition $\circ$, namely the symmetric group on Ω.

1.1.4 MATRIX GROUP

Definition 1.1.9 (Field)
A field is a set F equipped with two binary operations $+$ and $\cdot$ such that $(F, +)$ is an abelian group with its (additive) identity 0 and $(F \setminus \{0\}, \cdot)$ is an abelian group with its (multiplicative) identity 1 and the distributive law holds

$$a(b + c) = ab + ac \text{ for all } a, b, c \in F$$

Let $F^\times$ denotes $F \setminus \{0\}$

Definition 1.1.10 (General Linear Group)
Let $GL_n(F)$ be the set of all $n \times n$ matrices whose entries come from F and the determinant is nonzero. Then $GL_n(F)$ is a group under matrix multiplication, namely the general linear group of degree n

1.1.5 QUATERNION GROUP

Definition 1.1.11 (Quaternion Group)
The quaternion group Q_8 is defined by

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

where the operation is defined as follows

- $1a = a1 = a$ for all $a \in Q_8$
- $(-1)(-1) = 1$, $(-1)a = a(-1) = -a$ for all $a \in Q_8$
- $ii = jj = kk = -1$
- $ij = k$, $ji = -k$
- $jk = i$, $kj = -i$
- $ki = j$, $ik = -j$

1.1.6 HOMOMORPHISM AND ISOMORPHISM

Definition 1.1.12 (Homomorphism)
Let $(G, \star)$ and $(H, \diamond)$ be groups. A map $\phi : G \to H$ is said to be a homomorphism if

$$\phi(x \star y) = \phi(x) \diamond \phi(y) \text{ for all } x, y \in G$$

Definition 1.1.13 (Isomorphism)
Let $(G, \star)$ and $(H, \diamond)$ be groups. A map $\phi : G \to H$ is said to be an isomorphism if ϕ is a homomorphism that is also a bijection. G and H are said to be isomorphic or of the same isomorphism type, denoted by $G \cong H$

1.1.7 GROUP ACTION

Definition 1.1.14 (Group Action)
Let G be a group and A be a set. A map $\cdot : G \times A \to A$ (written in infix notation as $g \cdot a$ for $g \in G$ and $a \in A$) is said to be a group action of G on A if

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

Definition 1.1.15 (Permutation Representation of Group Action)
Let $\cdot$ be a group action of G on A. For each $g \in G$, let $\sigma_g : A \times A$ be a permutation on A such that $\sigma_g(a) = g \cdot a$ [a]. Let $\phi : G \to S_A$ be defined as $\phi(g) = \sigma_g$. Then, ϕ is a homomorphism from G to S_A, and it is said to be the permutation representation associated with $\cdot$.

[a] this operation is well-defined

1.2 SUBGROUPS

1.2.1 DEFINITION

Definition 1.2.1 (Subgroup)
A subset H of a group G is said to be a subgroup if it is a group under the same operation, denoted by $H \leq G$.

Proposition 1.2.2 (Subgroup Criterion)
A subset H of a group G is a subgroup if and only if

1. $H \neq \varnothing$
2. $xy^{-1} \in H$ for all $x, y \in H$

Furthermore, if H is finite, it suffices to check that H is nonempty and closed under multiplication.

1.2.2 CENTRALIZER AND NORMALIZER, STABILIZER AND KERNEL

Definition 1.2.3 (Centralizer, Center)
Given a group G and a nonempty subset A of G. Define

$$C_G(A) = \{g \in G : \forall a \in A, gag^{-1} = a\}$$

Then, $C_G(A)$ is said to be the centralizer of A in G. Furthermore, $C_G(A)$ is a subgroup of G. $Z(G) = C_G(G)$ is said to be the center of G.

Definition 1.2.4 (Normalizer)
Given a group G and a nonempty subset A of G. Let

$$N_G(A) = \{g \in G : gAg^{-1} = A\}$$

where $gAg^{-1} = \{gag^{-1} : a \in A\}$. Then, the centralizer can be written as

$$C_G(A) = \bigcap_{a \in A} N_G(\{a\})$$

Stabilizers and Kernels of Group Actions

Definition 1.2.5 (Stabilizer and Kernel)
Let $\cdot$ be a group action of G on S and $s \in S$, define

$$G_s = \{g \in G : g \cdot s = s\}$$

Then, G_s is said to be the stabilizer of s in G. Furthermore, G_s is a subgroup of G. Define the kernel of an action as

$$\{g \in G : \forall s \in S, g \cdot s = s\}$$

1.2.3 CYCLIC GROUPS AND CYCLIC SUBGROUPS

Definition 1.2.6 (Cyclic Group)
A group H is said to be cyclic if it can be generated by a single element, i.e. $H = \langle x \rangle$

Proposition 1.2.7
If $H = \langle x \rangle$, then $|H| = |x|$

Proposition 1.2.8
Let G be an arbitrary group and $x \in G$ and let $m, n \in \mathbb{Z}$. If $x^n = x^m = 1$, then $x^d = 1$ where $d = \gcd(m, n)$

Theorem 1.2.9
Any two cyclic groups of the same order are isomorphic. Hence, the cyclic group of order n, $n \in \mathbb{Z}$, is denoted by Z_n

Proposition 1.2.10
Let G be a group, $x \in G$, and $a \in \mathbb{Z} \setminus \{0\}$

1. If $|x| = \infty$, then $|x^a| = \infty$
2. If $|x| = n < \infty$, then $|x^a| = \frac{n}{\gcd(n,a)}$

Proposition 1.2.11

Let $H = \langle x \rangle$

1. If $|x| = \infty$, then $H = \langle x^a \rangle$ if and only if $a = \pm 1$
2. If $|x| = n < \infty$, then $H = \langle x^a \rangle$ if and only if $\gcd(a, n) = 1$

Theorem 1.2.12

Let $H = \langle x \rangle$,

1. Every subgroup of H is cyclic
2. If $|H| = \infty$, then for any distinct positive integers a, b, $\langle x^a \rangle \neq \langle x^b \rangle$, for any integer m, $\langle x^m \rangle = \langle x^{|m|} \rangle$
3. If $|H| = n < \infty$, for each positive integer a dividing n, there is a unique subgroup of H of order a that is $\langle x^d \rangle$ where $d = \frac{n}{a}$. Furthermore, for every integer m, $\langle x^m \rangle = \langle x^{(n,m)} \rangle$, that is, there is a one-to-one correspondence between subgroups of H and positive divisors of n

1.2.4 SUBGROUPS GENERATED BY SUBSETS OF A GROUP

Proposition 1.2.13

If $\mathcal{A}$ is a nonempty collection of subgroups of G, the $K = \bigcap_{A \in \mathcal{A}} A$ is also a group of G

Definition 1.2.14 (Subgroup Generated by a Subset)

Let A be a subset of group G, define

$$\langle A \rangle = \bigcap_{A \subseteq H, H \leq G} H$$

Then, $\langle A \rangle$ is said to be the subgroup generated by A

Proposition 1.2.15

Define the following

$$\overline{A} = \{a_1^{\epsilon_1} a_2^{\epsilon_2} ... a_n^{\epsilon_n} : n \in \mathbb{N}, a_i \in A, \epsilon_i \in \mathbb{Z}\}$$

Then, $\overline{A} = \langle A \rangle$

1.2.5 THE LATTICE OF SUBGROUPS OF A GROUP

1.3 QUOTIENT GROUPS AND HOMOMORPHISMS

1.3.1 DEFINITION

Definition 1.3.1 (Kernel of a Homomorphism)
Let $\phi : G \to H$ be a homomorphism, define

$$\ker \phi = \{g \in G : \phi(g) = 1\}$$

Then, $\ker \phi$ is said to be the kernel of ϕ.

Proposition 1.3.2
Let $\phi : G \to H$ be a homomorphism, then

1. $\phi(1_G) = 1_H$ where 1_G and 1_H are the identities of G and H respectively
2. $\phi(g^n) = \phi(g)^n$ for all $g \in G, n \in \mathbb{Z}$
3. $\ker \phi$ is a subgroup of G
4. $\operatorname{im} G$, the image of G under ϕ is a subgroup of H

Definition 1.3.3 (Quotient Group)
Let $\phi : G \to H$ be a homomorphism with kernel K. The quotient group, denoted by G/K, is the group whose elements are the fibers of ϕ over the elements of $\operatorname{im} G \subseteq H$ with group operation $\cdot$ defined as

$$\phi^{-1}(a) \cdot \phi^{-1}(b) = \phi^{-1}(ab)$$

for all $a, b \in \operatorname{im} G$

Proposition 1.3.4
Let $\phi : G \to H$ be a homomorphism with kernel K. Let $X \in G/K$ be the fiber if ϕ over a, that is, $X = \phi^{-1}(a)$. Then,

1. For any $u \in X$, $uX = \{uk : k \in K\}$
2. For any $u \in X$, $Xu = \{ku : k \in K\}$

Definition 1.3.5 (Coset)
Let G be a group, for any $N \leq G$ and any $g \in G$, let

$$gN = \{gn : n \in N\} \text{ and } Ng = \{ng : n \in N\}$$

Then, gN and Ng are said to be the left coset and the right coset of N in G.

Theorem 1.3.6

Let G be a group and K be the kernel of some homomorphism from G. Then the set whose elements are the left cosets of K in G with the operation defined as

$$uK \cdot vK = (uv)K$$

for $u, v \in G$ forms the quotient group G/K

Proposition 1.3.7

Let N be any subgroup of G, then the set of left cosets of N in G partitions G. Furthermore, for all $u, v \in G$, $uN = vN$ if and only if $uv^{-1} \in N$

Proposition 1.3.8

Let G be a group and let N be a subgroup of G

1. The operation on the left cosets of N in G described by

   $$uN \cdot vN = (uv)N$$

   is well-defined if and only $gng^{-1} \in N$ for all $g \in G$ and all $n \in N$

2. If the above operation is well-defined, then the set of left cosets of N in G forms a group. In particular, the identity of this group is N and the inverse of gN is $g^{-1}N$

Definition 1.3.9 (Conjugate, Normalize, Normal Subgroup)

The element gng^{-1} is called the conjugate of $n \in N$ by g. The set $gNg^{-1} = \{gng^{-1} : n \in N\}$ is said to be the conjugate of N by g. The element g is said to normalize N if $gNg^{-1} = N$, i.e $g \in N_G(N)$. A subgroup N of G is said to be normal, denoted by $N \trianglelefteq G$, if every element of G normalizes N, i.e. $N_G(N) = G$

Theorem 1.3.10

Let N be a subgroup of G. The following are equivalent:

1. $N \trianglelefteq G$
2. $N_G(N) = G$
3. $gN = Ng$ for all $g \in G$
4. the set of left cosets form a group under the operation $uN \cdot vN = (uv)N$

Proposition 1.3.11

A subgroup N of G is normal if and only if it is the kernel of some homomorphism

Definition 1.3.12 (Natural Projection, Complete Preimage)
Let $N \trianglelefteq G$. The homomorphism $\pi : G \to G/N$ defined by $\phi(g) = gN$ is said to be the natural projection of G onto G/N. If $\overline{H} \leq G/N$ is a subgroup of G/N, the complete preimage of $\overline{H}$ in G is $\pi^{-1}(\overline{H})$

1.3.2 MORE ON COSETS AND LAGRANGE THEOREM

Theorem 1.3.13 (Lagrange Theorem)
Let H be a subgroup of a finite group G, then the order of H divides G and the number of left cosets of H in G is $\frac{|G|}{|H|}$

Definition 1.3.14 (Index of a Subgroup)
Let $H \leq G$, the number of left cosets of H in G is said to be the index of H in G, denoted by $|G : H|$

Corollary 1.3.15
If G is a finite group and $x \in G$, the order of x divides the order of G. In particular, $x^{|G|} = 1$ for all $x \in G$

Corollary 1.3.16
If G is a group of prime order p, then G is cyclic, hence $G \cong Z_p$

Theorem 1.3.17 (Cauchy Theorem)
If G is a finite group and p is a prime dividing $|G|$, then G has an element of order p

Theorem 1.3.18 (Sylow Theorem)
If G is a finite group of order $p^\alpha m$ where p is a prime and p does not divide m, then G has a subgroup of order p^α

Definition 1.3.19
Let H, K be subgroups of a group, define

$$HK = \{hk : h \in H, k \in K\} = \bigcup_{h \in H} hK$$

Proposition 1.3.20
If H and K are finite subgroups of a group then

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

Proposition 1.3.21

If H and K are finite subgroups of a group then, HK is a subgroup if and only if $HK = KH$

Corollary 1.3.22

If H and K are subgroups of G and $H \leq N_G(K)$, then HK is a subgroup of G. In particular, if $K \trianglelefteq G$, the $HK \leq G$ for any $H \leq G$

Definition 1.3.23 (Normalize, Centralize)

A is said to normalize K (or centralize K) if $A \subseteq N_G(K)$ (or $A \subseteq C_G(K)$)

1.3.3 THE ISOMORPHISM THEOREMS

Theorem 1.3.24 (the first isomorphism theorem)

If $\phi : G \to H$ is a homomorphism, then $\ker \phi \trianglelefteq G$ and $G/\ker \phi \cong \operatorname{im} \phi$

The map $\phi : (x, y) \to (x, 0)$ on $G = \mathbb{R}^2$ has the kernel $\ker \phi = \{(0, y) : y \in \mathbb{R}\}$ which is the line parallel to the y-coordinate and intersects x-coordinate at $x = 0$. $G/\ker \phi$ is the set of all lines parallel to the y-coordinate which is isomorphic to the image $\operatorname{im} \phi = \{(x, 0) : x \in \mathbb{R}\}$

Corollary 1.3.25

If $\phi : G \to H$ is a homomorphism. Then,

1. ϕ is injective if and only if $\ker \phi = \{1\}$
2. $|G : \ker \phi| = |\operatorname{im} G|$

