Introduction to Module Theory

KYB

Contents

0 Preliminary

0.1 Sets

Text: Set theory / Thomas Jech. - 3rd Millennium ed, Springer, 2007 [Jec07]

Axiom 0.1.1 (Axioms of Zermelo-Fraenkel set theory)

(1) Axiom of Extensionality: If X and Y have the same elements, then $X = Y$.

(2) Axiom of Pairing: For any a and b there exists a set $\{a, b\}$ that contains exactly a and b.

(3) Axiom Schema of Separation: If P is a property with parameter p, then for any X and p there exists a set $Y = \{u \in X : P(u, p)\}$ that contains all those $u \in X$ that have property P.

(4) Axiom of Union: For any X there exists a set $Y = \bigcup X$, the union of all elements of X.

(5) Axiom of Power Set: For any X there exists a set $Y = P(X)$, the set of all subsets of X.

(6) Axiom of Infinity: There exists an infinite set.

(7) Axiom Schema of Replacement: If a class F is a function, then for any X there exists a set $Y = F(X) = \{F(x) : x \in X\}$.

(8) Axiom of Regularity: Every nonempty set has an $\in$-minimal element.

(9) Axiom of Choice: Every family of nonempty sets has a choice function.

For convenience, unless mentions otherwise,

- $a, b, c, \cdots$ implies a member(element) of a set;
- $A, B, C, \cdots$ implies a set;
- $\mathcal{A}, \mathcal{B}, \mathcal{C}, \cdots$ implies a collection(may not be a set) of sets.

Definition 0.1.2

- $A \subset B$ if and only if for all x, $x \in A$ implies $x \in B$.
- $A \cap B = \{x : x \in A \text{ and } x \in B\}$
- $A \cup B = \{x : x \in A \text{ or } x \in B\}$
- $A - B = \{x : x \in A \text{ and } x \notin B\}$
- $\bigcup_{S \in \mathcal{A}} S = \{x : x \in S \text{ for some } S \in \mathcal{A}\}$.

If $A = \{A_\alpha : \alpha \in J\}$ for some index set J, write the union of A by

$$\bigcup_{\alpha \in J} A_\alpha.$$

By the axiom of pairing, for any a and b, there is a set $\{a, b\}$ and by the axiom of extensionality, this set is unique.

The *singleton* $\{a\}$ is the set $\{a\} = \{a, a\}$.

Now we want to define an ordered pair (a, b). This pair will be satisfied the property: $(a, b) = (c, d)$ if and only if $a = c$ and $b = d$.

The only tool we can use is a set, but since $\{a, b\} = \{b, a\}$, we should find another tool.

Definition 0.1.3 (Ordered pair)
Define $(a, b) = \{\{a\}, \{a, b\}\}$.

Exercise 0.1.1
Prove that $(a, b) = (c, d)$ if and only if $a = c$ and $b = d$.

Remark 0.1.4
We can define ordered triples, quadrples, etc., as follows:

$$\begin{aligned}(a, b, c) &:= ((a, b), c),\\ (a, b, c, d) &:= ((a, b, c), d),\\ &\vdots\\ (a_1, \cdots, a_{n+1}) &:= ((a_1, \cdots, a_n), a_{n+1}).\end{aligned}$$

Then $(a_1, \cdots, a_n) = (b_1, \cdots, b_n)$ if and only if $a_1 = b_1, \cdots, a_n = b_n$.

Definition 0.1.5
For any set X, define $\mathcal{P}(X)$ the set of all subsets of X, i.e.

$$Y \in \mathcal{P}(X) \iff Y \subset X.$$

We call $\mathcal{P}(X)$ the *power* set of X.

Definition 0.1.6 (The Cartesian Product)
Using the axiom of power set, we can define the set of all pairs (x, y) such that $x \in X$ and $y \in Y$, i.e.

$$X \times Y = \{(x, y) : x \in X \text{ and } y \in Y\}.$$

We say $X \times Y$ is the Cartesian product of X and Y.

In general, we can define

$$X_1 \times \cdots \times X_{n+1} = (X_1 \times \cdots X_n) \times X_{n+1}.$$

If $X_i = X$ for $i = 1, \cdots, n$,

$$X^n = \underbrace{X \times \cdots \times X}_{n \text{ times}}.$$

If $X = \varnothing$, $X \times Y = \varnothing$ because if not, we can choose $(x, y) \in X \times Y$, but there is no $x \in X$.

Definition 0.1.7 (Relations)
A *relation* R of X and Y is a subset of $X \times Y$. Denote xRy for $(x, y) \in R$.

The *domain* of R is the set

$$\text{dom}(R) = \{u : \exists v \text{ such that } (u, v) \in R\},$$

and the *range* of R is the set

$$\text{ran}(R) = \{v : \exists u \text{ such that } (u, v) \in R\}.$$

Definition 0.1.8 (Functions)
Suppose f is a relation where $f \subset X \times Y$ such that

(1) $\text{dom}(f) = X$;

(2) if $(x, y) \in f$ and $(x, z) \in f$, then $y = z$.

Then we say f is a *function* from X to Y and the unique y such that $(x, y) \in f$ is the *value* of f at x; denote

$$y = f(x),$$

or

$$f : x \mapsto y,$$

for $(x, y) \in f$. We call the conditions 1 and 2 the well-defined conditions.

The set of all functions from X to Y is denoted by Y^X.

Remark 0.1.9

- Since $\varnothing \times Y = \varnothing$, $f = \varnothing$ is a function.
- Suppose X is nonempty. If there is a function $f : X \to \varnothing$, for all $x \in X$, there is $y \in \varnothing$ such that $f(x) = y$. However, there is no such y. Hence there is no function from nonempty set to empty set.

Definition 0.1.10
Suppose $f : X \to Y$.

- If $\text{ran}(f) = Y$, f is a function *onto* Y, or a *surjective* function.
- If $f(x) = f(y)$ implies $x = y$, f is a *one-to-one* function, or a *injective* function.
- If f is injective and surjective, then f is *bijective*.

Let $A \subset X$. We can define a *restriction* of f to A

$$f|A = \{(x, y) \in f : x \in A\}.$$

A function g is an *extension* of f if $f \subset g$, i.e.

- $\text{dom}(f) \subset \text{dom}(g)$ and
- $g(x) = f(x)$ for all $x \in \text{dom}(f)$.

If f and g are functions such that $\text{ran}(g) \subset \text{dom}(f)$, then *composition* of f and g is the function $f \circ g$ with domain $\text{dom}(f \circ g) = \text{dom}(g)$ such that

$$(f \circ g)(x) = f(g(x)) \text{ for all } x \in \text{dom}(g).$$

The *image* of X by f is the set

$$f(X) = \{y : \exists x \in X \text{ such that } y = f(x)\}$$

and the *inverse image* of a subset A of Y is the set

$$f^{-1}(A) = \{x : \exists y \in A \text{ such that } y = f(x)\}$$

If f is a bijective function, for each $y \in Y$, $f^{-1}(\{y\})$ is singleton. Thus we can define a function $f^{-1} : Y \to X$ such that $f^{-1}(y) = x$ if and only if $y = f(x)$.

0.2 Equivalence Relations and Partitions

Observe the equality symbol $=$ on a nonempty set X.

(1) For all $x \in X$, $x = x$.

(2) For $x, y \in X$, $x = y$ implies $y = x$.

(3) For $x, y, z \in X$, $x = y$ and $y = z$ implies $x = z$.

Then we can extend the concept of equality as follows:

Definition 0.2.1 (Equivalence relation)
Let $\sim$ be a relation on a nonempty set X such that

(1) (*reflexive*)For all $x \in X$, $x \sim x$.

(2) (*symmetric*)For $x, y \in X$, $x \sim y$ implies $y \sim x$.

(3) (*transitive*)For $x, y, z \in X$, $x \sim y$ and $y \sim z$ implies $x \sim z$.

We call $\sim$ a *equivalence relation* on X.

Definition 0.2.2 (Partition)
A *partition* $\mathcal{P}$ of a nonempty set X is a family of disjoint nonempty sets whose union is X, i.e.

- For all $P \in \mathcal{P}$, $P \neq \varnothing$ and $P \subset X$;
- For $P_1, P_2 \in \mathcal{P}$, $P_1 \cap P_2 \neq \varnothing$ implies $P_1 = P_2$;
- $\bigcup_{P \in \mathcal{P}} P = X$.

Proposition 0.2.3
If $\mathcal{P}$ is a partition of a nonempty set X, the relation $\sim$ defined by $x \sim y$ if and only if there is $P \in \mathcal{P}$ such that $\{x, y\} \subset P$ is an equivalence relation on X.

Proof.
- Let $x \in X$. Since $X = \bigcup_{P \in \mathcal{P}} P$, there is $P \in \mathcal{P}$ such that $\{x\} = \{x, x\} \subset P$. Thus $x \sim x$.
- Suppose $x \sim y$ with $\{x, y\} \subset P$. Then $\{y, x\} \subset P$. So $y \sim x$.
- Suppose $x \sim y$ and $y \sim z$ with $\{x, y\} \subset P_1$ and $\{y, z\} \subset P_2$. Since $y \in P_1 \cap P_2$, $P_1 = P_2$. So $\{x, z\} \subset P_1 = P_2$ and $x \sim z$.

Hence $\sim$ is an equivalence relation on X. □

Definition 0.2.4 (Equivalence class)
Let $\sim$ be an equivalence relation on a nonempty set X. Let $x \in X$. An *equivalence class* of x (with repect to $\sim$) is a set $[x]_\sim$ such that

$$[x]_\sim := \{y \in X : y \sim x\}.$$

Denote the set of all equivalence class of X (w.r.t $\sim$) by $X/\sim$, i.e.

$$X/\sim := \{[x]_\sim : x \in X\}.$$

We say $X/\sim$ is the *quotient* of X by $\sim$.

Exercise 0.2.1
$X/\sim$ is a partition of X.

0.3 (Partial) Ordered Sets

Definition 0.3.1
A relation $<$ on a set X is a *partial ordering* of X if

(1) $a \not< a$ for any $a \in X$;

(2) if $a < b$ and $b < c$, then $a < c$.

$(X, <)$ is called a *partially ordered* set.
If there is one more condition

(3) $a < b$ or $a = b$ or $a > b$ for all $a, b \in X$,

we say $<$ is *(linear, or totally) ordering* and $(X, <)$ is *(linear, or totally) ordered* set.
The relation $\leq$ is $a \leq b$ if and only if $a = b$ or $a < b$.

Definition 0.3.2
Suppose $(X, <)$ is a partially ordered set and S is a nonempty subset of X and $a \in X$.

- a is a *maximal* element of S if $a \in S$ and for all $x \in S$ $a \not< x$.
- a is a *minimal* element of S if $a \in S$ and for all $x \in S$ $x \not< a$.
- a is the *greatest* element of S if $a \in S$ and for all $x \in S$ $x \leq a$.
- a is the *least* element of S if $a \in S$ and for all $x \in S$ $a \leq x$.
- a is an *upper* bound of S if for all $x \in S$ $x \leq a$.
- a is an *lower* bound of S if for all $x \in S$ $a \leq x$.
- a is the *supremum* of S if a is the least upper bound.
- a is the *infimum* of S if a is the greatest lower bound.

0.4 Cardinality

The cardinality of a set X is, roughly speaking, a number of elements of X. Denote the cardinality of X by $|X|$. We omit the formal definition of the cardinality.

Definition 0.4.1
Let X and Y be sets. We say X and Y have the same cardinality if and only if there is a bijective function f from X to Y.

Example 0.4.2

- Consider $2\mathbb{N} = \{2n : n \in \mathbb{N}\}$. Define $f : \mathbb{N} \to 2\mathbb{N}$ by $f(n) = 2n$. You can easily check that f is bijective. So $|\mathbb{N}| = |2\mathbb{N}|$.
- Let $g : \mathbb{N} \to \mathbb{Z}$ by
$$g(n) = \begin{cases} \frac{n}{2} & n \text{ is even} \\ -\frac{n-1}{2} & n \text{ is odd.} \end{cases}$$
Then g is a bijective. So $|\mathbb{N}| = |\mathbb{Z}|$.

If X is bijective to $\{1, 2, \cdots, n\}$ for some $n \in \mathbb{N}$, denote $|X| = n$ and we say X is *finite*. If there is no bijective between X and $\{1, 2, \cdots, n\}$ for all $n \in \mathbb{N}$, we say X is *infinite*. If there is a bijective between X and $\mathbb{N}$, we say X is *countable*. (Sometimes we say X is countable if X is finite or countably infinite.)

We can define an ordering of cardinal numbers by

$$|X| \leq |Y| \text{ if and only if there is an injective function } f : X \to Y.$$

If $|X| \leq |Y|$ but $|X| \neq |Y|$, $|X| < |Y|$.

Theorem 0.4.3
For every set X, $|X| < |\mathcal{P}(X)|$.

Proof. The map $x \mapsto \{x\}$ is injective. Thus $|X| \leq |\mathcal{P}(X)|$.

Let $f : X \to \mathcal{P}(X)$ be a function. Let $Y = \{x \in X : x \notin f(x)\}$. If there is $z \in X$ such that $f(z) = Y$, then $z \in Y$. But $z \in Y$ implies $z \notin f(z)$, a contradiction. Thus f is not in the range of f. Hence there is no bijective function from X to $\mathcal{P}(X)$, $|\mathcal{P}(X)| \neq |X|$. □

Theorem 0.4.4
If $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$.

Proof. Let $f_1 : A \to B$ and $f_2 : B \to A$ be injective functions. Let $B' = f_2(B)$ and $A_1 = f_2(f_1(A))$, then $A_1 \subset B' \subset A$ and $|A_1| = |A|$. Thus we may assume $A_1 \subset B \subset A$ and $f : A \to A$ is injective whose image is A_1.

By induction, define A_n and B_n for all $n \in \mathbb{N}$ as follows:

$$A_0 = A, \quad A_{n+1} = f(A_n)$$
$$B_0 = B, \quad B_{n+1} = f(B_n).$$

Let $g : A \to A$ defined by

$$g(x) = \begin{cases} f(x) & \text{if } x \in A_n - B_n \text{ for some } n, \\ x & \text{otherwise.} \end{cases}$$

Then g is bijective mapping of A onto B. □

Let A and B be sets.

- $|A| + |B| = |A \cup B|$, where $A \cap B = \varnothing$,
- $|A| \cdot |B| = |A \times B|$,
- $\left|A^B\right| = |A|^{|B|}$.

Lemma 0.4.5
$|\mathcal{P}(\mathcal{A})| = 2^{|A|}$.

Proof. For $X \subset A$, define $\mathcal{X}_X : A \to \{0, 1\}$ by

$$\mathcal{X}_X(x) = \begin{cases} 1 & \text{if } x \in X, \\ 0 & \text{if } x \in A - X. \end{cases}$$

Let $f : X \mapsto \mathcal{X}_X$ is bijective from $\mathcal{P}(A)$ to $\{0, 1\}^A$. □

We call $\mathcal{X}_X$ the characteristic function of X.

If we assume the axiom of choice, $|A| \leq |B|$ if and only if there is a surjective function $f : B \to A$.

0.5 Cartesian Products

Let I be an index set of A, or $A = \{x_\alpha : \alpha \in I\}$. Using the axiom of choice, every set can be an indexing set.

Definition 0.5.1

(1) Let I be an index set and let $\{A_i : i \in I\}$ be a collection of sets. A *choice function* is any function

$$f : I \to \bigcup_{i \in I} A_i$$

such that $f(i) \in A_i$ for all $i \in I$.

(2) The *Cartesian product* of $\{A_i : i \in I\}$ is the set of all choice functions from I to $\bigcup_{i \in I} A_i$ and denoted by $\prod_{i \in I} A_i$. We sometimes write an element f of $\prod_{i \in I} A_i$ by $\prod_{i \in I} a_i$ or $(a_i)_{i \in I}$ where $f(i) = a_i$.

(3) For each $j \in I$, the set A_j is called the j^{th} *component* of $\prod_{i \in I} A_i$ and a_j is the j^{th} *coordinate* of $(a_i)_{i \in I}$.

(4) For $j \in I$, the *projection map* of $\prod_{i \in I} A_i$ onto A_j is defined by $(a_i)_{i \in I} \mapsto a_j$.

Remark 0.5.2

- We already define a finite Cartesian product of sets without the axiom of choice.
- To define an infinite Cartesian product, we need the axiom of choice.

0.6 Zorn's Lemma

Recall that the axiom of choice.

Axiom 0.6.1 (Axiom of Choice)
Every family of nonempty sets has a choice function.

There are some equivalent statement of the axiom of choice.(That means, assuming other statement, we can prove the axiom of choice, and vice versa.)

Definition 0.6.2
Let $(X, <)$ be an ordered set. We say X is *well-ordered* if every nonempty subset of X has a least element.

Example 0.6.3

- $(\mathbb{N}, <)$ with usual ordering is well-ordered. We say $\mathbb{N}$ has the well-oredring principle.
- $(\mathbb{Z}, <)$ is not well-ordered.

Theorem 0.6.4 (Well-ordering principle)
Every set can be well-oredered, i.e. every set has a well-ordered relation.

Lemma 0.6.5 (Zorn's lemma)
If A is a nonempty partially ordered set in which every chain has an upper bound then A has a maximal element.

To understand Zorn's lemma, we have to know what chain is.

Definition 0.6.6
Let A be nonempty partially ordered by $\leq$. A subset B of A is called a *chain* is B is ordered under the same $\leq$.

Recall that an upper bound of a subset B of A is an element $u \in A$ such that for all $b \in B$, $b \leq u$. And a maximal element of A is an element $m \in A$ such that for all $a \in A$, $a \not< m$. There is another equivalent definition of maximal element m:

$$\text{if } a \in A \text{ such that } m \leq a, \text{ then } m = a.$$

Theorem 0.6.7
Assuming ZF, the following are equivalent:

(1) the axiom of choice

(2) the well-ordering theorem

(3) Zorn's lemma.

Proof. See theorem 5.1 and theorem 5.4 and exercise 5.5 in [Jec07]. See Tutoring Top12 for Zorn's lemma implies the axiom of choice. □

Using Zorn's lemma, we can prove that every vector space has a basis (even infinite dimensional).

Theorem 0.6.8
Every vector space V over a field F has a basis.

Proof. If $V = \{0\}$, we allow that $\{0\}$ is a basis.

Suppose V is nontrivial vector space. You already know that for every nonzero vector v, $\{v\}$ is linearly independent. Let $\mathcal{V}$ the collection of all linearly independent subsets of V. We can give a partial order on $\mathcal{V}$ by the inclusion, i.e.

$$B_1 \leq B_2 \iff B_1 \subset B_2.$$

Now let $\mathcal{C} \subset \mathcal{V}$ be a nonempty chain. Let $C = \bigcup_{B \in \mathcal{C}} B$. Then for all $B \in \mathcal{C}$, $B \leq C$.

Claim) C is linearly independent.

Suppose $\alpha_1 v_1 + \cdots \alpha_n v_n = 0$ where $\alpha_i \in F$ and $v_i \in C$. Then we can find $B \in \mathcal{B}$ such that $\{v_1, \cdots, v_n\} \subset B$. Since B is linearly independent, $\alpha_i = 0$ for all i. So C is linearly independent.

Since our $\mathcal{V}$ is a collection of linearly independent subsets of V, $C \in \mathcal{V}$, which implies C is an upper bound of $\mathcal{C}$.

Then by Zorn's lemma, $\mathcal{V}$ has a maximal element B. Since $B \in \mathcal{V}$, B is linearly independent.

Claim) $\operatorname{span} B = V$.

Suppose not. Let $v \in V - \operatorname{span} B$. Suppose for $\{v_1, \cdots, v_n\} \subset B$ and $\alpha_1, \cdots, \alpha_n, \beta \in F$,

$$\alpha_1 v_1 + \cdots \alpha_n v_n + \beta v = 0.$$

Since $v \notin \operatorname{span} B$, $\beta = 0$. Then by the linearly independence of B, $\alpha_1 = \cdots = \alpha_n = 0$. So $B \cup \{v\}$ is also linearly independent. Then $B < B \cup \{v\}$ but it contradicts the maximality of B. Hence $V = \operatorname{span} B$ and B is a basis of V. □

0.7 The natural numbers

Remark 0.7.1 (Natural numbers)
$\mathbb{N}$ satisfies

- $1 \in \mathbb{N}$ is the minimal (least) element of $\mathbb{N}$.
- If $n \in \mathbb{N}$, then $n+1 \in \mathbb{N}$.
- There is no $n \in \mathbb{N}$ such that $n+1 = 1$.
- For $m, n \in \mathbb{N}$, $m = n$ or $m > n$ or $m < n$.
- $\cdots$.

Proposition 0.7.2 (Well-ordering principle of the nartual numbers)
Any nonempty subset S of $\mathbb{N}$ has a minimal element.

Proof. Suppose S is finite. Then we can find a minimal element.

Suppose S is infinite. Choose $n \in S$ and consider $A = S \cap \{1, \cdots, n\}$. We can find a minimal element $m \in A$ and m is also minimal element of S. □

Remark 0.7.3
If we put finitely many real numbers into $\mathbb{N}$, WoP still holds. For example, $\mathbb{N}_0 = \{0\} \cup \mathbb{N}$ has WoP.

Example 0.7.4 (Application of WoP, mathematical induction)
For each $n \in \mathbb{N}$, let $P(n)$ is a statement. Suppose

(1) $P(1)$ is true.

(2) If $P(n)$ is true, then $P(n+1)$ is true.

Then for all $n \in \mathbb{N}$, $P(n)$ is true.

Proof. Let $S = \{n \in \mathbb{N} \mid P(n) \text{ is false }\}$. Sinse $P(1)$ is true, $\mathbb{N} - S$ is nonempty. If S is empty, MI holds.

Suppose not. Choose a minimal element m of S. Then $P(m-1)$ is true and $P(m)$ is false. By condition 2, $P(m)$ must be true. (contradiction) □

Remark 0.7.5 (Unboundness of natural numbers)
$\mathbb{N}$ has no upper bound.

Proof. Suppose not and let M be an upper bound of $\mathbb{N}$. Then for all $n \in \mathbb{N}$, $n \leq M$. Since $M+1 \in \mathbb{N}$, $M+1 \leq M$. But this cannot happen. □

0.8 The integer numbers

Definition 0.8.1 (Divisor)
Let $m, n \in \mathbb{Z}$. Suppose $n \neq 0$. If there is $r \in \mathbb{Z}$ such that $m = nr$,

- n divides m,
- m is divided by n.

Write $n|m$, and n is called a diviosr of m and m is called a multiple of n.

Definition 0.8.2 (The Greatest Common divisor)
Let $m, n, d \in \mathbb{Z}$. Suppose one of m and n is nonzero.

(1) $d|m$ and $d|n$.

(2) If $c|m$ and $c|n$, then $c \leq d$.

If d satisfies (1), d is called a common divisor. If d also satisfies (2), d is called the greatest common divisor.

If d is a common diviosr, so is $-d$. So the GCD is positive.

Proposition 0.8.3 (The division algorithm)
Let $m, n \in \mathbb{Z}$ be nonzero elements with $n > 0$. Then there are unique $q, r \in \mathbb{Z}$ such that

- $0 \leq r < n$;
- $m = qn + r$.

Proof. Let $S = \{m - an : a \in \mathbb{Z}, m - an \geq 0\}$. Since $m + |m|n \geq 0$, S is nonempty. Choose minimal element r of S. Then $m - qn = r$ for some $q \in \mathbb{Z}$. If $r \geq n$, then $m = qn + r = (q + 1)n + (r - n)$ implies $r > r - n \in S$. But r is the minimal element of S. So $0 \leq r < n$. Similar way we can show that r is unique. □

Remark 0.8.4
If $n|m$, then $m = qn$. So $m|n$ and $n|m$ implies $m = \pm n$. Hence the GCD (the LCM) makes sense.

Theorem 0.8.5 (Linear combination of GCD)
If $m, n \in \mathbb{N}$ are both nonzero, then there is $a, b \in \mathbb{Z}$ such that

$$am + bn = \gcd(m, n).$$

Proof. Let $S = \{xm + yn > 0 : x, y \in \mathbb{Z}\}$. Clearly S is nonempty. Let d be the minimal element of S with $am + bn = d$.

Taking the division algorithm on m, then $m = qd + r$.

$$r = m - qd = m - q(am + bn) = (1 - qa)m + (-qb)n$$

So either $r = 0$ or $r \geq d$. But $r < d$ implies $r = 0$, or $m = qd$. Similarly $d|n$. Thus d is CD of m and n.

If c is another CD of m and n, we get $c|am + bn$. Thus $c|d$. □

Proposition 0.8.6 (The Euclidean algorithm)
Suppose $m \geq n > 0$. Apply the division algorithm to m and n, and get $m = q_1 n + r_1$ where $0 \leq n$. If $r_1 = 0$, n is a diviosr of m. If not, apply one more to n and r_1, $n = r_1 q_2 + r_2$ where $0 \leq r_2 \leq r_1$. Repeat this untill $0 < r_n < r_{n-1}$ and $r_{n+1} = 0$. Then $r_n = gcd(m, n)$.

Remark 0.8.7

$$\begin{aligned}
m &= q_1 n + r_1 \quad , 0 < r_1 < n \\
n &= q_2 r_1 + r_2 \quad , 0 < r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3 \quad , 0 < r_3 < r_2 \\
&\vdots \quad \vdots \\
r_{n-1} &= q_{n+1} r_n.
\end{aligned}$$

Proof. Since $r_n < r_{n-1} < \cdots < n$, we can find such r_n. So it suffices to show that $r_n = \gcd(m, n)$.

Claim) For $a \geq b > 0$, if $a = qb + r$, then $\gcd(a, b) = \gcd(b, r)$.

Clearly $\gcd(b, r) | a$. So $\gcd(b, r) | \gcd(a, b)$. Conversely, $a - qb = r$ implies $\gcd(a, b) | r$. So $\gcd(a, b) | \gcd(b, r)$.

By the claim,

$$\gcd(m, n) = \gcd(n, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{n-1}, r_n) = r_n.$$

□

Remark 0.8.8
Using the Euclidean algorithm, we can find $a, b \in \mathbb{Z}$ so that $am + bn = \gcd(m, n)$.

Example 0.8.9
$a = 257$, $b = 114$.

$$\begin{aligned} 257 &= 2 \times 114 + 29 \\ 114 &= 3 \times 29 + 27 \\ 29 &= 1 \times 27 + 2 \\ 27 &= 13 \times 2 + 1 \\ 2 &= 2 \times 1. \end{aligned}$$

Note that 257 is a prime number. So $\gcd(257, 114) = 1$.

$$\begin{aligned} 1 &= 27 - 13 \times 2 \\ &= 27 - 13 \times (29 - 1 \times 27) = -13 \times 29 + 14 \times 27 \\ &= -13 \times 29 + 14 \times (114 - 3 \times 29) = 14 \times 114 - 55 \times 29 \\ &= 14 \times 114 - 55 \times (257 - 2 \times 114) = -55 \times 257 + 124 \times 114. \end{aligned}$$

Thus $114^{-1} \equiv 124 \mod (257)$.

1 Groups

Text: Abstract algebra / David S. Dummit - 3rd ed, Wiley, 2003 [DF03]

1.1 Introduction to Groups

Definition 1.1.1 (Binary operators)

- A *binary operation* $\star$ on a set G is a function $\star : G \times G \to G$. For any $a, b \in G$, write $a \star b$ for $\star(a, b)$.
- We say $\star$ is *associative* if for all $a, b, c \in G$, $a \star (b \star c) = (a \star b) \star c$.
- For $a, b \in G$, we say a and b *commute* if $a \star b = b \star a$. If every two elements of G commutes, we say $\star$ is *commutative*.

Example 1.1.2

- $+, \times$ are commutative binary operations on $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$, respectively.
- $-$ is a noncommutative binary operation on Z, where $-(a, b) = a - b$. The map $a \mapsto -a$ is not a binary operation but a unitary operation.

Definition 1.1.3 (Groups)
Suppose G is a set and $\star : G \times G \to G$ is a binary operation. We say G is a *group* if

(1) $\star$ is associative;

(2) there is an element $e \in G$, called an *identity* of G, such that for all $a \in G$ we have $a \star e = e \star a = a$;

(3) for each $a \in G$ there is an element $a^{-1} \in G$, called an *inverse* of a, such that $a \star a^{-1} = a^{-1} \star a = e$.

In addition, we say G is an *abelian group* if $(G, \star)$ is a group and $\star$ is commutative.

Example 1.1.4

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, and $(\mathbb{C}, +)$ are abelian groups with respect to addition. 0 is an identity of them. In this case, write $-a$ instead of a^{-1}.
- A multiplication $\times$ on $\mathbb{Q} - \{0\}$, $\mathbb{R} - \{0\}$, or $\mathbb{C} - \{0\}$ forms an abelian group with identity 1.
- Any filed F is an abelian group under $+$ and $F - \{0\}$ is an abelian group under $\times$.
- Any vector sapce V over F is an abelian group under $\times$.
- For $n \in \mathbb{Z}^+$, the residue classes $\mathbb{Z}/n\mathbb{Z}$ of $\mathbb{Z}$ is an abelian group under $+$.
- Let X be any set and let $\mathrm{Bij}(X)$ be the set of all bijective functions on X. $(\mathrm{Bij}(X), \circ)$ forms a group under the composition $\circ$. Since $f \circ g \neq g \circ f$ in general, $\mathrm{Bij}(X)$ may not be abelian.

Remark 1.1.5
Let $(G, \star)$ and $(H, \diamond)$ be groups. We can give a group structure on $G \times H$ in a natural way.

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

Of course, we can give another structure on $G \times H$.

Example 1.1.6
Consider $(\mathbb{R}^\times)^2$ where $\mathbb{R}^\times = \mathbb{R} - \{0\}$.

1. Let $(a_1, a_2) \cdot (b_1, b_2) = (a_1 b_1, a_2 b_2)$. By the above remark, $((\mathbb{R}^\times)^2, \cdot)$ is a group induced by $(\mathbb{R}, \cdot)$.
2. Let $(a_1, a_2) \times (b_1, b_2) = (a_1 b_1 - a_2 b_2, a_1 b_2 + a_2 b_1)$. You can easily check $((\mathbb{R}^\times)^2, \times)$ is a group.

Proposition 1.1.7
If G is a group under the operation $\star$, then

(1) the identity of G is unique

(2) for each $a \in G$, a^{-1} is unique

(3) $(a^{-1})^{-1} = a$ for all $a \in G$

(4) $(a \star b)^{-1} = (b^{-1}) \star (a^{-1})$

(5) for any $a_1, \cdots, a_n \in G$, the value of $a_1 \star a_2 \star \cdots \star a_n$ is independent of how the expression is bracketed, for example

$$((a_1 \star a_2) \star a_3) \star a_4 = (a_1 \star a_2) \star (a_3 \star a_n) = (a_1 \star (a_2 \star a_3)) \star a_n = \cdots .$$

Proof. Left as an exercise. □

From now on, except when necessary, wrtie $a \cdot b$, or ab for $a \star b$. And the identity element e is denoted by 1 (if the operation is $+$, $e = 0$). For $x \in G$, denote $x^{-1}x^{-1} \cdots x^{-1}$ (n terms) by x^{-n}, If the operation is $+$, $-x - x - x \cdots - x = -nx$. Let $x^0 = 1$ (or $0x = 0$).

Proposition 1.1.8
Let G be a group. The left and right cancellation laws hold in G, i.e.,

(1) $au = av \implies u = v$, and

(2) $ub = vb \implies u = v$.

So for $a, b \in G$, the equation $ax = b$ and $ya = b$ have unique solutions for $x, y \in G$.

Proof. Applying a^{-1} and b^{-1}. □

Definition 1.1.9 (Orders)
Let G be a group and $x \in G$. The smallest positive integer n such that $x^n = 1$ is called the *order* of x, and denote $|x| = n$. If there is no such n, $|x| = \infty$.

The cardinal $|G|$ of G is also called an order.

Example 1.1.10

(1) $|x| = 1$ if and only if $x = 1$.

(2) $(\mathbb{Z}, +)$ (or $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$) has only one element of finite order, 1.

(3) $(\mathbb{Z} - \{0\}, \times)$ (or $\mathbb{Q} - \{0\}$, $\mathbb{R} - \{0\}$, $\mathbb{C} - \{0\}$) has exactly two elements of finite order, -1 and 1.

(4) Let $G = \mathbb{Z}/9\mathbb{Z}$. $\overline{6} + \overline{6} = \overline{3}$, $\overline{6} + \overline{6} + \overline{6} = \overline{0}$. Thus $\left|\overline{6}\right| = 3$.