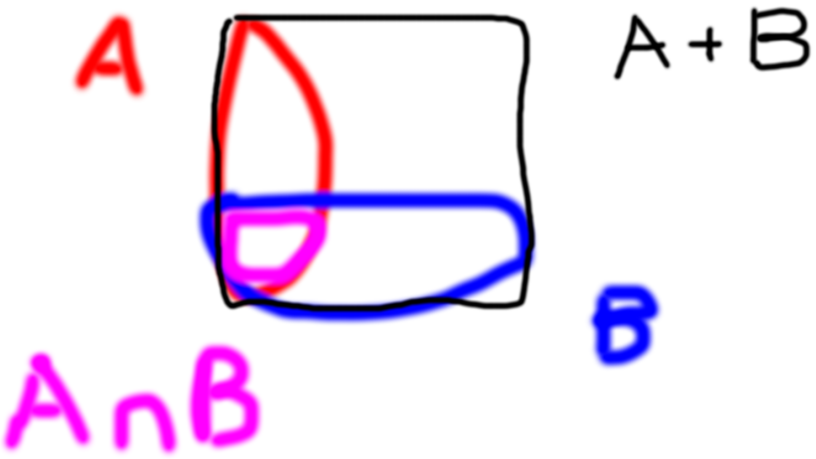
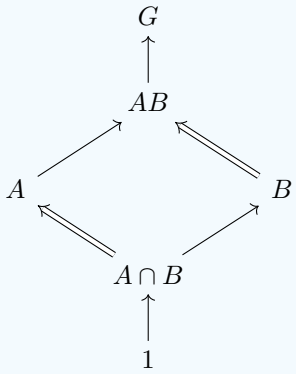


Figure 1.1: second isomorphsim theorem

Theorem 1.3.26 (the second isomorphism theorem, the diamond isomorphism theorem)
Let A, B be subgroups of G with A normalizes B, then AB is a subgroup of G, and

$$\frac{AB}{B} \cong \frac{A}{A \cap B}$$

where subgroups being normal as necessary



Additionally, A need not to be normal in AB, we still have $|AB : A| = |B : A \cap B|$
$A = \{(x, y, 0) : x, y \in \mathbb{R}\}$ and $B = \{(0, y, z) : y, x \in \mathbb{R}\}$ are subgroups of $G = \mathbb{R}^3$ with $AB = G = \{(x, y, z) : x, y, z \in \mathbb{R}\}$, $A \cap B = \{(0, y, 0) : y \in \mathbb{R}\}$. AB/B is the set of all planes orthogonal to the x-coordinate. $A/A \cap B$ is the set of all lines on (x, y)-plane that is orthogonal to the x-coordinate. Both are isomorphic to the x-coordinate

Theorem 1.3.27 (The Third Isomorphism Theorem)

Let H, K be normal subgroups of G with $H \leq K$. Then

$$\frac{G/H}{K/H} \cong \frac{G}{K}$$

where subgroups being normal as necessary

$G = \{(x, y, z) : x, y, z \in \mathbb{R}\} = \mathbb{R}^3$, $K = \{(x, y, 0) : x, y \in \mathbb{R}\}$, then G/K is the set of all planes orthogonal to the z-coordinate that is isomorphic to z-coordinate. $H = \{(x, 0, 0) : x \in \mathbb{R}\}$, G/H is the set of all lines paralllel to the x-coordinate that can be identified with the (y, z)-plane, K/H is the set of all lines on (x, y)-plane parallel to the x-coordinate that can be identified with the y-coordinate, then $(G/H)/(K/H)$ can be identified with the the z-coordinate

Theorem 1.3.28 (the forth isomorphism theorem, the lattice isomorphism theorem)

Let N be a normal subgroup of G, then there is a one-to-one correspondence between the set of subgroups of G containing N and the set of subgroups of $\overline{G} = G/N$. Let A be a subgroup of G containing N, then $\overline{A} = A/I$ is the corresponding subgroup of $\overline{G} = G/N$. The bijection has the following properties

1. $A \leq B$ if and only if $\overline{A} \leq \overline{B}$
2. if $A \leq B$, then $|B : A| = |\overline{B} : \overline{A}|$
3. $\overline{\langle A, B\rangle} = \langle \overline{A}, \overline{B}\rangle$
4. $\overline{A \cap B} = \overline{A} \cap \overline{B}$
5. $A \trianglelefteq G$ if and only if $\overline{A} \trianglelefteq \overline{G}$

In the 3-dimensional Cartesian coordinates $G = \{(x, y, z) : x, y, z \in \mathbb{R}\}$, the x-coordinate $N = \{(x, 0, 0) : x \in \mathbb{R}\}$ is a normal subgroup of G. G/N is the collection of lines parallel to the x-coordinate N, that is isomorphic to the (y, z)-plane $\{(0, y, z) : y, z \in \mathbb{R}\}$

On one hand, the set of subgroups of G containing N consists of N, G, and all planes containing N. Each plane containing N corresponds to a nonzero point on the (y, z)-plane

On the other hand, the set of subgroups of G/N consists of $\{0\}$, the whole space, and all lines going through 0 on the (y, z)-plane

1.3.4 COMPOSITION SERIES AND THE HÖLDER PROGRAM

Proposition 1.3.29 (Cauchy Theorem for abelian groups)

If G is a finite abelian group and p is a prime dividing $|G|$, then G contains an element of order p

Definition 1.3.30 (Simple Group)

A group G is said to be simple if $|G| > 1$ and the only normal subgroups of G are 1 and G

Definition 1.3.31 (Composition Series)
A sequence of groups

$$1 = N_0 \leq N_1 \leq ... \leq N_k = G$$

is said to be a composition series if $N_{i-1} \trianglelefteq N_i$ and N_i/N_{i-1} is simple for all $1 \leq i \leq k$. Moreover, the quotient groups N_i/N_{i-1} are said to be the composition factors of G

Theorem 1.3.32 (Jordan-Hölder)
Let G be a nontrivial finite group. Then

1. G has a composition series
2. The composition factors in a composition series are unique. That is, if $1 \trianglelefteq N_0 \trianglelefteq ... \trianglelefteq N_r = G$ and $1 \trianglelefteq M_0 \trianglelefteq ... \trianglelefteq M_s = G$, then $r = s$ and there is a permutation π such that

   $$M_{\pi(i)}/M_{\pi(i)-1} \cong N_i/N_{i-1}$$

   for all $1 \leq i \leq r$

Theorem 1.3.33 (Part 1 of the Hölder Program)
There is a list consisting of 18 families of simple groups and 26 simple groups not belong to these families (the sporadic simple groups) such that every finite simple group is isomorphic to one of the groups in this list

Theorem 1.3.34 (Feit-Thompson)
If G is a simple group of odd order, then $G \cong Z_p$ for some prime p

Definition 1.3.35 (Solvable Group)
A group G is said to be solvable if there is a chain of subgroups

$$1 \trianglelefteq G_0 \trianglelefteq ... \trianglelefteq G_s = G$$

such that G_i/G_{i-1} is abelian for all $1 \leq i \leq s$

Theorem 1.3.36
The finite group G is solvable if and only for every divisor n of $|G|$ such that $(n, \frac{|G|}{n}) = 1$, G has a subgroup of order n

1.3.5 TRANSPOSITION AND THE ALTERNATING GROUP

Transpositions and Generation of S_n

Definition 1.3.37 (Transposition)
A 2-cycle is said to be a transposition

Proposition 1.3.38
Every element of S_n can be written as a product of transpositions

The Alternating Group

Definition 1.3.39 (Parity of Permutation)
For any $\sigma \in S_n$, define the polynomial Δ

$$\Delta = \prod_{1 \le i < j \le n} (x_i - x_j)$$

Let σ act on Δ by

$$\sigma(\Delta) = \prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)})$$

Define the sign of σ as

$$\epsilon(\sigma) = \begin{cases} +1 & \text{if } \sigma(\Delta) = +\Delta \\ -1 & \text{if } \sigma(\Delta) = -\Delta \end{cases}$$

σ is said to be an even permutation if $\epsilon(\sigma) = +1$, and odd permutation if $\epsilon(\sigma) = -1$

Proposition 1.3.40
The map $\epsilon : S_n \to \{-1, +1\}^\times$ is a homomorphism

Proposition 1.3.41
Transpositions are all odd permutations and ϵ is a surjective homomorphism

Definition 1.3.42 (Alternating Group)
The kernel of homomorphism ϵ is said to be the alternating group of degree n, denoted by A_n

Proposition 1.3.43
The permutation σ is odd if and only the number of cycles of even length in its cycle decomposition is odd

1.4 GROUP ACTIONS

1.4.1 GROUP ACTIONS AND PERMUTATION REPRESENTATIONS

Definition 1.4.1

Some definitions related to group actions

1. The set of elements in G that act trivially on A, namely $\{g \in G : \forall a \in A, g \cdot a = a\}$, is said to be the kernel of the action
2. For each $a \in A$, the set of elements in G that fix a, namely $G_a = \{g \in G : g \cdot a = a\}$, is said to be the stabilizer of a
3. An action is said to be faithful if its kernel is the identity

Proposition 1.4.2

Let group G act on a nonempty set A, there is a one-to-one correspondence between the actions of G on A and the homomorphisms from G into S_A

Definition 1.4.3 (Permutation Representation)

For any group G and nonempty set A, any homomorphism from G into S_A is said to be a permutation representation of G

Proposition 1.4.4 (Orbit-Stabilizer Theorem)

Let group G act on a nonempty set A. The relation defined by

$$a \sim b \text{ if and only if for some } g \in G,\ b = g \cdot a$$

is an equivalence relation. Furthermore, for each $a \in A$, let C_a be the equivalence class containing a. impose the group structure on C_a with $\star : C_a \times C_a \to C_a$ defined by

$$x \star y = (g_x g_y) \cdot a$$

where $x = g_x \cdot a$, $y = g_y \cdot a$. Then, the map $g \mapsto g \cdot a$ is a surjective homomorphism from G to C_a. Consequently, $|C_a| = |G/G_a|$ where G_a is the stabilizer of a

Definition 1.4.5 (Orbit)

Let group G act on a nonempty set A

1. The equivalence class $C_a = \{g \cdot a : g \in G\}$ is said to be the orbit of G containing a
2. The action of G on a is said to be transitive if there is only one orbit

Cycle Decompositions

1.4.2 GROUPS ACTING ON THEMSELVES BY LEFT MULTIPLICATION - CAYLEY THEOREM

Theorem 1.4.6

Let H be a subgroup of G and G act by left multiplication on the set A of left cosets of H, i.e. the action is defined by $g \cdot xH = gxH$. Let $\pi_H : G \to S_A$ be the associated permutation representation afforded by this action. Then

1. G acts transitively on A
2. The stabilizer in G of the point $1H \in A$ is the subgroup H
3. $\ker \pi_H = \bigcap_{x \in G} xHx^{-1}$ and it is the largest normal subgroup of G contained in H

Corollary 1.4.7 (Cayley Theorem)

Every group is isomorphic to a subgroup of some symmetric group. If $|G| = n$, then G is isomorphic to a subgroup of S_n

TODO - add yoneda lemma here

Corollary 1.4.8

If G is a finite group of order n and p is the smallest prime dividing $|G|$, then any subgroup of of index p is normal

1.4.3 GROUPS ACTING ON THEMSELVES BY CONJUGATION - THE CLASS EQUATION

Definition 1.4.9 (Conjugate, Conjugacy Class)

Two elements $a, b \in G$ are said to be conjugate in G if there exists $g \in G$ such that $b = gag^{-1}$, i.e. a, b in the same orbit of G acting on itself by conjugation. The orbits of G acting on itself by conjugation is said to be the conjugacy classes of G

Definition 1.4.10 (Conjugate)

Two subsets $S, T \subseteq G$ are said to be conjugate in G if there exists $g \in G$ such that $T = gSg^{-1}$, i.e. S, T in the same orbit of G acting on its subsets by conjugation

Proposition 1.4.11

The number of conjugates of a subset S in a group G is the index of the normalizer of S, $|G : N_G(S)|$, i.e. the stabilizer of G acting on its subsets by conjugation. In particular, the number of conjugates of an element s of G is the index of the centralizer of s, $|G : C_G(s)|$

Theorem 1.4.12 (The Class Equation)

Let G be a finite group and $g_1, g_2, ..., g_r$ be representatives of the distinct conjugacy classes of G not contained in the center $Z(G)$. Then

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

Each element $z \in Z(G)$ can be considered as a singleton conjugacy class.

Theorem 1.4.13

If p is a prime and P is a group of prime power order p^α for some $\alpha \geq 1$, then P has a nontrivial center $Z(P) \neq 1$

Corollary 1.4.14

If $|P| = p^2$ for some prime p, then P is abelian. More precisely, P is isomorphic to either Z_{p^2} or $Z_p \times Z_p$

Conjugacy in S_n

Proposition 1.4.15

Let $\sigma, \tau \in S_n$ and suppose σ has the cycle decomposition

$$(a_1 a_2 ... a_{k_1})(b_1 b_2 ... b_{k_2})...$$

Then $\tau\sigma\tau^{-1}$ has the cycle decomposition

$$(\tau(a_1)\tau(a_2)...\tau(a_{k_1}))(\tau(b_1)\tau(b_2)...\tau(b_{k_2}))...$$

Definition 1.4.16 (Cycle Type)

If $\sigma \in S_n$ is the product of disjoint cycles of length $n_1, n_2, ..., n_r$ with $n_1 \leq n_2 \leq ... \leq n_r$ (including 1-cycles) then the sequence $n_1, n_2, ..., n_r$ is said to be the cycle type of σ

Definition 1.4.17 (Partition of a Positive Integer)

Given $n \in \mathbb{N}$, a sequence of nondecreasing positive integers whose sum is n is said to be a partition of n

Proposition 1.4.18

Two elements of S_n are conjugate in S_n if and only if they have the same cycle type. The number of conjugacy classes of S_n is the number of partitions of n

Proposition 1.4.19

Any normal subgroup of G is a union of conjugacy classes of G

Theorem 1.4.20

A_5 is a simple group

Right Group Actions

1.4.4 AUTOMORPHISMS

Definition 1.4.21 (Automorphism)
An isomorphism from a group G onto itself is said to be an automorphism of G. The set of all automorphisms of G is denoted by $\mathrm{Aut}(G) \subseteq S_G$

Proposition 1.4.22
Let H be a normal subgroup of G. Then G acts by conjugation on H as automorphisms of H. For each $g \in G$, conjugation by g is an automorphism of H. The permutation representation afforded by this action is a homomorphism from G into $\mathrm{Aut}(H)$ with kernel $C_G(H)$. In particular, $G/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$

Corollary 1.4.23
If K is any subgroup of G and $g \in G$, then $K \cong gKg^{-1}$. Conjugate elements and conjugate subgroups have the same order.

Corollary 1.4.24
For any subgroup H of G, the quotient group $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$. In particular, $G/Z(G)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$

Definition 1.4.25 (Inner Automorphism)
Let G be a group and $g \in G$. Conjugation by g is said to be an inner automorphism of G and the subgroup of $\mathrm{Aut}(G)$ consisting of all inner automorphisms is denoted by $\mathrm{Inn}(G)$

Definition 1.4.26 (Characteristic)
A subgroup H of G is said to be characteristic in G, denoted by $H \operatorname{char} G$, if every automorphism of G maps H into itself, i.e. for all $\sigma \in \mathrm{Aut}(G)$, $\sigma(H) = H$

Proposition 1.4.27
Some results concerning characteristic subgroups

1. Characteristic subgroups are normal
2. if H is the unique subgroup of G of a given order, then H is characteristic in G
3. if $K \operatorname{char} H$ and $H \trianglelefteq G$, then $K \trianglelefteq G$

Proposition 1.4.28
The automorphism group of the cyclic group of order n is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$, an abelian group of order $\phi(n)$ where ϕ is the Euler function.

Proposition 1.4.29

Some results on automorphism groups

1. If p is an odd prime and $n \in \mathbb{N}$, then the automorphism group of the cyclic group of order p is cyclic of order $p-1$. More generally, the automorphism group of the cyclic group of order p^n is cyclic of order $p^{n-1}(p-1)$
2. For all $n \geq 3$, the automorphism group of the cyclic group of order 2^n is isomorphic to $Z_2 \times Z_{2^{n-2}}$, and in particular, is not cyclic but has a cyclic subgroup of index 2
3. Let p be prime and let V be an abelian group (written additively) with the property that $pv = 0$ for all $v \in V$. If $|V| = p^n$, then V is an n-dimensional vector space over the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, also called elementary abelian group of order p^n. The automorphisms of V are precisely the nonsingular linear transformations from V to itself, that is
$$\mathrm{Aut}(V) \cong GL(V) \cong GL_n(\mathbb{F}_p)$$
4. For all $n \neq 6$, we have $\mathrm{Aut}(S_n) = \mathrm{Inn}(S_n) \cong S_n$. For $n = 6$, we have $|\mathrm{Aut}(S_6) : \mathrm{Inn}(S_6)| = 2$
5. $\mathrm{Aut}(D_8) \cong D_8$ and $\mathrm{Aut}(Q_8) \cong S_4$

1.4.5 SYLOW THEOREM

Definition 1.4.30 (p-group, Sylow p-group)

Let G be a group and p be a prime

1. A (sub)group of order p^α for some $\alpha \geq 1$ is said to be p-(sub)group
2. If G is a group of order $p^\alpha m$ where $p \nmid m$, then a subgroup of order p^α is said to be a Sylow p-subgroup [a]
3. The set of Sylow p-subgroups of G is denoted by $\mathrm{Syl}_p(G)$, the number of Sylow p-subgroups of G is denoted by $n_p(G)$

[a] some kind of maximal p-subgroup

Theorem 1.4.31 (Sylow Theorem)

Let G be a group of order $p^\alpha m$, where p is a prime not dividing m

1. Sylow p-subgroups of G exists
2. If P is a Sylow p-subgroup of G and Q is any p-subgroup of G, then there exists $g \in G$ such that $Q \leq gPg^{-1}$
3. The number of Sylow p-subgroups of G is of the form $1 + kp$, i.e.
$$n_p = 1 \pmod{p}$$
Further, n_p is the index in G of the normalizer $N_G(P)$ for any Sylow p-subgroup P. Hence, $n_p \mid m$

Lemma 1.4.32

Let $P \in \mathrm{Syl}_p(G)$. If Q is any p-subgroup of G, then $Q \cap N_G(P) = Q \cap P$

Corollary 1.4.33

Let P be a Sylow p-subgroup of G. Then the following are equivalent:

1. P is the unique Sylow p-subgroup of G
2. P is normal in G
3. P is characteristic in G
4. All subgroups generated by elements of p-power order are p-groups. That is, if X is any subset of G such that $|x|$ is a power of p for all $x \in X$, then $\langle X \rangle$ is a p-group.

Applications of Sylow Theorem

1.4.6 THE SIMPLICITY OF A_n

1.5 DIRECT AND SEMIDIRECT PRODUCTS AND ABELIAN GROUPS

1.5.1 DIRECT PRODUCTS

Definition 1.5.1 (Direct Product)

Let $\mathcal{G} = \{G_i : i \in I\}$ be a family of groups where I is an index set. The direct product of $\mathcal{G}$, denoted by $G = \prod_{i \in I} G_i$ (or $G_1 \times G_2 \times ... \times G_n$ in the finite case) is group where each element $g : I \to \bigcup_{i \in I} G_i$ such that $g(i) \in G_i$. The product is defined by $c = ab$

$$c(i) = a(i)b(i)$$

Proposition 1.5.2

Let $G_1, G_2, ..., G_n$ be groups, their direct product is a group of order $|G_1||G_2|...|G_n|$

Proposition 1.5.3

Let $G_1, G_2, ..., G_n$ be groups and $G = G_1 \times G_2 \times ... \times G_n$

1. For each fixed i, the set of elements $g \in G$ such that $g(j) = 1_{G_j}$ for all $j \neq i$ is a subgroup, namely the coordinate axis subgroup or the i-th component of G, and it is isomorphic to G_i,

$$G_i \cong \{g \in G : \forall j \neq i, g(j) = 1_{G_j}\} = \{(1, ..., 1, g_i, 1, ..., 1) : g_i \in G_i\}$$

   If we identify G_i with this group, then $G_i \trianglelefteq G$ and

$$G/G_i \cong G_1 \times ... \times G_{i-1} \times G_{i+1} \times ... \times G_n$$

2. For each fixed i, define $\pi_i : G \to G_i$ by

$$\pi_i(g) = g(i)$$

   Then π_i is a surjective homomorphism with

$$\ker \pi_i = \{g \in G : g(i) = 1_{G_i}\} \cong G/G_i$$

3. Under the identification of G_i, if $x \in G_i$ and $y \in G_j$ for some $i \neq j$, then $xy = yx$

1.5.2 THE FUNDAMENTAL THEOREM OF FINITELY GENERATED ABELIAN GROUPS

Definition 1.5.4 (Finitely Generated Group)

A group G is said to be finitely generated if there is a finite subset A of G such that $G = \langle A \rangle$. For each $r \in \{0, 1, ...\}$, let $\mathbb{Z}^r = \prod_{i=1}^{r} \mathbb{Z}$ with $\mathbb{Z}^0 = 1$, then the group $\mathbb{Z}^r$ is said to be free abelian group of rank r

Theorem 1.5.5 (Fundamental Theorem of Finitely Generated Abelian Groups)

If G is a finitely generated abelian group, then

$$G \cong \mathbb{Z}^r \times Z_{n_1} \times ... \times \mathbb{Z}_{n_s}$$

for some integers $r, n_1, ..., n_s$ satisfying the following conditions:

1. $r \geq 0$ and $n_j \geq 2$ for all j
2. $n_{i+1} \mid n_i$ for $1 \geq i \geq s - 1$

The integer r is said to be the free rank or Betti number of G and the integers $n_1, n_2, ..., n_s$ are said to be the invariant factors of G. The decomposition is unique and said to be the invariant factor decomposition of G.

Corollary 1.5.6

If n is the product of distinct primes, then up to isomorphism the only abelian group of order n is the cyclic group of order n, Z_n

Theorem 1.5.7

Let G be an abelian group of order $n > 1$ and the unique factorization of n into distinct prime powers be

$$n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$$

Then

1. $G \cong A_1 \times A_2 \times ... \times A_k$ where $|A_i| = p_i^{\alpha_i}$
2. For each $A \in \{A_1, A_2, ..., A_k\}$ with $|A| = p^{\alpha}$,

$$A \cong Z_{p^{\beta_1}} \times Z_{p^{\beta_2}} \times ... \times Z_{p^{\beta_k}}$$

with $\beta_1 \geq \beta_2 \geq ... \geq \beta_t \geq 1$ and $\alpha = \beta_1 + \beta_2 + ... + \beta_t$

The integers p^{β_j} are said to be the elementary divisors of G. The decomposition is unique and said to be the elementary divisor decomposition of G

Proposition 1.5.8

Let $m, n \in \mathbb{N}$,

1. $Z_m \times Z_n \cong Z_{mn}$ if and only if $(m, n) = 1$
2. If $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$, then $Z_n \cong Z_{p_1^{\alpha_1}} \times Z_{p_2^{\alpha_2}} \times ... \times Z_{p_k^{\alpha_k}}$

Obtaining Elementary Divisors from Invariant Factors

Obtaining Elementary Divisors from any Cyclic Decomposition

Obtaining Invariant Factors from Elementary Divisors

1.5.3 TABLE OF GROUPS OF SMALL ORDER

1.5.4 RECOGNIZING DIRECT PRODUCTS

Definition 1.5.9 (Commutator, Commutator Subgroup)

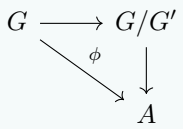
Let G be a group, $x, y \in G$, and A, B be nonempty subsets of G

1. $[x, y] = x^{-1} y^{-1} xy$ is said to be the commutator of x and y
2. $[A, B] = \langle [a, b] : a \in A, b \in B \rangle$ denotes the group generated by commutators of elements from A and B
3. $G' = [G, G] = \langle [x, y] : x, y \in G \rangle$ is said to be the commutator subgroup of G

Proposition 1.5.10

Let G be a group, $x, y \in G$ and $H \leq G$. Then

1. $xy = yx[x, y]$
2. $H \trianglelefteq G$ if and only if $[H, G] \leq H$
3. $\sigma[x, y] = [\sigma(x), \sigma(y)]$ for any automorphism σ on G, $G' \operatorname{char} G$, and G/G' is abelian
4. G/G' is the largest abelian quotient group of G. That is, if $H \trianglelefteq G$ and G/H is abelian, then $G' \leq H$. Conversely, if $G' \leq H$, then $H \trianglelefteq G$ and G/H is abelian
5. If $\phi : G \to A$ is any homomorphism from G into an abelian group A, then ϕ factors through G', i.e. $G' \leq \ker \phi$ and the following diagram commutes



Proposition 1.5.11

Let H, K be subgroups of G. The number of distinct ways of writing each element of HK in the form hk for some $h \in H, k \in K$ is $H \cap K$. In particular, if $H \cap K = 1$, then each element of HK can be written uniquely as a product hk for some $h \in H$ and $k \in K$, i.e. there is a one-to-one correspondence between HK and $H \times K$

Theorem 1.5.12 (Recognition Theorem)

Suppose G is a group with subgroups H and K such that

1. H and K are normal in G
2. $H \cap K = 1$

Then, $HK \cong H \times K$

Definition 1.5.13 (Interval Direct Product, External Direct Product)

If H, K are normal subgroups of G with $H \cap K = 1$, then HK is said to be the internal direct product and H and K and $H \times K$ are said to be the (external) direct product of H and K.

1.5.5 SEMIDIRECT PRODUCTS

Definition 1.5.14 (Semidirect Product)

Let H, K be groups and ϕ be a homomorphism from K into $\mathrm{Aut}(H)$, i.e. there is an associated action of K on H. Let $\cdot$ denote that (left) action of K on H determined by ϕ. Let G be the set of ordered pairs (h, k) with $h \in H, k \in K$ and define the multiplication on G as

$$(h_1, k_1)(h_2, k_2) = (h_1 k_1 \cdot h_2, k_1 k_2)$$

Then, $\{(h, 1) : h \in H\}$ and $\{(1, k) : k \in K\}$ are subgroups of G and isomorphic to H and K respectively. Identify H, K with their isomorphic copies in G.

1. $H \trianglelefteq G$
2. $H \cap K = 1$
3. For all $h \in H, k \in K$, $khk^{-1} = k \cdot h = \phi(k)(h)$
4. $G = HK$ and $|G| = |H||K|$

G is said to be the semidirect product of H and K with respective to ϕ and denoted by $G = H \rtimes_\phi K$ (or $G = H \rtimes K$ if ϕ is clear from the context)

Proposition 1.5.15

Let H, K be groups and $\phi : K \to \mathrm{Aut}(H)$ be a homomorphism. Then, the following are equivalent

1. The identity map between $H \rtimes K$ and $H \times K$ is an isomorphism
2. ϕ is the trivial homomorphism from K to $\mathrm{Aut}(H)$
3. $K \trianglelefteq K \rtimes K$

Theorem 1.5.16

Let H, K be subgroups of G such that

1. $H \trianglelefteq G$
2. $H \cap K = 1$

Let $\phi : K \to \mathrm{Aut}(H)$ be the homomorphism defined by the mapping from $k \in K$ to the automorphisms of left conjugation by k on H, i.e. $\phi(k)(h) = khk^{-1}$. Then $HK \cong H \rtimes K$. In particular, if $G = HK$ with $H \trianglelefteq G$ and $H \cap K = 1$, then G is the semidirect product of H and K

Definition 1.5.17 (Complement)

Let H be a subgroup of G. A subgroup K of G is said to be a complement of H in G if $G = HK$ and $H \cap G = 1$

1.6 FURTHER TOPICS IN GROUP THEORY

TODO

Chapter 2

RING THEORY

2.1 INTRODUCTION TO RINGS

2.1.1 BASIC DEFINITIONS AND EXAMPLES

Definition 2.1.1 (ring)
A non-unital R is a set together with two binary operations $+$ and $\times$ (called addition and multiplication) satisfying the following axioms

1. $(R, +)$ is an abelian group
2. $\times$ is associative, that is
$$(ab)c = a(bc)$$
for all $a, b, c \in R$
3. the distributive laws hold in R, that is, for all $a, b, c \in R$,
$$(a + b)c = ac + bc \text{ and } a(b + c) = ab + ac$$

If $\times$ is commutative, then R is called a commutative ring. If there is an element $1 \in R$ such that $1 \neq 0$ and
$$1a = a1 = a$$
for all $a \in R$, then R is called a unital ring and 1 is called multiplicative identity.