(5) Let $G = \mathbb{Z}/7\mathbb{Z} - \{\overline{0}\} = (\mathbb{Z}/7\mathbb{Z})^\times$.

$$\overline{2}^2 = \overline{4} \to \overline{2}^3 = 1$$
$$\overline{3}^2 = \overline{2} \to \overline{3}^3 = \overline{6} \to \overline{3}^4 = \overline{4} \to \overline{3}^5 = \overline{5} \to \overline{3}^6 = \overline{1}.$$

Thus $(\mathbb{Z}/7\mathbb{Z})^\times = \{\overline{3}^1, \overline{3}^2, \overline{3}^3, \overline{3}^4, \overline{3}^5, \overline{3}^6\}$. In this case, we say G is generated by $\overline{3}$.

1.2 Diheral Groups

For each $n \in \mathbb{Z}^+$, consider a regular n-gon. Give a labelling of the n-verices, for example as shown in the following figure.

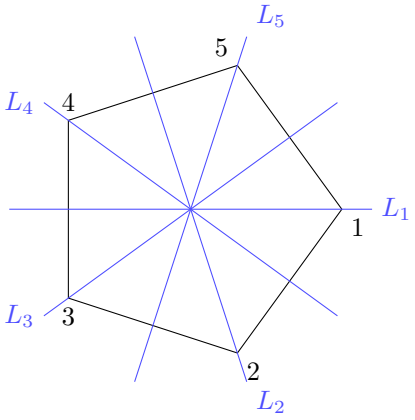


Figure 1: $n = 5$

We can construct a group D_{2n} which is the set of symmetries of a regular n-gon;

- r: rotation of $2\pi/n$ radians clockwise about the center of the n-gon.
- s : reflextion on L_1.
- composition of r and s. For example, rs is a symmetry obtained by first applying r then s. (read right to left)

Theorem 1.2.1

(1) $1, r, r^2, \cdots, r^{n-1}$ are all distinct and $r^n = 1$, so $|r| = n$.

(2) $|s| = 2$.

(3) $s \neq r^i$ for any i.

(4) $sr^i \neq s^j$, for all $0 \leq i, j \leq n-1$ with $i \neq j$. So

$$D_{2n} = \{1, r, r^2, \cdots, r^{n-1}, s, sr, sr^2, \cdots, sr^{n-1}\}.$$

Thus each element can be written uniquely in the form $s^k r^i$ for some $k = 0$ or $k = 1$ and $0 \leq i \leq n-1$. Moreover $|D_{2n}| = 2n$.

(5) $rs = sr^{-1}$.

(6) $r^i s = sr^{-i}$.

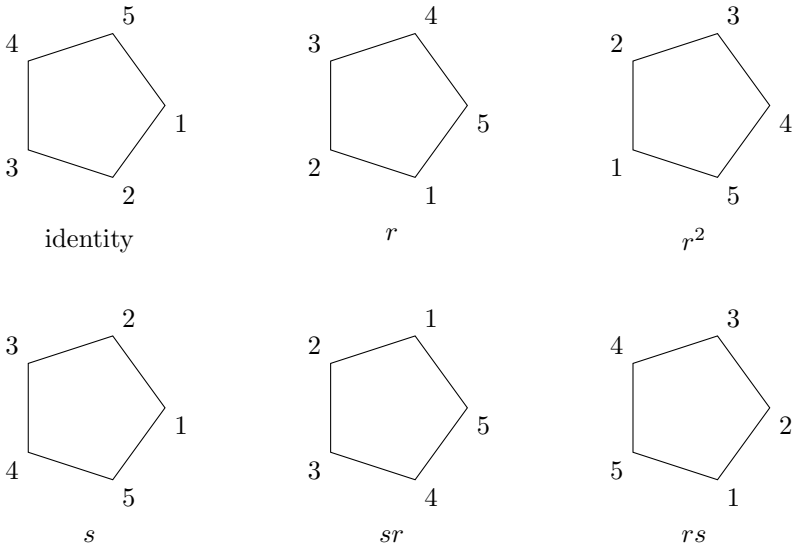


Figure 2: some elements of D_{10}

1.3 Symmetric Groups

Recall that a permutaion on a set X is just a bijective function on X. In $X = \{1, 2, \cdots, n\}$ for some n, the set of permutaions of X is S_n. In general, for any nonempty set X, S_X is the set of all bijections and we can give a group structure under composition. So $(S_X, \circ)$ is called the *symmetric group on the set* X. If $X = \{1, 2, \cdots, n\}$, S_n is called the *symmetric group of degree* n.

For each $\sigma \in S_n$ we can visualize σ by

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}.$$

We now describe an efficient notation for writing elements σ of S_n, the *cycle decomposition*.

Definition 1.3.1(1) A *cycle* is a string of integers which represents the element of S_n which cyclically permutes these integers. For example, the cycle $(a_1 a_2 \cdots a_m)$ is the permutaion which sends $a_i \mapsto a_{i+1}$ for $1 \leq i \leq m-1$ and $a_m \mapsto a_1$.

(2) Let σ_1 and σ_2 be two cycles. If there is no common integer in the string of σ_1 and σ_2, we say they are *disjoint*. For example, (2 1 3) and (4 8 5 7) are disjoint.

(3) If a cycle $\sigma = (a_1, \cdots, c_m)$, we say a_m is an *m-cycle*.

For example, let (2 1 3) be a cycle in S_5. Then

$$(2\ 1\ 3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix}.$$

Theorem 1.3.2
Let $n \in \mathbb{Z}^+$ and let S_n be a symmetric group of degree n.

(1) $|S_n| = n!$.

(2) Every permutaion is compositions of 3-cycles.

(3) If $n \geq 3$, S_n is not abelian.

(4) Every disjoint cycles are commute.

(5) Every permutaion is compositions of some disjoint cycles.

Proof. See Tutoring LA1 8. □

1.4 Group Homomorphism

Suppose there is an animal in front of you and you know that animal is one of dog and cat. How do you confirm it is a dog or it is a cat? Maybe you would check the differences of dogs and cats. To check a difference, you have to know commonalities of them.

Mathematicians want to distinguish a set(or structure or space, ect) from another one. To do this, they introduce a function which preserve some characteristics. For example, we define the cardinality of a set and two sets have the same cardinals if there is a bijective function. This implies any function preserve a cardinality. If two ordered sets X and Y are given, we can define an order-preserving function $f : X \to Y$, i.e.

$$a <_X b \implies f(a) <_Y f(b).$$

In topology, a set X having a structure of open sets is called a topological space. If X and Y are topological spaces, we define a topological-preserving function, say continuous function, as follows:

f is continuous if for any open subset V of Y, $f^{-1}(V)$ is an open subset of X.

In this concept, we can define a function which preserves the group structure, say *group homomorphism*.

Definition 1.4.1
Let $(G, \star)$ and $(H, \diamond)$ be groups. A map $\varphi : G \to H$ such that

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

is called a *(group) homomorphism*.

If a homomorphism $\varphi : G \to H$ is bijective, we say φ is an *isomorphism* and we say G and H are isomorphic.

Remark 1.4.2
If $\phi : G \to H$ is an isomorphism, so is ϕ^{-1}. This is the reason that the definition of 'isomorphism' requires only two conditions.

In topology, even f is bijective continuous, f^{-1} may not be continuous. So a homeomorphism (which is bijective and topology-preserving function)is required

(1) f is continuous,

(2) f is bijective,

(3) f^{-1} is continuous.

Example 1.4.3

- The identity map $G \to G$ is an isomorphism for any group G.

- Let $\phi : (\mathbb{R}, +) \to (\mathbb{R}^+, \times)$ by $\phi(x) = e^x$ is an isomorphism.
- In Example 1.1.6, $((\mathbb{R}^\times)^2, \cdot)$ is not isomorphic to $\mathbb{C}^\times$ but $((\mathbb{R}^\times)^2, \times)$ is isomorphic to $\mathbb{C}^\times$.
- $\varphi(1_G) = \varphi(1_g)\varphi(1_G)$ implies $\varphi(1_G)_H$.

Now we can say two groups are different if there is no isomorphism between them. Moreover we can classify groups. For example, every there are only two groups (up to isomorphism) of order 6, $\mathbb{Z}/6\mathbb{Z}$ and S_3.

Proposition 1.4.4
Suppose $\varphi : G \to H$ is an isomorphism.

(1) $|G| = |H|$.

(2) G is abelian if and only if H is abelian.

(3) for all $g \in G$, $|g| = |\varphi(g)|$.

Proof. (1) Since φ is bijective, $|G| = |H|$.

(2) It suffices to show that $\Rightarrow$. Let $h_1, h_2 \in H$. Then there are $g_1, g_2 \in G$ such that $h_i = \varphi(g_i)$.

$$h_1h_2 = \varphi(g_1)\varphi(g_2) = \varphi(g_1g_2) = \varphi(g_2g_1) = \varphi(g_2)\varphi(g_1) = h_2h_1.$$

(3) If $|g| = \infty$, $g^n \neq 1$ for all $n \in \mathbb{Z}^+$. So $\varphi(g^n) = \varphi(g)^n \neq 1$ and $|\varphi(g)| = \infty$.
If $|g| = n$, $g^m \neq 1$ for $1 \leq m \leq n-1$. Thus $\varphi(g^m) = \varphi(g)^m \neq 1$ but $\varphi(g^n) = \varphi(g)^n = 1$. Hence $|\varphi(g)| = |g|$.

□

Remark 1.4.5

- By the result 3, $(\mathbb{R} - \{0\}, \times)$ and $(\mathbb{R}, +)$ cannot be isomorphic because -1 is of order 2 in $(\mathbb{R} - \{0\}, \times)$ but there is no element of order 2 in $(\mathbb{R}, +)$.
- If φ is a homomorphism (may not isomorphism), $|g| \geq |\phi(g)|$.

1.5 Subgroups

Definition 1.5.1
Let $(G, \cdot)$ be a group. A subset H of G is called a *subgroup* if H is closed under products and inverses (in the same $\cdot$), i.e.

$$\begin{aligned} a, b \in H &\implies a \cdot b \in H, \\ a \in H &\implies a^{-1} \in H. \end{aligned}$$

You can easily show that a subgroup is also group under the same operator. This is the reason why we call it a sub'group'. There is an equivalent definition of subgroups.

Proposition 1.5.2 (The Subgroup Criterion)
Let G be a group. Suppose H is a subset of G satisfying the followings:

(1) $1 \in H$;

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

Then H is a subgroup of G. Furthermore, if H is finite, it suffices to check that H is nonempty and closed under multiplication.

Proof. Let $x \in H(\neq \varnothing)$. Since $1, x \in H$, $1 \cdot x^{-1} = x^{-1} \in H$. So H is closed under inverses.

Let $x, y \in H$. Then $xy = x(y^{-1})^{-1} \in H$. So H is closed under multiplication.

Now suppose H is finite and nonempty. Let $x \in H$. Then $\{x, x^2, x^3, x^4, \cdots\} \subset H$. Since H is finite, there are $m > n > 0$ such that $x^m = x^n$. Then $x^{m-n} = 1$ implies $1 \in H$. So we may assume $|x| = n$, then $x^{n-1} = x^{-1} \in H$. □

If H is a subgroup of G, denote $H \leq G$. If $H \neq G$, write $H < G$.

Example 1.5.3

(1) For any group G, G is a subgroup of G.

(2) $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$ under $+$.

(3) $\mathbb{Q}^\times \leq \mathbb{R}^\times \leq \mathbb{C}^\times$ under $\times$.

(4) Let $G = D_{2n}$. Then $H = \{1, r, r^2, \cdots, r^{n-1}\}$ is a subgroup of G.

(5) Consider $(\mathbb{Z}, +)$. For any $n \in \mathbb{Z}$, $(n\mathbb{Z}, +)$ is a subgroup of $\mathbb{Z}$.

(6) If $H \leq G$ and $K \leq H$, then $K \leq G$. Thus the relation $\leq$ on the set of all subgroups is partial ordering.

1.6 Some Special Subgroups

Definition 1.6.1
Let G be a group and A be a nonempty subset of G. Define $C_G(A) = \{g \in G : gag^{-1} = a \text{ for all } a \in A\}$. $C_G(A)$ is called the *centralizer* of A in G.

Remark 1.6.2

- Suppose $g \in C_G(A)$. Then for all $a \in A$, $gag^{-1} = a$, or $ga = ag$. So $C_G(A)$ is the set of all elements of G which commute with every element of A.
- Since $1 \in C_G(A)$, $C_G(A)$ is always nonempty.
- Let $x, y \in G$. For all $a \in A$,

  $$(xy)a(xy)^{-1} = (xy)a(y^{-1}x^{-1}) = x(yay^{-1})x^{-1} = xax^{-1} = a.$$

  So $xy \in G$. Moreover, $xax^{-1} = a$ implies $a = x^{-1}a(x^{-1})^{-1}$. So $x^{-1} \in G$. Hence $C_G(A)$ is a subgroup of G.
- If G is abelian, $C_G(A) = G$ for all subsets A.

Definition 1.6.3
Define $Z(G) = \{g \in G : gx = xg \text{ for all } x \in G\}$. $Z(G)$ is called the *center* of G.

Note that $Z(G) = C_G(G)$.

Definition 1.6.4
Define $gAg^{-1} = \{gag^{-1} : a \in A\}$. Define the *normalizer* of A in G to be the set $N_G(A) = \{g \in G : gAg^{-1} = A\}$.

Remark 1.6.5

- $N_G(A)$ is also subgroup of G.
- If G is abelian, $C_G(A) = N_G(A) = Z(G) = G$ for any subset A.
- $gAg^{-1} = A$ does not implies $gag^{-1} = a$ for $a \in A$ in general.
- Let $G = D_8$ and $A = \{1, r, r^2, r^3\}$. Then

$$sr^n s^{-1} = sr^n s = ssr^{-n} = r^{-n}$$
$$sr^k r^n (sr^k)^{-1} = sr^k r^n r^{-k} s = r^{-n}.$$

  So for all $g \in D_8$, $gAg^{-1} = A$, or $N_G(A) = G$, but $sr = r^{-1}s \neq rs$.

  Moreover $s \notin C_G(A)$. If $sr^i \in C_G(A)$, $s = (sr^i)(r^{-i}) \in C_G(A)$, a contradiction. So $C_G(A) = A$.
- If $g \in C_G(A)$, then $gAg^{-1} = A$. So $C_G(A) \leq N_G(A)$.

Definition 1.6.6
Let $\varphi : G \to H$ be a homomorphism.

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

(2) $\operatorname{img} \varphi = \varphi(G) = \{\varphi(g) : g \in G\}$.

$\ker \varphi$ is called the *kernel* of φ and $\operatorname{img} \varphi$ is called the *image* of φ.

Remark 1.6.7
$\ker \varphi \leq G$ and $\operatorname{img} \varphi \leq H$.

Let $x, y \in \ker \varphi$.

$$1 = \varphi(1) = \varphi(xx^{-1}) = \varphi(x)\varphi(x^{-1}) = \varphi(x^{-1})$$
$$\varphi(xy) = \varphi(x)\varphi(y) = 1.$$

Let $\varphi(x), \varphi(y) \in \operatorname{img} \varphi$.

$$1 = \varphi(1) = \varphi(xx^{-1}) = \varphi(x)\varphi(x^{-1})$$
$$\varphi(xy) = \varphi(x)\varphi(y).$$

1.7 Cyclic Groups and Cyclic Subgroups

Definition 1.7.1
A group H is *cyclic* if H can be generated by a single element, i.e. there is some element $x \in H$ such that $H = \{x^n : n \in \mathbb{Z}\}$.

In additive notation H is cyclic if $H = \{nx : n \in \mathbb{Z}\}$

In this case, we say x is a *generator* of H. And denote $H = \langle x \rangle$.

Remark 1.7.2
If $H = \langle x \rangle$, $H = \langle x^{-1} \rangle$.

Example 1.7.3

(1) $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$ in the addition.

(2) For all $n \in \mathbb{Z}$, $n\mathbb{Z} = \langle n \rangle$.

(3) Let $G = D_{2n}$. Then $H = \langle r \rangle$ is a subgroup of all rotations of the n-gon.

Proposition 1.7.4
Suppose $H = \langle x \rangle$.

(1) if $|H| = n < \infty$, then $|x| = n$.

(2) if $|H| = \infty$, then $x^n \neq 1$ for all $n \neq 0$ and $x^a \neq x^b$ for all $a \neq b$ in $\mathbb{Z}$.

Proposition 1.7.5
Let G be an arbitrary group, $x \in G$ and let $m, n \in \mathbb{Z}$. If $x^n = 1$ and $x^m = 1$, then $x^d = 1$ where $d = \gcd(m, n)$. In particular if $x^m = 1$ for some $m \in \mathbb{Z}$, then $|x|$ divides m.

Proof. By the Euclidean Algorithm, there exists $r, s \in \mathbb{Z}$ such that $d = mr + ns$. Thus

$$x^d = x^{mr+ns} = (x^m)^r (x^n)^s = 1^r 1^s = 1.$$

If $x^m = 1$, let $|x| = n$. If $m = 0$, $n|m$. So we may assume $m \neq 0$. Let $d = \gcd(m, n)$. Since $0 < d \leq n$ and $x^d = 1$, $d = n$. Hence $|x||m$. □

Theorem 1.7.6

(1) If $\langle x \rangle$ and $\langle y \rangle$ are both cyclic and of order n, then the map

$$\begin{aligned} \varphi : \langle x \rangle &\to \langle y \rangle \\ x^k &\mapsto y^k \end{aligned}$$

is well defined and is an isomorphism.

(2) If $\langle x \rangle$ is an infinite cyclic group, the map

$$\begin{aligned} \varphi : \mathbb{Z} &\to \langle x \rangle \\ k &\mapsto x^k \end{aligned}$$

is well defined and is an isomorphism.

Proof. Suppose $\langle x \rangle$ and $\langle y \rangle$ are both cyclic and of order n. If $x^r = x^s$, $x^{r-s} = 1$. So $n|r - s$. Write $r = tn + s$. Then

$$\varphi(x^r) = \varphi(x^{tn+s}) = y^t n + s = (y^n)^s y^s = y^s = \varphi(x^s).$$

So φ is well defined. Now it is a routine proof that φ is an isomorphism.

If $\langle x \rangle$ is an infinite cyclic group, $k \mapsto x^k$ is a bijective, so well defined. The remain □

Remark 1.7.7
Since a cyclic group of order n (maybe infinite) is unique up to isomorphism, we can define the cyclic group of order n Z_n. Then $Z_\infty \cong \mathbb{Z}$ and $Z_n = \mathbb{Z}/n\mathbb{Z}$ for $n \in \mathbb{Z}^+$.

Proposition 1.7.8
Let G be a group, let $x \in G$ and let $a \in \mathbb{Z}^\times$.

(1) If $|x| = \infty$, then $|x^a| = \infty$.

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

(3) In particular, if $|x| = n < \infty$ and a is a positive integer dividing n, then $|x^a| = \dfrac{n}{a}$.

Proof. (1) By way of contradiction assume $|x| = \infty$ but $|x^a| = m < \infty$. Then $1 = (x^a)^m = x^{am}$ and $x^{-am} = (x^{am})^{-1} = 1^{-1} = 1$. Now one of am or $-am$ is positive so $x^n = 1$ for some $n \in \mathbb{Z}^+$. Then $|x| < \infty$.

(2) Let $y = x^a$, $d = \gcd(n, a)$ and write $n = db$, $a = dc$ with $b > 0$. Then $\gcd(b, c) = 1$.

$$y^b = x^{ab} = x^{dcb} = (x^{db})^c = (x^n)^x = 1^c = 1.$$

So $|y||b$. Let $|y| = k$. Then

$$a^{ak} = y^k = 1.$$

So $n|ak$, or $db|dck$. So $b|ck$. Since $\gcd(b, c) = 1$, $b|k$. Scine $b|k$ and $k|b$, $b = k$.

□

Proposition 1.7.9
Let $H = \langle x \rangle$.

(1) Assume $|x| = \infty$. Then $H = \langle x^a \rangle$ if and only if $a = \pm 1$.

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

Proof. (2) By Proposition 1.7.8,

$$|x^a| = |x| \iff \frac{n}{\gcd(a, n)} = n \iff \gcd(a, n) = 1.$$

□

Example 1.7.10
In $\mathbb{Z}/12\mathbb{Z}$, $\gcd(1, 12) = \gcd(5, 12) = \gcd(7, 12) = \gcd(11, 12) = 1$. So $\mathbb{Z}/12\mathbb{Z} = \langle \overline{1} \rangle = \langle \overline{5} \rangle = \langle \overline{7} \rangle = \langle \overline{11} \rangle$.

Theorem 1.7.11
Let $H = \langle x \rangle$ be a cyclic group.

(1) Every subgroup of H is cycilc. More precisely, if $K \leq H$, then either $K = \{1\}$ or $K = \langle x^d \rangle$, where d is the smallest positive integer such that $x^d \in K$.

(2) If $|H| = \infty$, then for any distinct nonnegative integers a and b, $\langle x^a \rangle \neq \langle x^b \rangle$.

(3) If $|H| = n < \infty$, for each positive integer a dividing n, there is a unique subgroup of H of order a. This subgroup is the cyclic group $\langle x^d \rangle$ where $d = n/a$.

Proof. We will prove only (1). We may assume $K \neq \{1\}$. Then there exists some $a \neq 0$ such that $x^a \in K$. If $a < 0$, $x^{-a} \in K$, so we may assume $a > 0$.

Consider $\mathcal{P} = \{b \in \mathbb{Z}^+ : x^b \in K\}$. Since $a \in \mathcal{P}$, $\mathcal{P}$ is nonempty subset of $\mathbb{Z}^+$. Then there is a minimal positive integer d in $\mathcal{P}$. Since $\langle x^d \rangle \leq K \leq H$, $\langle x^d \rangle \leq H$.

Let $x^b \in K$. By the Division Algorithm, $b = qd + r$ for some q, r where $0 \leq r < d$. Then $x^r = x^(a - qd) = x^a(x^d)^{-q} \in K$. By the minimality of d, $r = 0$, or $d|b$. Thus $x^b = (x^d)^q$, $K \leq \langle x^d \rangle$. □

1.8 Subgroups Generated by Subsets of a Group

Let G be an object (such as a group, field, vector space, etc.) and A be a subset of G. Is there a unique minimal subobject of G which contains A? We already know that a vector space has a unique subspace containing A, say $\operatorname{span} A$. $\operatorname{span} A$ is the set of all linear combination of A over a field F.

Let G be a group and A be any subset of G. Then we can find the unique smallest subgroup of G containing A as follow:

Proposition 1.8.1
If $\mathcal{A}$ is any nonempty collection of subgroups of G, then the intersection of all members of $\mathcal{A}$ ia also a subgroup.

Proof. Let

$$K = \bigcap_{H \in \mathcal{A}} H.$$

Since each $H \in \mathcal{A}$ is a subgroup, $1 \in H$, so $1 \in K$. So K is nonempty. If $a, b \in K$, then $a, b \in H$ for all $H \in \mathcal{A}$. Since each H is a group, $ab^{-1} \in H$ for all $H \in \mathcal{A}$, hence $ab^{-1} \in K$. Hence $K \leq G$. □

Definition 1.8.2
If A is any subset of the group G, define

$$\langle A \rangle = \bigcap_{\substack{A \subset H \\ H \leq G}} H.$$

This is called the *subgroup of G generated by A*.

$\langle A \rangle$ is the intersection of all subgroups of G containing A, i.e. let $\mathcal{A} = \{H \leq G : A \subset H\}$ and then $\bigcap_{H \in \mathcal{A}} H = \langle A \rangle$ is a subgroup of G. And by the definition, if H is a subgroup of G containing A, then $\langle A \rangle \leq H$. In this sense, $\langle A \rangle$ is the smallest subgroup of G containing A.

Remark 1.8.3

- If A is finite, say $A = \{a_1, \cdots, a_n\}$, we write $\langle A \rangle = \langle a_1, \cdots, a_n \rangle$ and say $\langle A \rangle$ is finitely generated.
- If A and B are two subsets of G, we write $\langle A, B \rangle$ instead of $\langle A \cup B \rangle$.

The definition of $\langle A \rangle$ proves existence and uniqueness of the smallest subgroup of G containing A but it is not too enlightening as to how to construct the elements in it. So we define the set which is the closure of A under the group operation and prove this set equals $\langle A \rangle$. Let

$$\overline{A} = \{a_1^{\epsilon_1} a_2^{\epsilon_2} \cdots a_n^{\epsilon_n} : n \in \mathbb{Z}, n \geq 0, a_i \in A, \epsilon = \pm 1\},$$

where $\overline{A} = \{1\}$ if $A = \varnothing$. Then $\overline{A}$ is the set of all finite products (called *words*) of elements A and inverses of elements of A. Note that the a_i's need not be distinct. So a^2 is written as aa in the notation defining $\overline{A}$.

Proposition 1.8.4
$\overline{A} = \langle A \rangle$.

Proof. See Proposition 9 in section 2.4 [DF03]. □

Example 1.8.5

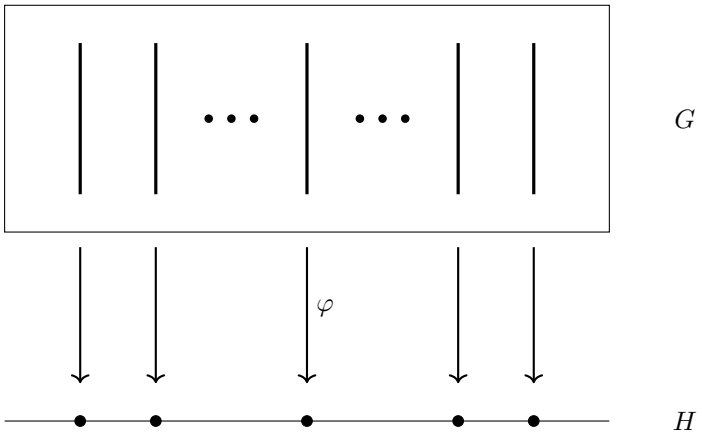
- $D_{2n} = \langle s, r \rangle$.
- If G is abelian and A is a subset of G, then

$$\langle A \rangle = \{a_1^{\alpha_1} \cdots a_n^{\alpha_n} : \{a_1, \cdots, a_n\} \subset A, \alpha_i \in \mathbb{Z}\}.$$

1.9 Quotient Groups and Homomorphisms

Let a group G be given. We show that there is a "smaller" group induced from G. a subgroup of G. In this chapter, we will construct another smaller group, say a *quotient* group of G.

Let $\varphi : G \to H$ be a homomorphism. For each $y \in H$, the inverse image of $\{y\}$ via φ is called the *fiber* of φ at y.



Proposition 1.9.1
Let $X_a = \varphi^{-1}(\{a\})$. Then $\mathcal{X} = \{X_a : a \in H\}$ is a partition of G.

Proof. Left as an exercise. □

To define a quotient group, we should an operation on subsets.

Definition 1.9.2
Let A and B be subsets of G. Define $AB = \{ab : a \in A, b \in B\}$.

Define an operation on $\mathcal{X}$ by $X_a \cdot X_b = X_{ab}$. This operation is well defined because :

- Let $g_a \in X_a$ and $g_b \in X_b$, $\varphi(g_a g_b) = \varphi(g_a)\varphi(g_b) = ab$. Then $g_a g_b \in X_{ab}$.

$$X_a \cdot X_b \subset X_{ab}$$

- Conversely, let $g \in X_{ab}$. Let $h \in X_a$. Then $\varphi(h^{-1}g) = (\varphi(h))^{-1}\varphi(g) = a^{-1}(ab) = b$. So $h^{-1}g \in X_b$.

$$X_a \cdot X_b \supset X_{ab}$$

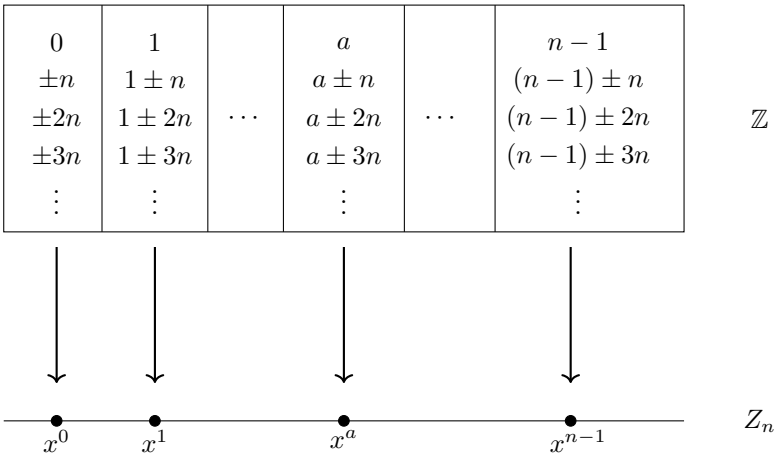
Furthermore, $X_{a^{-1}} = \{g^{-1} : g \in X_a\}$. So we can define $(X_a)^{-1} = X_{a^{-1}}$.

Finally, $(X_aX_b)X_c = (X_{ab})X_c = X_{(ab)c} = X_{a(bc)} = X_a(X_{bc}) = X_a(X_bX_c)$. So we can give a group structure on $\mathcal{X}$ induced from $\times_G$.

Remark 1.9.3
$x, y \in X_a$ if and only if $y^{-1}x \in \ker\varphi$. So for any $x \in G$, $[x] = X_{\varphi(x)}$. And $[x] = [y]$ if and only if $y^{-1}x \in \ker\varphi$. Hence we can write $\mathcal{X} = G/\ker\varphi$.

Example 1.9.4
Let $\varphi : \mathbb{Z} \to Z_n = \langle x \rangle$ by $\varphi(a) = x^a$. Then φ is a homomorphism. The fiber of φ over x^a is

$$\begin{aligned}\varphi^{-1}(x^a) &= \{m \in \mathbb{Z} : x^m = x^a\} = \{m \in \mathbb{Z} : x^(m-a) = x^1\} \\ &= \{m \in \mathbb{Z} : m - a \in \ker\varphi\} \\ &= \{m \in \mathbb{Z} : m \equiv a \mod n\} = \overline{a}.\end{aligned}$$



Definition 1.9.5
Let $\varphi : G \to H$ be a homomorphism with kernel K. The *quotient group* G/K (read G *modulo* K or simply G *mod* K), is the group whose elements are the fiber of φ with group operation defined above.

Proposition 1.9.6
Let $\varphi : G \to K$ be a homomorphism of groups with kernel K. Let $X \in G/K$ be the fiber above a. Then

(a) For any $u \in X$, $X = \{uk : k \in K\} = uK$.

(b) For any $u \in X$, $X = \{ku : k \in K\} = Ku$.

Proof. It suffices to show (1).

Let $k \in K$.

$$\varphi(uk) = \varphi(u)\varphi(k) = a.$$

So $uK \subset X$.

Let $g \in X$ and let $k = u^{-1}g$.

$$\varphi(k) = \varphi(u^{-1})\varphi(g) = \varphi(u)^{-1}\varphi(g) = a^{-1}a = 1.$$

Thus $k \in K$, or $X \subset uK$. □

Definition 1.9.7
For any $N \leq G$ and $g \in G$, let

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

called respectively a *left coset* and a *right coset* of N in G. Any element of a coset is called a *representative* for the coset.

Theorem 1.9.8
Let G be a group and let K be the kernel of some homomorphism from G to another group. Then the set whose elements are the left cosets of K in G with operation defined by

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

forms a group, G/K. In particular, this operation is well defined in the sense that if u_1 is any element in uK and v_1 is any element in vK, then $u_1v_1 \in uvK$, i.e. $u_1v_1K = uv = K$ so that the multiplication does no depend on the choice of representatives for the cosets. The same statement is true with "right coset" in place of "left coset."

Proof. Left as an exercise. □

Example 1.9.9

- For $n \in \mathbb{Z}$, let $\phi_n : \mathbb{Z} \to \mathbb{Z}$ by $\phi_n(x) = nx$. Then $\ker \phi_n = n\mathbb{Z}$, so $\mathbb{Z}/\ker \phi_n = \mathbb{Z}/n\mathbb{Z} = Z_n$.
- If $\varphi : G \to H$ is an isomorphism, then $K = 1$. So $G/1 \cong G$.
- Let G be any group and let $H = 1$. Then $\varphi : G \to H$ by $\varphi(g) = 1$ is the *trivial homomorphism*. Then $\ker \varphi = G$ and so $G/G = Z_1 = 1$.

By propostion 1.9.8, if K is a subgroup of a group G which is the kernel of some homomorphism, then G/K forms a group. This raises the question of whether it is possible to define the quotient group G/N simiarly for an subgroup N of G. The answer is no in general because this multiplication is not in general well defined.

Proposition 1.9.10
Let N be any subgroup of G. Then set of left cosets of N in G form a partition of G. Furthermore,

- for all $u, b \in G$, $uN = vN$ if and only if $v^{-1}u \in N$,
- in particular, $uN = vN$ if and only if u and v are representatives of the same coset.

Proof. Left as an exercise. □

Proposition 1.9.11
Let G be a group and let N be a subgroup of G.

(1) The operation on the set of left cosets of N in G described by

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

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

(2) If the above operation is well defined, then it makes the set of left cosets on N in G into a group. In particular the identity of this group G/N is the coset N and the inverse of gN is the coset $g^{-1}N$, i.e. $(gN)^{-1} = g^{-1}N$.

Proof. (1) Assume first that this operation is well defined, that is, for all $u, v \in G$,

$$\text{if } u, u_1 \in uN \text{ and } v, v_1 \in vN \text{ then } uvN = u_1v_1N.$$

Let $g \in G$ and $n \in N$. Letting $u = 1$, u_1 and $v = v_1 = g^{-1}$ and applying the assumption above we deduce that

$$1g^{-1}N = ng^{-1}N \text{ i.e., } g^{-1}N = ng^{-}1N.$$

Since $1 \in N$, $ng^{-1} \cdot 1 \in ng^{-1}N$. Thus $ng^{-1} \in g^{-1}N$, hence $ng^{-1} = g^{-1}n_1$, for some $n_1 \in N$. Multiplying both sides on the left by g gives $gng^{-1} = n_1 \in N$, as claimed.

Conversely, assume $gng^{-1}N$ for all $g \in G$ and $n \in N$. To prove the operation stated above is well defined, let $u, u_1 \in uN$ and $v, v_1 \in vN$. We may write

$$u_1 = un \text{ and } v_1 = vm, \text{ for some } n, m \in N.$$

$$u_1v_1 = (un)(vm) = u(vv^{-1})nvm = (uv)(v^{-1}nv)m = (uv)(n_1m),$$

where $n_1 = v^{-1}nv = (v^{-1})n(v^{-1})^{-1}$ is an element of N by assumption. Now N is closed under products, so $n_1m \in N$. Thus

$$u_1v_1 = (uv)n_2 \text{ for some } n_1 \in N.$$

Thus the left cosets uvN and u_1v_1N contain the common element u_1v_1. By the preceding proposition they are equal. This proves that the operation is well defined. □

Definition 1.9.12

(1) The element gng^{-1} is called the *conjugate* of $n \in N$ by g.

(2) The set $gNg^{-1} = \{gng^{-1} : n \in N\}$ is called the *conjugate* of N by g.

(3) The element g is said to *normalize* N if $gNg^{-1} = N$.

(4) A subgroup N of G is called *normal* if every element of G normalizes N, i.e., if $gNg^{-1} = N$ for all $g \in G$.

(5) If N is a normal subgroup of G we shall write $N \trianglelefteq G$.

Remark 1.9.13
Suppose $H \trianglelefteq G$ and $K \trianglelefteq H$. H may not be a normal subgroup of G.

For example, let $G = S_4$ and $A_4 \leq S_4$ (the alternating group of degree 4, see [DF03] section 3.5) and $H = \{1, (12)(34), (13)(24), (14)(23)\}$. Then $H \trianglelefteq A_4$ and $A_4 \trianglelefteq S_4$ but $H \not\trianglelefteq S_4$.

Theorem 1.9.14
Let N be a subgroup of the group G. The following are equivalent:

(1) $N \trianglelefteq G$

(2) $N_G(N) = G$

(3) $gN - Ng$ for all $g \in G$

(4) the operation on left cosets of N in G described in Proposition 1.9.11 makes the set of cosets into a group

(5) $gNg^{-1} \subset N$ for all $g \in G$.

Proposition 1.9.15
A subgroup N of the group G is normal if and only if it is the kernel of some homomorphism.

Proof. If N is the kernel of the homomorphism φ, then the left cosets of N are the sme as the right cosets of N. So N is a normal subgroup.

Conversely, if $N \trianglelefteq G$, let $H = G/N$ and define $\pi : G \to G/N$ by

$$\pi(g) = gN.$$

By definition of the operation in G/N,

$$\pi(g_1 g_2) = (g_1 g_2)N = (g_1 N)(g_2 N) = \pi(g_1)\pi(g_2).$$

So π is a homomorphism. Now

$$\begin{aligned} \ker \pi &= \{g \in G : \pi(g) = N\} \\ &= \{g \in G : gN = N\} \\ &= \{g \in G : g \in N\} = N. \end{aligned}$$

□

Definition 1.9.16
Let $N \trianglelefteq G$.

(1) The homomorphism $\pi : G \to G/N$ defined by $\pi(g) = gN$ is called the *natural projection (homomorphism)* of G onto G/N (or the *canonical projection*).

(2) If $\overline{H} \leq G/N$ is a subgroup of G/N, the *complete preimage* of $\overline{H}$ in G is the preimage of $\overline{H}$ under the natural projection homomorphism.

The complete preimage of a subgroup of G/N is a subgroup of G.

Example 1.9.17
Let G be a group.

(1) The subgroups 1 and G are always normal in G; $G/1 \cong G$ and $G/G \cong 1$.

(2) If G is an abelian group, any subgroup of N of G is normal.

(3) A quotient groups of a cyclic group are cyclic.

(4) If $N \leq Z(G)$, then $N \trianglelefteq G$.

1.10 Lagrange's Theorem

Theorem 1.10.1 (Lagrange's Theorem)
If G is a finite group and H is a subgroup of G, then the order of H divides the order of G (i.e. $|H|||G|$) and the number of left cosets of H in G equals $\dfrac{|G|}{|H|}$.

Proof. Let $|H| = n$ and let the number of left cosets of H in G eqaul k. Let $g \in G$ and define $\varphi_g : H \to gH$ by $\varphi_g(h) = gh$. φ_g is a bijective. So $|H| = |gH|$ for all $g \in G$. Since G is partitioned into k disjoint subsets each of which has cardinality n, $|G| = kn$. Thus $k = \dfrac{|G|}{n} = \dfrac{|G|}{|H|}$. □

Definition 1.10.2
If G is a group (possibly infinite) and $H \leq G$, the number of left cosets of H in G is called the *index* of H in G and is denoted by $|G : H|$.

Corollary 1.10.3
If G is a finite group and $x \in G$, then the order of x divides the order of G. In particular $x^{|G|} = 1$ for all $x \in G$.

Proof. Recall that $|x| = |\langle x \rangle|$ and $\langle x \rangle \leq G$. □

Corollary 1.10.4
If G is a group of prime order p, then G is cyclic, hence $G \cong Z_p$.

Proof. Let $x \in G$, $x \neq 1$. Thus $|\langle x \rangle| > 1$ and $|\langle x \rangle|$ divides $|G|$. Since $|G|$ is prime, we must have $|\langle x \rangle| = absG$, hence $G = \langle x \rangle$ is cyclic. □

Definition 1.10.5
Let H and K be subgroups of a group and define

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

Proposition 1.10.6
If H and K are finite subgroups of a group then

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

Proof. Notive that HK is a union of left cosets of K,

$$HK = \bigcup_{h \in H} hK.$$

Since each coset of K has $|K|$ elements it suffices to find the number of distinct left cosets of the form hK, $h \in H$. But $h_1K = h_2K$ for $h_1, h_2 \in H$ if and only if $h_2^{-1}h_1 \in K$. Thus

$$h_1K = h_2 \iff h_2^{-1}h_1 \in H \cap K \iff h_1(H \cap K) = h_2(H \cap K).$$

Thus the number of distinct cosets of the form hK, for $h \in H$ is the number of distinct cosets $h(H \cap K)$, for $h \in H$. Thus HK consists of $\dfrac{|H|}{|H \cap K|}$ distinct cosets of K. □

Proof. If H and K are subgroups of a group, HK is a subgroup if and only if $HK = KH$. □

Proof. Assume $HK = KH$ and $a, b \in HK$. Let $a = h_1k_1$ and $b = h_2k_2$, for some $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Thus $b^{-1} = k_2^{-1}h_2^{-1}$, so $ab^{-1} = h_1k_1k_2^{-1}h_2^{-1}$. Let $k_3 = k_1k_2^{-1} \in K$ and $h_3 = h_2^{-1}$. So $ab^{-1} = h_1k_3h_3$. Since $HK = KH$, $k_3h_3 = h_4k_4$ for some $h_4 \in H$ and $k_4 \in K$. Thus $ab^{-1} = h_1h_4k_4$, so $ab^{-1} \in HK$.

Conversely, assume HK is a subgroup of G. Since $K \leq HK$ and $H \leq HK$, $KH \subset HK$. Let $hk \in HK$. Since HK is a subgroup, write $hk = a^{-1}$ for some $a \in HK$. If $a = h_1k_2$, then

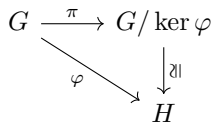
$$hk = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH.$$

□

Corollary 1.10.7
If H and K are subgorups of G and $H \leq N_G(K)$, then HK is a subgrou of G. In particular, if $K \trianglelefteq G$, then $HK \leq G$ for any $H \leq G$.

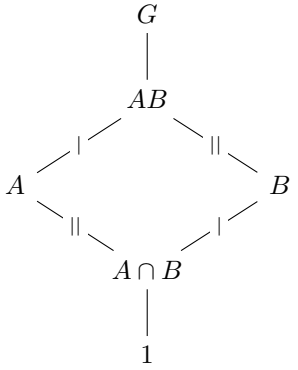
1.11 The Isomorphism Theorems

Theorem 1.11.1 (The First Isomorphism Theorem)
If $\varphi : G \to H$ is a homomorphism groups, then $\ker \varphi \trianglelefteq G$ and $G/\ker \varphi \cong \varphi(G)$.



Corollary 1.11.2
Let $\varphi : G \to H$ be a homomorphism of groups. Then φ is injective if and only if $\ker \varphi = 1$

Theorem 1.11.3 (The Second Isomorphism Theorem)
Let G be a group, let A and B subgroups of G and assume $A \leq N_G(B)$. Then AB is a subgroup of G, $B \trianglelefteq AB$ and $A \cap B \trianglelefteq A$ and $AB/B \cong A/A \cap B$.



Theorem 1.11.4 (The Third Isomorphism Theorem)
Let G be a group and H and K be normal subgroups of G with $H \leq K$. Then $K/H \trianglelefteq G/K$ and

$$(G/H)/(K/H) \cong (G/K).$$

Theorem 1.11.5 (The Fourth Isomorphism Theorem)
Let G be a group and let N be a normal subgroup of G. Then there is a bijective from the set of subgroups of G which contain N onto the set of subgroups $\overline{A} = A/N$ of G/N.

$$\{A \leq G : N \subset A\} \longleftrightarrow \{A/N \leq G/N\}.$$

In particular, every subgroup of $\overline{G} = G/N$ is of the form A/N for some subgroup A of G containing N. This bijection has the following properties: for all $A, B \leq G$ with $N \leq A$ and $N \leq B$,

(1) $A \leq B$ if and only if $\overline{A} \leq \overline{B}$,

(2) if $A \leq B$, then $|B : A| = \left|\overline{B} : \overline{A}\right|$,

(3) $\overline{\langle A, B\rangle} = \left\langle \overline{A}, \overline{B}\right\rangle$,

(4) $\overline{A \cap B} = \overline{A} \cap \overline{B}$, and

(5) $A \trianglelefteq G$ if and only if $\overline{A} \trianglelefteq \overline{G}$.

1.12 Direct Products and direct sums

Definition 1.12.1

(1) The *direct product* of $G_1 \times G_2 \times \cdots G_n$ of the groups $G_1, \cdots G_n$ with operations $\star_1, \star_2, \cdots, \star_n$, respectively, is the set of n-tuples $(g_1, g_2, \cdots, g_n)$ where $g_i \in G_i$ with operation defined componentwise:

$$(g_1, g_2, \cdots, g_n) \star (h_1, h_2, \cdots, h_n) = (g_1 \star_1 h_1, g_2 \star_2 h_2, \cdots, g_n \star_n h_n).$$

(2) Similarly, let $\{G_i\}$ be a collection of groups with index set I, the *direct product* $\prod_{i \in I} G_i$ is the set of all choice functions with opertaion defined componentwise:

$$(g_i)_{i \in I} \star (h_i)_{i \in I} = (g_i \star_i h_i)_{i \in I}.$$

Definition 1.12.2
Let $\{G_i\}$ be a collection of groups with index set I and let $G = \prod_{i \in I} G_i$. Let H be the set of all choice function f such that

$$f(i) = 1_i \text{ for all but only finitely many } i\text{'s},$$

i.e., for any $f \in H$, $f(i) \neq i$ for only finitely many i's. Then H is a subgroup of G and is called the *direct sum*.

Note that if J is finite, the direct product and the direct sum equal.

2 Rings

2.1 Introduction to Rings

Definition 2.1.1(1) A *ring* R is a set together with two binary operations $+$ and $\times$ (called addition and multiplication) satisfying the following axtioms:

(i) $(R, +)$ is an abelian group,

(ii) $\times$ is associative : $(a \times b) \times c = a \times (b \times x)$ for all $a, b, c \in R$,

(iii) the *distributive laws* hold in R : for all $a, b, c \in R$

$$(a + b) \times c = (a \times c) + (b \times c) \text{ and } a \times (b + c) = (a \times b) + (a \times c).$$

(2) The ring R is *commutative* if multiplication is commutative.

(3) The ring R is said to have an *identity* (or *contain* a 1) if there is an element $1 \in R$ with

$$1 \times a = a \times 1 = a \text{ for all } a \in R.$$

We shall usually write simply ab rather than $a \times b$. The additive identity of R will always be denoted by 0 (and called the *zero*) and the additive inverse of the ring element a will be denoted by $-a$.

If $1 \in R$, 1 is sometimes called the *unity*.

Remark 2.1.2
Suppose $1 \in R$ and let $a, b \in R$. We can compute $(1 + 1)(a + b)$ in two different wways,

$$(1 + 1)(a + b) = 1(a + b) + 1(a + b) = a + b + a + b$$
$$(1 + 1)(a + b) = (1 + 1)a + (1 + 1)b = a + a + b + b.$$

Thus we get $a + b = b + a$. This is the reason that $(R, +)$ have to be an abelian group to be a ring R.

Definition 2.1.3(1) A ring R with identity 1, where $1 \neq 0$, is called a *division ring* (or *skew filed*) if every nonzero element $a \in R$ has a multiplicative inverse, i.e., there exists $b \in R$ such that $ab = ba = 1$.

(2) A commutative division ring is called a *field*.

Example 2.1.4

(1) The *trivial rings* obtained by taking R to be any commutative group and defining the multiplication $\times$ on R by $a \times b = 0$ for all $a, b \in R$. In particular, if $R = \{0\}$ is the trivial group, the resulting ring R is called the *zero ring*, denoted $R = 0$. The zero ring has $1 = 0$. Except for the zero ring, a trivial ring does not contain an identity.

(2) $\mathbb{Z}$ under usual operation is a commutative ring with identity 1. Note that under multiplication $\mathbb{Z} - \{0\}$ is not a group.

(3) $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are commutative rings with identity. Moreover, they are fields.

(4) $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring with identity $\overline{1}$. And $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is a prime number.

(5) The (real) Hamilton Quaternions $\mathbb{H}$ is the collection of all elements of the form $a + bi + cj + dk$ where $a, b, c, d \in \mathbb{R}$ and

$$i^2 = j^2 = k^2 = -1, ij = -ji = k, jk = -kj = i, ki = -ik = j.$$

Then $\mathbb{H}$ is a noncommutative division ring. Note that

$$(a + bi + cj + dk)^{-1} = \frac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2}.$$

The quaternions are used in 3D graphics to compute a rotation in $\mathbb{R}^3$.

(6) Let X be any nonempty set and let A be any ring. The collection R of all functions $f : X \to A$ is a ring under the usual definition of pointwise addition and multiplocation of functions

$$(f + g)(x) := f(x) + g(x) \text{ and } (fg)(x) := f(x)g(x).$$

Then

- R is commutative if and only if A is commutative.
- R has a 1 (which is a function $x \mapsto 1$) if and only if A has a 1.

(7) An example of a ring which does not have an identity is the ring $2\mathbb{Z}$ if even integers.

(8) The set of all $n \times n$ matrices with entries from some field (or ring) F, $F^{n\times n}$ or $M_n(F)$, forms a ring under pointwise addition and multiplication defined by

$$(AB)_{ij} = \sum_{k=1}^{n} A_{ik}B_{kj}.$$

Then $M_n(F)$ is a noncommutative ring.

Proposition 2.1.5
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 has an identity 1, the the identity is unique and $-a = (-1)a$.

Proof. Left as an exercise. □

Definition 2.1.6
Let R be a ring.

(1) A nonzero element a of R is called a *zero divisor* if there is a nonzero element b in R such that either $ab = 0$ or $ba = 0$.

(2) Assume R has an identity $1 \neq 0$. An element u of R is called a *unit* in R if there is some $v \in R$ such that $uv = vu = 1$. The set of units in R is denoted $R^\times$.

Remark 2.1.7

(1) A field is a commutative ring with identity $1 \neq 0$ in which every nonzero element is a unit, i.e. $F^\times = F - \{0\}$.

(2) A zero divisor can never be a unit.

(3) For any ring with identity $1 \neq 0$, $R^\times$ forms a group under multiplication.

Example 2.1.8

(1) $\mathbb{Z}$ has no zero divisor and its only units are ± 1.

(2) Let $n \geq 2$ be an integer. In the ring $\mathbb{Z}/n\mathbb{Z}$, the elements $\overline{u}$ for which u and n are relatively prime are units because $\gcd(u, n) = 1$ implies there are $x, y \in \mathbb{Z}$ such that $au + bn = 1$ and then $\overline{a}\overline{u} = \overline{1}$. If a is nonzero integer and is not relatively prime to n with $d = \gcd(a, n)$, then let $b = \dfrac{n}{b}$. By assumption $d > 1$ so $0 < b < n$, i.e. $\overline{b} \neq \overline{0}$. But $\overline{a}\overline{b} = \overline{n} = \overline{0}$. Hence $\overline{a}$ is a zero diviosr.

Definition 2.1.9
A commutative ring with identity $1 \neq 0$ is called an *integral domain* if it has no zero divisors.

Proposition 2.1.10
Assume a, b and c are elements of any ring with a not a zero divisior. If $ab = ac$,then either $a = 0$ or $b = c$. In particular, if a, b, c are any elements in an integral domain and $ab = ac$, then either $a = 0$ or $b = c$.

Thus an integral domain has a cancellation property.

Proof. If $ab = ac$, then $a(b-c) = 0$. Since a is not a zero divisor, either $a = 0$ or $b - c = 0$. □

Corollary 2.1.11
Any finite integral domain is field.

Proof. Let R be a fintie integral domain and let a be a nonzero element of R. By the cancellation law the map $x \mapsto ax$ is an injective function. Since R is finite, this map is also surjective. In particular, there is some $b \in R$ such that $ab = 1$, i.e. a is a unit in R. □

2.2 Subrings

Definition 2.2.1
A *subring* of the ring R is a subgroup of R that is closed under multiplication.

Example 2.2.2

(1) $\mathbb{Z}$ is a subring of $\mathbb{Q}$ and $\mathbb{Q}$ is a subring of $\mathbb{R}$ and $\mathbb{R}$ is a subring of $\mathbb{C}$. The property "is a subring of" is clearly transitive.

(2) $n\mathbb{Z}$ is a subring of $\mathbb{Z}$ for any integer n. This shows that even R has a 1, there may be a subring which does not containing 1. $\mathbb{Z}/n\mathbb{Z}$ is not a subring of $\mathbb{Z}$ for any $n \geq 2$.

(3) If R is a subring of a field F that contains the identity F then R is an integral domain.

(4) Let R be a ring with $1 \neq 0$. Then $R \times R$ forms a ring in a natural way with identity $(1, 1)$

$$\begin{aligned}(a_1, a_2) + (b_1, b_2) &= (a_1 + b_1, a_2 + b_2)\\ (a_1, a_2)(b_1, b_2) &= (a_1 b_1, a_2 b_2)\\ (a, b)(1, 1) &= (1, 1)(a, b) = (a, b).\end{aligned}$$

Then $R \times \{0\}$ is a subring of $R \times R$. Moreover $R \times \{0\}$ has an identity $(1, 0)$

$$(a, 0)(1, 0) = (1, 0)(a, 0) = (a, 0).$$

This shows that if R is a ring with 1_R and S is a subring with 1_S, it may $1_R \neq 1_S$.

2.3 Polynomial Rings, Matrix Rings

Polynomial Rings

Fix a commutative ring R with identity. We define the ring of polynomials. Let x be an indeterminate. The formal sum

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

with $n \geq 0$ and each $a_i \in R$ is called a *polynomial* in x with coefficients a_i in R. If $a_n \neq 0$,

- the the polynomial is said to be of *degee* n,
- $a_n x^n$ is called the *leading term*,
- and a_n is called the *leading coefficient*.
- If $a_n = 1$, the polynomial is called *monic*.

The set of all such polynomials is called the ring of *polynomials in the variable x with coefficients in R* and will be denoted $R[x]$.

The operation of addition and multiplication which make $R[x]$ into a ring are the same operations familiar from elementary algebra

- addition is "componentwise":

$$\begin{aligned}(a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0) + (b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0) \\ = (a_n + b_n) x^n + (a_{n-1} + b_{n-1}) x^{n-1} + \cdots + (a_1 + b_1) x + (a_0 + b_0)\end{aligned}$$

  (a_n or b_0 may be zero in order fo addition of polynomials of different degrees to be defined).

- mutiplication is performed by first defining $(ax^i)(bx^j) = abx^{i+j}$ for polynomials with only one nonzero term (say monomials) and exteding to all polynomials by the distributive laws:

$$\left(\sum_{i=0}^{n} a_i x^i \right) \left(\sum_{j=0}^{m} b_i x^i \right) = \left(\sum_{\substack{k=0 \\ i+j=k}}^{m+n} a_i b_j x^l \right)$$

  where if $i > n$ (resp. $j > m$), $a_i = 0$ (resp. $b_j = 0$).

The ring R appears in $R[x]$ as the *constant polynomials*. Note that by definition of the multiplication, $R[x]$ is a *commutative ring with identity* (the identity 1 from R).

Proposition 2.3.1
Let R be an integral domain and let $p(x)$, $q(x)$ be nonzero elements of $R[x]$. Then

(1) $\deg p(x)q(x) = \deg p(x) + \deg q(x)$,

(2) the units of $R[x]$ are just the units of R, i.e. $(R[x])^\times = R^\times$,

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

Proof. If R has no zero divisors, then neither does $R[x]$. If $p(x)$ and $q(x)$ are polynomials with leading terms $a_n x^n$ and $b_m x^m$, respectively, then the leading term of $p(x)q(x)$ is $a_n b_m x^{m+n}$, and $a_n b_m \neq 0$. This proves (1) and (3).

If $p(x)$ is a unit, say $p(x)q(x) = 1$, then $\deg p(x) + \deg q(x) = 0$, so both $p(x)$ and $q(x)$ are elements of R, hence are units in R. □

Remark 2.3.2
If S is a subring of R, then $S[x]$ is a subring of $R[x]$.

Matrix Rings

Fix an arbitrary ring R and let n be a positive integer. Let $M_n(R)$ be the set of all $n \times n$ *matrices with entries from* R. The element (a_{ij}) of $M_n(R)$ is an $n \times n$ square array of elements of R whose in row i and column j is $a_{ij} \in R$. $M_n(R)$ becomes a ring under the usual rules

- addition is componentwise: $(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij})$.
- multiplication is the matrix product $(ab)_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$.

If R is any nontrivial ring (even a commutative one) and $n \geq 2$, $M_n(R)$ is not commutative. And $M_n(R)$ has zero divisors.

An element (a_{ij}) of $M_n(R)$ is called a *scalar matrix* if for some $a \in R$, $a_{ii} = a$ for all $i = 1, \cdots, n$ and $a_{ij} = 0$ for all $i \neq j$. The set of scalar matrices is a subring of $M_n(R)$. This subring is a copy of R (i.e. is isomorphic to R).

- If R is commutative, then the scalar matrices commute with all elements of $M_n(R)$.
- If R has a 1, then the scalar matrix with 1's down the diagonal, the $n \times n$ identity matrix, is the 1 of $M_n(R)$.
- In this case the units in $M_n(R)$ are the invertible $n \times n$ matrices and the group of units is denoted $GL_n(R)$, the *general linear group* of degree n over R.

If S is a subring of R, then $M_n(S)$ is a subring of $M_n(R)$.

2.4 Ring Homomorphisms and Quotient Rings

Definition 2.4.1
Let R and S be rings.

(a) A *ring homomorphism* is a map $\varphi : R \to S$ satisfying

(i) $\varphi(a + b) = \varphi(a) + \varphi(b)$ (φ is a group homomorphism on the additive groups),

(ii) $\varphi(ab) = \varphi(a)\varphi(b)$ (φ is multiplicative).

(b) The *kernel* of the ring homomorphism φ, denoted $\ker \varphi$, is the set of elements of R that map to 0 in S.

(c) A bijective ring homomorphism is called an *isomorphism*.

Example 2.4.2

(1) $\varphi : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ by $\varphi(n) = \overline{n}$ is a ring homomorphism.

(2) For $n \in \mathbb{Z}$, $\varphi_n : \mathbb{Z} \to \mathbb{Z}$ by $\varphi_n(x) = nx$ are not in general ring homomorphism because $\varphi_n(x) = nxy$ whereas $\varphi_n(x)\varphi)n(y) = n^2xy$. Hence φ_n is a ring homomorphism only when $n^2 = n$, i.e. $n = 0$ or $n = 1$.

Proposition 2.4.3
Let R and S be rings and let $\varphi : R \to S$ be a homomorphism.

(1) The image of φ is a subring of S.

(2) The kernel of φ is a subring of R. Furthermore, if $\alpha \in \ker \varphi$, then $r\alpha$ and $\alpha r \in \ker \varphi$ for every $r \in R$.

Proof. Left as an exercise. □

Let $\varphi : R \to S$ be a ring homomorphism with kernel I. Since R and S are in particular additive abelian groups, φ is in particular a homomorphism of abelian groups and the fibers of φ are the additive cosets $r + I$ of the kernel I. These fibers have the structure of a ring naturally isomorphic to the image of φ:
if X is the fiber over $a \in S$ and Y is the fiber over $b \in S$, then

- $X + Y$ is the fiber over $a + b$,
- XY is the fiber over ab.

In terms of cosets of the kernel I,

$$(r + I) + (s + I) := (r + s) + I$$
$$(r + I) \times (s + I) := (rs) + I.$$

This ring of cosets is called the *quotient ring* of R by I.

Since R is an abelian additive group, the subgroup I is necessarily normal so that the quotient R/I of cosets of I is automatically an additive group. The question is whether this quotient group also has a multiplicative structure induces from the multiplication of R. The answer is no in general, which leads to the notion of an *ideal* of R.

Definition 2.4.4
Let R be a ring, let I be a subset of R and $r \in R$.

(1) $rI = \{ra : a \in I\}$ and $Ir = \{ar : a \in I\}$.

(2) A subset I of R is a *left ideal* (resp.*right ideal*) of R is

  (i) I is a subring of R,

  (ii) I is closed under left (resp. right) multiplication by element from R, i.e.

$$rI \subset I (\text{resp. } Ir \subset I), \text{ for all } r \in R$$

.

(3) A subset I that is both a left ideal and a right ideal is called an *ideal* of R.

Remark 2.4.5
Let $r, s \in R$ and $\alpha, \beta \in I$.

$$(r+\alpha)(s+\beta) = rs + r\beta + \alpha s + \alpha\beta \in rs + rI + Is + I = rs + I.$$

So $(r+I)(s+I) = (rs) + I$ is well- defined.

Proposition 2.4.6
Let R be a ring and let I be an ideal of R. Then the quotient group R/I is a ring under the binary operations:

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

Conversely, if I is any subgroup such that the above operations are well defined, then I is an ideal of R.

In this case, R/I is called the *quotient ring* of R by I.

Theorem 2.4.7

1. (*The First Isomorphism Theorem for Rings*) If $\varphi : R \to S$ is a homomorphism is rings, then the kernel of φ is an ideal of R, the image of φ is a subring of S and $R/\ker\varphi$ is isomorphic to $\operatorname{img}\varphi$.

2. If I is any ideal of R, then the map

   $$R \to R/I \text{ defined by } r \mapsto r + I$$

   is a surjective ring homomorphism with kernel I. Thus every idel is the kernel of a ring homomorphism and vice versa.

Proof. Left as an exercise. □

Example 2.4.8
Let R be a ring.

(1) The subring R and $\{0\}$ are ideals. An ideal I is *proper* if $I \neq R$. The ideal $\{0\}$ is called the *trivial ideal* and is denoted by 0.

(2) $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

(3) Let $R = \mathbb{Z}[x]$. Let I be the collection of polynomials whose terms of degree at least 2 together with the zero polynomial. Then I is an ideal.

Two polynomials $p(x), q(x)$ are in the same coset of I if and only if $p(x) - q(x) \in I$.

Note that in R/I, $\overline{x}\overline{x} = \overline{x^2} = \overline{0}$, so that R/I has zero divisors, even though $R = Z[x]$ does not.

(4) Let A be a ringm let X be any nonempty set and let R be the ring of all functions from X to A. For each fixed $c \in X$ the map

$$E_c : R \to A \text{ defined by } E_c(f) = f(c)$$

(called *evaluation at c*) is a ring homomorphism. The kernel of E_c is given by $\{f \in R : f(c) = 0\}$. Also, E_c is surjective : given $a \in A$, there is an constant function $f(x) = a$. Thus $R/\ker E_c \cong A$.

Theorem 2.4.9
Ler R be a ring.

(1) (*The Second Isomorphism Theorem for Rings*) Let A be a subring and let B be an ideal of R. Then $A + B = \{a + b : a \in A, b \in B\}$ is a subring of R and $A \cap B$ is an ideal of A and $(A + B)/B \cong A/(A \cap B)/$

(2) (*The Third Isomorphism Theorem for Rings*) Let I and J be ideals of R with $I \subset J$. Then J/I is an ideal of R/I and $(R/I)/(J/I) \cong R/J$.

(3) (*The Fourth Isomorphism Theorem for Rings*) Let I be an ideal of R. THe correspondence $A \longleftrightarrow A/I$ is an inclusion preserving bijection between the set of subrings A of R that contain I and the set of subrings of R/I. Furthermore, A (a subring containing I) is an ideal of R if any only if A/I is an ideal of R/I.

Definition 2.4.10
Let I and 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, denoted by IJ, to be the set of all finite sums of elements of the form ab with $a \in I$ and $b \in J$

$$IJ = \{\sum_{i=1}^{n} a_i b_i : n \in \mathbb{Z}_+, a_i \in I, b_i \in J\}.$$

(3) For any $n \geq 1$, define the n^{th} *power* of I, denoted by I^n, to be the set consisting of all finite sums of elements of the form $a_1 a_2 \cdots a_n$ with $a_i \in I$ for all i. Equivalently, I^n is defined inductively by $I^1 = I$, and $I^n = II^{n-1}$ for $n = 2, \cdots$.

2.5 Properties of Ideals

Throughout this section R is a ring with identity $1 \neq 0$.

Definition 2.5.1
Let A be any subset of the ring R.

(1) Let (A) denote the smallest ideal of R containing A, called *the ideal generated by A*.

(2) Let RA denote the set of all finite sums of elements of the form ra with $r \in R$ and $a \in A$, i.e.

$$RA = \{r_1 a_1 + r_2 a_2 + \cdots + r_n a_n : r_i \in R, a_i \in A, n \in \mathbb{Z}+\}$$

(where the convention is $RA = 0$ if $A = \varnothing$).

Similarly

$$AR = \{a_1 r_1 + a_2 r_2 + \cdots + a_n r_n : r_i \in R, a_i \in A, n \in \mathbb{Z}^+\}$$
$$RAR = \{r_1 a_1 r_1' + r_2 a_2 r_2' + \cdots + r_n a_n r_n : r_i, r_i' \in R, a_i \in A, n \in \mathbb{Z}^+\}$$

(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*.