Remark 2.1.2
From now on, whenever we refer to a ring R, R is a non-unital ring.

Definition 2.1.3 (division ring, field)
A unital ring R is called a division ring if every nonzero element in R has a multiplicative inverse. A commutative division ring is called a field.

Proposition 2.1.4

Let R be a ring, then

1. $0a = a0 = 0$ for all $a \in R$
2. $(-a)b = a(-b) = -(ab)$ for all $a, b \in R$
3. $(-a)(-b) = ab$ for all $a, b \in R$
4. if R is unital, then the multiplicative identity is unique and $(-1)a = -a$

Definition 2.1.5 (zero divisor)

Let R be a ring, then

1. A nonzero element $a \in R$ is called a zero divisor if there is a nonzero element $b \in R$ such that either $ab = 0$ or $ba = 0$
2. If R is unital, an element $u \in R$ is called unit if there is an element $v \in R$ such that $uv = vu = 1$. The set of units is denoted by $R^\times$. With respect to muliplication, $R^\times$ is a group called multiplicative group of units

Definition 2.1.6 (integral domain)

A commutative unital ring is called an integral domain if it has no zero divisors.

Proposition 2.1.7 (cancellation property)

Let R be a ring and $a, b, c \in R$. If a is not a zero divisor, then

$$ab = ac \implies a(b - c) = 0 \implies a = 0 \text{ or } b = c$$

Corollary 2.1.8

Any finite integral domain is a field [a]

[a] seems not trivial https://math.stackexchange.com/a/62551/700122

Definition 2.1.9 (subring)

A subring of the ring R is a subgroup of R that is closed under multiplication. That is, a subset of R that is also a ring.

2.1.2 EXAMPLES: POLYNOMIAL RINGS, MATRIX RINGS, AND GROUP RINGS

POLYNOMIAL RINGS

there is a dedicated section this polynomial rings

MATRIX RINGS

Proposition 2.1.10 (matrix ring)
Let R be a ring and $n \in \mathbb{N}$, the set of all $n \times n$ matrices $M_{n\times n}[R]$ with coefficients in R is a ring. If $n \geq 2$, then $M_{n\times n}[R]$ is not a commutative ring.

TODO - there are more things in here

GROUP RINGS

Definition 2.1.11 (group ring)
Let R be a commutative unital ring and $G = \{g_1, g_2, ..., g_n\}$ be a finite group. Define group ring RG of G with coefficients in R be the set of all formal sums

$$a_1 g_1 + a_2 g_2 + ... + a_n g_n$$

for $a_i \in R$ with addition defined by

$$\left(\sum_{i=1}^{n} a_i g_i\right) + \left(\sum_{i=1}^{n} b_i g_i\right) = \sum_{i=1}^{n} (a_i + b_i) g_i$$

and multiplcation defined by

$$\left(\sum_{i=1}^{n} a_i g_i\right) \times \left(\sum_{i=1}^{n} b_i g_i\right) = \sum_{k=1}^{n} \left(\sum_{i,j:g_i g_j = g_k} a_i b_j\right) g_k$$

Proposition 2.1.12
RG is commutative if and only if G is commutative

2.1.3 RING HOMOMORPHSIMS AND QUOTIENT RINGS

Definition 2.1.13 (ring homomorphism)
Let R, S be rings

1. A ring homomorphism is a map $\phi : R \to S$ such that
   (a) ϕ is a group homomorphism on additive groups
   (b) $\phi(ab) = \phi(a)\phi(b)$, if R is unital, then $\phi(1_R) = 1_S$
2. The kernel of ϕ, denoted by $\ker \phi$, is the set of elements of R that is mapped to 0 by ϕ.
3. A bijective ring homomorphism is called an isomorphism

Proposition 2.1.14

Let R, S be rings and $\phi : R \to S$ be a ring homorphism

1. The image of ϕ is a subring of S
2. The kernel of ϕ is a subring of R. Moreover, if $r \in R$, $\alpha \in \ker \phi$, then $r\alpha \in \ker \phi$ and $\alpha r \in \ker \phi$, that is, $\ker phi$ is an (two-sided) ideal of R

Definition 2.1.15 (ideal)

Let R be a ring, I be a subring of R, and $r \in R$

1. $rI = \{ra : a \in R\}$ and $Ir = \{ar : a \in R\}$
2. A subring I of R is a left ideal of R if $rI \subseteq I$, that is, I is closed under left multiplication by elements from R
3. A subring I of R is a right ideal of R if $Ir \subseteq I$, that is, I is closed under right multiplication by elements from R
4. A subring R is called an (two-sided) ideal if it is both a left ideal and right ideal

$2\mathbb{Z}$, $3\mathbb{Z}$, $4\mathbb{Z}$, $5\mathbb{Z}$, $6\mathbb{Z}$ *are ideals of* $\mathbb{Z}$

Proposition 2.1.16

Let R be a ring and I be an ideal of R, then the additive quotient group R/I is a ring under the binary operations

$$(r + I) + (s + I) = (r + s) + I \text{ and } (r + I) \times (s + I) = (rs) + I$$

for all $r, s \in R$. Conversely, if any subgroup I of R having the above operations well-defined then I is an ideal of R.

Definition 2.1.17 (quotient ring)

When I is an ideal of R, the ring R/I is called quotient ring of R by I

Theorem 2.1.18 (the first isomorphism theorem for rings)

If $\phi : R \to S$ is a homomorphism of rings, then the kernel of ϕ is an ideal of R, the image of ϕ is a subring of S and

$$R/\ker \phi \cong \operatorname{im} \phi$$

If I is any ideal of R, then the map

$$R \to R/I$$
$$r \mapsto r + I$$

is a surjective ring homomorphism with kernel I (this homomorphism is called the natural projection of R onto R/I). Thus, every ideal is the kernel of a ring homomorphism and vice versa.

Theorem 2.1.19 (other isomorphism theorems for rings)

Let R be a ring

1. (the second isomorphism theorem) Let A be a subring and B be an ideal of R, then
$$\frac{A+B}{B} \cong \frac{A}{A \cap B}$$
where subrings being ideals as necessary
2. (the third isomorphism theorem) Let I, J be ideals of R with $I \subseteq J$, then
$$\frac{R/I}{J/I} = \frac{R}{J}$$
where subrings being ideals as necessary
3. (the forth isomorphism theorem, the lattice isomorphism theorem) Let I be an ideal of R. Then there is a one-to-one correspondence between the set of subrings of R containing I and the set of subrings of R/I. Let A be a subring of R containing I, then the corresponding subring of R/I is $\overline{A} = A/I$. Moreover, A is an ideal if and only if $\overline{A}$ is an ideal.

Definition 2.1.20 (sum, product)

Let I, J be ideals of R

1. Define the sum of I and J by
$$I + J = \{a + b : a \in I, b \in J\}$$
2. Define the product of I and J by
$$IJ = \langle ab : a \in I, b \in J \rangle$$
That is, the additive group generated by $\{ab : a \in I, j \in J\}$
3. For any $n \geq 1$, define the n-th power of I by $I^n = II^{n-1}$ and $I^1 = I$

2.1.4 PROPERTIES OF IDEALS

Remark 2.1.21

Through out this section, let R be a nontrivial unital ring.

Definition 2.1.22 (ideal generated by a set, principal ideal, finitely generated ideal)
Let A be any subset of R

1. Let (A) be the smallest ideal of R containing A, that is called the ideal generated by A
2. $$RA = \langle ra : r \in R, a \in A \rangle$$
$$AR = \langle ar : r \in R, a \in A \rangle$$
3. An ideal generated by a single element is called a principal ideal
4. An ideal generated by a finite set is called a finitely generated ideal.

(A) is the collection of all finite linear combinations of elements in A with coefficients in R
as the intersection of arbitrary number of ideals is an ideal, the smallest ideals containing A is defined as the intersection of all ideals containing A

Proposition 2.1.23
Let I be an ideal of R

1. $I = R$ if and only if I contains a unit
2. If R is commutative, then R is a field if and only if its only ideals are 0 and R

Corollary 2.1.24
If R is a field then any nonzero ring homomorphism from R into another ring is an injection.

Definition 2.1.25 (maximal ideal)
An ideal M in a ring S is called a maximal ideal if $M \neq S$ and the only ideals containing M are M and S
$2\mathbb{Z} \supset 6\mathbb{Z}$, then $6\mathbb{Z}$ is not maximal in $\mathbb{Z}$. $2\mathbb{Z}$ is

Proposition 2.1.26
In an unital ring, every proper ideal is contained in a maximal ideal. *Zorn lemma argument*

Proposition 2.1.27
If R is commutative, the ideal M in R is maximal if and only if the quotient ring R/M is a field.

Definition 2.1.28 (prime ideal)
If R is commutative, an ideal P is called prime ideal if $P \neq R$ and if $ab \in P$ for $a, b \in R$, then at least one of a and b is an element of P.
p prime, $p\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$ and these are the only prime ideals of $\mathbb{Z}$

Proposition 2.1.29

If R is commutative, then P is a prime ideal if and only if the quotient ring R/P is an integral domain.

Corollary 2.1.30

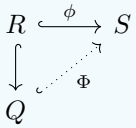
If R is commutative, then every maximal ideal is prime.

2.1.5 RING OF FRACTIONS

Theorem 2.1.31 (ring of fractions)

Let R be a commutative ring and D by any nonempty subset of R that does not contain 0, does not contain any zero divisors, and closed under multiplication. Then, there is a commutative unital ring Q such that Q contains R as a subring and every element of D is a unit in Q. The ring has the following additional properties

1. every element of Q is of the form rd^{-1} for some $r \in R$ and $d \in D$. In particular, if $D = R - \{0\}$, then Q is a field.
2. (uniqueness of Q) the ring Q is the smallest ring containing R in which all elements of D become units, in the following sense. Let S be any commutative unital ring, let $\phi : R \to S$ be any injective ring homomorphism such that $\phi(d)$ is a unit in S for every $d \in D$. Then there is an injective homomorphism $\Phi : Q \to S$ such that $\Phi|_R = \phi$



Construction of Q: Let $\mathcal{F} = R \times D = \{(r, d) : r \in R, d \in D\}$, define an equivalence relation of $\mathcal{F}$ by

$$(r, d) \sim (s, e) \text{ if and only if } re = sd$$

Denote the equivalence class of (r, d) by

$$[(r, d)] = \frac{r}{d} = \{(a, b) \in R \times D : rb = ad\}$$

Addition and multiplication are defined by

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

□

Definition 2.1.32 (ring of fractions, field of fractions, quotient field)

The ring Q is called the ring of frations of D with respect to R and denoted by $D^{-1}R$. If R is an integral domain (R has no zero divisors), $D = R - \{0\}$, then Q is a field and called field of fractions or quotient field of R

Corollary 2.1.33
Let R be an integral domain and Q be the field of fractions. If any field F containing a subring R' isomorphic to R and the subfield of F generated by R' is isomorphic to Q

2.1.6 THE CHINESE REMAINDER THEOREM

Remark 2.1.34
In this section, we assume that all rings are commutative unital

Definition 2.1.35 (comaximal)
The ideals A and B of a ring R is called comaximal if $A + B = R$

Theorem 2.1.36 (chinese remainder theorem)
Let $A_1, A_2, ..., A_k$ be ideals in R. The map

$$R \to R/A_1 \times R/A_2 \times ... \times R/A_k$$
$$r \mapsto (r + A_1, r + A_2, ..., r + A_k)$$

is a ring homomorphism with kernel $A_1 \cap A_2 \cap ... \cap A_k$. For each $i, j \in \{1, 2, ..., k\}$ with $i \neq j$ the ideals A_i and A_j are comaximal, then this map is surjective and

$$A_1 \cap A_2 \cap ... \cap A_k = A_1 A_2 ... A_k$$

so,

$$R/(A_1 A_2 ... A_k) = R/(A_1 \cap A_2 \cap ... \cap A_k) \cong R/A_1 \times R/A_2 \times ... \times R/A_k$$

Corollary 2.1.37
Let m, n be relatively prime $(m, n) = 1$, then

$$\mathbb{Z}/mn\mathbb{Z} \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$$

Moreover, the multiplicative groups of units are isomorphic

$$(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$$

2.2 EUCLIDEAN DOMAINS, PRINCIPAL IDEAL DOMAINS, UNIQUE FACTORIZATION DOMAINS

Remark 2.2.1
All rings in this section are commutative

2.2.1 EUCLIDEAN DOMAINS

Definition 2.2.2 (norm, positive norm)
Any function $N : R \to \mathbb{N}_0$ with $N(0) = 0$ on the integral domain R (no zero divisor) is called norm. If $N(a) > 0$ for all $a \neq 0$, then N is called a positive norm.

Definition 2.2.3 (Euclidean domain, division algorithm)
The integral domain R is called Euclidean domain (or posses a division algorithm) if there is a norm $N : R \to \mathbb{N}_0$ such that for any two elements $a, b \in R$ with $b \neq 0$, there exists two elements $q, r \in R$ such that

$$a = qb + r \text{ with } r = 0 \text{ or } N(r) < N(b)$$

The element q is called quotient and the element r is called remainder.

Remark 2.2.4 (Euclidean algorithm)
The existence of a division algorithm on an integral domain enables a Euclidean algorithm for two elements $a, b \in R$ as follows:

$$\begin{aligned} a &= q_0 b + r_0 \\ b &= q_1 r_0 + r_1 \\ r_0 &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\dots \\ r_{n-2} &= q_n r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} r_n \end{aligned}$$

with $N(b) > N(r_0) > N(r_1) > ... > N(r_n)$. And the algorithm terminates in a finite number of steps n

Proposition 2.2.5
Every ideal in an Euclidean domain is principal, that is, if I is a nonzero ideal in an Euclidean domain R then $I = (d)$ where d is a nonzero element of I with minimum norm.

Definition 2.2.6 (multiple, divide, divisor, greatest common divisor)
Let R be a commutative ring and $a, b \in R$ with $b \neq 0$

1. a is called a multiple of b if there exists an element $x \in R$ such that $a = xb$. In this case, b is said to divide a or b is a divisor of a, denoted by $b|a$
2. A greatest common divisor of a, b is a nonzero element d such that
   (a) $d|a$ and $d|b$
   (b) if $d'|a$ and $d'|b$ then, $d'|d$

   A greatest common divisor of a, b is denoted by $\gcd(a, b)$ or (a, b).

   note, $b|a \iff a \in (b) \iff (a) \subseteq (b)$. Hence, if d is a divisor of a and b, then (d) contains both (a) and (b) hence must contain the ideal (a, b)

Proposition 2.2.7
If a, b are nonzero elements of a commutative ring R such that the ideal (a, b) generated by a and b is a principal ideal d, then d is a greatest commondivisor of a and b
$(a, b) = (d) \iff d = \gcd(a, b)$

Proposition 2.2.8
Let R be in integral domain, if two elements $d, d' \in R$ generate the same principal ideal, that is, $(d) = (d')$ then $d' = ud$ for some unit u. In particular, if both d and d' are greatest common divisor of a and b, then d and d' differ by a unit.
the set of units in $R[x]$ is $R^\times$

Theorem 2.2.9
Let R be an Euclidean domain and let $a, b \in R$ be nonzero elements. Let $d = r_n$ be the last nonzero remainder in the Euclidean algorithm for a and b. Then

1. d is the greatest common divisor of a and b
2. the principal ideal (d) is the ideal generated by a and b. In particular, d can be written as an R-linear combination of a and b, that is, there exist $x, y \in R$ such that

$$d = xa + yb$$

Definition 2.2.10 (universal side divisor)
Let R be a ring, then $\tilde{R} = R^\times \cup \{0\}$ is the collection of units together with zero. An element $u \in R - \tilde{R}$ is called universal side divisor if there is a type of "division algorithm" for u, that is, every $x \in R$ can be written as $x = qu + z$ where z is either zero or a unit.

Proposition 2.2.11

Let R be an integral domain that is not a field, if R is an Euclidean domain then there are universal side divisors in R

2.2.2 PRINCIPAL IDEAL DOMAINS (PID)

Definition 2.2.12 (principal ideal domain)

A principal ideal domain (PID) is an integral domain in which every ideal is principal

Proposition 2.2.13

Let R be a PID and a, b be nonzero elements of R. Let d be a generator for the principal ideal generated by a and b. Then

1. d is a greatest common divisor of a and b
2. d can be written as an R-linear combination of a and b, that is, there exist $x, y \in R$ such that

$$d = xa + yb$$

3. d is unique up to multiplication by a unit of R

Proposition 2.2.14

Every nonzero prime ideal in a PID is a maximal ideal

Definition 2.2.15 (Dedekind-Hasse norm)

A positive norm N is a Dedekind-Hasse norm if for every nonzero $a, b \in R$, either $a \in (b)$ or there is a nonzero element in (a, b) of norm strictly smaller than the norm of b

Proposition 2.2.16

The integral domain R is a PID if and only if R has a Dedekind-Hasse norm

Corollary 2.2.17

The norm in Euclidean domain is a Dedekind-Hasse norm, hence, every Euclidean domain is a PID

2.2.3 UNIQUE FACTORIZATION DOMAINS (UFD)

Definition 2.2.18 (irreducible, prime, associate)
Let R be an integral domain

1. If $r \in R$ is nonzero and not a unit, then r is called irreducible if whenever $r = ab$ for $a, b \in R$, then at least one of a or b must be a unit. Otherwise, r is called reducible. That is, every element in R can be written as a product of irreducble elements
2. The nonzero element $p \in R$ is called prime in R if the ideal (p) is a prime ideal. That is, if p divides ab, then p must divide at least one of a or b
3. Two elements a and b differing by a unit ($a = ub$ for some unit u) is called associate.

Proposition 2.2.19
In an integral domain, a prime element is irreducible

Proposition 2.2.20
In a PID, a nonzero element is a prime if and only if it is irreducible.

Proposition 2.2.21
In a UFD, a nonzero element is a prime if and only if it is irreducible

Proposition 2.2.22
Let R be a UFD, a, b be two nonzero elements of R, and

$$a = up_1^{e_1}p_2^{e_2}...p_n^{e_n} \text{ and } b = vp_1^{f_1}p_2^{f_2}...p_n^{f_n}$$

are prime factorizations for a and b where u, v are units and the primes $p_1, p_2, ..., p_n$ are distinct and the exponents $e_1, e_2, ..., e_n$, $f_1, f_2, ..., f_n$ are nonnegative. Then

$$d = p_1^{\min\{e_1,f_1\}}p_2^{\min\{e_2,f_2\}}...p_n^{\min\{e_n,f_n\}}$$

is a greatest common divisor of a and b

Theorem 2.2.23
Every PID is a UFD

Corollary 2.2.24 (fundamental theorem of arithmetic)
The integers $\mathbb{Z}$ is a UFD

Corollary 2.2.25
Let R is a PID, then there eixsts a multiplicative ($N(ab) = N(a)N(b)$) Dedekind-Hasse norm on R

Factorization in the Gaussian Integers

number theory shit, skip for now

2.3 POLYNOMIAL RINGS

Remark 2.3.1
In this section, all rings are commutative unital

Definition 2.3.2 (polynomial over a commutative ring)
Let R be a commutative unital ring, a function $f : \mathbb{N} \to R$ such that $\operatorname{im} f$ is a finite set is called a polynomial over R, given an indeterminate x, f is denoted by the formal sum

$$a_0 + a_1 x + a_2 x^2 + ...a_n x^n$$

where $a_i = f(i) \neq 0$ and $f(m) = 0$ for all $m > n$. a_i is called the i-coefficient, n is called degree, a_n is called leading coefficient, if $a_n = 0$, the polynomial is called monic. The set of all polynomials in the variable x over R is denoted by $R[x]$. *TODO: definition of addition and multiplication on $R[x]$*

Proposition 2.3.3
$R[x]$ is a ring *moreover, it is a graded-ring*

Proposition 2.3.4
Let R be an integral domain

1. $\deg p(x)q(x) = \deg p(x) + \deg q(x)$ if $p(x)$ and $q(x)$ are nonzero
2. the set of units of $R[x]$ is the set of units of R, that is, $R[x]^\times = R^\times$
3. $R[x]$ is an integral domain.

Proposition 2.3.5
Let I be an ideal of the ring R and let $(I) = I[x]$ denote the ideal in $R[x]$ generated by I, then

$$R[x]/(I) \cong (R/I)[x]$$

In particular, if I is a prime ideal of R, then (I) is a prime ideal of $R[x]$

Definition 2.3.6 (polynomial ring of multivariate over a commutative ring)
The polynomial ring in the variable $x_1, x_2, ..., x_n$ with coefficients in R denoted by $R[x_1, x_2, ..., x_n]$ is defined by

$$R[x_1, x_2, ..., x_n] = R[x_1, x_2, ..., x_{n-1}][x_n]$$

2.3.1 POLYNOMIAL RINGS OVER FIELDS I

Theorem 2.3.7 (polynomial ring over field is an Euclidean domain)
Let F be a field, the polynomial ring $F[x]$ is an Euclidean domain. That is, the norm on $F[x]$ is the degree of a polynomial, if $a(x), b(x) \in F[x]$ with $b(x)$ nonzero, then there are unique $q(x), r(x) \in F[x]$ such that

$$a(x) = q(x)b(x) + r(x) \text{ with } r(x) = 0 \text{ or } \deg r(x) < \deg b(x)$$

Corollary 2.3.8
If F is a field, then $F[x]$ is a PID and UFD

2.3.2 POLYNOMIAL RINGS THAT ARE UNIQUE FACTORIZATION DOMAINS

Proposition 2.3.9 (Gauss lemma)
Let R be a UFD with field of fractions F and let $p(x) \in R[x]$. If $p(x)$ is reducible in $F[x]$ then $p(x)$ is reducbile in $R[x]$

Proof. Let $p(x) = a(x)b(x)$ with $a(x), b(x) \in F[x]$. $a(x), b(x)$ are polynomials with coefficients in F which are fractions of elements in R. Let d be the common denominators of all these coefficients, then $dp(x) = a'(x)b'(x)$ for $a'(x), b'(x) \in R[x]$. *TODO - continue* □

Corollary 2.3.10
Let R be a UFD, F be its field of fractions, and $p(x) \in R[x]$. If the greatest common divisor of coefficients of $p(x)$ is 1, then $p(x)$ is irreducible in $R[x]$ if and only if it is irreducible in $F[x]$. In particular, if $p(x)$ is a monic polynomial that is irreducible in $R[x]$, then $p(x)$ is irreducible in $F[x]$

Theorem 2.3.11
R is a UFD if and only if $R[x]$ is a UFD

2.3.3 IRREDUCIBILITY CRITERIA

Proposition 2.3.12
Let F be a field and let $p(x) \in F[x]$, then $p(x)$ has a factor of degree one if and only if $p(x)$ has a root in F, that is, there is an $\alpha \in F$ such that $p(\alpha) = 0$

Proposition 2.3.13
A polynomial of degree two or three over a field F is reducible if and only if it has a root in F

Proposition 2.3.14

Let $p(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ be a polynomial of degree n with integer coefficients. If $r, s \in \mathbb{Z}$ are relatively prime integers and $r/s \in \mathbb{Q}$ is a root of $p(x)$, the r divides the constant term and s divides the leading coefficient of $p(x)$, that is, $r|a_0$ and $s|a_n$. In particular, if $p(x)$ is monic and $p(d) \neq 0$ for all integers d dividing the constant term of $p(x)$ then $p(x)$ has no root in $\mathbb{Q}$

there is a version in my secondary school books when $R = \mathbb{Z}$, $F = \mathbb{Q}$

Proposition 2.3.15

Let I be a proper ideal in the integral domain R and let $p(x)$ be a nonconstant monic polynomial in $R[x]$. If the image of $p(x)$ under the map induced by natural projection $R \to R/I$ in $(R/I)[x]$ cannot be factored in $(R/I)[x]$ into two polynomials of smaller degree, then $p(x)$ is irreducible in $R[x]$

polynomial of integers coefficients is irreducible if it is irreducible in $\mod p$

Proposition 2.3.16 (Eisenstein Criterion)

Let P be a prime ideal of integral domain R and let $f(x) = x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ be a polynomial $R[x]$ (here $n > 1$). Suppose $a_{n-1}, ..., a_1, a_0$ are all elements of P and suppose a_0 is not an element of P^2. Then, $f(x)$ is irreducible in $R[x]$

Proposition 2.3.17 (Eisenstein Criterion for integer polynomials)

Let p be a prime for $\mathbb{Z}$ and let $f(x) = x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 \in \mathbb{Z}[x], n \geq 1$. Suppose p divides a_i for all $i \in \{0, 1, ..., n-1\}$ but that p^2 does not divide a_0. Then $f(x)$ is irreducible in both $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$

2.3.4 POLYNOMIAL RINGS OVER FIELD II

Proposition 2.3.18

The maximal ideals in $F[x]$ are the ideals $(f(x))$ generated by irreducible polynomials $f(x)$. In particular, $F[x]/(f(x))$ is a field if and only if $f(x)$ is irreducible.

Proposition 2.3.19

Let $g(x)$ be a nonconstant element $F[x]$ and let

$$g(x) = f_1(x)^{n_1} f_2(x)^{n_2} ... f_k(x)^{n_k}$$

be its factorization into irreducibles where $f_i(x)$ are distinct. Then we have the following ring isomorphism

$$F[x]/(g(x)) \cong F[x]/(f_1(x)^{n_1}) \times F[x]/(f_2(x)^{n_2}) \times ... \times F[x]/(f_k(x)^{n_k})$$

Proposition 2.3.20

If the polynomial $f(x)$ has roots $\alpha_1, \alpha_2, ..., \alpha_k$ in F (not necessary distinct), then $f(x)$ has $(x-\alpha_1)(x-\alpha_2)...(x-\alpha_k)$ as a factor. In particular, a polynomial of degree n over F has at most n roots in F even counted with multiplicities.

Proposition 2.3.21

Any finite subgroup of a multiplicative group of a field is cyclic. In particular, if F is a finite field, then the multiplicative group $F^\times$ of nonzero elements of F is a cyclic group.

Corollary 2.3.22

Let p be a prime, then the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ of nonzero residue classes $\mod p$ is cyclic.

Corollary 2.3.23

Let $n \geq 2$ be integer with factorization $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$ where $p_1, p_2, ..., p_r$ are distinct primes, we have the following isomorphisms of multiplicative groups.