Remark 2.5.2

1. (A) is the intersection of all ideals containing A, i.e.
$$A = \bigcap_{\substack{I \text{ an ideal} \\ A \subseteq I}} I.$$
2. In general $RA \neq AR$.
3. If R is commutative, then $RA = AR = RAR = (A)$.
4. If I is a finitely generated left(resp. right) ideal with generator $\{a_1, \cdots, a_n\}$, then $I = Ra_1 + Ra_2 + \cdots Ra_n$ (resp. $I = a_1R + a_2R + \cdots a_nR$).

Example 2.5.3

1. Every ring R is itself an principal ideal, i.e. $R = (1)$.
2. Let $R = \mathbb{Z}$. We will show that every ideal of $\mathbb{Z}$ is principal.

   Let I be an ideal of $\mathbb{Z}$. If $I = \mathbb{Z}$, $I = (1)$. Suppose I is a proper ideal. Let $A = \{|a| : a \in I - \{0\}\}$. Then A is a subset of $\mathbb{Z}^+$. Let $n = \min A$. Note that $n > 1$. By the definition of an ideal, $(n) \subset I$. Let $m \in I$.

   Claim) m is a multiple of n.

   Suppose not. Then by the division algorithm, there are $a, b \in \mathbb{Z}$ such that $an + bm = \gcd(m, n)$ where $0 < \gcd(m, n) < n$. Since an ideal is closed under addition and multiplication over $\mathbb{Z}$, $an + bm \in I$, or $\gcd(m, n) \in I$. It contradicts the minimality of n. Thus m is a multiple of n, or $m \in (n)$. Hence $(n) = I$.
3. Let $R = \mathbb{Z}[x]$. Then $(2, x)$ is not a principal ideal.

Proposition 2.5.4
Let I be an ideal of R.

(1) $I = R$ if and only if I contains a unit.

(2) Assume R is commutative. Then R is a field if and only if its only ideals are 0 and R.

Proof. (1) If $I = R$, I contanins 1. Conversely if u is a unit in I with inverse v, them for any $r \in R$,
$$r = r \cdot 1 = r(vu) = (rv)u \in I$$
hence $I = R$.

(2) The ring R is a field if and only if every nonzero element is a unit. If R is a field, every nonzero ideal contains a unit, so R is the only nonzero ideal. Conversely, if 0 and R the only ideals of R, let u be any nonzero element of R. By hypothesis, $(u) = R$ and so $1 \in (u)$. Thus there is some $v \in R$ such that $1 = vu$. Hence u is a unit, and R is a field. □

Corollary 2.5.5
If R is a field, then any nonzero ring homomorphism from R into another ring is an injection.

Proof. Recall that the kernel of a ring homomorphism is an ideal. □

Definition 2.5.6
An ideal M in an arbitrary ring S is called a *maximal ideal* if $M \neq S$ and the only ideals containing M are M and S.

Proposition 2.5.7
In a ring with identity every proper ideal is contanined in a maximal ideal.

Proof. The main idea of this proof is that make a partial ordered collection and apply Zorn's lemma.

Let R be a ring with identity and let I be a proper ideal. Let $\mathcal{S}$ be the set of all proper ideals of R which contain I. Then $\mathcal{S}$ is nonempty and is partially ordered by inclusion. If $\mathcal{C}$ is a chain in $\mathcal{S}$, define J to be the union of all ideals in $\mathcal{C}$:

$$J = \bigcup_{A \in \mathcal{C}} A.$$

Claim 1) J is an ideal.

Since 0 is in every ideal A, $0 \in J$. If $a, b \in J$, there are ideals $A, B \in \mathcal{C}$ such that $a \in A$ and $b \in B$. By definition of a chain either $A \subseteq B$ or $B \subseteq A$. In either case $a - b \in J$, so J is closed under subtraction. By the criterion for subgroup, J is a subgroup under addition. Also, since each $A \in \mathcal{C}$ is closed under left and right multiplication by elements of R, so is J. Hence J is an ideal.

Claim 2) J is a proper ideal. So $J \in \mathcal{S}$ and J is an upper bound of $\mathcal{C}$.

Suppose not. Then $1 \in J$. By definition of J, there is some $A \in \mathcal{C}$ such that $1 \in A$. But A is a proper ideal, so $1 \notin A$ (contradiction).

Now apply Zorn's lemma on $\mathcal{S}$ and we get a proper ideal M which is maximal under inclusion. Then M is a maximal ideal. □

Proposition 2.5.8
Assume R is commutative. The ideal M is a maximal ideal if and only if the quotient ring R/M is a field.

Proof. This follows from the fourth isomorphism theorem together with Proposition 2.5.4.

The ideal M is maximal if and only if there are no ideals I with $M \subsetneq I \subsetneq R$. By the fourth isomorphism theorem, the ideals of R containing M correspond bijectively with the ideals of R/M, so M is maximal if and only if the only ideals of R/M are 0 and R/M. By Proposition 2.5.4, we see that M is maximal if and only if R/M is a field. □

Using above proposition, we can *construct* some fields.

Example 2.5.9

(1) Let n be a nonnegative integer. The ideal $n\mathbb{Z}$ of $\mathbb{Z}$ is a maximal ideal if and only if $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is a prime number.

(2) The ideal $(2, x)$ is a maximal ideal in $\mathbb{Z}[x]$. Note that $\mathbb{Z}[x]/(2, x) \cong \mathbb{Z}/2\mathbb{Z}$ is a field.

Definition 2.5.10
Assume R is commutative. An ideal P is called a *prime ideal* if $P \neq R$ and whenever the product ab of two elements $a, b \in R$ is an element of P, then at least one of a and b is an element of P.

Proposition 2.5.11
Assume R is commutative. Then the ideal P is a prime ideal in R if and only if the quotient ring R/P is an integral domain.

Proof. Recall that P is prime if and only if $P \neq R$ and whenever $ab \in P$ then either $a \in P$ or $b \in P$. Let $\overline{r} = r + P$ for $r \in R$.

- $r \in P$ if and only if $\overline{r} = \overline{0} \in R/P$.
- Thus P is a prime ideal if and only if $R/P \neq \overline{0}$ and whenever $\overline{ab} = \overline{0}$ then either $\overline{a} = \overline{0}$ or $\overline{b} = \overline{0}$, i.e. R/P is an integral domain.

□

Corollary 2.5.12
Assume R is commutative. Every maximal ideal of R is a prime ideal.

Proof. If M is maximal, then R/M is a field, so it is a integral domain. □

3 Modules

3.1 Introduction to Modules

Definition 3.1.1
Let R be a ring (not necessarily commutative nor with 1). A *left R-module* or a *left module over R* is a set M together with

(1) a binary operation $+$ on M under which M is an abelian group

(2) a map $R \times M \to M$ denoted by rm, for all $r \in R$ and for all $m \in M$ which satisfies

(a) $(R + s)m = rm + sm$, for all $r, s \in R$, $m \in M$,

(b) $(rs)m = r(sm)$, for all $r, s \in R$, $m \in M$,

(c) $r(m + n) = rm + rn$, for all $r \in R$, $m, n \in M$.

If the ring R has a 1 we impose the additional axiom:

(d) $1m = m$ for all $m \in M$.

We can define a *right R-module* analogously. If the ring R is commutative and M is a left R-module, we can make M into a right R-module by defining $mr = rm$ for $m \in M$ and $r \in R$. Unless explicitly mentioned otherwise the term "module" will always mean "left module". Modules satisfying axiom 2(d) are called *unital* modules and in this paper all modules will be unital.

When R is a field F the axtioms for an R-module are precisely the same as those for a vector space over F, so that

modules over a field F and vector spaces over F are the same.

Definition 3.1.2
Let R be a ring and let M be an R-module. An *R-submodule* of M is a subgroup N of M and the image of the map of $R \times N \to M$ is contained in N, i.e.

$$rn \in N \text{ for all } r \in R, n \in N.$$

Example 3.1.3

(1) Every R-module M has the two submodules M and 0. 0 is called the *trivial submodule.*

(2) Let R be any ring. Then $M = R$ is a left R-module, where rm is just usual multiplication in the ring R. Similarly R is a right module over itself. When R is considered as a left module over itself, the submodules of R are precisely the left ideals of R. Thus if R is not commutative, it has a left and right module structure over itself and these structures may be different.

(3) Let R be a ring with 1 and let $n \in \mathbb{Z}^+$. Define

$$R^n = \{(a_1, \cdots, a_n)" a_i \in R, \text{ for all } i\}.$$

Make R^n into an R-module by componentwise addition and multiplication. The module R^n is called *the free module of rank n over R.*

(4) If M is an R-module and for some (2-sides) ideal I of R, $am = 0$ for all $a \in I$ and all $m \in M$, we say M is *annihilated by* I. In this situation we can make M into an (R/I)-module by defining the multiplication of R/I on M as follows: for each $m \in M$ and coset $r + I$ in R/I let

$$(r + I)m = rm.$$

Since $am = 0$ for all $a \in I$ and all $m \in M$, this is well defined and one easily checks that it makes M into an (R/I)-module.

The next example is of sufficient importance as to be singled out.

Example 3.1.4 ($\mathbb{Z}$-modules)
Let $R = \mathbb{Z}$, let A be any abelian group (finite or infinite) and write the operation of A as $+$. Make A into a $\mathbb{Z}$-module as follows: for any $n \in \mathbb{Z}$ and $a \in A$ define

$$na = \begin{cases} a + a + \cdots + a \ (n \text{ times}) & \text{if } n > 0 \\ 0 & \text{if } n = 0 \\ -a - a - \cdots - a \ (-n \text{ times}) & \text{if } n < 0 \end{cases}$$

This definition on A makes A into a $\mathbb{Z}$-module. Thus every abelian group is a $\mathbb{Z}$-module.

If A is an abelian group containing an element x of finite order n, then $nx = 0$. Thus, in contrast to vector spaces, a $\mathbb{Z}$-module may have nonzero elements x such that $nx = 0$ for some nonzero ring element n. In particular, if A has order m, then by Lagrange's Theorem $mx = 0$ for all $x \in A$. Then A is a module over $\mathbb{Z}/m\mathbb{Z}$.

In particular, if p is a prime and A is an abelian group such that $px = 0$ for all $x \in A$, then A is a $\mathbb{Z}/p\mathbb{Z}$-module, i.e., can be considered as a vector space over the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Example 3.1.5 ($F[x]$-modules)
Let F be a field, let x be an indeterminate and let R be the polynomial ring $F[x]$. Let V be a vector space over F and let T be a linear transformation from V to V. We have already seen that V is an F-module; the linear map T will enable us to make V into an $F[x]$-module.

First, for the nonnegative integer n, define

$$T^0 = I, T^1 = T, \cdots, T^n = T \circ T \circ \cdots \circ T \ (n \text{ times})$$

where I is the identity map from V to V and $\circ$ denotes function composition.

We now define the multiplication of any polynomial in x on V with $F[x]$. Let $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, where $a_0, \cdots, a_n \in F$. For each $v \in V$, define

$$\begin{aligned} p(x)v &= (a_n T^n + a_{n-1}T^{n-1} + \cdots + a_1 T + a_0)(v) \\ &= a_n T^n(v) + a_{n-1}T^{n-1}(v) + \cdots + a_1 T(v) + a_0 v. \end{aligned}$$

This makes V into an $F[x]$-module.

Proposition 3.1.6 (The submodule Criterion)
Let R be a ring and let M be an R-module. A subset N of 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 for all $x, y \in N$.

Proof. If N is a submodule, then $0 \in N$ so $N \neq \varnothing$. Also $x + ry \in N$ for all $r \in R$ and $x, y \in N$. Conversely, suppose (1) and (2) hold. Let $r = -1$ and apply the subgroup criterion to see that N is a subgroup of M. In particular, $0 \in N$. Now let $x = 0$ and apply hypothesis (2) to see that N is sent to itself under the multiplication of N with R. □

Definition 3.1.7
Let R be a commutative ring with identity. An *R-algebra* is a ring A with identity together with a ring homomorphism $f : R \to A$ mapping $1_R \to 1_A$ such that the subring $f(R)$ of A is contained in the center of A, $C(A) = \{a \in A : ab = ba \text{ for all } b \in A\}$.

Remark 3.1.8
If A is an R-algebra, then $R \times A \to A$ by $r \cdot a = f(r)a$ makes A 2-sided R-module because $f(r) \in C(A)$;

$$r \cdot a = f(r)a = af(r) = a \cdot r,$$
$$(rs) \cdot a = f(rs)a = f(r)f(s)a = f(r) \cdot (s \cdot s) = r \cdot (s \cdot a).$$

Thus an R-algebra is a R-module.

Definition 3.1.9
If A and B are two R-algebras, an *R-algebra homomorphism* is a ring homomorphism $\varphi : A \to B$ mapping $1_A \to 1_B$ such that $\varphi(r \cdot a) = r \cdot \varphi(a)$ for all $r \in R$ and $a \in A$. If an R-algebra homomorphism is bijective, then it is an *R-algebra isomorphism.*

Example 3.1.10
Let R be a commutative ring with 1.

(1) Any ring with identity is a $\mathbb{Z}$-algebra.

(2) For any ring A with identity, if R is a subring of the center of A containing the identity of A, then A is an R-algebra.

(3) In particular, a commutative ring A containing 1 is an R-algebra for any subring R of A containing 1.

(4) If A is an R-algebra then the R-module structure of A depends only on the subring $f(R)$ contained in the center of A as in the previous example.

3.1.1 Exercises

In these exercises R is a ring with 1 and M is a left R-module.

Exercise 3.1.1
Prove that $0m = 0$ and $(-1)m = -m$ for all $m \in M$.

Exercise 3.1.2
Let $M = R^n$ and let $I_1, \cdots, I_n$ be left ideals of R. Prove that the following are submodules of M:

(a) $\{(x_1, \cdots, x_n) : x_i \in I_i\}$

(b) $\{(x_1, \cdots, x_n) : x_i \in R \text{ and } x_1 + \cdots + x_n = 0\}$.

Exercise 3.1.3
For any left ideal I of R define

$$IM = \left\{ \sum_{\text{finite}} a_i m_i : a_i \in I, m_i \in M \right\}$$

to be the collection of all finite sums of elements of the form am where $a \in I$ and $m \in M$. Prove that IM is a submodule of M.

Exercise 3.1.4
Show that the intersection of any nonempty collection of submodules of an R-module is a submodule.

Exercise 3.1.5
Let $N_1 \subseteq N_2 \subseteq \cdots$ be an ascending chain of submodules of M. Prove that $\bigcup_{i=1}^{\infty} N_i$ is a submodule of M.

Exercise 3.1.6
Let z be an element of the center of R, i.e., $zr = rz$ for all $r \in R$. Prove that zM is a submodule of M, where $zM = \{zm : m \in M\}$.

Exercise 3.1.7
Suppose that A is a ring with identity 1_A that is a left R-module satisfying $r \cdot (ab) = (r \cdot a)b = a(r \cdot b)$ for all $r \in R$ and $a, b \in A$. Prove that the map $f : R \to A$ defined by $f(r) = r \cdot 1_A$ is a ring homomorphism mapping $1_R \mapsto 1_A$ and that $f(R)$ is contained in the center of A. Conclude that A is an R-algebra and that the R-module structure on A induced by its algebra structure if precisely the original R-module structure.

3.2 Quotient Modules and Module Homomorphisms

Definition 3.2.1
Let R be a ring and let M and N be R-modules.

(a) A map $\varphi : M \to N$ is an *R-module homomorphism* if it respects the R-module structures of M and N, i.e.,

  (a) $\varphi(x + y) = \varphi(x) + \varphi(y)$, for all $x, y \in M$,
  (b) $\varphi(rx) = r\varphi(x)$, for all $r \in R$, $x \in M$.

(b) An R-module homomorphism is an *isomorphism* if it is bijective.

(c) If $\varphi : M \to N$ is an R-module homomorphism, let

  (a) $\ker \varphi = \{m \in M : \varphi(m) = 0\}$,
  (b) $\operatorname{img} \varphi = \{\varphi(m) : m \in M\}$.

(d) Let M and N be R-modules and define $\operatorname{Hom}_R(M, N)$ to be the set of all R-module homomorphisms from M into N.

Example 3.2.2

(1) If R is a ring and $M = R$ is a module over itself, then R-module homomorphisms need not be ring homomorphisms and ring homomorphisms need not be R-module homomorphisms.

- Let $R = \mathbb{Z}$. Then $x \mapsto 2x$ is a $\mathbb{Z}$-module homomorphism but is not a ring homomorphism.
- Let $R = F[x]$. Then $\varphi : f(x) \mapsto f(x^2)$ is a ring homomorphism but is not a $F[x]$-module homomorphism.

(2) Let R be a ring, let $n \in \mathbb{Z}^+$ and let $M = R^n$. For each $i \in \{1, \cdots, n\}$, the projection map

$$\pi_i(x_1, \cdots, x_n) = x_i$$

is a surjective R-module homomorphism with kernel

$$\ker \pi_i = \{(x_1, \cdots, x_n) : x_i \in R \text{ and } x_i = 0\} = R \times \cdots \times \underbrace{0}_{i\text{th}} \times \cdots \times R.$$

(3) $\mathbb{Z}$-module homomorphisms are the same as abelian group homomorphisms.

Proposition 3.2.3
Let M and N and L be R-modules.

(1) A map $\varphi : M \to N$ is an R-module homomorphism if and only if

$$\varphi(rx + y) = r\varphi(x) + \varphi(y) \text{ for all } x, y \in M, r \in R.$$

(2) (a) Let φ, ψ be elements of $\mathrm{Hom}_R(M, N)$. Define $\varphi + \psi$ by

$$(\varphi + \psi)(m) = \varphi(m) + \psi(m) \text{ for all } m \in M.$$

Then $\varphi + \psi \in \mathrm{Hom}_R(M, N)$ and with this operation $\mathrm{Hom}_R(M, N)$ is an abelian group.

(b) If R is a commutative ring, then for $r \in R$ define $r\varphi$ by

$$(r\varphi)(m) = r(\varphi(m)) \text{ for all } m \in M.$$

Then $r\varphi \in \mathrm{Hom}_R(M, N)$ and with this multiplication of R and M the abelian group $\mathrm{Hom}_R(M, N)$ is an R-module.

(3) If $\varphi \in \mathrm{Hom}_R(L, M)$ and $\psi \in \mathrm{Hom}_R(M, N)$ then $\psi\circ \in \mathrm{Hom}_R(L, N)$.

(4) With addition as above and multiplication defined as function composition, $\mathrm{Hom}_R(M, M)$ is a ring with 1. Then R is commutative, $\mathrm{Hom}_R(M, M)$ is an R-algebra.

Proof. (1)-(3) Exercises.

(4) Since the domain and codomain of the elements of $\mathrm{Hom}_R(M, M)$ are the same, function composition is defined. By (3), it is a binary operation on $\mathrm{Hom}_R(M, M)$. As usual, function composition is associative. For all $\varphi, \psi, \phi \in \mathrm{Hom}_R(M, M)$,

$$((\varphi + \psi) \circ \phi)(m) = (\varphi + \psi)(\phi(m)) = \varphi(\phi(m)) + \psi(\phi(m)) = (\varphi \circ \phi)(m) + (\psi \circ \phi)(m)$$
$$(\varphi \circ (\psi + \phi))(m) = \varphi((\psi + \phi)(m)) = \varphi(\psi(m)) + \varphi(\phi(m)) = (\varphi \circ \psi)(m) + (\varphi \circ \phi)(m)$$

Thus $\mathrm{Hom}_R(M, M)$ is a ring. The identity function, I, is seen to be the multiplicative identity of $\mathrm{Hom}_R(M, M)$.

If R is commutative, then (2) shows that the ring $\mathrm{Hom}_R(M, M)$ is a left R-module and defining $\varphi r = r\varphi$ for all $\varphi \in \mathrm{Hom}_R(M, M)$ and $r \in R$ makes $\mathrm{Hom}_R(M, M)$ into an R-algebra. □

Definition 3.2.4
The ring $\mathrm{Hom}_R(M, M)$ is called the *endomorphism ring of* M and will often be denoted by $\mathrm{End}_R(M)$, or just $\mathrm{End}(M)$ when the ring R is clear from the context. Elements of $\mathrm{End}(M)$ are called *endomorphisms*.

Remark 3.2.5
When R is commutative, there is a natural map from R into $\mathrm{End}(M)$ given by $r \mapsto rI$, where the latter endomorphism of M is just multiplication by r on M. The image of R is contained in the centor of $\mathrm{End}(M)$ so if R has an identity, $\mathrm{End}(M)$ is an R-algebra.

The ring homomorphism from R to $\mathrm{End}_R(M)$ may not be injective since for some r we may have $rm = 0$ for all $m \in M$ (e.g.,$R = \mathbb{Z}$, $M = \mathbb{Z}/2\mathbb{Z}$, and $r = 2$).

Suppose M is an R-module and N is a submodule of M. Since M is an additive abelian group, M/N is also additive abelian group in the natural way. Consider the natural projection $\pi : M \to M/N$ by $m \mapsto m+N$. We already show that π is a (additive) group homomorphism.

Proposition 3.2.6
Let R be a ring, let M be an R-module and let N be a submodule of M. The quotient group M/N can be made into an R-module by defining

$$r(x + N) = (rx) + N, \text{ for all } r \in R, x + N \in M/N.$$

Moreover π is an R-homomorphism with kernel N.

Proof. Suppose $x+N = y+N$. Then $x-y \in N$. Since N is a submodule, $r(x-y) = rx-ry \in N$, i.e., $rx+N = ry+N$. Thus this multiplication is well defined. The other axioms are easy to show. □

Definition 3.2.7
Let A, B be submodules of the R-module M. The *sum* of A and B is the set

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

One can easily check that the sum of two modules A and B is a submodule and is the smallest submodule which contains both A and B.

Theorem 3.2.8 (Isomorphism Theorems)

(1) Let M, N be R-modules and let $\varphi : M \to N$ be an R-module homomorphism. Then $\ker \varphi$ is a submodule of M and $M/\ker \varphi \cong \mathrm{img}\, \varphi$.

(2) Let A, B be submodules of the R-module M. Then $(A + B)/B \cong A/(A \cap B)$.

(3) Let M be an R-module, and let A and B submodules of M with $A \subseteq B$. Then $(M/A)/(B/A) \cong M/B$.

(4) Let N be a submodule of the R-module M. There is a bijection between the submodules of M which contain N and the submodules of M/N. The correspondence is given by $A \leftrightarrow A/N$, for all $A \supseteq N$. This correspondence commutes with the processes of taking sums and intersections.

3.2.1 Exercises

In these exercises R is a ring with 1 and M is a left R-module.

Exercise 3.2.1
Let A be any $\mathbb{Z}$-module, let a be any element of A and let n be a positive integer. Prove that the map $\varphi_a : \mathbb{Z}/n\mathbb{Z} \to A$ given by $\varphi(\overline{k}) = ka$ is a well defined $\mathbb{Z}$-module homomorphism if and only if $na = 0$. Prove that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A) \cong A_n$, where $A_n = \{a \in A : na = 0\}$.

Exercise 3.2.2
Prove that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/\gcd(n, m)\mathbb{Z}$.

Exercise 3.2.3
Let z be a fixed element of the center of R. Prove that the map $m \mapsto zm$ is an R-module homomorphism from M to itself. Show that for a commutative ring R the map from R to $\mathrm{End}_R(M)$ given by $r \mapsto rI$ is a ring homomorphism where I is the identity endomorphism.

Exercise 3.2.4
Let R be a commutative ring. Prove that $\mathrm{Hom}_R(R, M)$ and M are isomorphic as left R-modules. [Hint: show that each element of $\mathrm{Hom}_R(R, M)$ is determined by its value on the identity of R, that is, $\varphi \in \mathrm{Hom}_R(R, M)$ is determined by $\varphi(1)$.]

Exercise 3.2.5
Let R be a commutative ring. Prove that $\mathrm{Hom}_R(R, R)$ and R are isomorphic as rings.

3.3 Generation of Modules, Direct Sums, and Free Modules

From now on, a ring R has 1. The term "module" will mean "left module."

Definition 3.3.1
Let M be an R-module and let $N_1, \cdots, N_n$ be submodules of M.

(1) The *sum* of $N_1, \cdots, N_n$ is the set of all finite sums of elements from the sets N_i:

$$N_1 + N_2 + \cdots + N_n = \{a_1 + a_2 + \cdots + a_n : a_i \in N_i \text{ for all } i\}.$$

(2) For any subset A of M, let

$$RA = \{r_1a_1 + r_2a_2 + \cdots + r_ma_m : r_1, \cdots, r_m \in R, a_1, \cdots, a_m \in A, m \in \mathbb{Z}^+\}$$

where by convention $RA = \{0\}$ if $A = \varnothing$.

- If A is the finite set $\{a_1, \cdots, a_n\}$ we shall write $Ra_1 + \cdots + Ra_n$ for RA.
- If N is a submodule of M (possibly $N = M$) and $N = RA$, for some subset A of M, we call A a *set of generators or generating set* for N, and we say N *is generated by* A.

(3) A submodule N of M (possibly $N = M$) is *finitely generated* if there is some finite subset A of M such that $N = RA$, that is, if N is generated by some finite subset.

(4) A submodule N of M (possibly $N = M$) is *cyclic* if there exists an element $a \in M$ such that $N = Ra$, that is, if N is generated by one element:

$$N = Ra = \{ra : r \in R\}.$$

Remark 3.3.2
Let M be a R-module and let A be a nonempty subset of M. A *R-linear combination of A* is a element x of M of the form

$$x = r_1a_1 + \cdots + r_ka_k \text{ for some } r_1, \cdots, r_k \in R, a_1, \cdots, a_k \in A.$$

Remark 3.3.3
It is easy to see using the Submodule Criterion that for any subset A of M, RA is indeed a submodule of M and is the smallest submodule of M which contains A. In particular,

- for submodules of $N_1, \cdots, N_n$ of M, $N_1 + \cdots + N_n$ is just the submodule generated by the set $N_1 \cup \cdots \cup N_n$ and is the smallest submodule of M containing N_i for all i.
- if $N_1, \cdots, N_n$ are generated by sets $A_1, \cdots, A_n$ repectively, then $N_1 + \cdots + N_n$ is generated by $A_1 \cup \cdots \cup A_n$.

Remark 3.3.4
A submodule N of an R-module M may have many different generating sets.

- If N is finitely generated, then there is a smallest nonnegative integer d such that N is generated by d elements and now fewer.
- Any generating set consisting of d elements will be called a *minimal set of generators for N* (it is not unique in general).
- If N is not finitely generated, it need not have a minimal generating set.

Example 3.3.5

(1) Let $R = \mathbb{Z}$ and let M be any R-module, that is abelian group. If $a \in M$, then $\mathbb{Z}a$ is just the cyclic subgroup of M generated by a: $\langle a \rangle$.

(2) Let R be a ring with 1 and let M be the (left) R-module R itself. Note that R is a finitely generated (moreover cyclic), $R = R1$.

(3) Submodules of a finitely generated module need not be finitely generated: take M to be the cyclic R-module R itself where R is the polynomial ring in infinitely many variables $x_1, x_2, \cdots$ with coefficients in some field F. The submodule generated by $\{x_1, x_2, \cdots\}$ cannot be generated by any finite set.

(4) Let R be a ring with 1 and let $M = R^n$. For each $i \in \{1, \cdots, n\}$ let $e_i = (\cdots, 0, 1, 0, \cdots)$, where the 1 appears in position i. Since

$$(s_1, \cdots, s_n) = \sum_{i=1}^{n} s_i e_i,$$

it is clear that M is generated by $\{e_1, \cdots, e_n\}$. If R is commutative then this is a minimal generating set.

Definition 3.3.6
Let $M_1, \cdots, M_k$ be a collection of R-modules. The collection of k-tuples $(m_1, \cdots, m_k)$ where $m_i \in M_i$ with addition and multiplication with R defined componentwise is called the *direct product* of $M_1, \cdots, M_k$, denoted by $M_1 \times \cdots \times M_k$.

Proposition 3.3.7
Let $N_1, \cdots, N_k$ be submodules of the R-module M. Then the following are equivalent:

(1) The map $\pi : N_1 \times \cdots \times N_k \to N_1 + \cdots + N_k$ defined by

$$\pi(a_1, \cdots, a_k) = a_1 + \cdots + a_k$$

is an isomorphism: $N_1 + N_2 + \cdots + N_k \cong N_1 \times N_2 \times \cdots \times N_k$.

(2) $N_j \cap (\cdots + N_{j-1} + N_{j+1} + \cdots) = 0$ for all $j \in \{1, \cdots, k\}$.

(3) Every $x \in N_1 + \cdots + N_k$ can be written *uniquely* in the form $a_1 + \cdots + a_k$ with $a_i \in N_i$.

Proof. (1) $\Longrightarrow$ (2). Suppose not and let $a_j \in N_j \cap (\cdots + N_{j-1} + N_{j+1} + \cdots)$ with $a_j \neq 0$. Then

$$a_j = a_1 + \cdots + a_{j-1} + a_{j+1} + \cdots + a_k$$

for some $a_i \in N_i$, and $(\cdots, a_{j-1}, -a_j, a_{j+1}, \cdots)$ would be a nonzero element of $\ker \pi$, a contradiction.

(2) $\Longrightarrow$ (3). Let $a_i, b_i \in N_i$ be such that

$$a_1 + \cdots + a_k = b_1 + \cdots + a_k.$$

For each j,

$$a_j - b_j \in N_j \cap (\cdots + N_{j-1} + N_{j+1} + \cdots) = 0.$$

Thus $a_j = b_j$ for all j.

(3) $\Longrightarrow$ (1) Clearly, π is a surjective R-module homomorphism. By (3) π is injective. Hence π is an isomorphism. □

Remark 3.3.8
If $N_1, \cdots, N_k$ satisfy one of the above conditions, the sum of them is called the *direct sum* of $N_1, \cdots, N_k$, written

$$N_1 + \cdots + N_k = N_1 \oplus \cdots \oplus N_k.$$

Definition 3.3.9
An R-module F is said to be *free* on the subset A of F if

- for every nonzero element x of F, there exist unique nonzero elements $r_1, \cdots, r_n$ of R and unique $a_1, \cdots, a_n$ in A such that

$$x = r_1 a_1 + \cdots + r_n a_n, \text{ for some } n \in \mathbb{Z}^+.$$

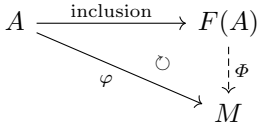
In this situation we say A is a *basis* or *set of free generators* for F. If R is a commutative ring the cardinality of A is called the *rank* of F.

Remark 3.3.10
One should be careful to note the difference between the uniqueness property of direct sums and the uniqueness property of free modules.

- In $N_1 \oplus N_2$, each element can be written uniquely as $n_1 + n_2$; here the uniqueness refers to the *module elements* n_1 and n_2.
- In the case of free modules, the uniqueness is on the *ring elements as well as the module elements*.

For example, if $R = \mathbb{Z}$ and $N_1, N_2 = \mathbb{Z}/2\mathbb{Z}$, then $N_1 \oplus N_2$ has a unique representation in the form $n_1 + n_2$ where each $n_i \in N_i$, however n_1 can be expressed as n_1 or $3n_1$ or $5n_1 \ldots$ etc., so each element does not have a unique representation in the form $r_1a_1 + r_2a_2$, where $r_1, r_2 \in R$, $a_1 \in N_1$ and $a_2 \in N_2$. Thus $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ is not a free $\mathbb{Z}$-module on the set $\{(1,0),(0,1)\}$. Similarly, it is not free on any set.

Theorem 3.3.11 (The Universal Property of Free R-modules)
For any set A there is a free R-module $F(A)$ on the set A and $F(A)$ satisfies the following *universal property*: if M is any R-module and $\varphi : A \to M$ is any map of sets, then there is a unique R-module homomorphism $\Phi : F(A) \to M$ such that $\Phi(a) = \varphi(a)$ for all $a \in A$, that is, the following diagram commutes.



When A is the finite set $\{a_1, \cdots, a_n\}$, $F(A) = Ra_1 \oplus Ra_2 \oplus \cdots \oplus Ra_n \cong R^n$.

Proof. (Uniqueness) Since A is a basis of $F(A)$, every nonzero element is of the form

$$r_1a_1 + \cdots r_na_n.$$

Suppose $\Psi : F(A) \to M$ is another R-module homomorphism such that $\Psi|A = \varphi$ as a set function. Then for all $a \in A$, $\Psi(a) = \varphi(a) = \Phi(a)$. In general,

$$\begin{aligned}\Psi(r_1a_1 + \cdots r_na_n) &= r_1\Psi(a_1) + \cdots + r_1\Psi(a_n) \\ &= r_1\Phi(a_1) + \cdots + r_1\Phi(a_n) = \Phi(r_1a_1 + \cdots r_na_n).\end{aligned}$$

Thus $\Phi = \Psi$.