1. $(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times (\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z})^\times \times ... \times (\mathbb{Z}/p_r^{\alpha_r}\mathbb{Z})^\times$
2. $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ is the direct product of a cyclic group of order 2 and a cyclic group of order $2^{\alpha-2}$ for all $\alpha \geq 2$
3. $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ is a cyclic group of order $p^{\alpha-1}(p-1)$ for all odd primes p

2.3.5 POLYNOMIALS IN SEVERAL VARIABLES OVER A FIELD AND GRÖBNER BASES

TODO

Chapter 3

MODULES AND VECTOR SPACES

3.1 INTRODUCTION TO MODULE THEORY

3.1.1 BASIC DEFINITIONS AND EXAMPLES

Definition 3.1.1 (left module over ring)
Let R be a nonunital ring, a left R-modue or a left module over R is an (additive) abelian group M together with a scalar multiplication map (action) $\cdot : R \times M \to M$ such that if $r, s \in R$, $m, n \in M$, then

$$(r+s)m = rm + sm$$
$$(rs)m = r(sm)$$
$$r(m+n) = rm + rn$$

If R is unital, then $1m = m$ for $m \in M$

Remark 3.1.2 (right module over ring, (two sided) module over commutative ring)
Right module is defined by the scalar multiplication map $M \times R \to M$ analogously. If R is commutatitive, we can make a left module M over R into a right module by defining $mr = rm$ for $r \in R$, $m \in M$, then M is called an R-module or a module over R. When R is not commutative, this definition does not satisfy the condition $m(rs) = (mr)s$.

Remark 3.1.3
From now on, assume all modules to be unital, that is, R is unital.

Remark 3.1.4 (vector space)
If F is a field, an module over F is a vector space over F

Definition 3.1.5 (submodule)
Let R be a ring and M be an R-module, a R-submodule of M is a subgroup N of M which is closed under the action of ring elements, that is, $rn \in N$ for $r \in R, n \in N$

Remark 3.1.6
Some examples of modules

1. $\mathbb{Z}$-module is an abelian group, sub-$\mathbb{Z}$-module is an abelian subgroup where $\mathbb{Z} \times M \to M$ is defined by
$$nm = m + m + ... + m \ (m \text{ times})$$
2. $F[x] - module$. Let F be a field and V be a vector space over F, fix a linear map $T : V \to V$, define an action of $F[x]$ on V by
$$\begin{aligned} \times_T : F[x] \times V &\to V \\ (p(x), v) &\mapsto p(T)(v) \end{aligned}$$
The action makes V into an $F[x]$-module. Moreover, this construction describes all $F[x]$-modules. That is, an $F[x]$-module on an abelian group V defines a F-vector space structure on V and a linear map $T : V \to V$ and on the other hand, a F-vector space V and a linear map $T : V \to V$ define an $F[x]$-module. Moreover, the $F[x]$-submodules of V are precisely the T-stable subspaces of V ($U \subseteq V$ is a T-stable subspace of V if $T(U) \subseteq U$)
3. $\mathcal{E}(U)$-module. Let $U \subseteq M$ be an open set on a smooth manifold, then the collection of differential p-forms $\mathcal{E}^p(U)$ on U is an $\mathcal{E}(U)$-module.

Proposition 3.1.7 (submodule criterion)
Let R be a ring and M be an R-module. A subset $N \subseteq M$ is a submodule of M if and only if

1. $N \neq \varnothing$
2. $x + ry \in N$ for all $r \in R$ and $x, y \in N$

Definition 3.1.8 (algebra over commutative ring)
Let R be a commutative unital ring, an algebra over R or R-algbera is a unital ring A together with a ring homomorphism $f : R \to A$ such that the subring $\operatorname{im} f$ of A is contained in the center of A.

Remark 3.1.9 (alternative definition of algebra)
Let R be a commutative unital ring, an R-algebra is an R-module structure on a unital ring A and
$$r(ab) = (ra)b = a(rb)$$
where $r \in R$, $a, b \in A$

Proof. R-module structure of A induced from $f : R \to A$ as follows:

$$ra = f(r)a = af(r) = ar$$

where the middle equality is due to $\operatorname{im} f$ is contained is the center of A. map $f : R \to A$ induced from R-module structure of A as follows:

$$f(r) = r1_A$$

$\operatorname{im} f$ is in the center of A as required □

Definition 3.1.10 (R-algebra homomorphism)
If A and B are two R-algebras, an R-algebra homomorphism $f : A \to B$ is a ring homomorphism and it respects the R-algebra structure

$$\phi(ra) = r\phi(a)$$

for $r \in R$, $a \in A$

3.1.2 QUOTIENT MODULES AND MODULE HOMOMORPHISMS

Definition 3.1.11 (R-module homomorphism, R-linear)
Let M, N be R-modules

1. A mao $\phi : M \to N$ is an R-module homomorphism (or R-linear) if it is a group homomorphism and it respect the R-module structure, that is
$$\phi(rx) = r\phi(x)$$
2. An R-module homomorphism $M \to N$ is an isomorphism if it is bijective. M and N are called isomorphic and write $M \cong N$
3. Denote the set of all R-module homorphism from M to N by $\operatorname{Hom}_R(M, N)$.

Proposition 3.1.12 (R-module homomorphism criterion)
A map $\phi : M \to N$ is an R-module homomorphism if and only if

$$\phi(rx + y) = r\phi(x) + \phi(y)$$

for all $r \in R$ and $x, y \in M$

Proposition 3.1.13 (the structure of $\mathrm{Hom}_R(M,N)$)

Let $\phi, \psi \in \mathrm{Hom}_R(M,N)$, define the addition on $\mathrm{Hom}_R(M,N)$ by

$$(\phi+\psi)(x) = \phi(x) + \psi(x)$$

for $x \in M$. The addition makes $\mathrm{Hom}_R(M,N)$ into an abelian group. If R is commutative, then for $r \in R$, define action of R on $\mathrm{Hom}_R(M,N)$ by

$$(r\phi)(x) = r\phi(x)$$

for $x \in M$. This action makes $\mathrm{Hom}_R(M,N)$ into an R-module. If $\phi \in \mathrm{Hom}_R(M,N)$ and $\psi \in \mathrm{Hom}_R(N,L)$, then the composition is $\phi\psi \in \mathrm{Hom}_R(L,N)$. The composition in $\mathrm{Hom}_R(M,M)$ defines a multiplication on $\mathrm{Hom}_R(M,M)$ and makes it into an R-algebra.

this makes the category of R-modules $\mathrm{R\text{-}Mod}$ an preadditive category (or Ab-enriched category), that is, the Hom set in $\mathrm{R\text{-}Mod}$ is itself an object of $\mathrm{R\text{-}Mod}$, has the structure of abelian group and composition of morphisms is bilinear

Definition 3.1.14

The ring $\mathrm{Hom}_R(M,M)$ is called the endomorphism ring of M and be denoted by $\mathrm{End}_R(M)$. Elements of $\mathrm{End}_R(M)$ are called endomorphisms.

Proposition 3.1.15

Let M be an R-module and N be a submodule of M. The additive abelian quotient group M/N can be made into an R-module by defining an action by

$$r(x+N) = rx + N$$

for $r \in R$ and $x+N \in M/N$. The natural projection $\pi : M \to M/N$ defined by $\pi(x) = x+N$ is an R-module homomorphism with kernel N

Definition 3.1.16 (sum of submodules)

Let A, B be submodules of R-module M. The sum of A and B s the set

$$A + B = \{a+b : a \in A, b \in B\}$$

The sum of two submodules is a submodule and is the smallest submodule which contains both A and B

Theorem 3.1.17 (isomorphism theorems)

Isomorphism theorems for modules

1. (first isomorphism theorem) Let M, N be R-modules, and $\phi : M \to N$ be module homomorphism. Then $\ker \phi$ is a submodule of M and
$$\frac{M}{\ker \phi} \cong \operatorname{im} \phi$$
2. (second isomorphism theorem) Let A, B be submodules of the R-module M, then
$$\frac{A+B}{B} \cong \frac{A}{A \cap B}$$
3. (third isomorphism theorem) Let A, B be submodules of the R-module M with $A \subseteq B$, then
$$\frac{M/A}{B/A} \cong \frac{M}{B}$$
4. (fourth isomorphism theorem) Let N be a submodule of the R-module M. There is a bijection between the submodules of M containing N and the submodules of M/N. The correspondence is given by $A \mapsto A/N$ with $A \supseteq N$.

   Moreover, this correspondence commutes with sum and intersection, *that is, this is an isomorphism between the lattice of submodules of M/N and the lattice of submodules of M containing N*

3.1.3 GENERATION OF MODULES, DIRECT SUMS, AND FREE MODULES

Remark 3.1.18

Let R be a unital ring and module means left module

Definition 3.1.19 (sum, submodule generated by a subset, finitely generated submodule, cyclic submodule)
Let M be an R-module

1. Let $N_1, N_2, ..., N_n$ be submodules of M, the sum of $N_1, N_2, ..., N_n$ is the set of all finite sums of elements from N_i
$$N_1 + N_2 + ... + N_n = \{a_1 + a_2 + ... + a_n : a_i \in N_i\}$$
2. For any subset $A \subseteq M$, let
$$RA = \{r_1a_1 + r_2a_2 + ... + r_ma_m : r_i \in R, a_i \in A, m \in \mathbb{N}\}$$
where by convention $A = \varnothing$, $RA = \{0\}$. RA is a submodule of M and called the submodule generated by A. A is called set of generators or generating set and RA is generated by A
3. A submodule $N \subseteq M$ is called finitely generated if there is a finite subset $A \subseteq M$ such that $N = RA$
4. A submodule $N \subseteq M$ is called cyclic if it is generated by a single element.

if R is unital, then $A \subseteq RA$. Moreover, RA is the smallest submodule containing A
In vector space theory, RA is like taking the span of set of vectors A. In category theory, R in RA is (probably) a functor from $\mathrm{Set} \to \mathrm{R\text{-}Mod}$

Definition 3.1.20 (direct product, external direct sum)
Let $M_1, M_2, ..., M_k$ be a collection of R-modules, the direct product (or external direct sum) of $M_1, M_2, ..., M_k$ is defined by
$$M_1 \oplus M_2 \oplus ... \oplus M_k = \{(m_1, m_2, ..., m_k) : m_i \in M_i\}$$
with addition and scalar multiplication defined component-wise. In Dummit-Foote, the authors also denoted direct product (or external direct sum) by
$$M_1 \times M_2 \times ... \times M_k$$

Proposition 3.1.21
Let $N_1, N_2, ..., N_k$ be submodules of R-module M, the following are equivalent

1. the map $\pi : N_1 \times N_2 \times ... \times N_k \to N_1 + N_2 + ... + N_k$ defined by
$$\pi(a_1, a_2, ..., a_k) = a_1 + a_2 + ... + a_k$$
is an module isomorphism.
2. for $j \in \{1, 2, ..., k\}$
$$N_j \cap (N_1 + N_2 + ... + N_{j-1} + N_{j+1} + ... + N_k) = \{0\}$$
3. Every element $x \in N_1 + N_2 + ... + N_k$ can be written uniquely in the form $a_1 + a_2 + ... + a_k$ where $a_i \in N_i$

the condition in analogous to being orthogonal in vector space

Remark 3.1.22 (internal direct sum)
the modules are submodules of a module and it satisfies the above condition, the sum is called internal direct sum

Definition 3.1.23 (free module, basis, rank)
An R-module F is called free on the subset $A \subseteq F$ if for every nonzero element of $x \in F$, there exist unique $r_1, r_2, ..., r_n \in R$ and $a_1, a_2, ..., a_n \in A$ such that

$$x = r_1 a_1 + r_2 a_2 + ... + r_n a_n$$

for some $n \in \mathbb{N}$. A is called basis or set of free generators of F. If R is commutative, then the cardinality of A is called rank of F.

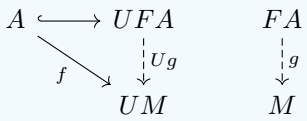
Remark 3.1.24
note that, the uniqueness condition of free module requires both r_i and a_i to be unique. Hence, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ is not a free $\mathbb{Z}$-module on the set $\{(0,1),(1,0)\}$ since

$$(0,1) = 1(0,1) = 3(0,1)$$

Theorem 3.1.25 (free module functor)
Let $U : \text{R-Mod} \to \text{Set}$ be the forgetful function, there exists a left adjoint functor of U, namely the free module functor $F : \text{Set} \to \text{R-Mod}$, that is

$$\text{Hom}_{\text{R-Mod}}(FA, M) \cong \text{Hom}_{\text{Set}}(A, UM)$$

where M is an R-module. Moreover, for any set A, there is a monomorphism $A \hookrightarrow UFA$ such that for any R-module M and map $f : A \to UM$, the adjunction induces a map $g : FA \to M$ and the diagram below commutes



Corollary 3.1.26
Any two free modules on the same set are isomorphic.

3.1.4 TENSOR PRODUCT OF MODULES

A motivation for tensor product
Let $R \subseteq S$ be a subring and N be an S-module then S is also an R-module. More generally, if there is a ring morphsim $f : R \to S$. An S-module N can be extended to an R-module by defining

$$R \times N \to N$$
$$(r, n) \mapsto f(r)n$$

In this case, S can be considered as an extension of the ring R and the resulting R-module is said to obtained from N by **restricting** of scalars from S to R. *maybe $f : R \to S$ defines a functor from S-Mod to R-Mod*
Now, let N be an R-module, consider the problem of **extending** N into an S-module. This is not always possible. In particular, let $R = \mathbb{Z}$, $S = \mathbb{Q}$

1. If $N = \mathbb{Q}$ be an $\mathbb{Z}$-module, it is also a $\mathbb{Q}$-module.
2. If $N = \mathbb{Z}$, then it is not a $\mathbb{Q}$-module since if $\mathbb{Z}$ is a $\mathbb{Q}$-module, then let $z = \frac{1}{2} \cdot 1 \in \mathbb{Z}$, then $z + z = 1$. However, $\mathbb{Z}$ can be embedded into $\mathbb{Q}$ by the canonical inclusion $\mathbb{Z} \hookrightarrow \mathbb{Q}$
3. If N is a finite order $\mathbb{Z}$-module which is an abelian group, then the (additive) order of every element in N is finite. While for any $\mathbb{Q}$-module M, it is a vector space, every non-zero element in $\mathbb{Q}$ is of infinite order. Hence, every group morphism $N \to M$ must be zero, hence there is no embedding of $\mathbb{Z}$-module of finite additive order into a $\mathbb{Q}$-module.