(Existence) At first, we will construct $F(A)$. If $A = \varnothing$, let $F(A) = \{0\}$. If $A \neq \varnothing$, let $F(A)$ be the collection of all set functions $f : A \to R$ such that $\{a : f(a) \neq 0\}$ is finite (we call it a *support of* f and denote $\operatorname{supp} f$). Give operations on $F(A)$ by

- $(f + g)(a) = f(a) + g(a)$,
- $(rf)(a) = r(f(a))$.

It is easy to show that $F(A)$ satisfies all the R-module axioms. Identify A as a subset of $F(A)$ by $a \mapsto f_a$, where

$$f_a(x) = \begin{cases} 0 & x \neq a \\ 1 & x = a \end{cases}.$$

In this way, we can thick of $F(A)$ as all finite R-linear combinations of elements of A by identifying each function f with the sum

$$f = r_1a_1 + r_2a_2 + \cdots r_na_n,$$

where $r_i = f(a_i)$ (since f has a finite support, there are only finitely many nonzero r_i's). Then this expression of f is unique.

Finally, define $\Phi : F(A) \to M$ by

$$\Phi(r_1a_1 + \cdots + r_na_n) = r_i\varphi(a_1) + \cdots + r_n\varphi(a_n).$$

By the uniqueness of the expression for the elements of $F(A)$ as R-linear combinations of the a_i, Φ is a well defined R-module homomorphism. By definition, $\Phi(a) = \varphi(a)$ for all $a \in A$.

When A is the finite set $\{a_1, \cdots, a_n\}$, $F(A) = Ra_1 \oplus \cdots \oplus Ra_n$. Since $R \cong Ra_i$, $F(A) \cong R^n$. □

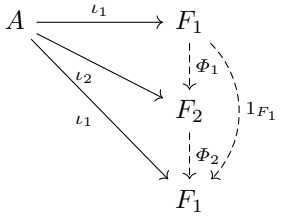
Remark 3.3.12
The finite case of A says that $F(A)$ is not unique. But, $F(A)$ is unique up to isomorphic by the following Corollary.

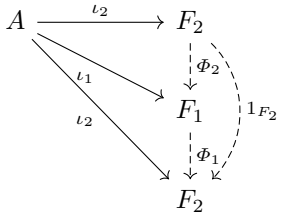
Corollary 3.3.13

(1) If F_1 and F_2 are free modules on the same set A, there is a unique isomorphism between F_1 and F_2 which is the identity map on A.

(2) If F is any free R-module with basis A, then $F \cong F(A)$. In particular, F enjoys the same universal property with respect to A as $F(A)$ does in Theorem 10.

Proof. (1) Let $\iota_i : A \to F_i$ be inclusions. Apply the universal property for free module by $F(A) = F_1$, $M = F_2$, $\varphi = \iota_2$. Then there is a unique R-module homomorphism $\Phi_1 : F_1 \to F_2$ such that $\Phi_1(a) = \iota_2(a) = a$. In the same way, we get $\Phi_2 : F_2 \to F_1$ such that $\Phi_2(a) = \iota_1(a) = a$. Then $\Phi_2 \circ \Phi_1 : F_1 \to F_2$ is an extension of ι_1 and by the uniqueness $\Phi_2 \circ \Phi_1 = 1_{F_1}$. Similarly, $\Phi_1 \circ \Phi_2 = 1_{F_2}$. These two relations says that Φ_i are isomorphisms. □





3.3.1 Exercises

Exercise 3.3.1
Prove that if M is a finitely generated R-module that is generated by n elements, then every quotient of M may be generated by n (or fewer) elements. Deduce that quotients of cyclic modules are cyclic.

Exercise 3.3.2
Let N be a submodule of M. Prove that if both M/N and N are finitely generated then so is M.

Exercise 3.3.3
Let R be a commutative ring and let A, B and M be R-modules. Prove the following isomorphisms of R-modules:

(a) $\mathrm{Hom}_R(A \times B, M) \cong \mathrm{Hom}_R(A, M) \times \mathrm{Hom}_R(B, M)$.

(b) $\mathrm{Hom}_R(M, A \times B) \cong \mathrm{Hom}_R(M, A) \times \mathrm{Hom}_R(M, B)$.

Exercise 3.3.4
Let R be a commutative ring and let F be a free R-module of finite rank. Prove that $\mathrm{Hom}_R(F, R) \cong F$.

Exercise 3.3.5
Let R be a commutative ring and let F be a free R-module of rank n. Prove that

$$\mathrm{Hom}_R(F, M) \cong M \times \cdots \times M \ (n \text{ times}).$$

[Use $\mathrm{Hom}_R(R, M) \cong M$.]

Exercise 3.3.6
Show that any direct sum of free R-modules is free.

3.4 Tensor Products of Modules

3.4.1 Motivation

Suppose a ring R is a subring of the ring S with $1_R = 1_S$. Then S is a R-module. If N is an S-module, then N can also be naturally considered as an R-module:

- $(r_1 + r_2)n = r_1 n + r_2 n$ and $r(n_1 + n_2) = rn_1 + rn_2$;
- $(r_1 r_2)n = r_1(r_2 n)$.

More generally, if $f : R \to S$ is a ring homomorphism with $f(1_R) = 1_S$, an S-module N can be considered as an R-module with $rn = f(r)n$. In this case, S can be considered as an *extension* of R and the resulting R-module is said to be obtained from N by *restriction of scalars* from S to R.

Now consider the converse, that is, suppose R is a subring of S and N is an R-module. Can we extend the scalar R to S so that N is a S-module?

Example 3.4.1
$\mathbb{Z}$ is a $\mathbb{Z}$ module but it cannot be made into a $\mathbb{Q}$-module: suppose there is an extension structure on $\mathbb{Z}$ into $\mathbb{Q}$-module. Let $z = \frac{1}{2} \circ 1$. Then $z + z = 1$, but there is no such z in $\mathbb{Z}$.

Although $\mathbb{Z}$ can not be made into a $\mathbb{Q}$-module, it is contained in a $\mathbb{Q}$-module, namely $\mathbb{Q}$ itself.

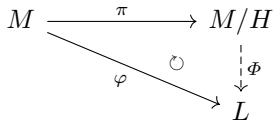
Then the question is changed, "is there a S-module containing a R-module N?". If there is an R-module homomorphism from N to S-module, we can consider the image of N via this homomorphism as a subset of S-module.

3.4.2 Tensor Products

We will construct the tensor products. To do this, we need two universal properties. One is the universal property of free modules(Theorem 3.3.11) and and the other is the universal property of quotient modules.

Theorem 3.4.2 (The Universal Property of Quotient Modules)
Let R be a ring with 1 and let M be R-module and let H be a submodule of M. Then $\pi : M \to M/H$ by $\pi(m) = m + H$ is a surjective R-module homomorphism.

- Suppose L is an R-module and $\varphi : M \to L$ is a R-module homomorphism whose kernel contains H. Then there is a unique R-module homomorphism $\Phi : M/H \to L$ such that φ factors through Φ, i.e. $\varphi = \Phi \circ \pi$ and the diagram commutes.



Proof. Define $\Phi : M/H \to L$ by $\Phi(m + H) = \varphi(m)$. This map is well defined because : suppose $m + H = m' + H$. Then $m - m' \in H \subset \ker\varphi$. Thus $\varphi(m + H) = \varphi(m) = \varphi(m') = \Phi(m' + H)$. By definition, Φ is an R-module homomorphism. Suppose there is another R-module homomorphism $\Psi : M/H \to L$ such that $\varphi = \Psi \circ \pi$. Since $m+H = \pi(m)$, $\Psi(m + H) = \Psi \circ \pi(m) = \varphi(m) = \Phi \circ \pi(m) = \Phi(m + H)$. □

By combining these two theorems, we can construct the tensor product. Suppose M is a right R-module and N is a left R-module. Consider the free $\mathbb{Z}$-module on the set $M \times N$, $F(M \times N)$. Let H be the subgroup of $F(M \times N)$ 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 $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$, and $r \in R$. Then $F(M \times N)/H$ is an abelian group, denoted by $M \otimes_R N$, or simply $M \otimes N$ if the ring R is clear from the context, and is call the *tensor product of M and N over R*. The elements of $M \otimes_R N$ are called *tensors*, and the coset $m \otimes n$ of (m, n) in $M \otimes_R N$ is called a *simple tensor*. We have the relations

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

Every tensor can be written (non-uniquely in general) as a finite sum of simple tensors. And a tensor may not be a simple tensor.

Mapping $M \times N$ to $F(M \times N)$ and then passing to the quotient defines a map $\iota : M \times N \to M \otimes_R N$ with $\iota(m, n) = m \otimes n$. This map is in general not a group homomorphism and not injective, but it is additive in both m and n separately and satisfies $\iota(mr, n) = mr \otimes n = m \otimes rn = \iota(m, rn)$.

Definition 3.4.3
Let M be a right R-module, let N be a left R-module and let L be an abelian group. A map

$\varphi : M \times N \to L$ is called *R-balanced* if

$$\begin{aligned}\varphi(m_1 + m_2, n) &= \varphi(m_1, n) + \varphi(m_2, n),\\ \varphi(m, n_1 + n_2) &= \varphi(m, n_1) + \varphi(m, n_2),\\ \varphi(mr, n) &= \varphi(m, rn),\end{aligned}$$

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

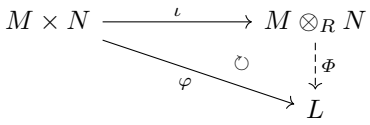
With this terminlonogy, $\iota : M \times N \to M \otimes_R N$ is R-balanced.

Theorem 3.4.4 (The Universal properties of Tensor Products)
Suppose R is a ring with 1, M is a right R-module, and N is a left R-module. Let $M \otimes_R N$ be the tensor product of M and N over R and let $\iota : M \times N \to M \otimes_R N$ be the R-balanced map defined above.

(1) If $\Phi : M \otimes_R N \to L$ is any group homomorphism from $M \otimes_R N$ to an abelian group L, then the composite map $\varphi = \Phi \circ \iota$ is an R-balanced map from $M \times N$ to L.

(2) Conversely, suppose L is an abelian group and $\varphi : M \times N \to L$ is any R-balanced map. Then there is a unique group homomorphism $\Phi : M \otimes_R N \to L$ such that φ factors through ι, i.e. $\varphi = \Phi \circ \iota$ as in (1).

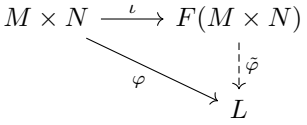
Equivalently, the correspondence $\varphi \leftrightarrow \Phi$ in the commutative diagram



establishes a bijection

$$\{R\text{-balanced maps, } \varphi : M \times N \to L\} \leftrightarrow \{\text{group homomorphisms, } \Phi : M \otimes N \to L\}$$

Proof. The proof of (1) is immediate from the properties of ι above. For (2), the map φ defines a unique $\mathbb{Z}$-module homomorphism $\tilde{\varphi}$ from $F(M \times N)$ to L such that $\tilde{\varphi}(m, n) = \varphi(m, n) \in L$.



Since φ is R-balanced, $\tilde{\varphi}$ maps each of the elements in H to 0;

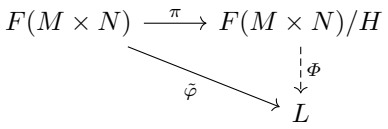
$$\begin{aligned}\tilde{\varphi}((m_1 + m_2, n) - (m_1, n) - (m_2, n)) &= \varphi(m_1 + m_2, n) - \varphi(m_1, n) - \varphi(m_2, n) = 0,\\ \tilde{\varphi}((m, n_1 + n_2) - (m, n_1) - (m, n_2)) &= \varphi(m, n_1 + n_2) - \varphi(m, n_1) - \varphi(m, n_2) = 0,\\ \tilde{\varphi}((mr, n) - (m, rn)) &= \varphi(mr, n) - \varphi(m, rn) = 0.\end{aligned}$$

It follows that the kernel of $\tilde{\varphi}$ contains the subgroup H, hence $\tilde{\varphi}$ induces a homomorphism Φ on $F(M \times N)/H = M \otimes_R N$ to L.

By definition we have

$$\Phi(m \otimes n) = \tilde{\varphi}(m, n) = \varphi(m, n),$$

i.e., $\varphi = \Phi \circ \iota$. The homomorphism Φ is uniquely determined by this equation because the elements $m \otimes n$ generate $M \otimes_R N$ as an abelian group. This completes the proof. □



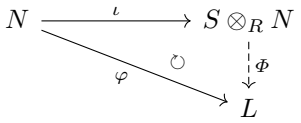
This theorem is extremely useful in defining homomorphisms on $M \otimes_R N$ since it replaces the often tedious check that maps defined on simple tensors $m \times n$ are well-defined with a check that a related map defined on ordered pairs (m, n) is balanced.

Example 3.4.5
Let R be a subring of a ring S with $1_R = 1_S$ and let N be a left R-module. As right R-module S, we can product R and N over R, $S \otimes_R N$. In this case, $s\left(\sum s_i \otimes n_i\right) = \sum (ss_i) \otimes n_i$ induces a left S-module structure.

Let $\iota : N \to S \otimes_R N$ by $n \mapsto 1 \otimes n$. ι is an R-module homomorphism but may not be injective in general. We can apply the universal property as follows:

Corollary 3.4.6
Let R be a subring S with $1_S = 1_R$, let N be a left R-module and let $\iota : N \to S \otimes_R N$ be the R-module homomorphism defined by $\iota(n) = 1 \otimes n$.

- Suppose L is a left S-module and $\varphi : N \to L$ is an R-module homomorphism. Then there is a unique S-module homomorphism $\Phi : S \otimes_R N \to L$ such that φ factors through Φ, i.e. $\varphi = \Phi \circ \iota$ and the diagram



  commutes.

Proof. Define $i : S \times N \to S \otimes_R N$ by $i(s, n) = s \otimes n$ and $\psi : S \times N \to L$ by $\psi(s, n) = s\varphi(n)$. It is easy to show that ψ is R-balanced map. Then there is unique abelian group homomorphism $\Phi : S \otimes_R N \to L$ such that $\psi = \Phi \circ i$. Moreover, $\Phi(s(s' \otimes n)) = \Phi((ss') \otimes n) = ss'\varphi(n) = s\Phi(s' \otimes n)$ implies Φ is a S-module homomorphism. Finally, $\varphi(n) = 1\varphi(n) = \psi(1, n) = \Phi(i(1, n)) = \Phi(1 \otimes n) = \Phi \circ \iota(n)$. □

Remark 3.4.7
Using this theorem, we can "extend" a scalar R on an R-module N to S. The universal property of $S \otimes_R N$ shows that $S \otimes_R N$ is the smallest S-module such that contains $\iota(N)$ (as a subset of $S \otimes_R N$).

The caution part is that ι may not be injective. Let $N = \mathbb{Z}/2\mathbb{Z}$. Consider $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$. For $q \otimes n \in \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$, $q \otimes n = \frac{q}{2} \otimes 2n = 0$. (The last equation is followed from $q \otimes 0 = q \otimes (0 + 0) = q \otimes 0 + q \otimes 0$). This means $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} = 0$. Thus $\iota : \mathbb{Z} \to \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$ is not injective.

Example 3.4.8

(1) For any ring R and any left R-module N, $R \otimes_R N \cong N$.

(2) Let $R = \mathbb{Z}$ and $S = \mathbb{Q}$ and let A be a finite abelian group of order n. In this case, the $\mathbb{Q}$-module $\mathbb{Q} \otimes_{\mathbb{Z}} A$ obtained by extension of scalars from the $\mathbb{Z}$-module is 0: $1 \otimes 0 = 1 \otimes (0 + 0) = 1 \otimes 0 + 1 \otimes 0$ implies $1 \otimes 0 = 0$. In general, $q \otimes a \in \mathbb{Q} \otimes_{\mathbb{Z}} A$, let $n = |a|$. Then

$$q \otimes a = \frac{q}{n} \otimes na = \frac{q}{n}(1 \otimes 0) = 0.$$

(3) If $N \cong R^n$, $S \otimes_R N \cong S^n$.

3.4.3 Module structure on $M \otimes_R N$

We observed in the special case of extending scalars from R to S for the R-module N, the S-module structure on $S \otimes_R N$ required only a left S-module structure on S together with the compatibility relation $s'(sr) = (s's)r$.

To obtain an S-module structure on $M \otimes_R N$ more generally, we impose a similar structure on M:

Definition 3.4.9
Let R and S be any rings with 1. 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 $s \in S$, $r \in R$, and $m \in M$.

Example 3.4.10

(1) Any ring S is an (S, R)-bimodule for any subring R with $1_R = 1_S$. More generally, if $f : R \to S$ is any ring homomorphism with $f(1_R) = 1_S$, then S can be considered as a right R-module with multiplication $s \cdot r = sf(r)$, and becomes an (S, R)-bimodule.

(2) Let I be an (two-sided) ideal in the ring R. Then the quotient ring R/I is an $(R/I, R)$-bimodule : $\pi : R \to R/I$ by $\pi(r) = r + I$ is a ring homomorphism with $\pi(1) = 1$.

(3) Suppose that R is a commutative ring. Then a left (resp., right) R-module M can always be given the structure of a right (resp., left) R-module by defining $mr = rm$ (resp., $rm = mr$), and this makes M into an (R, R)-bimodule.

Definition 3.4.11
Suppose M is a left (or right) R-module over the commutative ring R. Then the (R, R)-bimodule structure on M defined by letting the left and right R-multiplication coincide, i.e., $mr = rm$ for all $m \in M$ and $r \in R$, will be called the *standard* R-module structure on M.

Remark 3.4.12
Suppose N is a left R-module and M is an (S, R)-bimodule. Then $M \otimes_R N$ is an abelian group. Now give a multiplication by $s(\sum m_i \otimes n_i) = \sum (sm_i) \otimes n_i$. This induces a S-module structure on $M \otimes_R N$. To show that this multiplication is well-defined, given $s \in S$, consider map $M \times N \to M \otimes_R N$ by $(m, n) \mapsto (sm) \otimes n$. Then there is a well-defined group homomorphism $\lambda_s : M \otimes_R N \to M \otimes_R N$ such that $\lambda_s(m \otimes n) = (sm) \otimes n$. λ_s is the desired multiplication.

By a completely parallel argument, if M is a right R-module and N is an (R, S)-bimodule, then $M \otimes_R N$ is a right S-module.

Recall that if R is a commutative ring, the standard R-module structure on M gives M the structure of an (R, R)-bimodule of a left R-module. The corresponding map $\iota : M \times N \to M \otimes_R N$ is additive in each factor. Since $r(m \otimes n) = (rm) \otimes n = (mr) \otimes n = m \otimes (rn)$,

$$r\iota(m, n) = \iota(rm, n) = \iota(m, rn).$$

Definition 3.4.13
Let R be a commutative ring with 1 and let M, N, and L be left R-modules. The map $\varphi : M \times N \to L$ is called R-*bilinear* if it is R-linear in each factor, i.e., if

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

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

With this terminology Theorem 3.4.4 gives

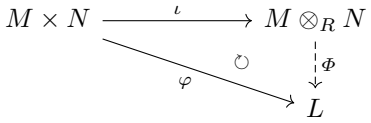
Corollary 3.4.14
Suppose R is a commutative ring. Let M and N be two left R-modules and let $M \otimes_R N$ be the tensor product of M and N over R, where M is given the standard R-module structure. Then $M \otimes_R N$ is a left R-module with

$$r(m \otimes n) = (rm) \otimes n = m \otimes (rn),$$

and the map $\iota : M \times N \to M \otimes_R N$ with $\iota(m, n) = m \otimes n$ is an R-bilinear map. If L is any left R-module then there is a bijection

$$\{R\text{-bilinear maps } \varphi : M \times N \to L\} \leftrightarrow \{R\text{-module homomorphisms } \Phi : M \otimes_R N \to L\}$$

where the correspondence between φ and Φ is given by the commutative diagram



Proof. It suffices to show that in the bijective correspondence in Theorem 3.4.4, the bilinear maps correspond with the R-module homomorphisms. Given bilinear map $\varphi : M \times N \to L$, the corresponding $\Phi : M \otimes_R N \to L$ is a group homomorphism. Moreover, on simple tensor $\Phi((rm) \otimes n) = \varphi(rm, n) = r\varphi(m, n) = r\Phi(m \otimes n)$. Since Φ is additive, this extends to sums of simple tensors to show Φ is an R-module homomorphism. Conversely, if Φ is an R-modules homomorphism, the corresponding balanced map φ is bilinear. □

Example 3.4.15

(1) In any tensor product $M \otimes_R N$, we have $m \otimes 0 = 0$. Likewise $0 \otimes n = 0$.

(2) We have $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z} = 0$, since $3a = a$ for $a \in \mathbb{Z}/2\mathbb{Z}$, so that

$$a \otimes b = 3a \otimes b = a \otimes 3b = a \otimes 0 = 0.$$

In particular $1 \otimes 1 = 0$. It follows that there are no nonzero balanced maps from $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ to any abelian group.

(3) On the other hand, $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$ is generated by $0 \otimes 0 = 1 \otimes 0 = 0 \otimes 1 = 0$ and $1 \otimes 1$. In this case, $1 \otimes 1 \neq 0$ because, the map $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ defined by $(a, b) \mapsto ab$ is clearly nonzero and bilinear over $\mathbb{Z}$. Since $2(1 \otimes 1) = 2 \otimes 1 = 0 \otimes 1 = 0$, the element $1 \otimes 1$ is of order 2. Hence, $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}$.

(4) In general,

$$\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/d\mathbb{Z}$$

where $d = \gcd(m, n)$. To show this, observe that

$$a \otimes b = ab(1 \otimes 1),$$

from which it follows that $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}$ is a cyclic group with $1 \otimes 1$ as generator. Since $m(1 \otimes 1) = m \otimes 1 = 0$ and $n(1 \otimes 1) = 1 \otimes n = 0$, we have $d(1 \otimes 1) = 0$, so the cyclic group has order dividing d. The map $\varphi : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ defined by $\varphi(a \mod m, b \mod n) = ab \mod d$ is well defined $\mathbb{Z}$-bilinear map. Then $\varphi(1, 1) = 1$ is of order d. Since order of $1 \otimes 1$ is divided by order of $\varphi(1 \otimes 1)$, $1 \otimes 1$ is of order d.

(5) In $\mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z}$, a simple tensor has the form $(a/b \mod \mathbb{Z}) \otimes (c/d \mod \mathbb{Z})$ for some rational numbers a/b and c/d. Then

$$\begin{aligned}(\frac{a}{b} \mod \mathbb{Z}) \otimes (\frac{c}{d} \mod \mathbb{Z}) &= (\frac{ad}{bd} \mod \mathbb{Z}) \otimes (\frac{c}{d} \mod \mathbb{Z}) \\ &= (\frac{a}{bd} \mod \mathbb{Z}) \otimes (\frac{cd}{d} \mod \mathbb{Z}) \\ &= (\frac{a}{bd} \mod \mathbb{Z}) \otimes 0 = 0.\end{aligned}$$

So $\mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} = 0$.

(6) The structure of a tensor product can vary considerably depending on the ring over which the tensors are taken. For example, $\mathbb{Q} \otimes_{\mathbb{Q}} \mathbb{Q}$ and $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$ are isomorphic as left $\mathbb{Q}$-modules: In $\mathbb{Q} \otimes_{\mathbb{Q}} \mathbb{Q}$,

$$p \otimes q = pq(1 \otimes 1).$$

Thus every tensor generated by $1 \otimes 1$. Moreover, $\mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ by $(p, q) \mapsto pa$ implies, $1 \otimes 1$ is nonzero. Thus $\mathbb{Q} \otimes_{\mathbb{Q}} \mathbb{Q}$ is a 1-dimensional vector space over $\mathbb{Q}$.

Similarly, $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$ is also generated by $1 \otimes 1$ which is nonzero. Thus $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$ is also a 1-dimensional vector space over $\mathbb{Q}$.

On the other hand, $\mathbb{C} \otimes_{\mathbb{C}} \mathbb{C}$ and $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ are not isomorphic C-modules, because the former is a 1-dimensional but the latter is 2-dimensional.

(7) *General extension of scalars or change of base*: Let $f : R \to S$ be a ring homomorphism with $f(1_R) = 1_S$. Then $s \cdot r = sf(r)$ gives S the structure of a right R-module with respect to which S is an (S, R)-bimodule. Then for any left R-module N, the resulting tensor product $S \otimes_R N$ is a left S-module obtained by *changing the base* from R to S. This gives a slight generalization of the notion of extension of scalars.

(8) Let $f : R \to S$ be a ring homomorphism as in the preceding example. Then we have $S \otimes_R R \cong S$ as left S-modules, as follows. The map $\varphi : S \times R \to S$ defined by $(s, r) \mapsto sr$ (where $sr = sf(r)$ by definition), is an R-balanced map, as is easily checked.

By Theorem 3.4.4 we have an associated group homomorphism $\Phi : S \otimes_R R \to S$ with $\Phi(s \otimes r) = sr$. Since $\Phi(s'(s \otimes r)) = \Phi(s's \otimes r) = s'sr = s'\Phi(s \otimes r)$, it follows that Φ is also an S-module homomorphism. The map $\Phi' : S \to S \otimes_R R$ with $s \mapsto s \otimes 1$ is an S-module homomorphism that is inverse to Φ because $\Phi \circ \Phi'(s) = \Phi(s \otimes 1) = s$ gives $\Phi\Phi' = 1$, and $\Phi' \circ \Phi(s \otimes r) = \Phi'(sr) = sr \otimes 1 = s \otimes r$ shows that $\Phi'\Phi$ is the identity on simple tensors, hence $\Phi'\Phi = 1$.

(9) Let R be a ring (not necessarily commutative), let I be a two sided ideal in R, and let N be a left R-module. Then as previously mentioned, R/I is an $(R/I, R)$-bimodule, so the tensor product $R/I \otimes_R N$ is a left R/I-module. This is an example of "extension of scalars" with respect to the natural projection homomorphism $R \to R/I$. Define

$$IN = \left\{ \sum_{\text{finite}} a_i n_i : a_i \in I, n_i \in N \right\},$$

which is easily seen to be a left R-submodule of N. Then

$$(R/I) \otimes_R N \cong N/IN,$$

as left R-modules, as follows. $(R/I) \otimes_R N$ is generated as an abelian group by the simple tensor $(r+I) \otimes n = r(1 \otimes n)$. Hence $(R/I) \otimes_R N$ is generated by $1 \otimes n$ as an R/I-module. Consider two maps

- $N \to (R/I) \otimes_R N$ by $n \mapsto 1 \otimes n$;
- $(R/I) \otimes_R N \to N/IN$ by $(r+I) \otimes n \mapsto rn + IN$.

The formal is a surjective R-module homomorphism. For $a_i \otimes n_i$ where $a_i \in I$ and $n_i \in N$, $1 \otimes a_i n_i = a_i \otimes n_i = 0$, and so IN is contained in the kernel. Thus this induces a surjective R-module homomorphism $f : N/IN \to (R/I) \otimes_R N$ with $f(n + IN) = 1 \otimes n$.

The latter is well defined because $(R/I) \times N \to N/IN$ by $(r+I, n) \mapsto rn + IN$ is an R-balanced map. Then there is an associated group homomorphism $g : (R/I) \otimes_R N \to N/IN$ with $g((r+I) \otimes n) = rn + IN$.

Finally, you can easily check that $fg = 1$ and $gf = 1$. Hence f and g are isomorphisms.

As an example, let $R = \mathbb{Z}$ and $I = m\mathbb{Z}$ and let $N = \mathbb{Z}/n\mathbb{Z}$. Then $IN = d\mathbb{Z}/n\mathbb{Z}$ where $d = \gcd(m, n)$. Then $N/IN \cong \mathbb{Z}/d\mathbb{Z}$ and $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/d\mathbb{Z}$.

Theorem 3.4.16 (The "Tensor Product" of Two Homomorphisms)
Let M, M' be right R-modules, let N, N' be left R-modules, and suppose $\varphi : M \to M'$ and $\psi : N \to N'$ are R-module homomorphisms.

(1) There is a unique group homomorphism, denoted by $\varphi \otimes \psi$, mapping $M \otimes_R N$ into $M' \otimes_R N'$ such that $(\varphi \otimes \psi)(m \otimes n) = \varphi(m) \otimes \psi(n)$ for all $m \in M$ and $n \in N$.

(2) If M, M' are also (S, R)-bimodules for some ring S and φ is also an S-module homomorphism, then $\varphi \otimes \psi$ is a homomorphism of left S-modules. In particular, if R is commutative, then $\varphi \otimes \psi$ is always an R-module homomorphism for the standard R-module structures.

(3) If $\lambda : M' \to M''$ and $\mu : N' \to N''$ are R-module homomorphisms, then $(\lambda \otimes \mu) \circ (\varphi \otimes \psi) = (\lambda \circ \varphi) \otimes (\mu \otimes \psi)$.

Proof. (1) Consider $(m, n) \mapsto \varphi(m) \otimes \psi(n)$ from $M \times N \to M' \otimes_R N'$. This is an R-balanced map, so (1) follows immediately from Theorem 3.4.4.

(2) For simple tensor $m \otimes n \in M \otimes_R N$ and $s \in S$,

$$(\varphi \otimes \psi)(s(m \otimes n)) = (\varphi \otimes \psi)(sm \otimes n) = \varphi(sm) \otimes \psi(n) = s\varphi(m) \otimes \psi(n).$$

Thus $\varphi \otimes \psi$ is an S-module homomorphism.

(3) For simple tensor $m \otimes n \in M \otimes_R N$

$$(\lambda \otimes \mu) \circ (\varphi \otimes \psi)(m \otimes n) = (\lambda \otimes \mu)(\varphi(m) \otimes \psi(n)) = (\lambda \circ \varphi(m)) \otimes (\mu \circ \psi(n)).$$

By the uniqueness, $(\lambda \otimes \mu) \circ (\varphi \otimes \psi)$.

□

Theorem 3.4.17 (Associativity of the Tensor Product)
Suppose M is a right R-module, N is an (R, T)-bimodule, and L is a left T-module. Then there is a unique isomorphism

$$(M \otimes_R N) \otimes_T L \cong M \otimes_R (N \otimes_T L)$$

of abelian groups such that $(m \otimes n) \otimes l \mapsto m \otimes (n \otimes l)$. If M is an (S, R)-bimodule, then this is an isomorphism of S-modules.

Proof. At first, the (R,T)-bimodule structure on N makes $M \otimes_R N$ into a right T-module and $N \otimes_T L$ into a left R-module, so both sides of the isomorphism are well defined.

Define $(M \otimes_R N) \times L \to M \otimes_R (N \otimes_T L)$ as follows: Fix $l \in L$. Then the mapping $(m,n) \mapsto m \otimes (n \otimes l)$ is R-balanced map, so there is a homomorphism $M \otimes_R N \to M \otimes_R (N \otimes_T L)$ with $m \otimes n \mapsto m \otimes (n \otimes l)$. Thus there is a well defined map $(M \otimes_R N) \times L \to M \otimes_R (N \otimes_T L)$ by $(m \otimes n, l) \mapsto m \otimes (n \otimes l)$. It is easily seen to be T-balanced, so it induces a homomorphism $M \otimes_R N) \otimes_T L \to M \otimes_R (N \otimes_T L)$ such that $(m \otimes n) \otimes l \mapsto m \otimes (n \otimes l)$. In a similar way, we can construct a homomorphism in the opposite direction that is inverse to this one. This proves the group isomorphism.

Assume in addition M is an (S,R)-bimodule. Then for $s \in S$ and $t \in T$, we have

$$s((m \otimes n)t) = s(m \otimes nt) = sm \otimes nt = (sm \otimes n)t = (s(m \otimes n))t$$

so that $M \otimes_R N$ is an (S,T)-bimodule. Hence $(M \otimes_R N) \otimes_T L$ is a left S-module. Since $N \otimes_T L$ is a left R-module, also $M \otimes_R (N \otimes_T) L$ is a left S-module. The group isomorphism just established is easily seen to be a homomorphism of left S-modules by the same arguments used in previous proofs. □

Corollary 3.4.18
Suppose R is commutative and M, N, and L are left R-moudules. Then

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

as R-modules for the standard R-module structures on M, N, and L.

Using this results, we can denote $M \otimes N \otimes L$ which is any one of $(M \otimes N) \otimes L$ and $M \otimes (N \otimes L)$. More generally, we can define $M_1 \otimes \cdots \otimes M_n$.