In the case $N = \mathbb{Z}$, it is not possible to make N to be a $\mathbb{Q}$-module but it is possible to **embed** into a $\mathbb{Q}$-module.
Consider the problem of embedding an R-module N into and S-module M where S is a subring of R. We have to define the scalar multiplication $S \times M \to M$. It is natural to consider M as a quotient group of the free $\mathbb{Z}$-module (abelian group) of the set $S \times N$. For $(s, n) \in S \times N$, let $[s, n]$ denote the class of (s, n). Let the inclusion $N \to M$ be defined by $n \mapsto [1, n]$, and the scalar multiplcation is defined by

$$\begin{aligned} S \times M &\to M \\ (r, [s, n]) &\mapsto [rs, n] \end{aligned}$$

Then, the class of (s, n) must satisfy for $m, n \in N$, then

$$\begin{aligned} [s_1 + s_2, n] &= [s_1, n] + [s_2, n] && \text{(for } s_1, s_2 \in S\text{)} \\ [s, m + n] &= [s, m] + [s, n] && \text{(for } s \in S\text{)} \\ [sr, n] &= [s, rn] && \text{(for } s \in S,\ r \in R\text{)} \end{aligned}$$

The resulting quotient group is the tensor product $S \otimes_R N$ and called the left S-module obtained by extension of scalars from the left R-module N

Definition 3.1.27 (tensor product of right module and left module)
Let M be a right R-module, N be a left R-module, the tensor product $M \otimes_R N$ is the quotient of the free $\mathbb{Z}$-module on the set $M \times N$, denoted by $F(M \times N)$ by the subgroup generated by all elements of the form

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

for $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$. Elements of $M \otimes_R N$ are called tensors. The class of (m, n) is denoted by $m \otimes n$ and called simple tensor. We have the following relations for simple tensors

$$(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n$$
$$m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2$$
$$mr \otimes n = m \otimes rn$$

Tensors can be written as a finite sum (non-uniquely) of simple tensors

Proposition 3.1.28 (extension of scalars)
Let R be a subring of S and N be a left R-module, there exist unique S-module $S \otimes_R N$ and an inclusion map $i : N \to S \otimes_R N$ given by

$$i : N \to S \otimes_R N$$
$$n \mapsto 1 \otimes n$$

so that i commutes with the R-module operations in N. That is

$$i(n_1 + n_2) = in_1 + in_2$$
$$i(rn) = ri(n)$$

The left S-module $S \otimes_R N$ is called the left S-module obtained by extension of scalars from the left R-module N
analogous to complexification $V \hookrightarrow V \otimes_{\mathbb{R}} \mathbb{C}$ where V is a real vector space

Definition 3.1.29 (R-balanced map)
Let M be a right R-module, N be a left R-module and L be an additive abelian group. A map $phi : M \times N \to L$ is called R-balanced if

$$\phi(m_1 + m_2, n) = \phi(m_1, n) + \phi(m_2, n)$$
$$\phi(m, n_1 + n_2) = \phi(m, n_1) + \phi(m, n_2)$$
$$\phi(m, rn) = \phi(mr, n)$$

Theorem 3.1.30 (tensor product of right module and left module)

Let R be a unital ring, M be a right R-module and N be a left R-module. Then, there exists a unique (up to isomorphism) abelian group $M \otimes_R N$ and an R-balanced inclusion map $i : M \times N \hookrightarrow M \otimes_R N$ such that any R-balanced map $\phi : M \times N \to L$ factors through i by a group morphism $\Phi : M \otimes_R N \to L$

$$\begin{array}{ccc} M \times N & \xrightarrow{i} & M \otimes_R N \\ & \searrow^{\phi} & \downarrow{\scriptstyle \Phi} \\ & & L \end{array}$$

On the other hand, given any group morphism $\Phi : M \otimes_R N \to L$, the composition Φi is an R-balanced map. In other words, this is an isomorphism from the set of R-balanced map $M \times N \to L$ into the set of group morphism $M \otimes_R N \to L$

Definition 3.1.31 (bimodule)

Let R, S be any unital rings. An abelian group M is called an (S, R)-bimodule if M is a left S-module, a right R-module, and $s(mr) = (sm)r$ for all $s \in S$, $r \in R$, $m \in M$

Definition 3.1.32 (module over a commutative ring)

Let M be a left (or right) module over a commutative unital ring R, then the (R, R)-bimodule structure on M by defining the left and right scalar multiplication coincide, that is $rm = mr$ for $r \in R$, $m \in M$. The (R, R)-bimodule structure is called the (standard) R-module structure.

Definition 3.1.33 (bilinear over a commutative ring)

Let R be a commutative unital ring and M, N, L be R-modules. A map $\phi : M \times N \to L$ is called R-bilinear if it is R-linear in each factor , that is

$$\phi(r_1 m_1 + r_2 m_2, n) = r_1 \phi(m_1, n) + r_2 \phi(m_2, n)$$
$$\phi(m, r_1 n_1 + r_2 n_2) = r_1 \phi(m, n_1) + r_2 \phi(m, n_2)$$

for all $r_1, r_2 \in R$, $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$

Theorem 3.1.34 (tensor product of R-modules)

Let R be a commutative unital ring, M, N be R-modules. Then there exists a unique (up to isomorphism) R-module $M \otimes_R N$ and an R-bilinear inclusion map $i : M \times N \hookrightarrow M \otimes_R N$ such that any R-blinear map $\phi : M \times N \to L$ factors through i by an R-linear (R-module morphism) map $\Phi : M \otimes_R N \to L$.

$$\begin{array}{ccc} M \times N & \xrightarrow{i} & M \otimes_R N \\ & \searrow^{\phi} & \downarrow{\scriptstyle \Phi} \\ & & L \end{array}$$

On the other hand, given any R-linear map $\Phi : M \otimes_R N \to L$, the composition Φi is R-bilinear. In other words, this is an isomorphism from the set of R-bilinear map $M \times N \to L$ into the set of R-linear map $M \otimes_R N \to L$

Theorem 3.1.35 (tensor product of two R-module homomorphisms)

Let M, M_1 be right R-modules, N, N_1 be left R-modules, let $\phi : M \to M_1$ and $\psi : N \to N_1$ be left and right R-module homomorphisms

1. there exists a unique group homomorphism denoted by $\phi \otimes \psi : M \otimes_R N \to M_1 \otimes_R N_1$ such that for all $m \in M$, $n \in N$, $(\phi \otimes \psi)(m \otimes n) = \phi(m) \otimes \psi(n)$

$$\begin{array}{ccc} M \times N & \xrightarrow{\phi \times \psi} & M_1 \times N_1 \\ {\scriptstyle \otimes_R}\downarrow & & \downarrow{\scriptstyle \otimes_R} \\ M \otimes_R N & \xrightarrow[\phi \otimes \psi]{} & M_1 \otimes_R N_1 \end{array}$$

2. If M, M_1 are also (S, R)-bimodules for some ring S and $\phi : M \to M_1$ is also an S-module homomorphism, then $\phi \otimes \psi$ is a homomorphsim of left S-modules. In particular, if R is commutative, then $\phi \otimes \psi$ is an R-module homomorphism.

3. If $\lambda : M_1 \to M_2$ and $\mu : N_1 \to N_2$ are left and right R-module homomophisms, then $(\lambda \otimes \mu)(\phi \otimes \psi) = (\lambda\phi) \otimes (\mu\psi)$

$$\begin{array}{ccccc} & & (\lambda\times\mu)(\phi\times\psi)=(\lambda\phi)\times(\mu\psi) & & \\ & \overset{\frown}{} & & \overset{\frown}{} & \\ M \times N & \xrightarrow[\phi\times\psi]{} & M_1 \times N_1 & \xrightarrow[\lambda\times\mu]{} & M_2 \times N_2 \\ {\scriptstyle \otimes_R}\downarrow & & \downarrow{\scriptstyle \otimes_R} & & \downarrow{\scriptstyle \otimes_R} \\ M \otimes_R N & \xrightarrow[\phi\otimes\psi]{} & M_1 \otimes_R N_1 & \xrightarrow[\lambda\otimes\mu]{} & M_2 \times N_2 \\ & \underset{\smile}{} & & \underset{\smile}{} & \\ & & (\lambda\otimes\mu)(\phi\otimes\psi)=(\lambda\phi)\otimes(\mu\psi) & & \end{array}$$

Theorem 3.1.36 (associativity of tensor product)

Let M be a right R-module, N be a (R, T)-bimodule, L be a left T-module, then there is a unique isomorphism *possibly natural*

$$(M \otimes_R N) \otimes_T L \to M \otimes_R (N \otimes_T L)$$
$$(m \otimes n) \otimes l \mapsto m \otimes (n \otimes l)$$

of groups for $m \in M$, $n \in N$, $l \in L$. If M is an (S, R)-bimodule, then this is an isomorphism of left S-modules.

Corollary 3.1.37

If R is commutative, and M, N, L are left R-modules. Then

$$(M \otimes N) \otimes L \cong M \otimes (N \otimes L)$$

as R-modules

Definition 3.1.38 (multilinear over a commutative ring)
Let R be a commutative unital ring and $M_1, M_2, ..., M_n$ and L be R-modules. A map $\phi : M_1 \times M_2 \times ... \times M_n \to L$ is called n-multilinear over R if it is R-linear in each component.

Corollary 3.1.39 (tensor product of n modules)
Let R be a commutative unital ring and $M_1, M_2, ..., M_n$ and L be R-modules. There exists a unique (up to isomorphism) R-module $M_1 \otimes M_2 \otimes ... \otimes M_n$ and an R-multilinear inclusion map $i : M_1 \times M_2 \times ... \times M_n \hookrightarrow M_1 \otimes M_2 \otimes ... \otimes M_n$ such that any R-multilinear map $\phi : M_1 \times M_2 \times ... \times M_n \to L$ factors through i by an R-linear map $\Phi : M_1 \otimes M_2 \otimes ... \otimes M_n \to L$

$$\begin{array}{ccc} M_1 \times M_2 \times ... \times M_n & \xhookrightarrow{i} & M_1 \otimes M_2 \otimes ... \otimes M_n \\ & \searrow^{\phi} & \downarrow \Phi \\ & & L \end{array}$$

On the other hand, given any R-linear map $\Phi : M_1 \otimes M_2 \otimes ... \otimes M_n \to L$, the composition Φi is R-multilinear. In other words, this is an isomorphism from the set of R-multilinear map $M_1 \times M_2 \times ... \times M_n \to L$ into the set of R-linear map $M_1 \otimes M_2 \otimes ... \otimes M_n \to L$

Theorem 3.1.40 (tensor product of direct sum)
Let M, M_1 be right R-modules and N, N_1 be left R-modules. Then there are unique group isomorphisms

$$(M \oplus M_1) \otimes N \to (M \otimes N) \oplus (M_1 \otimes N)$$
$$(m, m_1) \otimes n \mapsto (m \otimes n, m_1 \otimes n)$$

$$M \otimes (N \oplus N_1) \to (M \otimes N) \oplus (M \otimes N_1)$$
$$m \otimes (n, n_1) \mapsto (m \otimes n, m \otimes n_1)$$

If M, M_1 are also (S, R)-bimodule, then these isomorphisms are left S-module isomorphisms. In particular, if R is commutative then these are R-module isomorphisms

Corollary 3.1.41 (extension of scalars for free modules)
The module obtained from the free module R^n by extension of scalars from R to S is the free module S^n. That is,

$$S \otimes_R R^n \cong S^n$$

as left S-modules

Corollary 3.1.42
Let R be a commutative ring, then

$$R^s \otimes_R R^t \cong R^{st}$$

if $\{m_1, m_2, ..., m_s\}$ is a basis for R^s and $\{n_1, n_2, ..., n_t\}$ is a basis for R^t, then a basis for $R^s \otimes_R R^t$ is

$$\{m_i \otimes n_j : 1 \leq i \leq s, 1 \leq j \leq t\}$$

Proposition 3.1.43

Suppose R is a commutative ring and M, N are R-modules, then there is a unique R-module isomorphism

$$M \otimes N \to N \otimes M$$
$$m \otimes n \mapsto n \otimes m$$

Proposition 3.1.44

Let R be a commutative ring and A, B be R-algebras, then the multiplication below is well-defined

$$(A \otimes B) \times (A \otimes B) \to A \otimes B$$
$$(a \otimes b, a_1 \otimes b_1) \mapsto aa_1 \otimes bb_1$$

The multiplication makes $A \otimes B$ into an R-algebra.

3.1.5 EXACT SEQUENCES PROJECTIVE, INJECTIVE, FLAT MODULES

Some motivation for exactness: extension problem

Consider whether given two R-modules A and B, there exists a module B such that B contains A as a submodule and $B/A = C$. In this case, B is said to be the extension of C by A. (*analogous to multiply C by A times*)

Definition 3.1.45 (exact, exact sequence)

Let A, B, C, A_n be left R-modules

1. The pair of homomorphisms

$$A \xrightarrow{\alpha} B \xrightarrow{\beta} C$$

is said to be exact at B if $\operatorname{im}\alpha = \ker\beta$

2. A sequence of homomorphisms

$$\ldots \longrightarrow A_{n-1} \longrightarrow A_n \longrightarrow A_{n+1} \longrightarrow \ldots$$

is said to be exact of it is exact at every A_n

Remark 3.1.46

Let A, B, C be left R-modules

1. $0 \longrightarrow B \xrightarrow{\beta} C$ is exact at B if and only if β is injective.
2. $A \xrightarrow{\alpha} B \longrightarrow 0$ is exact at B if and only if α is surjective.

Definition 3.1.47 (short exact sequence)
The sequence

$$0 \longrightarrow A \xhookrightarrow{i} B \xrightarrow{p} C \longrightarrow 0$$

is exact if and only if i is injective, p is surjective and $\operatorname{im} i = \ker p$. If that sequence is exact, it is called short exact sequence.

Remark 3.1.48
Some remarks on short exact sequence

1. splitting short exact sequence

   Given two R-modules A, C, the sequence below is exact

   $$0 \longrightarrow A \xhookrightarrow{i} A \oplus C \xrightarrow{p} C \longrightarrow 0$$

   where $i : A \to A \oplus C$ and $p : A \oplus C \to C$ are the canonical inclusion and canonical projection.

2. exactness induces a short exact sequence

   A sequence $A \xrightarrow{\alpha} B \xrightarrow{\beta} C$ is exact at B if and only if the sequence

   $$0 \longrightarrow \operatorname{im} \alpha \hookrightarrow Y \twoheadrightarrow Y/\ker \beta \longrightarrow 0$$

   is short exact.

3. homomorphism induces a short exact sequence

   If $\phi : B \to C$ is an R-module homomorphism, then

   $$0 \longrightarrow \ker \phi \xhookrightarrow{i} B \xrightarrow{\phi} \operatorname{im} \phi \longrightarrow 0$$

   is exact where $i : \ker \phi \to B$ is the canonical inclusion map.

4. homomorphism induces a short exact sequence

   In particular, if M is an R-module generated by a set S and FS be the free R-module on S, then

   $$0 \longrightarrow \ker \phi \xhookrightarrow{i} FS \xrightarrow{\phi} M \longrightarrow 0$$

   is exact where ϕ is the composition $S \to FS \to M$. The short exact sequence describes a presentation of M (*read this*)

Definition 3.1.49 (homomorphism of short exact sequences, equivalent)
Let $0 \to A \to B \to C \to 0$ and $0 \to A_1 \to B_1 \to C_1 \to 0$ be short exact sequences of R-modules

1. A homomorphism of short exact sequences is a triple α, β, γ of module homomorphisms so that the diagram below commutes

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \hookrightarrow & B & \twoheadrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A_1 & \hookrightarrow & B_1 & \twoheadrightarrow & C_1 & \longrightarrow & 0 \end{array}$$

   This is called an isomorphism if the triplets are isomorphisms of R-modules, in that case, B and B_1 are called isomorphic extensions.

2. Two short exact sequences are called equivalent if $\alpha : A \to A_1$ and $\gamma : C \to C_1$ are identities ($A = A_1$ and $C = C_1$), in that case, B and B_1 are called equivalent extensions.

Remark 3.1.50
Some remarks on homomorphism of short exact sequences

1. If B and B_1 are isomorphism extensions then there is an R-module isomorphism $B \to B_1$ that restricts to an isomorphism $A \to A_1$ and induces an isomorphism $C \to C_1$
2. If B and B_1 are equivalent extensions then there is an R-module isomorphism $B \to B_1$ that restricts to the identity map $A \to A_1$ and induces the identity map $C \to C_1$
3. The notion of equivalent extensions measures how many different extensions of C by A and the notion of isomorphism extensions measure how many different extensions of C by A allowing C and A changed by isomorphisms.
4. (the category of short exact sequences of R-modules) homomorphism of short exact sequences makes it a category, namely the category of short exact sequences of R-modules, that is, composition of homomorphisms of short exact sequences is also a homomorphism. Isomorphism of short exact sequence is isomorphism in that category.

Remark 3.1.51
Some examples of short exact sequences

1. the diagram below represents a homomorphism of short exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z} & \xhookrightarrow{3} & \mathbb{Z} & \xrightarrow{\pi} & \mathbb{Z}/3\mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \cong} & & \\ 0 & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \xhookrightarrow{i} & \mathbb{Z}/6\mathbb{Z} & \xrightarrow{\pi'} & (\mathbb{Z}/6\mathbb{Z})/(3\mathbb{Z}/6\mathbb{Z}) & \longrightarrow & 0 \end{array}$$

   where $\pi : \mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$, $\pi' : \mathbb{Z}/6\mathbb{Z} \to (\mathbb{Z}/6\mathbb{Z})/(3\mathbb{Z}/6\mathbb{Z})$, $\alpha : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$, $\beta : \mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ are the natural projections, and $i : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ is the natural inclusion.

2. *TODO*

Proposition 3.1.52 (the short five lemma)

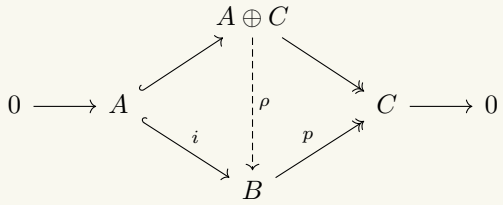
Let (α, β, γ) be a homomorphism of short exact sequences *in the book, these are SES of groups but it should be true to any R-module*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \hookrightarrow & B & \twoheadrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A_1 & \hookrightarrow & B_1 & \twoheadrightarrow & C_1 & \longrightarrow & 0 \end{array}$$

1. α, γ being injective implies β being injective
2. α, γ being surjective implies β being surjective

Definition 3.1.53 (split short exact sequence)

Let R be a ring, a short exact sequence $0 \longrightarrow A \xhookrightarrow{i} B \xtwoheadrightarrow{p} C \longrightarrow 0$ is called split if there exists a map $\rho : A \oplus C \to B$ such that the diagram below commutes



where the map $A \to A \oplus C$ is the natural inclusion and the map $A \oplus C \to C$ is the natural projection.

Remark 3.1.54 (split short exact sequence)

Some remarks on short exact sequence being split

1. By the short five lemma, the map $\rho : A \oplus C \to B$ is an isomorphism. Hence, B and $A \oplus C$ are both isomorphism extensions and equivalent extensions.
2. Two other equivalent characterizations of short exact sequence: Let R be a ring, a short exact sequence $0 \longrightarrow A \xhookrightarrow{i} B \xtwoheadrightarrow{p} C \longrightarrow 0$ is called split if one of the following is true

   (a) there exists a map : $B \to A$ such that $i = 1_A$

   $$0 \longrightarrow A \underset{}{\overset{i}{\hookrightarrow}} B \xtwoheadrightarrow{p} C \longrightarrow 0$$

   (b) there exists a map $\sigma : C \to B$ such that $p\sigma = 1_C$

   $$0 \longrightarrow A \xhookrightarrow{i} B \underset{\sigma}{\overset{p}{\twoheadrightarrow}} C \longrightarrow 0$$

Proposition 3.1.55

Let $0 \longrightarrow A \xhookrightarrow{\psi} B \xtwoheadrightarrow{\phi} C \longrightarrow 0$ be a short exact sequence of R-modules then $B = \psi A \oplus C'$ for some submodule C' of B with $\phi C' \cong C$ if and only if there is a homomorphism $\lambda : B \to A$ such that $\lambda\psi = 1_A$, that is, the short exact sequence is split. *this seems redundant with my definition*

Remark 3.1.56 ($\mathrm{Hom}_R(M,N)$ is an R-module)
Let M, N be R-modules then $\mathrm{Hom}_R(M,N)$ admits an R-module structure defined by

$$(f+g)(x) \mapsto f(m) + f(n)$$
$$(rf)(x) \mapsto rf(x)$$

for every $f, g \in \mathrm{Hom}_R(M,N)$, $r \in R$

Proposition 3.1.57
Let D, L, N be R-modules, then

$$\mathrm{Hom}_R(D, L \oplus N) \cong \mathrm{Hom}_R(D,L) \oplus \mathrm{Hom}_R(D,N)$$
$$\mathrm{Hom}_R(L \oplus N, D) \cong \mathrm{Hom}_R(L,D) \oplus \mathrm{Hom}_R(N,D)$$

PROJECTIVE MODULES AND $\mathrm{Hom}_R(D,-)$

Proposition 3.1.58 ($\mathrm{Hom}_R(D,-)$ is a covariant functor)
Let D, L, M be R-modules and $\psi : L \to M$ be an R-module be an R-module homomorphism, then ψ induces an R-module homomorphism

$$\psi^* : \mathrm{Hom}_R(D,L) \to \mathrm{Hom}_R(D,M)$$
$$f \mapsto \psi f$$

Moreover if ψ is injective then ψ^* is injective

Theorem 3.1.59 ($\mathrm{Hom}_R(D,-)$ is a left exact functor)
Let D, L, M, N be R-modules. If

$$0 \longrightarrow L \xhookrightarrow{\psi} M \xrightarrow{\phi} N \longrightarrow 0$$

is exact then the following sequence is also exact

$$0 \longrightarrow \mathrm{Hom}_R(D,L) \xhookrightarrow{\psi^*} \mathrm{Hom}_R(D,M) \xrightarrow{\phi^*} \mathrm{Hom}_R(D,N)$$

Definition 3.1.60 (projective module)

An R-module P is called projective if it satisfies one of the following equivalent conditions

1. For any R-modules L, M, N if

$$0 \longrightarrow L \xrightarrow{\psi} M \xrightarrow{\phi} N \longrightarrow 0$$

exact then

$$0 \longrightarrow \mathrm{Hom}_R(P, L) \xrightarrow{\psi^*} \mathrm{Hom}_R(P, M) \xrightarrow{\phi^*} \mathrm{Hom}_R(P, N) \longrightarrow 0$$

is also exact.

2. For any R-modules M, N, if $\psi : M \to N$ is surjective, then every R-module homomorphism $f : P \to N$ factors through ψ by an R-module homomorphism $F : P \to M$

$$\begin{array}{ccccc} & & & & P \\ & & \swarrow^{F} & & \downarrow f \\ M & \xrightarrow[\psi]{} & & N & \longrightarrow 0 \end{array}$$

3. If P is a quotient of the R-module M, then P isomorphic to a direct summand of M, that is, every short exact sequence

$$0 \longrightarrow L \hookrightarrow M \twoheadrightarrow P \longrightarrow 0$$

splits

4. P is a direct summand of a free R-module, that is, there exists a free R-module M such that

$$M = P \oplus Q$$

Corollary 3.1.61

Free modules are projective. A finitely generated module is projective if and only if it is a direct summand of a finitely generated free module. Every module is a quotient of a projective module.

Remark 3.1.62 (left exact functor, exact functor)

Let $F : C \to D$ be a functor from an abelian category to an abelian category (*e.g. the category of R-modules*), for any short exact sequence

$$0 \longrightarrow A \hookrightarrow B \twoheadrightarrow C \longrightarrow 0$$

F is called left exact if the induced sequence is exact

$$0 \longrightarrow F(A) \hookrightarrow F(B) \longrightarrow F(C)$$

F is called exact if the induced sequence is exact

$$0 \longrightarrow F(A) \hookrightarrow F(B) \twoheadrightarrow F(C) \longrightarrow 0$$

Remark 3.1.63 (functor, left exact functor, exact functor)
Some remarks on $\mathrm{Hom}_R(D,-)$

1. $\mathrm{Hom}_R(D,-)$ is a functor from R-Mod to R-Mod
2. $\mathrm{Hom}_R(D,-)$ is left exact and it is exact if and only if D is projective.

INJECTIVE MODULES AND $\mathrm{Hom}_R(-,D)$

Proposition 3.1.64 ($\mathrm{Hom}_R(-,D)$ is a contravariant functor)
Let D,M,N be R-modules and $\phi : M \to N$ be an R-module be an R-module homomorphism, then ϕ induces an R-module homomorphism

$$\begin{aligned}\phi^* : \mathrm{Hom}_R(N,D) &\to \mathrm{Hom}_R(M,D)\\ f &\mapsto f\phi\end{aligned}$$

Moreover if ϕ is surjective then ϕ^* is injective.

Theorem 3.1.65 ($\mathrm{Hom}_R(-,D)$ is right exact)
Let D,L,M,N be R-modules, if

$$0 \longrightarrow L \xhookrightarrow{\psi} M \xrightarrow{\phi} N \longrightarrow 0$$

is exact then the following sequence is also exact

$$\mathrm{Hom}_R(L,D) \xleftarrow{\psi^*} \mathrm{Hom}_R(M,D) \xleftarrow{\phi^*} \mathrm{Hom}_R(N,D) \longleftarrow 0$$

Definition 3.1.66 (injective module)

An R-module Q is called injective if it satisfies one of the following equivalent conditions

1. For any R-modules L, M, N if

$$0 \longrightarrow L \overset{\psi}{\hookrightarrow} M \overset{\phi}{\twoheadrightarrow} N \longrightarrow 0$$

   exact then

$$0 \longleftarrow \mathrm{Hom}_R(L,Q) \overset{\psi^*}{\twoheadleftarrow} \mathrm{Hom}_R(M,Q) \overset{\phi^*}{\hookleftarrow} \mathrm{Hom}_R(N,Q) \longleftarrow 0$$

2. For any R-module L, M, if $\psi : L \to M$ is injective, then every R-module homomorphism $f : L \to Q$ factors through ψ by an R-module homomorphism $F : M \to Q$

$$\begin{array}{ccccc} 0 & \longrightarrow & L & \overset{\psi}{\hookrightarrow} & M \\ & & {\scriptstyle f}\downarrow & \swarrow_{F} & \\ & & Q & & \end{array}$$

3. If Q is a submodule of the R-module M then Q is a direct summand of M, that is, every short exact sequence

$$0 \longrightarrow Q \hookrightarrow M \twoheadrightarrow N \longrightarrow 0$$

   splits

Remark 3.1.67 (left exact functor, exact functor)

Let $F : C \to D$ be a **contravariant** functor from an abelian category to an abelian category (*e.g. the category of R-modules*), for any short exact sequence

$$0 \longrightarrow A \hookrightarrow B \twoheadrightarrow C \longrightarrow 0$$

F is called left exact if the induced sequence is exact

$$F(A) \longleftarrow F(B) \hookleftarrow F(C) \longleftarrow 0$$

F is called exact if the induced sequence is exact

$$0 \longleftarrow F(A) \twoheadleftarrow F(B) \hookleftarrow F(C) \longleftarrow 0$$

Remark 3.1.68 (functor, left exact functor, exact functor)

Some remarks on $\mathrm{Hom}_R(-, D)$

1. $\mathrm{Hom}_R(-, D)$ is a **contravariant** functor from R-Mod to R-Mod
2. $\mathrm{Hom}_R(-, D)$ is left exact and it is exact if and only if D is injective.

Proposition 3.1.69

Let Q be an R-module

1. (Baer Criterion)

TODO

FLAT MODULES AND $D \otimes_R -$