Definition 3.4.19
Let R be a commutative ring with 1 and let $M_1, \cdots, M_n$ and L be R-modules with the standard R-module structures. A map $\varphi : M_1 \times \cdots \times M_n \to L$ is called *n-multilinear over R* if it is an R-module homomorphism in each component when the other component entries are kept constant, i.e., for each i,

$$\begin{aligned}\varphi(m_1, \cdots, m_{i-1}, &rm_i + r'm_i', m_{i+1}, \cdots, m_n) \\ &= r\varphi(m_1, \cdots, m_i, \cdots, m_n) + r'\varphi(m_1, \cdots, m_i', \cdots, m_n)\end{aligned}$$

for all $m_i, m_i' \in M$ and $r, r' \in R$.

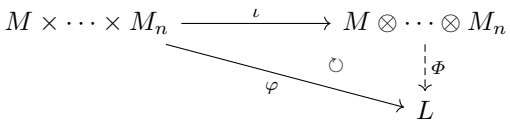
Corollary 3.4.20
Let R be a commutative ring and let $M_1, \cdots, M_n, L$ be R-modules. Let $M_1 \otimes M_2 \otimes \cdots \otimes M_n$ denote any bracketing of the tensor product of these modules and let

$$\iota : M_1 \times \cdots \times M_n \to M_1 \otimes \cdots \otimes M_n$$

be the map defined by $\iota(m_1, \cdots, m_n) = m_1 \otimes \cdots \otimes m_n$. Then

(1) for every R-module homomorphism $\Phi : M_1 \otimes \cdots \otimes M_n \to L$, the map $\varphi = \Phi \circ \iota$ is n-multilinear from $M_1 \times \cdots \times M_n \to L$, and

(2) if $\varphi : M_1 \times \cdots \times M_n \to L$ is an n-multilinear map, then there is a unique R-module homomorphism $\Phi : M_1 \otimes \cdots \otimes M_n \to L$ such that $\varphi = \Phi \circ \iota$.



Hence there is a bijection

$$\{n\text{-multilinear maps } \varphi : M_1 \times \cdots \times M_n \to L\} \leftrightarrow \{R\text{-module homomorphisms } \Phi : M_1 \otimes \cdots \otimes M_n \to L\}$$

with respect to which the following diagram commutes:

Theorem 3.4.21 (Tensor Products of Direct Sums)
Let M, M' be right R-modules and let N, N' be left R-modules. Then there are unique group isomorphisms

$$(M \oplus M') \otimes_R N \cong (M \otimes_R N) \oplus (M' \otimes_R N)$$
$$M \otimes_R (N \oplus N') \cong (M \otimes_R N) \oplus (M \otimes_R N')$$

such that $(m, m') \otimes n \mapsto (m \otimes n, m' \otimes n)$ and $m \otimes (n, n') \mapsto (m \otimes n, m \otimes n')$ respectively. If M, M' are also (S, R)-bimodules, then these are isomorphisms of left S-modules. In particular, if R is commutative, these are isomorphisms of R-modules.

Proof. The map $(M \oplus M') \times N \to (M \otimes_R N) \oplus (M' \otimes_R N)$ defined by $((m, m'), n) \mapsto (m \otimes n, m' \otimes n)$ is well defined since m and m' in $M \oplus N$ are uniquely defined in the direct sum. The map is clearly R-balanced, so induces a homomorphism f from $(M \oplus M') \times N$ to $(M \otimes_R N) \oplus (M' \otimes_R N)$ with

$$f((m, m') \otimes n) = (m \otimes n, m' \otimes n)$$

In the other direction, the R-balanced maps $M \times N \to (M \oplus M') \otimes_R N$ and $M' \times N \to (M \oplus M') \otimes_R N$ given by $(m, n) \mapsto (m, 0) \otimes n$ and $(0, m') \otimes n$, respectively, define homomorphisms from $M \otimes_R N$ and $M' \otimes_R N$ to $(M \otimes M') \otimes_R N$. There in turn give a homomorphism g from the direct sum $(M \otimes_R N) \oplus (M' \otimes_R N)$ to $(M \oplus M') \otimes_R N$ with

$$g((m \otimes n_1, m' \otimes n_2)) = (m, 0) \otimes n_1 + (0, m') \otimes n_2.$$

An each check shows that f and g are inverse homomorphisms and are S-module isomorphisms when M and M' are (S, R)-bimodules. □

We can extends by induction to any finite direct sum of R-modules. The corresponding result is also true for arbitrary direct sums.

$$M \otimes (\bigoplus_{i \in I} N_i) \cong \bigoplus_{i \in I} (M \otimes N_i).$$

Corollary 3.4.22 (Extension of Scalars for Free Modules)
The module obtained from the free R-module, $N \cong R^n$ by extension of scalars from R to S is the free S-module S^n, i.e.,

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

as left S-modules.

Corollary 3.4.23
Let R be a commutative ring and let $M \cong R^s$ and $N \cong R^t$ be free R-modules with bases $m_1, \cdots, m_s$ and $n_1, \cdots, n_t$, respectively. Then $M \otimes_R N$ is a free R-module of rank st, with bases $m_i \otimes n_j$, $1 \leq i \leq s$ and $1 \leq j \leq t$, i.e.,

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

More generally, the tensor product of two free modules of arbitrary rank over a commutative ring is free.

Proposition 3.4.24
Suppose R is a commutative ring and M, N are left R-modules, considered with the standard R-module structures. Then there is a unique R-module isomorphism

$$M \otimes_R N \cong N \otimes_R M$$

mapping $m \otimes n$ to $n \otimes m$.

Proof. Take $(m, n) \mapsto n \otimes m$ and $(n, m) \mapsto m \otimes n$. These two R-balanced maps induce R-module homomorphisms and these two homomorphism are inverse of each other. □

We end this section by showing that the tensor product of R-algebras is again an R-algebra.

Proposition 3.4.25
Let R be a commutative ring and let A and B be R-algebras. Then the multiplication $(a \otimes b)(a' \otimes b') = aa' \otimes bb'$ is well defined and makes $A \otimes_R B$ into an R- algebra.

Proof. To show that $A \otimes B$ is an R-algebra, the main task is showing that the specified multiplication is well defined. Consider $\varphi : A \times B \times A \times B \to (A \otimes B)$ defined by $f(a, b, a', b') = aa' \otimes bb'$. Then φ is multilinear over R and thus there is a corresponding R-module homomorphism $\Phi : A \otimes B \otimes A \otimes B$ to $A \otimes B$ with $\Phi(a \otimes b \otimes a' \otimes b') = aa' \otimes bb'$. Viewing $A \otimes B \otimes A \otimes B$ as $(A \otimes B) \otimes (A \otimes B \otimes)$, we can apply the universal property on $(A \otimes B) \times (A \otimes B)$. Thus there is a well defined R-bilinear map $\varphi' : (A \otimes B) \times (A \otimes B) \to A \otimes B$ with $\varphi'(a \otimes b, a' \otimes b') = aa' \otimes bb'$. This shows that the multiplication is indeed well defined. □

Example 3.4.26
The tensor product $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ is free of rank 4 as a module over $\mathbb{R}$ with basis given by $e_1 = 1 \otimes 1$, $e_2 = 1 \otimes i$, $e_3 = i \otimes 1$, and $e_4 = i \otimes i$. This tensor product is also a ring with $1 = e_1$, and, for example,

$$e_4^2 = (i \otimes i)(i \otimes i) = i^2 \otimes i^2 = (-1) \otimes (-1) = (-1)(-1) \otimes 1 = 1.$$

Then $(e_4 - 1)(e_4 + 1) = 0$, so $\mathbb{C} \otimes_{\mathbb{R}} \otimes \mathbb{C}$ is not an integral domain.

The ring $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ is an $\mathbb{R}$-algebra and the left and right multiplication are the same $xr = rx$ for all $r \in \mathbb{R}$ and $x \in \mathbb{C} \otimes_{\mathbb{R}} \otimes \mathbb{C}$. The ring $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ has a structure of a left $\mathbb{C}$-module and also a right $\mathbb{C}$-module. For example,

$$i \cdot e_1 = i \cdot (1 \otimes 1) = (i \otimes 1) = e_3$$
$$e_1 \cdot i = (1 \otimes 1) \cdot i = 1 \otimes i = e_2.$$

This example also shows that even when the rings involved are commutative there may be natural left and right module structures that are not the same.

3.4.4 Exercises

Exercise 3.4.1
Let $f : R \to S$ be a ring homomorphism from the ring R to the ring S with $f(1_R) = 1_S$. Verify the details that $sr = sf(r)$ defines a right multiplication on S under which S is an (S, R)-bimodule.

Exercise 3.4.2
Show that the element "$2 \otimes 1$" is 0 in $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$ but is nonzero in $2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$.

Exercise 3.4.3
Show that $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ and $\mathbb{C} \otimes_{\mathbb{C}} \mathbb{C}$ are both left $\mathbb{R}$-modules but are not isomorphic as $\mathbb{R}$-modules.

Exercise 3.4.4
Suppose R is commutative and $N \cong R^n$ is a free R-module of rank n with R-module basis $e_1, \cdots, e_n$.

(a) For any nonzero R-module M show that every element of $M \otimes N$ can be written uniquely in the form $\sum_{i=1}^n m_i \otimes e_i$ where $m_i \in M$. Deduce that if $\sum_{i=1}^n m_i \otimes e_i = 0$ in $M \otimes N$, then $m_i = 0$ for all $i = 1, \cdots, n$.

(b) Show that if $\sum m_i \otimes n_i = 0$ in $M \otimes N$ where the n_i are merely assumed to be R-linearly independent, then it is not necessarily true that all the m_i are 0. [Consider $R = \mathbb{Z}$, $n = 1$, $M = \mathbb{Z}/2\mathbb{Z}$, and the element $1 \otimes 2$.]

Exercise 3.4.5
Let $\{e_1, e_2\}$ be a basis of $V = \mathbb{R}^2$. Show that the element $e_1 \otimes e_2 + e_2 \otimes e_1$ in $V \otimes_{\mathbb{R}} V$ cannot be written as a simple tensor $v \otimes w$ for any $v, w \in \mathbb{R}^2$.

Exercise 3.4.6
Suppose R is commutative and let I and J be ideals of R, so R/I and R/J are naturally R-modules.

(a) Prove that every element of $R/I \otimes_R R/J$ can be written as a simple tensor of the form $(1 + I) \otimes (r + J)$.

(b) Prove that there is an R-module isomorphism $R/I \otimes_R R/J \cong R/(I + J)$ mapping $(r + I) \otimes (r' + J)$ to $rr' + (I + J)$.

Exercise 3.4.7
Let R be a subring of the commutative ring S and let x be an indeterminate over S. Prove that $S[x] \cong S \otimes_R R[x]$ as S-algebras.

3.5 Exact Sequences

The first isomorphism theorem says given two modules B and C and a homomorphism $\varphi : B \to C$ which is surjective, there is a submodule A of B such that $B/A \cong C$. Now we consider the reverse situation: given two A and C, is there a module B such that A is a submodule of B and $B/A \cong B$? If there exists such B, we say B is an *extension of C by A*. We introduce a very convenient notation.

Definition 3.5.1
Suppose a ring has a 1 and $X, Y, Z, \cdots$ are R-modules.

(1) The pair of homomorphisms $X \xrightarrow{\alpha} Y \xrightarrow{\beta} Z$ is said to be *exact* (at Y) if $\operatorname{img}\alpha = \ker\beta$.

(2) A sequence $\cdots \to X_{n-1} \to X_n \to X_{n+1} \to \cdots$ of homomorphisms is said to be an *exact sequence* if it is exact at every X_n between a pair of homomorphisms.

Proposition 3.5.2
Let A, B and C be R-modules over some ring R. Then

(1) The sequence $0 \to A \xrightarrow{\psi} B$ is exact (at A) if and only if ψ is injective.

(2) The sequence $B \xrightarrow{\varphi} C \to 0$ is exact (at C) if and only if φ is surjective.

Proof. Left as an exercise. □

Corollary 3.5.3
The sequence $0 \to A \xrightarrow{\psi} B \xrightarrow{\varphi} C \to 0$ is exact if and only if ψ is injective, φ is surjective, and $\operatorname{img}\psi = \ker\varphi$.

Definition 3.5.4
The exact sequence $0 \to A \xrightarrow{\psi} B \xrightarrow{\varphi} C \to 0$ is called a *short exact sequence*.

Remark 3.5.5
Suppose $X \xrightarrow{\alpha} Y \xrightarrow{\beta} Z$ is exact at Y. Consider the sequence

$$0 \to \operatorname{img}\alpha \xrightarrow{\iota} Y \to Y/\ker\beta \xrightarrow{\pi} 0$$

where $\iota : \operatorname{img}\alpha \to Y$ is an inclusion and $\pi : Y \to Y/\ker\beta$ is a natural projection. Then this sequence is a short exact sequence. So any exact sequence can be written as a succession of short exact sequences.

Example 3.5.6

(1) Given modules A and C, we can always form their direct sum $B = A \oplus C$ and the sequence

$$0 \to A \xrightarrow{\iota} A \oplus C \xrightarrow{\pi} C \to 0$$

where $\iota(a) = (a, 0)$ and $\pi(a, c) = c$ is a short exact sequence.

(2) Consider the two $\mathbb{Z}$-modules $A = \mathbb{Z}$ and $C = \mathbb{Z}/n\mathbb{Z}$:

$$0 \to \mathbb{Z} \xrightarrow{\iota} \mathbb{Z} \oplus (\mathbb{Z}/n\mathbb{Z}) \xrightarrow{\varphi} \mathbb{Z}/n\mathbb{Z} \to 0$$

is a short exact sequence and $\mathbb{Z} \oplus (\mathbb{Z}/n\mathbb{Z})$ is an extension of $\mathbb{Z}/n\mathbb{Z}$ by $\mathbb{Z}$.

Another extension of $\mathbb{Z}/n\mathbb{Z}$ by $\mathbb{Z}$ is given by the short exact sequence

$$0 \to \mathbb{Z} \xrightarrow{n} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/n\mathbb{Z} \to 0$$

where n denotes the map $x \mapsto nx$ given by multiplication by n, and π denotes the natrual projection.

(3) If $\varphi : B \to C$ is any homomorphism we may form an exact sequence:

$$0 \to \ker \varphi \xrightarrow{\iota} B \xrightarrow{\varphi} \operatorname{img} \varphi \to 0.$$

(4) Suppose M is an R-module and S is a set of generators for M. Let $F(S)$ be the free R-module on S. Then the inclusion $S \to M$ induces a homomorphism $F(S) \to M$. Let K be the kernel of this homomorphism. Then

$$0 \to K \xrightarrow{\iota} F(S) \xrightarrow{\varphi} M \to 0$$

is a short exact sequence.

Example 2 shows that for a fixed A and C, in general there may be several extensions of C by A. To distinguish different extensions, we define the notion of a homomorphism between two exact sequences.

A diagram involving various homomorphisms is said to *commute* if any compositions of homomorphisms with the same starting and ending points are equal, i.e., the composite map defined by following a path of homomorphisms in the diagram depends only on the starting and ending points and not on the choice of the path taken.

Definition 3.5.7
Let $0 \to A \to B \to C \to 0$ and $0 \to A' \to B' \to C' \to 0$ be two short exact sequences of modules.

(1) A *homomorphism of short exact sequences* is a triple α, β, γ of module homomorphisms such that the following diagram commutes:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \end{array}$$

The homomorphism is an *isomorphism of short exact sequences* if α, β, γ are all isomorphisms, in which case the extensions B and B' are said to be *isomorphic extensions*.

(2) The two exact sequences are called *equivalent* if $A = A'$, $C = C'$, and there is an isomorphism between them as in (1) that is the identity maps on A and C. (i.e., α and γ are the identity). In this case, the corresponding extensions B and B' are said to be *equivalent* extensions.

Example 3.5.8

(1) Let m and n be integers greater than 1. Assume n divides m and let $k = m/n$. Define

- $\alpha : \mathbb{Z} \to \mathbb{Z}/k\mathbb{Z}, \beta : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ the natural projections
- $\gamma : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ the identity map
- $\iota : \mathbb{Z}/k\mathbb{Z}$ maps $a + k\mathbb{Z} \mapsto na + m\mathbb{Z}$
- $\pi' : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ maps $b + m\mathbb{Z} \mapsto b + n\mathbb{Z}$.

These maps are all well defined and form a homomorphism of exact sequences:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{n} & \mathbb{Z} & \xrightarrow{\pi} & \mathbb{Z}/n\mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & \mathbb{Z}/k\mathbb{Z} & \xrightarrow{\iota} & \mathbb{Z}/m\mathbb{Z} & \xrightarrow{\pi'} & \mathbb{Z}/n\mathbb{Z} & \longrightarrow & 0 \end{array}$$

Hence this is a homomorphism of short exact sequences.

(2) Map each module to itself by $x \mapsto -x$. This is an isomorphism of short exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{n} & \mathbb{Z} & \xrightarrow{\pi} & \mathbb{Z}/n\mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle -1} & & \downarrow{\scriptstyle -1} & & \downarrow{\scriptstyle -1} & & \\ 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{n} & \mathbb{Z} & \xrightarrow{\pi} & \mathbb{Z}/n\mathbb{Z} & \longrightarrow & 0 \end{array}$$

but is not equivalence of sequences.

(3) Consider the maps where

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \xrightarrow{\psi} & \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} & \xrightarrow{\varphi} & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 0 & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \xrightarrow{\psi'} & \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} & \xrightarrow{\varphi'} & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & 0 \end{array}$$

- $\psi(a) = (a, 0)$, $\varphi(a, b) = b$;
- $\psi'(b) = (0, b)$, $\varphi'(a, b) = a$.

If $\beta(a, b) = (b, a)$, this diagram commutes, hence giving an equivalence of the two exact sequences that is not identity isomorphism.

Proposition 3.5.9 (The Short Five Lemma)
Let α, β, γ be a homomorphism of short exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{\psi} & B & \xrightarrow{\varphi} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A' & \xrightarrow{\psi'} & B' & \xrightarrow{\varphi'} & C' & \longrightarrow & 0 \end{array}$$

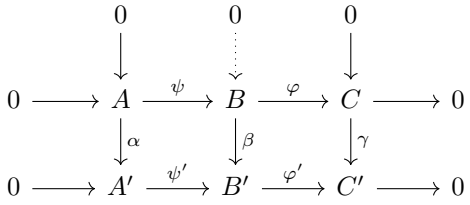
(1) If α and γ are injective, then so is β.

(2) If α and γ are surjective, then so is β.

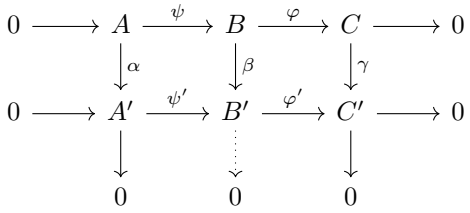
(3) Hence, if α and γ are isomorphisms, then so is β.

Proof. (1) Let $b \in \ker \beta$. Then $\varphi'(\beta(b)) = \varphi'(0) = 0$. Since $\varphi'\beta = \gamma\varphi$, $\gamma(\varphi(b)) = 0$, but γ is injective. Thus $\varphi(b) = 0$, or $b \in \ker \varphi$. Since $\ker \varphi = \operatorname{img} \psi$, $b = \psi(a)$ for some $a \in A$. Then $\beta(\psi(a)) = 0 = \psi'(\alpha(a))$. ψ' is injective and so $\alpha(a) = 0$. Since α is injective, $a = 0$. Finally, $b = \psi(a) = \psi(0) = 0$ and hence β is injective.

As a diagram notation, we can express this result by



(2) Let $b' \in B'$. Since γ is surjective, there is $c \in C$ such that $\gamma(c) = \varphi'(b')$. Since φ is surjective, there is $b \in B$ such that $\varphi(b) = c$, so $\varphi'(b') = \gamma\varphi(b)$. Since $\gamma\varphi = \varphi'\beta$, $\varphi'(b') = \varphi'(\beta(b))$. So $b' - \beta(b) \in \ker\varphi' = \operatorname{img}\psi'$. Let $a' \in A'$ such that $\psi'(a') = b' - \beta(b)$. Since α is surjective, there is $a \in A$ such that $\alpha(a) = a'$. Then $b' - \beta(b) = \psi\alpha(a) = \beta(\varphi(a))$. This implies $b' = \beta(b + \varphi(a))$. Hence β is surjective.



□

This kind of proof is called "diagram chasing". Using finger tips (it may need countably many finger tips), you can follow the diagram.

Definition 3.5.10
Let R be a ring and let $0 \to A \xrightarrow{\psi} B \xrightarrow{\varphi} C \to 0$ be a short exact sequence of R-modules. The sequence is said to be *split* if there is an R-module complement to $\psi(A)$ in B. In this case, up to isomorphism, $B = A \oplus C$ (more precisely, $B = \psi(A) \oplus C'$ for some submodule C, and C' is mapped isomorphically onto C by φ: $\varphi(C') \cong C$).

The question of whether an extension splits is the question of the existence of a complement to $\psi(A)$ in B isomorphic by φ to C, so the notion of a split extension may equivalently be phrased in the language of homomorphisms:

Proposition 3.5.11
The short exact sequence $0 \to A \xrightarrow{\psi} B \xrightarrow{\varphi} C \to 0$ of R-modules is split if and only if there is an R-module homomorphism $\mu : C \to B$ such that $\varphi \circ \mu$ is identity map on C.

Proof. Suppose the short exact sequence is split with $B = A \oplus C'$ where $C \cong \varphi(C')$ via φ. Since $\varphi|C' : C' \to C$ is an isomorphism, we can define $\mu = \varphi^{-1} : C \cong B$ and $\varphi \circ \mu = \varphi \circ \varphi^{-1}$ is the identity map on C.

Suppose $\mu : C \to B$ is given. At first, we will show that every element of B can be written as $\psi(a) + \mu(c)$. Let $b \in B$. Then

$$\varphi(b - \mu(\varphi(b)) = \varphi(b) - \underbrace{\varphi \circ \mu}_{\mathrm{id}}(\varphi(b)) = \varphi(b) - \varphi(b) = 0.$$

Thus $b - \mu(\varphi(b)) \in \ker \varphi = \operatorname{img} \psi$. Let $a \in A$ such that $\psi(a) = b - \mu(\varphi(b))$. Thus $b = \psi(a) + \mu(\varphi(b))$, or $B = \psi(A) + \mu(C)$. Let $b \in \psi(A) \cap \mu(C)$. Then $b = \psi(a) = \mu(c)$ for some $a \in A$ and $c \in C$. Since $\varphi(\psi(a)) = 0$, $\varphi(b) = \varphi(\mu(c)) = c = 0$. Thus $b = \mu(0) = 0$. This implies $B = \psi(A) \oplus \mu(C)$. □

Definition 3.5.12

- With notation as in Proposition 3.5.11, any set map $\mu : C \to B$ such that $\varphi \circ \mu = \mathrm{id}$ is called a *section* of φ.
- If μ is a *homomorphism* as in Proposition 3.5.11, then μ is called a *splitting homomorphism* for the sequence.

Proposition 3.5.13
Let $0 \to A \xrightarrow{\psi} B \xrightarrow{\varphi} C \to 0$ be a short exact sequence of modules. Then $B = \psi(A) \oplus C'$ for some submodule C' of B with $\varphi(C') \cong C$ if and only if there is a homomorphism $\lambda : B \to A$ such that $\lambda \circ \psi$ is the identity map on A.

Proof. This is similar to the proof of Proposition 3.5.11. If C' is given, define $\lambda : B \to A$ by $\lambda(\psi(a) + c') = a$. The unique representation guarantees the well definedness.
Conversely, if λ is given, let $C' = \ker \lambda$. □

3.5.1 Some Examples of a Commutative Diagram

In the beginning, we saw that for given exact sequence $A \xrightarrow{f} B \xrightarrow{g} C$, there is a short exact sequence $0 \to \operatorname{img} f \to B \to B/\ker g \to 0$. The last term is $B/\ker g = B/\operatorname{img} f$. So

$$0 \to \operatorname{img} f \to B \to B/\operatorname{img} f \to 0$$

is a short exact sequence.

Definition 3.5.14
Let $f : A \to B$ be a R-module homomorphism. Then the *cokernel* of f is the quotient module $B/\operatorname{img} f$, denoted by $\operatorname{coker} f$.

Consider a homomorphism of short exact sequences:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{\psi} & B & \xrightarrow{\varphi} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A' & \xrightarrow{\psi'} & B' & \xrightarrow{\varphi'} & C' & \longrightarrow & 0 \end{array}$$

For example, $B \to B'$ indues short exact sequences

$$0 \to \ker \beta \to B \to B/\ker \beta \cong \operatorname{img} \beta \to 0$$

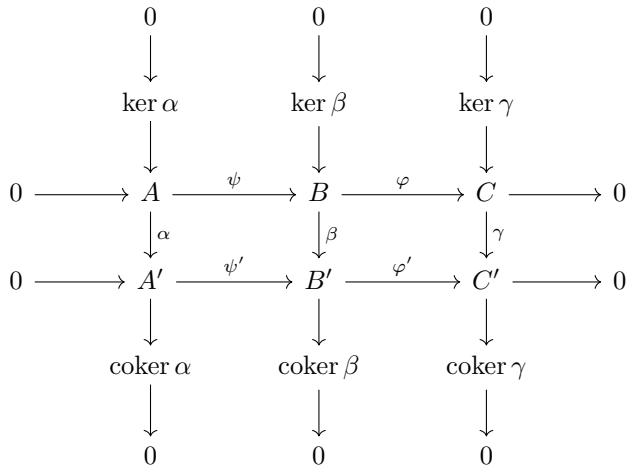
and

$$0 \to \operatorname{img} \beta \to B' \to B'/\operatorname{img} \beta \to 0.$$

Combining these an exact sequence,

$$0 \to \ker \beta \to B \to B' \to \operatorname{coker} \beta \to 0.$$

So we have a commutative diagram whose columns are also exact:



Let $\overline{\psi} = \psi|\ker\alpha$ and $\overline{\varphi} = \varphi|\ker\beta$. For $a \in \ker\alpha$, $\beta(\psi(a)) = \psi'\alpha(a) = \psi'(0) = 0$. So $\psi(a) = \overline{\psi}(a) \in \ker\beta$. Hence $\overline{\psi} : \ker\alpha \to \ker\beta$. Similarly, $\overline{\varphi} : \ker\beta \to \ker\gamma$. Moreover, $0 \to \ker\alpha \to \ker\beta \to \ker\gamma$ is a short exact sequence:

- The exactness of $0 \to \ker\alpha \to \ker\beta$ comes from the exactness of $0 \to A \to B$.
- The exactness of $\ker\alpha \to \ker\beta \to \ker\gamma$ comes from the exactness of $A \to B \to C$: let $b \in \ker\overline{\varphi}$. Then $\overline{\varphi}(b) = \varphi(b) = 0$, so $b \in \ker\varphi = \operatorname{img}\psi$. Let $a \in A$ so that $b = \psi(a)$.

  Since $b \in \ker\beta$, $\beta(b) = \beta\psi(a) = \psi'\alpha(a) = 0$, and the injectivity of ψ' implies $\alpha(a) = 0$. Hence $a \in \alpha$ and $b = \psi(a) = \overline{\psi}(a)$.

Now consider the map $\overline{\psi'} : \operatorname{coker}\alpha \to \operatorname{coker}\beta$ by $\overline{\psi'}(a' + \operatorname{img}\alpha) = \psi'(a) + \operatorname{img}\beta$:

- for $a' + \operatorname{img}\alpha \in \operatorname{coker}\alpha$, consider $\psi'(a' + \alpha(a))$ for any $a \in A$.

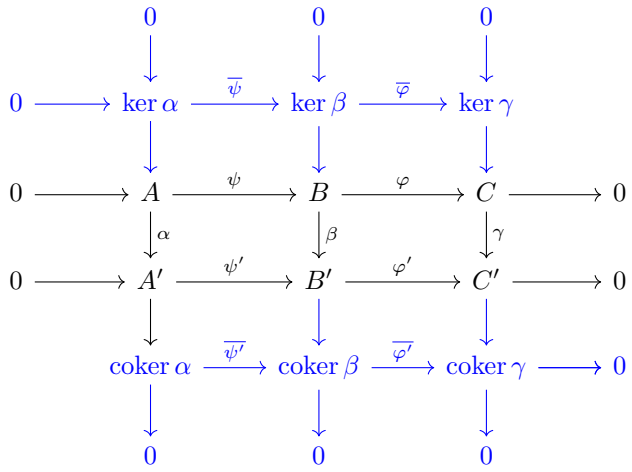
$$\psi'(a' + \alpha(a)) = \psi'(a') + \psi'\alpha(a) = \psi'(a') + \beta\psi(a);$$

- if $a' + \operatorname{img}\alpha = a'' + \operatorname{img}\alpha$, then $a' - a'' = \operatorname{img}(a)$ for some $a \in A$. Then $\psi'(a' - a'') = \psi'\alpha(a) = \beta\psi(a) \in \operatorname{img}\beta$. Thus $\overline{\psi'}(a' + \operatorname{img}\alpha) = \overline{\psi'}(a'' + \operatorname{img}\alpha)$.

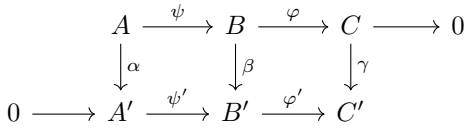
So this map is well defined and you can easily check that it is a homomorphism. Similarly, we can define $\overline{\varphi'} : \operatorname{coker}\beta \to \operatorname{coker}\gamma$. Furthermore, we can show that $\operatorname{coker}\alpha \to \operatorname{coker}\beta\ \operatorname{coker}\gamma \to 0$ is exact:

- The exactness of $\operatorname{coker}\alpha \to \operatorname{coker}\beta \to \operatorname{coker}\gamma$: Since $\varphi'\psi' = 0$, $\overline{\varphi'\psi'} = 0$, that is, $\operatorname{img}\overline{\psi'} \subset \ker\overline{\varphi'}$. Let $b' + \operatorname{img}\beta \in \ker\overline{\varphi'}$. Then $\overline{\varphi'}(b' + \operatorname{img}\beta) = \varphi'(b) + \operatorname{img}\gamma = 0 + \operatorname{img}\gamma$ implies $\varphi'(b') \in \operatorname{img}\gamma$. Let $c \in C$ such that $\varphi'(b') = \gamma(c)$. Since φ is surjective, we have $\varphi'(b') = \gamma\varphi(b) = \varphi'\beta(b)$ for some $b \in B$. Then $\varphi'(b' - \beta(b)) = 0$, so $b' - \beta(b) \in \ker\varphi' = \operatorname{img}\psi$. Let $a' \in A'$ so that $b' - \beta(b) = \psi'(a')$. Thus $b' = \psi'(a') + \beta(b) \in \psi'(a') + \operatorname{img}\beta$, or $b' + \operatorname{img}\beta = \overline{\psi'}(a' + \operatorname{img}\alpha)$.
- The exactness of $\operatorname{coker}\beta \to \operatorname{coker}\gamma \to 0$: it suffices to show that $\overline{\varphi'}$ is surjective. Let $c' + \operatorname{img}\gamma \in \operatorname{coker}\gamma$. From the surjectivity of φ', we have $c' = \varphi'(b')$ for some $b' \in B'$. Thus $c' + \operatorname{img}\gamma = \overline{\varphi'}(b' + \operatorname{img}\beta)$.

Finally, the diagram commutes with rows and columns are exact:



Lemma 3.5.15 (The Snake Lemma)
Suppose



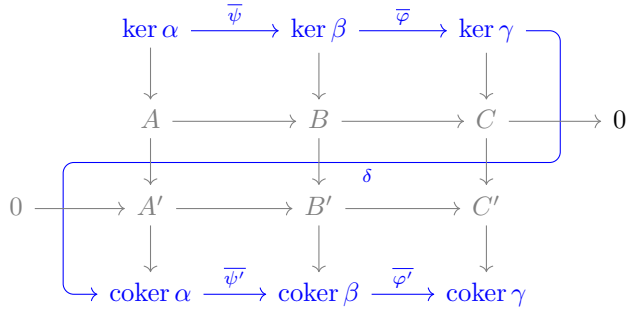
is a commutative diagram of R-modules with exact rows. Then there is a homomorphism $\delta : \ker\gamma \to \operatorname{coker}\alpha$, called a *connecting map* such that

$$\ker\alpha \to \ker\beta \to \ker\gamma \xrightarrow{\delta} \operatorname{coker}\alpha \to \operatorname{coker}\beta \to \operatorname{coker}\gamma$$

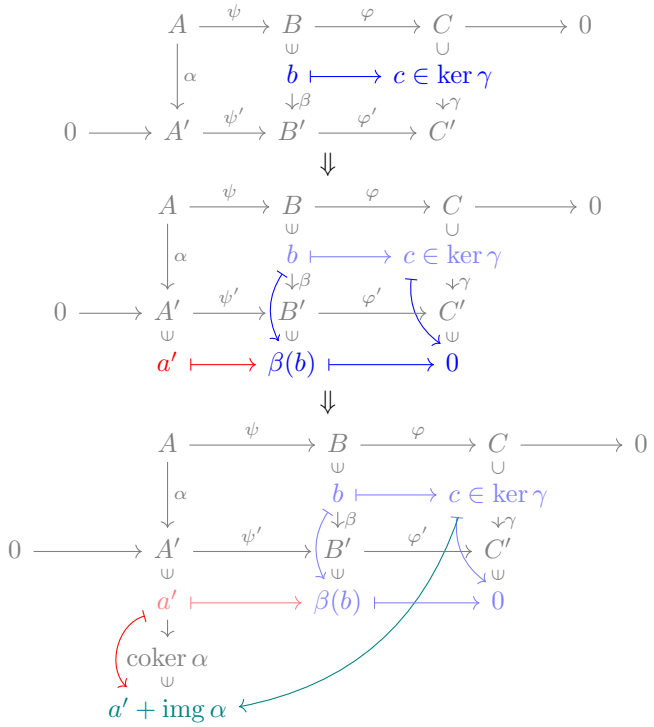
is an exact sequence. If ψ is injective and φ' is surjective, then

$$0 \to \ker\alpha \to \ker\beta \to \ker\gamma \xrightarrow{\delta} \operatorname{coker}\alpha \to \operatorname{coker}\beta \to \operatorname{coker}\gamma \to 0$$

is exact.



Proof. We will construct $\delta : \ker\gamma \to \operatorname{coker}\alpha$ by diagram chasing. Let $c \in \ker\gamma$. Since φ is surjective, we have $b \in B$ such that $\varphi(b) = c$. Then $\gamma(c) = \gamma\varphi(b) = \varphi'\beta(b) = 0$. Thus $\beta(b) \in \ker\varphi' = \operatorname{img}\psi'$. So there is $a' \in A'$ such that $\beta(b) = \psi'(a')$. Now map c to $a' + \operatorname{img}\alpha$.



We must check that this map is well defined.

- Clearly $\delta(c) = a' + \operatorname{img}\alpha \in \operatorname{coker}\alpha$.
- When we choose $b \in B$ such that $\varphi(b) = c$, there may be several choice of such b, but the choice of a' depends on only $\beta(b)$ (not b). Let $\psi'(a'_1) = \beta(b_1)$ and $\psi'(a'_2) = \beta(b_2)$. It may $a'_1 \neq a'_2$, but $a'_1 + \operatorname{img}\alpha = a'_2 + \operatorname{img}\alpha$ as follows: Suppose $\varphi(b_1) = \varphi(b_2) = c$. Then $\varphi(b_1 - b_2) = c - c = 0$, or $b_1 - b_2 \in \ker\varphi = \operatorname{img}\psi$. Let $a \in A$ such that $b_1 - b_2 = \psi(a)$. Then $\beta(b_1 - b_2) = \beta\psi(a) = \psi'\alpha(a)$. Thus

$$\psi'(a'_1) = \beta(b_1) = \beta(b_2) + \psi'\alpha(a) = \psi'(a'_2) + \psi'\alpha(a),$$

or

$$a'_1 = a'_2 + \alpha(a) \implies a'_1 + \operatorname{img}\alpha = a'_2 + \operatorname{img}\alpha$$

because ψ' is injective. Hence $\delta(c)$ is well defined.

By definition, δ is clearly R-module homomorphism and you can easily check that $\ker\beta \to \ker\gamma \to \operatorname{coker}\alpha \to \operatorname{coker}\beta$ is exact. (other positions are already shown).

If ψ is injective and φ' is surjective, we already show that $0 \to \ker\alpha \to \ker\beta$ and $\operatorname{coker}\beta \to \operatorname{coker}\gamma \to 0$ are exact. □

An application of the snake lemma is the short five lemma(Lemma 3.5.9) which is already shown.

If α and γ are injective, we have the diagram whose columns and rows are exact and which commutes:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & 0 & \longrightarrow & \ker\beta & \longrightarrow & 0 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & A & \xrightarrow{\psi} & B & \xrightarrow{\varphi} & C & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} & & \\
0 & \longrightarrow & A' & \xrightarrow{\psi'} & B' & \xrightarrow{\varphi'} & C' & \longrightarrow & 0
\end{array}$$

$0 \to \ker\beta \to 0$ is exact means $\ker\beta \cong 0$. So $\ker\beta = 0$, or β is also injective.

Similarly, if α and γ are surjective, then we have

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A & \xrightarrow{\psi} & B & \xrightarrow{\varphi} & C & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} & & \\
0 & \longrightarrow & A' & \xrightarrow{\psi'} & B' & \xrightarrow{\varphi'} & C' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & 0 & \longrightarrow & \operatorname{coker}\beta & \longrightarrow & 0 & \longrightarrow & 0
\end{array}$$

Then $\operatorname{coker}\beta = B'/\operatorname{img}\beta \cong 0$, or $B' = \operatorname{img}\beta$. Hence β is surjective.

Lemma 3.5.16 (The Five Lemma)
Consider a commutative diagram of R-modules and homomorphisms such that each row is exact:

$$\begin{array}{ccccccccccc}
A_1 & \xrightarrow{\psi_1} & A_2 & \xrightarrow{\psi_2} & A_3 & \xrightarrow{\psi_3} & A_4 & \xrightarrow{\psi_4} & A_5 \\
\downarrow{\scriptstyle\alpha_1} & & \downarrow{\scriptstyle\alpha_2} & & \downarrow{\scriptstyle\alpha_3} & & \downarrow{\scriptstyle\alpha_4} & & \downarrow{\scriptstyle\alpha_5} \\
B_1 & \xrightarrow{\varphi_1} & B_2 & \xrightarrow{\varphi_2} & B_3 & \xrightarrow{\varphi_3} & B_4 & \xrightarrow{\varphi_4} & B_5
\end{array}$$

(1) If α_1 is surjective and α_2 and α_4 are injective, then α_3 is injective.

(2) If α_5 is injective and α_2 and α_4 are surjective, then α_3 is surjective.

The easiest proof is "diagram chasing", but this proof is not 'beautiful'. I want to use the snake lemma (in fact, use the short five lemma). To do this, we should manipulate the diagram.

Proposition 3.5.17
Consider a commutative diagram of R-modules and homomorphisms such that each row is exact and suppose α_1 is surjective :

$$\begin{array}{ccccccc}
A_1 & \xrightarrow{\psi_1} & A_2 & \xrightarrow{\psi_2} & A_3 & \xrightarrow{\psi_3} & A_4 \\
\downarrow{\scriptstyle \alpha_1} & & \downarrow{\scriptstyle \alpha_2} & & \downarrow{\scriptstyle \alpha_3} & & \downarrow{\scriptstyle \alpha_4} \\
B_1 & \xrightarrow{\varphi_1} & B_2 & \xrightarrow{\varphi_2} & B_3 & \xrightarrow{\varphi_3} & B_4 \\
\downarrow & & & & & & \\
0 & & & & & &
\end{array}$$

Then

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \operatorname{coker}\psi_1 & \xrightarrow{\widetilde{\psi}_2} & A_3 & \xrightarrow{\psi_3} & \operatorname{img}\psi_3 & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \widetilde{\alpha}_2} & & \downarrow{\scriptstyle \alpha_3} & & \downarrow{\scriptstyle \widetilde{\alpha}_4} & & \\
0 & \longrightarrow & \operatorname{coker}\varphi_1 & \xrightarrow{\widetilde{\varphi}_2} & B_3 & \xrightarrow{\varphi_3} & \operatorname{img}\varphi_3 & \longrightarrow & 0
\end{array}$$

is a homomorphism of short exact sequences, where

- $\widetilde{\psi}_2(a_2 + \operatorname{img}\psi_1) = \psi_2(a_2)$,
- $\widetilde{\varphi}_2(b_2 + \operatorname{img}\varphi_1) = \varphi_2(b_2)$,
- $\widetilde{\alpha}_2(a_2 + \operatorname{img}\psi_1) = \alpha_2(a_2) + \operatorname{img}\varphi_1$,
- $\widetilde{\alpha}_4 = \alpha_4|\operatorname{img}\psi_3$.

Moreover, if α_2 is injective, so is $\widetilde{\alpha}_2$.

Proof. We must show (i) each function is well defined, (ii) each row is exact, and (iii) the diagram commutes.

(i) and (ii):

- Suppose $a_2 + \operatorname{img}\psi_1 = a_2' + \operatorname{img}\psi_1$. Then $a_2 - a_2' \in \operatorname{img}\psi_1 = \ker\psi_2$. Thus $\psi_2(a_2) = \psi_2(a_2')$. Hence $\widetilde{\psi}_2$ is well defined.

  Also, $\alpha_2(a_2 - a_2') = \alpha_2\psi_1(a) = \varphi_1\alpha_1(a)$ implies $\alpha_2(a_2) + \operatorname{img}\varphi_1 = \alpha_2(a_2') + \operatorname{img}\varphi_1$. Hence $\widetilde{\alpha}_2$ is also well defined.

- Since $\psi_3\widetilde{\psi}_2(a_2 + \operatorname{img}\psi_1) = \psi_3\psi_2(a_2) = 0$, $\operatorname{img}\widetilde{\psi}_2 \subset \ker\psi_3$. Let $a_3 \in \ker\psi_3$. Since $\ker\psi_3 = \operatorname{img}\psi_2$, $a_3 = \psi_2(a_2)$ for some $a_2 \in A_2$, hence $a_3 = \widetilde{\psi}_2(a_2 + \operatorname{img}\psi_1)$. So this row is exact. This proof is also true for the second row.

(iii): Clearly, $\widetilde{\alpha}_3\psi_3 = \varphi_3\alpha_3$. Let $a_2 + \operatorname{img}\psi_1 \in \operatorname{coker}\psi_1$. Then

$$\begin{aligned}
\alpha_3\widetilde{\psi}_2(a_2 + \operatorname{img}\psi_1) &= \alpha_3\psi_2(a_2) = \varphi_2\alpha_2(a_2) \\
&= \widetilde{\varphi}_2(\alpha_2(a_2) + \operatorname{img}\varphi_1) = \widetilde{\varphi}_2\widetilde{\alpha}_2(a_2 + \operatorname{img}\psi_1).
\end{aligned}$$

Moreover, suppose α_2 is injective. If $\widetilde{\alpha_2}(a_2 + \operatorname{img}\psi_1) = 0 + \operatorname{img}\varphi_1$, then $\alpha_2(a_2) \in \operatorname{img}\varphi_1$. Let $b_1 \in B_1$ such that $\alpha_2(a_2) = \varphi_1(b_1)$. Since α_1 is surjective, we have $a_1 \in A_1$ such that $b_1 = \alpha_1(a_1)$. So $\alpha_2(a_2) = \varphi_1\alpha_1(a_1) = \alpha_2\psi_1(a_1)$. But α_2 is injective, so $a_2 = \psi_1(a_1)$, or $a_2 + \operatorname{img}\psi_1 = 0 + \operatorname{img}\psi_1$. Hence $\widetilde{\alpha}_2$ is also injective. □

Note that if α_4 is injective, then so is $\widetilde{\alpha}_4$. So (1) of the five lemma is immediate from this proposition.

Similarly, we can prove (2) of the five lemma.

Proposition 3.5.18
Consider a commutative diagram of R-modules and homomorphisms such that each row is exact and suppose α_5 is injective :

$$\begin{array}{ccccccccc}
 & & & & & & & & 0 \\
 & & & & & & & & \downarrow \\
A_2 & \xrightarrow{\psi_2} & A_3 & \xrightarrow{\psi_3} & A_4 & \xrightarrow{\psi_4} & A_5 \\
\downarrow{\scriptstyle \alpha_3} & & \downarrow{\scriptstyle \alpha_4} & & \downarrow{\scriptstyle \alpha_5} & & \downarrow{\scriptstyle \alpha_5} \\
B_2 & \xrightarrow{\varphi_2} & B_3 & \xrightarrow{\varphi_3} & B_4 & \xrightarrow{\varphi_4} & B_5
\end{array}$$

Then

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \ker\psi_3 & \xrightarrow{\iota_3} & A_3 & \xrightarrow{\psi_3} & \operatorname{img}\psi_3 & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \widetilde{\alpha}_2} & & \downarrow{\scriptstyle \alpha_3} & & \downarrow{\scriptstyle \widetilde{\alpha}_4} & & \\
0 & \longrightarrow & \ker\varphi_3 & \xrightarrow{\jmath_3} & B_3 & \xrightarrow{\varphi_3} & \operatorname{img}\varphi_3 & \longrightarrow & 0
\end{array}$$

is a homomorphism of short exact sequences, where

- ι_3 and $\jmath_3$ are inclusions,
- $\widetilde{\alpha}_2 = \alpha_2|\ker\psi_3$,
- $\widetilde{\alpha}_4 = \alpha_4|\operatorname{img}\psi_3$.

Moreover, if α_2 is surjective, so is $\widetilde{\alpha}_2$ and if α_4 is surjective, so is $\widetilde{\alpha}_4$.

Proof. Left as an exercise. □

3.5.2 Exercise

Exercise 3.5.1 (3×3 Lemma)
Consider the following commutative diagram in R-modules having exact rows.

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & A'' & \longrightarrow & B'' & \longrightarrow & C'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

(1) If the last two columns are exact, prove that the first column is exact.

(2) If the first two columns are exact, prove that the last column is exact.

3.6 Direct Products and Direct Sums

3.6.1 Arbitrary Direct Products and Direct Sums

Given $M_1, \cdots, M_n$, we have $M_1 \times \cdots \times M_n$, $M_1 \oplus \cdots \oplus M_n$ and $M_1 \otimes \cdots \otimes M_n$. In this case, $M_1 \times \cdots \times M_n \cong M_1 \oplus \cdots \oplus M_n$. Now we will construct direct products, direct sums and tensor products on arbitrary collections.

Recall that a Cartesian product $\prod_{i\in I} A_i$ of some collection of sets $\{A_i : i \in I\}$ with some index set I is the collection of all choice function $f : I \to \bigcup_{i\in I} A_i$. (Definition 0.5.1). If each A_i is R-module, $\prod A_i$ is again R-module with componentwise operations:

$$(a_i)_{i\in I} + (b_i)_{i\in I} = (a_i + b_i)_{i\in I}, r(a_i)_{i\in J} = (ra_i)_{i\in I}.$$

We call it the direct product of $\{A_i\}$.

Consider a subset A of $\prod A_i$ containing all choice function such that $f(i) = 0$ except for only finitely many i's, i.e., $\{i : f(i) \neq 0\}$ is finite. Then for $f, g \in A$ and for $r \in R$, $f + g$ and rf also belong to A. Thus A is a submodule of $\prod A_i$. We call A the direct sum of $\{A_i\}$.

Proposition 3.6.1
Let I be a nonempty index set and for each $i \in I$, let N_i be a submodule of M. The following are equivalent:

(1) the submodule of M generated by all the N_i's is isomorphic to the dirct sum of the N_i's;

(2) if $\{i_1, \cdots, i_k\}$ is any finite subset of I, then $N_{i_1} \cap (N_{i_2} + \cdots + N_{i_k}) = 0$;

(3) if $\{i_1, \cdots, i_k\}$ is any finite subset of I, then $N_{i_1} + \cdots + N_{i_k} = N_{i_1} \oplus \cdots \oplus N_{i_k}$;

(4) for every element x of the submodule of M generated by the N_i's, there are unique elements $a_i \in N_i$ for all $i \in I$ such that all but only finite number of the a_i are zero and x is the (finite) sum of the a_i.

In (4), the sum is well defined because only finitely many a_i's are nonzero.

Proof. (2) $\iff$ (3) comes from 3.3.7. The proof of (2), (3) $\iff$ (4) is almost same: If x is an element of the submodule generated by N_i, there is finite number of $n_{i_j} \in N_{i_j}$ such that $x = n_{i_1} + \cdots + n_{i_k}$. Then $x \in N_{i_1} + \cdots + N_{i_k}$. By (2) or (3), this sum is unique in $N_{i_1} + \cdots + N_{i_k}$. If $x = n_{j_1} + \cdots + n_{j_l}$, $x \in N_{i_1} + \cdots + N_{i_k} + N_{j_1} + \cdots + N_{j_l}$. Since $N_{i_1} + \cdots + N_{i_k}$ is a submodule of $N_{i_1} + \cdots + N_{i_k} + N_{j_1} + \cdots + N_{j_l}$, $n_{j_t} = 0$ for $j_t \notin \{i_1, \cdots, i_k\}$. This implies the expression is unique. In similar way, the converse holds.

Finally, (1) implies (4) because $x \in \bigoplus N_i$ has a unique expression. Conversely, using (4) we can define a map $x = n_{i_1} + \cdots + n_{i_k}$ mapping (x_i where $x_{i_j} = n_{i_j}$ and otherwise $x_i = 0$. This map is isomorphic. □

Proposition 3.6.2
Suppose F is a free R-module with basis A. Then $F \cong \bigoplus_{a\in A} R$.

Proof. Define a map $a \mapsto 1_a$, where $1_a(x) = 0$ for $x \neq a$ and $1_a(a) = 1$. This map can be extended to a map $\varphi : F \to \bigoplus_{a\in A} R$. Clearly, φ is injective. For $(x_a)_{a\in A} \in \bigoplus_{a\in A} R$, $(x_a)_{a\in A} = \sum x_a 1_a$. Since only finitely many x_a are nonzero, this sum is well defined. So $x = \varphi(\sum x_a a)$. □

So every free module isomorphic to some direct sum of R copies.

Corollary 3.6.3
Let $\{F_i : i \in I\}$ be a collection of free R-modules. Then $\bigoplus F_i$ is again free.

Proof. Let A_i be a basis of F_i for each i. Let $A = \bigcup A_i \times \{i\}$ (we call this union a disjoint union denoted by $\bigcup\!\!\!\cdot\, A_i$). Then $A \to \bigoplus F_i$ by $(a, i) \mapsto f_a$ where $f_a(i) = a$ and $f_a(j) = 0$ otherwise induces an isomorphism between $\bigoplus_A R$ and $\bigoplus F_i$. Since $\bigoplus_A R$ is free, so is $\bigoplus F_i$. □

Example 3.6.4 (An arbitrary direct product of free modules need not be free) For each $i \in \mathbb{Z}^+$, let M_i be the free $\mathbb{Z}$-module $\mathbb{Z}$, and let M be the direct product $\prod_{i\in\mathbb{Z}^+} M_i$. Each element of M can be written uniquely in the form $(a_1, a_2, \cdots)$ with $a_i \in \mathbb{Z}$ for all i. Let N be the submodule of M consisting of all such tuples with only finitely many nonzero a_i. Assume M is a free $\mathbb{Z}$-module with basis $\mathcal{B}$.

(1) N is countable: Let $N_n = \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{n \text{ times}} \times 0 \times \cdots$. Then $N_n \subset N$ and for each $x \in N - \{0\}$, let $n = \max\{i : x_i \neq 0\}$. then $x_n \in N_n$. Thus $N = \bigcup_{n=1}^{\infty} N_n$ and each N_n is countable. So N is countable.

(2) For each n, N_n is a submodule of M and is generated by $\{e_1, \cdots, e_n\}$. Then for each i, there is $\{b_{i1}, \cdots, b_{ik_i}\} \subset \mathcal{B}$ such that e_i is a $\mathbb{Z}$-linear combination of $\{b_{i1}, \cdots, b_{ik_i}\}$. Collect all such b_{ij}'s and denote $\mathcal{B}_1$. Then $\mathcal{B}_1$ is countable. Let N_1 be the module generated by $\mathcal{B}_1$ and N_2 be the module generated by $\mathcal{B} - \mathcal{B}_1$. Since $\mathcal{B}_1$ is countable, so is N_1. You can easily show that $M = N_1 \oplus N_2$, $N \subset N_1$ and N_1, N_2 are free. Then $M/N_1 \cong N_2$ is free.

(3) Let $\overline{M} = M/N_1$. Suppose $\overline{x} \in \overline{M}$ is nonzero. Then $\overline{x} = n_1\overline{b}_1 + \cdots + n_k\overline{b}_k$ for some $b_1, \cdots, b_k \in \mathcal{B} - \mathcal{B}_1$ (and this $\mathbb{Z}$-linear combination is unique). So there is only finitely many k's such that $\overline{x} = k\overline{m}$ for some $m \in M$.

(4) Let $\mathcal{S} = \{(b_1, b_2, b_3, \cdots) : b_i = \pm i!\}$ where $k! = k \cdot (k-1) \cdots 1$. By using Cantor method, you can show that $\mathcal{S}$ is uncountable, and so there is $s \in \mathcal{S} - N_1$. Since $s \notin N_1$, $\overline{s} \neq 0$. Let k be any positive integer. Note that $\overline{s} = \overline{s}'$ where $s' = (\underbrace{0, \cdots, 0}_{k-1 \text{ terms}}, \pm k!, \pm(k+1)!, \cdots)$ (the sign is the same of s). Since $s' = k(\underbrace{0, \cdots, 0}_{k-1 \text{ terms}}, \pm(k-1)!, \pm(k)!, \cdots)$. But it contradicts that there is only finitely many such k. Hence M is not free.

In summary,

- (Finite or infinite) Direct sum of free modules is again free.
- Finite direct product of free modules is free.
- But when we product infinitely many free modules, the result module may not be free.

3.6.2 Basic Properties

Proposition 3.6.5
Let $\{M_i : i \in I\}, \{N_i : i \in I\}$ be collections of R-modules and let M and N be R-modules. Then the followings are isomorphic as groups, respectively. If R is commutative, they are isomorphic as R-modules.

(1) $\mathrm{Hom}_R(M, \prod_{i\in I} N_i) \cong \prod_{i\in I} \mathrm{Hom}_R(M, N_i)$.

(2) $\mathrm{Hom}_R(\bigoplus_{i\in I} M_i, N) \cong \prod_{i\in I} \mathrm{Hom}_R(M_i, N)$.

Proof. (1) Define $f \mapsto (\pi_i \circ f)_{i\in I}$ where $\pi_j : \prod_{i\in I} N_i \to N_j$ is the projection map.

(2) Define $f \mapsto (f_i)_{i\in I}$ where $f_i = f|M_i : M_i \to N$.

□

Proposition 3.6.6
Let M be a right R-module and $\{N_i : i \in I\}$ be collections of left R-modules. Then

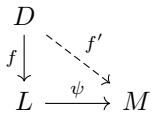
$$M \otimes \left(\bigoplus N_i\right) \cong \bigoplus (M \otimes N_i) .$$

as gruops. If M is (S, R)-bimodule, the isomorphism is an S-module isomorphism. Hence if R is commutative, it is an isomorphism of R-modules.

Proof. Define $M \times (\bigoplus N_i)$ by $(m, \bigoplus n_i) \mapsto \bigoplus m \otimes n_i$. Since $n_i = 0$ for all but finite many i's, this map is well-defined and R-balanced. Then it induces a group homomorphism $M \otimes (\bigoplus N_i) \to \bigoplus (M \otimes N_i)$ such that $m \otimes (\bigoplus n_i) \mapsto \bigoplus m \otimes n_i$. It remains to show that it is an isomorphism. □

3.7 Projective Modules

Let $f : D \to L$ and $\psi : L \to M$ be two homomorphisms. Then we get a homomorphism $\psi \circ f : D \to L$. That means we have the following commutative diagram:



Thus ψ induces a group homomorphism $\psi' : \mathrm{Hom}_R(D, L) \to \mathrm{Hom}_R(D, M)$.

Theorem 3.7.1
Let D,L, and M be R-modules and let $\psi : L \to M$ be an R-module homomorphism. Then the map

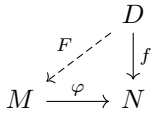
$$\psi'(f) = \psi \circ f.$$

is a group homomorphism. If ψ is injective, then ψ' is also injective, i.e.,

$$\text{if } 0 \to L \xrightarrow{\psi} M \text{ is exact,}$$
$$\text{then } 0 \to \mathrm{Hom}_R(D, L) \xrightarrow{\psi'} \mathrm{Hom}_R(D, M) \text{ is also exact.}$$

Proof. To show that ψ' is a homomorphism is easy. Suppose ψ is injective. Let $\psi'(f) = 0$. Then for all $x \in D$, $\psi'(f)(x) = \psi(f(x)) = 0$. Since ψ is injective, $f(x) = 0$ for all $x \in D$. Hence $f = 0$. □

Given homomorphism $f : D \to N$, consider whether there exists an homomorphism $F : D \to M$ that *extends* or *lifts* f to M, i.e. that makes the following diagram commute: Unfortunately, there may not exist such F in general.



Example 3.7.2
Consider the nonsplit exact sequence $0 \to \mathbb{Z} \xrightarrow{2} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/2\mathbb{Z} \to 0$. Let $D = \mathbb{Z}/2\mathbb{Z}$ and $f : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ be the identity map. There is only one homomorphism $F : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}$, namely the zero map. (because $0 = F(0) = F(\overline{1}) + F(\overline{1})$.) Thus there is no extension of f to $\mathbb{Z}$ via π.

This example shows that

$$\text{if } M \xrightarrow{\varphi} N \to 0 \text{ is exact,}$$
$$\text{then } \mathrm{Hom}_R(D, M) \xrightarrow{\varphi'} \mathrm{Hom}_R(D, N) \to 0 \text{ is } \textit{not necessarily} \text{ exact.}$$

Theorem 3.7.3
Let D, L, M, and N be R-modules.

(1) If

$$0 \to L \xrightarrow{\psi} M \xrightarrow{\varphi} N \to 0 \text{ is exact,}$$

then the associated sequence

$$0 \to \mathrm{Hom}_R(D, L) \xrightarrow{\psi'} \mathrm{Hom}_R(D, M) \xrightarrow{\varphi'} \mathrm{Hom}_R(D, N) \text{ is exact.}$$

(2) $f : D \to N$ lifts to $F : D \to M$ if and only if $f \in \mathrm{img}\, \varphi'$.

(3) φ' is surjective if and only if every homomorphism from D to N lifts to a homomorphism from D to M.

(4) $0 \to \mathrm{Hom}_R(D, L) \xrightarrow{\psi'} \mathrm{Hom}_R(D, M) \xrightarrow{\varphi'} \mathrm{Hom}_R(D, N)$ is exact for all D if and only if $0 \to L \xrightarrow{\psi} M \xrightarrow{\varphi} N$ is exact.

Proof. We will prove only (1). (2),(3), and (4) are almost trivial.

Suppose $0 \to L \xrightarrow{\psi} M \xrightarrow{\varphi} N \to 0$ is exact. Then we have

$$0 \to \mathrm{Hom}_R(D, L) \xrightarrow{\psi'} \mathrm{Hom}_R(D, M).$$

So it suffices to show that

$$\mathrm{Hom}_R(D, L) \xrightarrow{\psi'} \mathrm{Hom}_R(D, M) \xrightarrow{\varphi'} \mathrm{Hom}_R(D, N)$$

is exact.

Let $f \in \mathrm{Hom}_R(D, L)$. For all $d \in D$, $\varphi'\psi'(f)(d) = \varphi\psi(f(d)) = 0$. So $\varphi'\psi'(f) = 0$, or $\mathrm{img}\, \psi' \subset \ker \varphi'$.

Let $f \in \ker \varphi'$. Then $\varphi'(f)(d) = 0 = \varphi(f(d))$ for all $d \in D$. So $f(d) \in \ker \varphi = \mathrm{img}\, \psi$. Then for each $d \in D$, there is $l \in L$ such that $f(d) = \psi(l)$. Define $F : D \to L$ by $F(d) = l$. F is well defined because ψ is injective. It is an easy check to verify that F is a homomorphism. Finally, $\psi'(F)(d) = \psi(F(d)) = \psi(l) = f(d)$ for all d. So $f = \psi'(F)$, or $\ker \varphi' \subset \mathrm{img}\, \psi'$. □

Proposition 3.7.4
Let P be an R-module. Then the following are equivalent:

(1) For any R-modules L, M, and N, if

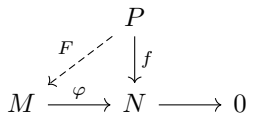
$$0 \to L \xrightarrow{\psi} M \xrightarrow{\varphi} N \to 0$$

is a short exact sequence, then

$$0 \to \mathrm{Hom}_R(P, L) \xrightarrow{\psi'} \mathrm{Hom}_R(P, M) \xrightarrow{\varphi'} \mathrm{Hom}_R(P, N) \to 0$$

is also a short exact sequence.

(2) For any R-modules M and N, if $M \xrightarrow{\varphi} N \to 0$ is exact, then every R-module homomorphism from P into N lifts to an R-module homomorphism into M, i.e., given $f \in \mathrm{Hom}_R(P, N)$, there is a lift $F \in \mathrm{Hom}_R(P, M)$ making the following diagram commute:

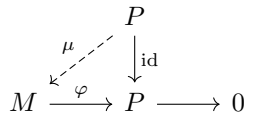


(3) If P is a quotient of the R-module M, then P is isomorphic to a direct summand of M, i.e., every short exact sequence $0 \to L \to M \to P \to 0$ splits.

(4) P is a direct summand of a free R-module.

Proof. The equivalence of (1) and (2) is a restatement of a result in above theorem.

(2) $\Longrightarrow$ (3) Suppose P is a quotient of M, i.e., $M \to P \to O$ is exact. Then the following diagram commutes:



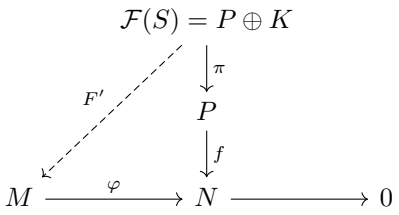
So $\varphi \circ \mu = \mathrm{id}$, or μ is a splitting homomorphism, i.e.,

$$0 \to \ker \varphi \to M \to P \to 0$$

splits.

(3) $\Longrightarrow$ (4) Recall that every module is a quotient module of a free module, say F. Then by (3), $0 \to \ker \varphi \to F \xrightarrow{\varphi} P \to 0$ splits. Thus $F = P \oplus \ker \varphi$, or P is a direct summand of a free module.

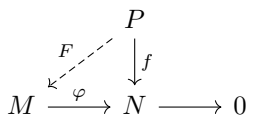
(4) $\Longrightarrow$ (2) Suppose $M \xrightarrow{\varphi} N \to 0$ is exact and $f : P \to N$ is a homomorphism. Then P is a direct summand of a free module $\mathcal{F}(S)$ with basis S, i.e., $\mathcal{F}(S) = P \oplus K$. Then we have the following commutative diagram:



Since φ is surjective, we can define $F'(s)$ so that $\varphi F'(s) = f\pi(s)$ for all $s \in S$ and it can be extended to a homomorphism $\mathcal{F}(S) \to M$. Define $F : P \to M$ by $F(d) = F'(d, 0)$. Since F is the composite of the injection $P \to \mathcal{F}(S)$ with F', F is an R-module homomorphism and

$$\varphi F(d) = \varphi F'(d, 0) = f\pi(d, 0) = f(d),$$

i.e., $\varphi F = f$ and the diagram



commutes. □

Definition 3.7.5
An R-module P is called *projective* if it satisfies any of the equivalent condition of Proposition 3.7.4.

Corollary 3.7.6

(1) Free modules are projective.

(2) A finitely generated module is projective if and only if it is a direct summand of a finitely generated free module.

(3) Every module is a quotient of a projective module.

Proof. This results are immediate from Proposition 3.7.4. □

3.7.1 Covariant functor

Fix D. Then given R-module X, $\mathrm{Hom}_R(D, X)$ is an abelian group. So $\mathrm{Hom}_R(D, \_\_)$ behaves like a function. Moreover, if $f : X \to Y$ is a R-module homomorphism, then there is an associated group homomorphism $\mathrm{Hom}_R(D, f) : \mathrm{Hom}_R(D, X) \to \mathrm{Hom}_R(D, Y)$. Roughly speaking, $\mathrm{Hom}_R(D, \_\_)$ maps not only R-modules to abelian groups but also R-module homomorphisms to group homomorphisms. We call this correspondence a covariant functor.

A covariant functor $\mathcal{F}$ is called a *left exact* functor if

$$0 \to X \xrightarrow{f} Y \xrightarrow{g} Z \to 0$$

is an exact sequence, then

$$0 \to \mathcal{F}(X) \xrightarrow{\mathcal{F}(f)} \mathcal{F}(Y) \xrightarrow{\mathcal{F}(g)} \mathcal{F}(Z)$$

is exact. If

$$0 \to \mathcal{F}(X) \xrightarrow{\mathcal{F}(f)} \mathcal{F}(Y) \xrightarrow{\mathcal{F}(g)} \mathcal{F}(Z) \to 0,$$

$\mathcal{F}$ is called an *exact functor*. In this language, we can say

Corollary 3.7.7

(1) For every R-module D, $\mathrm{Hom}_R(D, \_\_)$ is a left exact functor.

(2) P is projective module if and only if $\mathrm{Hom}_R(P, \_\_)$ is an exact functor.

Example 3.7.8

(1) If F is a field, every F-module (F-vector space) is projective.

(2) $\mathbb{Z}$ is a projective $\mathbb{Z}$-module (because it is free). We can show this directly as follows: suppose $f : \mathbb{Z} \to N$ is a $\mathbb{Z}$-module homomorphism and $\varphi : M \to N$ is a surjective homomorphism. f is uniquely determined by $n = f(1)$. Then f can be lifted to a homomorphism $F : \mathbb{Z} \to M$ by $F(1) = m$ where $\varphi(m) = n$.

(3) $\mathbb{Z}$-module $\mathbb{Z}/n\mathbb{Z}$ is not projective for $n \geq 2$. Consider the following short exact sequence

$$0 \to \mathbb{Z} \xrightarrow{n} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/n\mathbb{Z} \to 0.$$

After taking $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \_\_)$, we get

$$0 \to 0 \xrightarrow{n'} 0 \xrightarrow{\pi'} \mathbb{Z}/n\mathbb{Z} \to 0$$

which is not exact at $\mathbb{Z}/n\mathbb{Z}$.

(4) $\mathbb{Q}/\mathbb{Z}$ is not projective.

$$0 \to \mathbb{Z} \to \mathbb{Q} \xrightarrow{\pi} \mathbb{Q}/\mathbb{Z} \to 0$$

does not split since $\mathbb{Q}$ contains no submodule isomorphic to $\mathbb{Q}/\mathbb{Z}$.

(5) $\mathbb{Z}$-module $\mathbb{Q}$ is not projective.

(6) The direct sum of two projective modules is again projective.

3.8 Injective Modules

Let $0 \to L \xrightarrow{\psi} M \xrightarrow{\varphi} N \to 0$ be a short exact sequence. Then a homomorphism $f : N \to D$ can be extended to $f' : M \to D$ by $f' = f \circ \varphi$. So φ induces a group homomorphism

$$\begin{aligned} \varphi' : \mathrm{Hom}_R(N, D) &\to \mathrm{Hom}_R(M, D) \\ f &\mapsto f' = f \circ \varphi \end{aligned}$$

Theorem 3.8.1
Let D,M, and N be R-modules and let $\varphi : M \to N$ be an R-module homomorphism. Then the map

$$\varphi'(f) = f \circ \varphi.$$

is a group homomorphism. If φ is surjective, then φ' is injective, i.e.,

$$\text{if } M \xrightarrow{\varphi} N \to 0 \text{ is exact,}$$

$$\text{then } 0 \to \mathrm{Hom}_R(N, D) \xrightarrow{\varphi'} \mathrm{Hom}_R(M, D) \text{ is also exact.}$$

(The arrows are reversed!)

Theorem 3.8.2
Let D, L, M, and N be R-modules.

(1) If

$$0 \to L \xrightarrow{\psi} M \xrightarrow{\varphi} N \to 0 \text{ is exact,}$$

then,

$$0 \to \mathrm{Hom}_R(N, D) \xrightarrow{\varphi'} \mathrm{Hom}_R(M, D) \xrightarrow{\psi'} \mathrm{Hom}_R(L, D) \text{ is exact.}$$

(2) $f : L \to D$ lifts to $F : M \to D$ if and only if $f \in \mathrm{img}\, \psi'$.

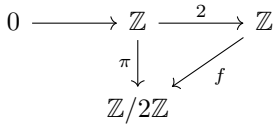
(3) ψ' is surjective if and only if every homomorphism from L to D lifts to a homomorphism from M to D.

(4) $0 \to \mathrm{Hom}_R(N, D) \xrightarrow{\varphi'} \mathrm{Hom}_R(M, D) \xrightarrow{\psi'} \mathrm{Hom}_R(L, D)$ is exact for all D if and only if $L \xrightarrow{\psi} M \xrightarrow{\varphi} N \to 0$ is exact.

In general, the exactness of $0 \to L \to M$ does not guarantee the exactness of $\mathrm{Hom}_R(M, D) \to \mathrm{Hom}_R(L, D) \to 0$. For example, consider $0 \to \mathbb{Z} \xrightarrow{2} \mathbb{Z}$ and $\pi : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ the natural projection and suppose there is $f : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ such that $\pi = 2 \circ f$.

Then $\pi(x) = f(2x) = 2f(x) = 0$ but π is not 0.

Proposition 3.8.3
Let Q be an R-module. Then the following are equivalent:



(1) For any R-modules L, M, and N, if

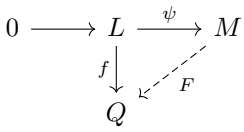
$$0 \to L \xrightarrow{\psi} M \xrightarrow{\varphi} N \to 0$$

is a short exact sequence, then

$$0 \to \mathrm{Hom}_R(N, Q) \xrightarrow{\varphi'} \mathrm{Hom}_R(M, Q) \xrightarrow{\psi'} \mathrm{Hom}_R(L, Q) \to 0$$

is also a short exact sequence.

(2) For any R-modules L and M, if $0 \to L \xrightarrow{\psi} M$ is exact, then every R-module homomorphism from L into Q lifts to an R-module homomorphism of M into Q, i.e., given $f \in \mathrm{Hom}_R(L, Q)$, there is a lift $F \in \mathrm{Hom}_R(M, Q)$ making the following diagram commute:



(3) If Q is a submodule of the R-module M, then Q is a direct summand of M, i.e., every short exact sequence $0 \to Q \to M \to N \to 0$ splits.

Proof. (1) $\iff$ (2) is a part of Theorem 3.7.4

(2) $\implies$ (3) Let $0 \to Q \xrightarrow{\psi} M \xrightarrow{\varphi} N \to 0$ be exact. Taking $L = Q$ and $f : Q \to Q$ the identity map, there is a homomorphism $F : M \to Q$ with $F \circ \psi = q$, so F is a splitting homomorphism for the sequence.

To show (3) $\implies$ (2), see Exercise 3.9.7 □

Definition 3.8.4
An R-module P is called *injective* if it satisfies any of the equivalent condition of Proposition 3.8.3.

3.8.1 Covariant functor

Given D, $\mathrm{Hom}_R(\_\_, D)$ has a name, a *contravariant functor*. ('contravariant' means 'direction revsersing').

A contravariant functor $\mathcal{F}$ is called a *left exact* functor if

$$0 \to X \xrightarrow{f} Y \xrightarrow{g} Z \to 0$$

is an exact sequence, then

$$0 \to \mathcal{F}(Z) \xrightarrow{\mathcal{F}(g)} \mathcal{F}(Y) \xrightarrow{\mathcal{F}(f)} \mathcal{F}(X)$$

is exact. If

$$0 \to \mathcal{F}(Z) \xrightarrow{\mathcal{F}(g)} \mathcal{F}(Y) \xrightarrow{\mathcal{F}(f)} \mathcal{F}(X) \to 0,$$

$\mathcal{F}$ is called an *exact functor*. In this language, we can say

Corollary 3.8.5

(1) For every R-module D, $\mathrm{Hom}_R(\_\_, D)$ is a left exact functor.

(2) Q is injective module if and only if $\mathrm{Hom}_R(\_\_, Q)$ is an exact functor.

We have seen that an R-module is projective if and only if it is a direct summand of a free R-module. But to show injectivity is not so easy.

Definition 3.8.6
A $\mathbb{Z}$-module A is called *divisible* if $A = nA$ for all nonzero integers n.

Example 3.8.7
$\mathbb{Q}$ and $\mathbb{Q}/\mathbb{Z}$ are divisibe.

Proposition 3.8.8
Let Q be an R-module.

(1) *(Baer's Criterion)* The module Q is injective if and only if for every left ideal I of R, any R-module homomorphism $g : I \to Q$ can be extended to an R-module homomorphism $G : R \to Q$.

(2) If R is a P.I.D.(that is, every ideal is principal), then Q is injective if and only if $rQ = Q$ for every nonzero $r \in R$.

(3) In particular, a $\mathbb{Z}$-module is injective if and only if it is divisible.

(4) When R is a P.I.D., quotient modules of injective R-modules are again injective.

Proof. (3) and (4) are followed by (2).

(1) Suppose Q is injective. Let I be an ideal of R and $g : I \to Q$ be a homomorphism. Since $0 \to I \to R$ is exact, we can apply the equivalent condition of injective module. So g can be extended to a homomorphism $G : R \to Q$.

Conversely, suppose any homomorphism $g : I \to Q$ can be extended to $G : R \to Q$. Suppose $0 \to L \to M$ is exact and $f : L \to Q$ is a homomorphism. Without loss of generality, we may assume L is a submodule of M. By using Zorn's lemma, we will show that there is a lift $F : M \to Q$.

- Let $\mathcal{S}$ be the collection of all $(f' : L' \to Q, L'$ where L' is a submodule of M containing L and f' is a lift of f.
- Define a partial order $(f', L') \leq (f'', L'')$ if $L' \subset L''$ and $f''|L' = f'$ (i.e., f'' is a lift of f').

Since $(f, L) \in \mathcal{S}$, $\mathcal{S}$ is nonempty. Given chain $\mathcal{C}$, let $L^* = \bigcup_{(f', L') \in \mathcal{S}} L'$ and define $f^* : L^* \to Q$ by $f^*(x) = f'(x)$ where $(f', L') \in \mathcal{S}$ and $x \in L'$. f^* is well defined and L^* is a submodule of M containing L. Moreover f^* is a lift of any f' where $(f', L') \in \mathcal{S}$. So (f^*, L^*) is an upper bound of $\mathcal{C}$. By Zorn's lemma, there is a maximal element (F, M') in $\mathcal{S}$. Since $F : M' \to Q$ is a lift of f, it suffices to show that $M' = M$. Suppose there is some $m \in M \setminus M'$. Define $I = \{r \in R : rm \in M'\}$. It is easy to check that I is a left ideal in R, and the map $g : I \to Q$ defined by $g(x) = F(xm)$ is an homomorphism. Then there is a lift $G : R \to Q$ of g. Consider $M' + Rm$ which is a submodule of M. Since $m \notin M'$, $M' \subsetneq M' + Rm$. Define $F' : M' + Rm \to Q$ by $F'(m' + rm) = F(m') + G(r)$. This map is a well defined homomorphism, and F' is a lift of F. Thus $(F, M') \lneq (F', M' + Rm)$ but it contradicts that (F, M') is a maximal element of $\mathcal{S}$. Hence $M' = M$.

(2) Suppose R is a P.I.D. Any nonzero ideal I of R is of the form $I = (r)$ for some nonzero element $r \in R$. A homomorphism $f : I \to Q$ is completely determined by $f(r) = q \in Q$. Thus f can be extended to $F : R \to Q$ if and only if there is $q' \in Q$ with $F(1) = q'$ satisfying $q = f(r) = F(r) = rq'$. By (1), Q is injective if and only if $rQ = Q$. □

Example 3.8.9

(1) Since $\mathbb{Z}$ is not divisible, $\mathbb{Z}$ is not an injective $\mathbb{Z}$-module.

(2) $\mathbb{Q}$ is an injective $\mathbb{Z}$-module.

(3) Since $\mathbb{Z}$ is P.I.D and $\mathbb{Q}$ is injective, $\mathbb{Q}/\mathbb{Z}$ is an injective $\mathbb{Z}$-module.

(4) A direct sum of divisible $\mathbb{Z}$-modules is again divisible. Hence a direct sum of injective $\mathbb{Z}$-modules is again injective.

(5) Suppose R is an integral domain (that is, $ab = 0$ implies $a = 0$ or $b = 0$). An R-module A is said to be a *divisible* R-module if $rA = A$ for every nonzero $r \in R$. The proof of Proposition 3.8.8 shows that an injective R-module is divisible.

(6) In a field F, every F-module is injective.

Corollary 3.8.10
Every $\mathbb{Z}$-module is a submodule of an injective $\mathbb{Z}$-module.

Proof. Let M be a $\mathbb{Z}$-module and let A be any set of $\mathbb{Z}$-module generator of M. Let $\mathcal{F} = F(A)$ be the free $\mathbb{Z}$-module on A. Then there is a canonical projection $\mathcal{F} \to M$, and if we denote $\mathcal{K}$ be the kernel, we have an isomorphism $M \cong \mathcal{F}/\mathcal{K}$. Let $\mathcal{Q}$ be the free $\mathbb{Q}$-module on A. Recall that a free module is a direct sum of a number of copies of $\mathbb{Q}$. Then $\mathbb{Q}$ is a divisible $\mathbb{Z}$-module, so injective. Moreover $\mathcal{F}$ is a submodule of $\mathcal{Q}$. Thus $\mathcal{F}/\mathcal{K}$ is a submodule of $\mathcal{Q}/\mathcal{K}$. If we identify M with $\mathcal{F}/\mathcal{K}$, M is a submodule of $\mathcal{Q}/\mathcal{K}$ which is injective. □

Theorem 3.8.11
Let R be a ring with 1 and let M be an R-module. Then M is contained in an injective R-module.

Proof. See Exercises 3.9.5 and 3.9.6. □

3.9 Flat Modules

We now consider the behavior of extensions $0 \to L \to M \to N \to 0$ of R-modules with respect to tensor products.

Suppose F os a right R-module. For any homomorphism $f : X \to Y$ of left R-modules, $1 \otimes f : D \otimes_R X \to D \otimes_R Y$ is a group homomorphism of abelian groups. If in addition F is an (S, R)-bimodule, then $1 \otimes f$ is a left R-module homomorphism. Put another way,

$$D \otimes_R \_\_ : X \mapsto D \otimes_R X$$

is a covariant functor. In a similar way, if D is a left R-module, then $\_\_ \otimes_R D$ is a covariant functor.

We have already seen examples where the map $1 \otimes \psi : D \otimes_R L \to D \otimes_R M$ induced by an injective map $\psi : L \hookrightarrow M$ is no longer injective. For example, $\mathbb{Z} \hookrightarrow \mathbb{Q}$ of $\mathbb{Z}$-modules induces the zero map from $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}$ to $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}$. On the other hand, suppose $\varphi : M \to N$ is a surjective homomorphism. $D \otimes_R N$ is generated as an abelian group by the simple tensors

$d \otimes n$ for $d \in D$ and $n \in N$. The surjectivity of φ implies that $n = \varphi(m)$ for some $m \in M$, and then

$$1 \otimes (d \otimes m) = d \otimes \varphi(m) = d \otimes n$$

shows that $1 \otimes \varphi$ is a surjective homomorphism of abelian groups from $D \otimes_R M$ to $D \otimes_R N$.

Theorem 3.9.1
Suppose D is a right R-module and L, M, and N are left R-modules.

(1) If

$$0 \to L \xrightarrow{\psi} M \xrightarrow{\varphi} N \to 0 \text{ is exact,}$$

then the associated sequence of abelian groups

$$D \otimes_R L \xrightarrow{1\otimes\psi} D \otimes_R M \xrightarrow{1\otimes\varphi} D \otimes_R N \to 0 \text{ is exact.}$$

(2) If D is an (S, R)-bimodule, then the associated sequence is exact as left S-modules.

(3) The sequence

$$D \otimes_R L \xrightarrow{1\otimes\psi} D \otimes_R M \xrightarrow{1\otimes\varphi} D \otimes_R N \to 0$$

is exact for all right R-module D if and only if

$$L \xrightarrow{\psi} M \xrightarrow{\varphi} N \to 0$$

is exact.

Proof. (1) It remains to show that the sequence is exact at $D \otimes_R M$. Since $\varphi \circ \psi = 0$, we have

$$(1 \otimes \varphi)\left(\sum d_i \otimes \psi(l_i)\right) = \sum d_i \otimes (\varphi \circ \psi(l_i)) = 0.$$

Thus $\operatorname{img} 1 \otimes \psi \subset \ker 1 \otimes \varphi$. In particular, there is a natural projection

$$\pi : D \otimes_R M / \operatorname{img} 1 \otimes \psi \to D \otimes_R \ker 1 \otimes \varphi = D \otimes_R N.$$

(The last isomorphism comes from $M/\ker\varphi = N$).

We shall show that π is isomorphism. To see that, we define an inverse map. Define $\pi' : D \times N \to (D \otimes_R M)/\operatorname{img}(1 \otimes \psi)$ by $\pi'(d, n) = d \otimes m$ for any $m \in M$ with $\varphi(m) = n$. Note that this map is well defined : if m, m' map to n, $\varphi(m - m') =$ implies $m' = m + \psi(l)$ for some $l \in L$. Then $d \otimes m' = d \otimes m + d \otimes \psi(l)$. It is easy to show that π' is a balanced map. So there is an induced homomorphism $\overline{\pi} : D \otimes_R N \to (D \otimes_R M)/\operatorname{img} 1 \otimes \psi)$ with $\overline{\pi}(d \otimes n) = d \otimes m$. Since for every simple tensor $\overline{\pi} \circ \pi(d \otimes m) = d \otimes m$, $\overline{\pi} \circ \pi = 1$. Similarly, $\pi \circ \overline{\pi} = 1$, and hence π is isomorphism.

(2) and (3) left as exercises. □

Then we have the following proposition:

Proposition 3.9.2
Let A be a right R-module. Then the following are equivalent:

(1) For any left R-modules L, M, and N, if

$$0 \to L \xrightarrow{\psi} M \xrightarrow{\varphi} N \to 0$$

is a short exact sequence, then

$$0 \to A \otimes_R L \xrightarrow{1\otimes\psi} A \otimes_R M \xrightarrow{1\otimes\varphi} A \otimes_R N \to 0$$

is also a short exact sequence.

(2) For any left R-modules L and M, if $0 \to L \xrightarrow{\psi} M$ is an exact sequence of left R-modules, then $0 \to A \otimes_R L \xrightarrow{1\otimes\psi} A \otimes_R M$ is an exact sequence of abelian groups.

Definition 3.9.3
A right R-module A is called *flat* if it satisfies either of the two equivalent conditions of above proposition.

For a fixed right R-module D, $D \otimes_R \_\_$ is said to be right exact.

Corollary 3.9.4
If D is a right R-module, then the functor $D \otimes_R \_\_$ is right exact. The functor is exact if and only if D is a flat R-module.

Corollary 3.9.5
Free modules are flat; more generally, projective modules are flat.

Proof. Suppose $F = \bigoplus R$ is a free R-module and let $\psi : L \to M$ is an injective homomorphism. Then

$$F \otimes_R L = (\bigoplus R) \otimes_R L \cong \bigoplus (R \otimes_R L) \cong \bigoplus L,$$
$$F \otimes_R M = (\bigoplus R) \otimes_R M \cong \bigoplus (R \otimes_R M) \cong \bigoplus M$$

Thus $1 \otimes \psi$ is just the natural map $\bigoplus L \to \bigoplus M$ induced by the inclusion ψ in each component. Thus $1 \otimes \psi$ is injective.

Suppose P is a projective module. Then P is a direct summand of a free module F, say $F = P \oplus P'$. If $\psi : L \to M$ is injective, then $1 \otimes \psi : F \otimes_R L \to F \otimes_M$ is also injective. Since tensor products commute with direct sums,

$$1 \otimes \psi : (P \otimes_R L) \oplus (P' \otimes_R L) \to (P \otimes_R M) \oplus (P' \otimes_R M)$$

is injective. Hence $1 \otimes \psi | P \otimes_R L : P \otimes_R L \to P \otimes_R M$ is injective. □

Example 3.9.6

(1) Since $\mathbb{Z}$ is a projective $\mathbb{Z}$-module, it is flat. $\mathbb{Z}/2\mathbb{Z}$ is not a flat $\mathbb{Z}$-module.

(2) The $\mathbb{Z}$-module $\mathbb{Q}/\mathbb{Z}$ is injective, but is not flat: the injective map $\psi(z) = 2z$ from $\mathbb{Z}$ to $\mathbb{Z}$ does not remain injective after tensoring with $\mathbb{Q}/\mathbb{Z}$.

(3) The direct sum of flat modules is flat. In particular, $\mathbb{Q} \oplus \mathbb{Z}$ is flat which is neither projective nor injective.

3.9.1 Fundamental Theorem of Tensor Products

Theorem 3.9.7 (Hom-Tensor Adjoint)
Let M be a right R-module, N be an (R, S)-bimodule, and L be a right S-module. Then there is a group isomorphism

$$\mathrm{Hom}_S(M \otimes_R N, L) \cong \mathrm{Hom}_R(M, \mathrm{Hom}_S(N, L)),$$

such that $f \mapsto \widetilde{f}$ where $\widetilde{f}(m)(n) = f(m \otimes n)$.

Proof. Since $M \otimes_R N$ is a right S-module, $\mathrm{Hom}_S(M \otimes_R N, L)$ makes sense. We know that $\mathrm{Hom}_S(N, L)$ is an abelian group. For $r \in R$ and $f \in \mathrm{Hom}_S(N, L)$, define fr by

$$(fr)(n) = f(rn).$$

(It looks $(ar) \otimes b = a \otimes (rb)$). This multiplication induces a right R-module structure. So $\mathrm{Hom}_R(M, \mathrm{Hom}_S(N, L))$ also makes sense.

Now we will check that the map $f \mapsto \widetilde{f}$ is a group isomorphism.

- Since $m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2$ and $m \otimes rn = mr \otimes n$, $\widetilde{f}$ is R-module homomorphism. (Note that this R-module homomorphism is a right R-module homomorphism, that is $(\widetilde{f}(m)r)(n) = \widetilde{f}(m)(rn) = \widetilde{f}(mr)(n) \Rightarrow \widetilde{f}(m)r = \widetilde{f}(mr)$.)
- Suppose $\widetilde{f} = 0$, that is, $\widetilde{f}(m)(n) = 0$ for all $m \in M$ and $n \in N$. Then $f(m \times n) = 0$ for all simple tensor, and hence $f = 0$.
- Let $g \in \mathrm{Hom}_R(M, \mathrm{Hom}_S(M, L))$. Define $F : M \times N \to L$ by $F(m, n) = g(m)(n)$. Then F satisfies

$$F(m_1 + m_2, n) = g(m_1 + m_2)(n) = g(m_1)(n) + g(m_2)(n) = F(m_1, n) + F(m_2, n)$$
$$F(m, n_1 + n_2) = g(m)(n_1 + n_2) = g(m)(n_1) + g(m)(n_2) = F(m, n_1) + F(m, n_2)$$
$$F(mr, n) = g(mr)(n) = (g(m)r)(n) = g(m)(rn) = F(m, rn).$$

  Thus F is R-balanced, and it induces an S-module homomorphism $\widetilde{F} : M \otimes_R N \to L$ such that $F(m, n) = \widetilde{F}(m \otimes n) = g(m)(n)$. Hence $\widetilde{F} \mapsto g$.

□

Theorem 3.9.8
Let M be an (S, R)-bimodule, N be a left R-module, and L be a left S-module. Then there is a group isomorphism

$$\mathrm{Hom}_S(M \otimes_R N, L) \cong \mathrm{Hom}_R(N, \mathrm{Hom}_S(M, L)),$$

such that $f \mapsto \widetilde{f}$ where $\widetilde{f}(n)(m) = f(m \otimes n)$.

As a first application of Hom-Tensor adjoint, we give an alternate proof of the first result in Theorem 3.9.2. If $0 \to L \to M \to M \to N \to 0$ is exact, then

$$0 \to \mathrm{Hom}_R(N, E) \to \mathrm{Hom}_R(M, E) \to \mathrm{Hom}_R(L, E)$$

is exact for every R-module E. Then Hence

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Hom}_R(D, \mathrm{Hom}_R(N, E)) & \longrightarrow & \mathrm{Hom}_R(D, \mathrm{Hom}_R(M, E)) & \longrightarrow & \mathrm{Hom}_R(D, \mathrm{Hom}_R(L, E)) \\
 & & \| & & \| & & \| \\
0 & \longrightarrow & \mathrm{Hom}_R(D \otimes_R N, E)) & \longrightarrow & \mathrm{Hom}_R(D \otimes_R M, E)) & \longrightarrow & \mathrm{Hom}_R(D \otimes_R L, E))
\end{array}$$

$$D \otimes_R L \to D \otimes_R M \to D \otimes_R N \to 0$$

is exact for all D.

Corollary 3.9.9
If R is commutative, then the tensor product of two projective R-modules is projective.

Proof. Let P_1 and P_2 be projective modules. Then $\mathrm{Hom}_R(P_2, \_\_)$ is an exact functor from R-modules to R-modules. Then $\mathrm{Hom}_R(P_1, \mathrm{Hom}_R(P_2, \_\_))$ is an exact functor. Then $\mathrm{Hom}_R(P_1 \otimes_R P_2, \_\_)$ is an exact functor on R-modules. Hence $P_1 \otimes_R P_2$ is projective. □

3.9.2 Summary

(1) Let A be a left R-module. The functor $\mathrm{Hom}_R(A, \_\_)$ is covariant and left exact; A is projective if and only if $\mathrm{Hom}_R(A, \_\_)$ is exact.

(2) Let A be a left R-module. The functor $\mathrm{Hom}_R(\_\_, A)$ is contravariant and left exact; A is injective if and only if $\mathrm{Hom}_R(\_\_, A)$ is exact.

(3) Let A be a right R-module. The functor $A \otimes_R \_\_$ is covariant and right exact; A is flat if and only if $A \otimes_R \_\_$ is exact.

(4) Let A be a left R-module. The functor $\_\_ \otimes_R A$ is covariant and right exact; A is flat if and only if $\_\_ \otimes_R A$ is exact.

(5) Projective modules are flat. The $\mathbb{Z}$-module $\mathbb{Q}/\mathbb{Z}$ is injective but not flat. The $\mathbb{Z}$-module $\mathbb{Z} \oplus \mathbb{Q}$ is flat but neither projective nor injective.

3.9.3 Exercises

Exercise 3.9.1
Let P_1 and P_2 be R-modules. Prove that $P_1 \oplus P_2$ is a projective R-module if and only if both P_1 and P_2 are projective.

Exercise 3.9.2
Let Q_1 and Q_2 be R-modules. Prove that $Q_1 \oplus Q_2$ is a injective R-module if and only if both Q_1 and Q_2 are injective.

Exercise 3.9.3
Let A_1 and A_2 be R-modules. Prove that $A_1 \oplus A_2$ is a flat R-module if and only if both A_1 and A_2 are flat. More generally, an arbitrary direct sum $\bigoplus A_i$ of R-modules is flat if and only if each A_i is flat.

Exercise 3.9.4
Assume R is commutative with 1.

(a) Prove that the tensor product of two free R-modules is free.

(b) Use (a) to prove that the tensor product of two projective R-modules is projective.

Exercise 3.9.5
Let M be a left R-module where R is a ring with 1.

(a) Show that $\mathrm{Hom}_{\mathbb{Z}}(R, M)$ is a left R-module under the multiplication $(r\varphi)(r') = \varphi(r'r)$.

(b) Suppose that $0 \to A \xrightarrow{\psi} B$ is an exact sequence of R-modules. Prove that if every homomorphism $f : A \to M$ lifts to a homomorphism $F : B \to M$ with $f = F \circ \psi$, then every homomorphism $f' : A \to \mathrm{Hom}_{\mathbb{Z}}(R, M)$ lifts to a homomorphism $F' : B \to \mathrm{Hom}_{\mathbb{Z}}(R, M)$ with $f' = F' \circ \psi$. [hint: given f', show that $f(a) = f'(a)(1_R)$ is a homomorphism from A to M. If F is the associated lift of f to B, show that $F'(b)(r) = F(rb)$ is a homomorphism from B to $\mathrm{Hom}_{\mathbb{Z}}(R, M)$ that lifts f'.]

(c) Prove that if Q is an injective R-module, then $\mathrm{Hom}_{\mathbb{Z}}(R, Q)$ is also an injective R-module.

Exercise 3.9.6
This exercise proves that every left R-module M is contained in an injective left R-module.

(a) Show that M is contained in an injective $\mathbb{Z}$-module Q.

(b) Show that $\mathrm{Hom}_R(R, M) \subset \mathrm{Hom}_{\mathbb{Z}}(R, M) \subset \mathrm{Hom}_{\mathbb{Z}}(R, Q)$.

(c) Use the R-module isomorphism $M \cong \mathrm{Hom}_R(R, M)$ and the previous exercise to conclude that M is contained in an injective module.

Exercise 3.9.7
This exercise completes the proof of Proposition 3.8.3. Suppose that Q is an R-module with the property that every short exact sequence $0 \to Q \to M_1 \to N \to 0$ splits and suppose that the sequence $0 \to L \xrightarrow{\psi} M$ is exact. Prove that every R-module homomorphism $f : L \to Q$ can be lifted to an R-module homomorphism $F : M \to Q$ with $f = F \circ \psi$. [hint: By the previous exercise, Q is contained in an injective R-module. Use the splitting property together with Exercise 3.9.2. Note that Exercise 3.9.2 can be proved using (2) in Proposition 3.8.3.]

Exercise 3.9.8
Prove that the (right) module $M \otimes_R S$ obtained by changing the base from the ring R to the ring S (by some homomorphism $f : R \to S$ with $f(1_R) = 1_S$) of the flat (right) R-module M is a flat S-module.

Exercise 3.9.9
Prove that A is a flat R-module if and only if for any left R-modules L and M where L is finitely generated, then $\psi : L \to M$ injective implies that also $1 \otimes \psi : A \otimes_R L \to A \otimes_R M$ is injective.

Exercise 3.9.10

Theorem 3.9.10 (A Flatness Criterion)
A is a flat R-module if and only if for every finitely generated ideal I of R, the map from $A \otimes_R I \to A \otimes_R R \cong A$ induced by the inclusion $I \subset R$ is again injective (or, equivalently, $A \otimes_R I \cong AI \subset A$).

(a) Prove that if A is flat, then $A \otimes_R I \to A \otimes_R R$ is injective.

(b) If $A \otimes_R I \to A \otimes_R R$ is injective for every finitely generated ideal I, prove that $A \otimes_R I \to A \otimes_R R$ is injective for every ideal I. Show that if K is any submodule of a finitely generated free module F, then $A \otimes_R K \to A \otimes_R F$ is injective. Show that the same is true for any free module F.

(c) Under the assumption in (b), suppose L and M are R-modules and $\psi : L \to M$ is injective. Prove that $1 \otimes \psi : A \otimes_R L \to A \otimes_R M$ is injective and conclude that A is flat. [hint: Write M as a quotient of the free module F, giving a short exact sequence

$$0 \to K \to F \xrightarrow{f} M \to 0.$$

Show that if $J = f^{-1}(\psi(L))$ and $\iota : J \to F$ is the natural injection, then the diagram is commutative with exact rows. Show that the induced diagram is commutative with

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K & \longrightarrow & J & \longrightarrow & L & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \iota} & & \downarrow{\scriptstyle \psi} & & \\ 0 & \longrightarrow & K & \longrightarrow & F & \longrightarrow & M & \longrightarrow & 0 \end{array}$$

exact rows. Use (b) to show that $1 \otimes \iota$ is injective.]

$$\begin{array}{ccccccc} A \otimes_R K & \longrightarrow & A \otimes_R J & \longrightarrow & A \otimes_R & \longrightarrow & 0 \\ \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle 1\otimes\iota} & & \downarrow{\scriptstyle 1\otimes\psi} & & \\ A \otimes_R K & \longrightarrow & A \otimes_R F & \longrightarrow & A \otimes_R M & \longrightarrow & 0 \end{array}$$

(d) *A Flatness Criterion for quotients* Suppose $A = F/K$ where F is flat and K is an R-submodule of F. Prove that A is flat if and only if $FI \cap K = KI$ for every finitely generated ideal I of R. [hint: Use (a) to prove that $F \otimes_R I \cong FI$ and observe the image of $K \otimes_R I$ is KI; tensor the exact sequence $0 \to K \to F \to A \to 0$ with I to prove that $A \otimes_R I \cong FI/KI$, and apply the flatness criterion.]

References

[DF03] D.S. Dummit and R.M. Foote. *Abstract Algebra*. Wiley, 2003.

[Jec07] T. Jech. *Set Theory: The Third Millennium Edition, revised and expanded*. Springer Monographs in Mathematics. Springer Berlin Heidelberg, 2007.