NOTES FOR ABSTRACT ALGEBRA

Based on lectures provided by Dima Arinkin on MATH 742 2025 SPRING

Author
Wells Guan

Contents

1 Rings and Ideals

1.1 Rings

Definiton 1.1.1. (Ring)

A ring R is an abelian group with an associative multiplication distributive over the addition. (We always assume a ring has a multiplicative identity and commutative if not marked)

A unit is an element u with a reciprocal $1/u$ such that $u \cdot 1/u = 1$, which is also denoted u^{-1} and called a numtiplicative inverse and the units form a multiplicative group, denoted $R^{\times}$.

Definiton 1.1.2. (Homomorphism)

A ring homomorphism is a ring map $\phi : R \to R'$ which preserving sums, products and 1. If $R' = R$ we call ϕ an endomorphism and if it is also bijective we call it an automorphism.

Definiton 1.1.3. (Subring)

A subset $R'' \subset R$ is a buting if R'' is a ring and the inclusion $R'' \hookrightarrow R$ is a ring map. We call R a extension of R'' and the inclusion an extension.

Definiton 1.1.4. (Algebra)

An R-algebra is a ring R' that comes equipped with a ring homomorphism $\phi : R \to R'$ called the structure map. An R-algebta hormormorphism $R' \to R''$ is a ring homomorphism between R-algebtas compatible with structure maps.

Definiton 1.1.5. (Group action)

A group G is said to act on R if there is a homomorphism given from G into the group of automorphisms of R. The ring of invariants R^G is the subring defined by

$$R^G := \{x \in R | gx = g \text{ for all } g \in G\}$$

Definiton 1.1.6. (Boolean)

A ring B is called Boolean if $f^2 = f$ for all $f \in B$, then $2f = 0$ since

$$2f = (f + f)^2 = 4f$$

Definiton 1.1.7. (Polynomial rings)

Let R be a ring, $P := R[X_1, \cdots, X_n]$ the polynomial ring in n variables. P has the Universal Mapping Property (UMP), i.e. given a ring homomorphism $\phi : R \to R'$ and given an element x_i of R' for each i, there is a unique ring map $\pi : P \to R'$ with $\pi|_R = \phi$ and $\pi(X_i) = x_i$.

Similarly, let $X := \{X_\lambda\}_{\lambda \in \Lambda}$ be any set of variables. Set $P' := R[X]$ the elements of P' are the polynomials in any finitely many of X.

Definiton 1.1.8. (Ideals)

Let R be a ring. An ideal I is a subset containing 0 of R such that $xa \in I$ for any $x \in R, a \in I$ and closed under addition.

For a subset $S \subset R$, $\langle S \rangle$ means the smallest ideal containing S.

Given a single element a, we say that the ideal $\langle a \rangle$ is principal. For a number of ideals I_λ, the sum $\sum I_\lambda$ mean the set of all finite linear combinations $\sum x_\lambda a_\lambda$ for $x_\lambda \in R, a_\lambda \in I_\lambda$. If

Λ is finite, then the product $\prod I_\lambda$ means the ideal generated by all products $\prod a_\lambda, a_\lambda \in I_\lambda$.

For two ideals I and J, the transporter of J into I mean the set

$$(I : J) := \{x \in R | xJ \subset I\}$$

If $I \subset J$ a subsring such that $I \neq J$, then we call I proper.

For a ring homomorphism $\phi : R \to R'$, $I \subset R$ a subring, denote by IR' or I^e the ideal of R' generated by $\phi(I)$ can we call it the extension of I.

Given an ideal J of R' and its preimage $\phi^{-1}(J)$ is an ideal of R and we call ti the contraction of J denoted with J^c.

Definiton 1.1.9. (Residue Rings)

Let I be an ideal of R and the cosets of I

$$R/I := \{x + I | x \in R\}$$

have a ring structure and it will be called the residue ring or quotient ring or factor ring of R modulo I and the quotient map:

$$\kappa : R \to R/I, \quad \kappa(x) = x + I$$

and κx is called the residue of x.

Proposition 1.1.1.

For $I \subset R$ a subring and a ring homomorphism from R to R', then $\ker(\phi) \supset I$ implies that is a ring homomorphism $\psi : R/I \to R'$ with $\psi\kappa = \phi$.

ψ is surjective iff ϕ is surjective. ψ is injective iff $I = \ker(\phi)$.

Corollary 1.1.2. $R/\ker(\phi) \cong Im(\phi)$

Proposition 1.1.3.

R/I is universal among R-algebras R' such that $IR' = 0$, i.e. for $\phi : R \to R'$ such that $\phi(I) = 0$, there is a unique ring homomorphism $\psi : R/I \to R'$ such that $\psi\kappa = \phi$.

Definiton 1.1.10. The UMP serves to determine R/I up to unique isomorphism, i.e. if R' equipped with $\phi : R \to R'$ has the UMP too, then R' is isomorphic to R/I.

Proof.

If R' has the UMP among the R-algebras R'' such that $IR'' = 0$, then $\phi(I) = 0$ and hence there is a unique $\psi : R/I \to R'$ such that $\psi\kappa = \phi$ and since $\kappa I = 0$, we know there exists unique ψ' such that $\psi'\phi = \kappa$ and then $(\psi'\psi)\kappa = \kappa$ and hence $\psi'\psi = 1$ and we are done by the uniqueness.

Proposition 1.1.4. Let R be a ring, $P := R[X]$ the polynomial ring in one variable, $a \in R$ and $\pi : P \to R$ the R-algebra mao define by $\pi(X) := a$, then

- $\ker \pi = \{F(X) \in P | F(a) = 0\} = \langle X - a\rangle$
- $P/\langle X - a\rangle \cong R$

Definiton 1.1.11. (Order of a polynomial)

Let R be a ring, P the polynomial ring in variables X_λ for $\lambda \in \Lambda$ and $(x_\lambda) \in R^\Lambda$ a vector. Let $\phi_{(x_\lambda)} P \to P$ denote the R-algebra homomorphism defined by $\phi_{(x_\lambda)} X_\mu := X_\mu + x_\mu$.

The order of F at the vector (x_λ) is defined as the smallest degree of monomials M in $(\phi_{(x_\lambda)}F)$.

We know $\mathrm{ord}_{(x_\lambda)}F = 0$ iff $F(x_\lambda) \neq 0$.

Definiton 1.1.12. Let R be a ring, I an ideal and κ the quotient map. Given an ideal $J \supset I$ then the cosets

$$J/I := \{b + I | b \in J\} = \kappa(J)$$

and then J/I is an ideal of R/I and also $J/I = J(R/I)$.

Proposition 1.1.5. Given $J \supset I$ and we know

$$\phi : R \to R/I \to (R/I)/(J/I)$$

then we have the commutative diagram:

$$\begin{tikzcd} R \arrow[r] \arrow[d] & R/J \arrow[d, "\cong"] \\ R/I \arrow[r] & (R/I)/(J/I) \end{tikzcd}$$

Proof.

Since $\phi(J) = 0$, so there exists unique $\psi : R/J \to (R/I)/(J/I)$ such that $\psi\kappa_J = \phi$ and since $\kappa_J(I) = 0$ and there exists p such that $p\kappa_I = \kappa_J$ and consider $p(J/I) = 0$ and there exists h such that $h\kappa_{(J/I)} = p$ and it is easy to check $h\psi = 1$ by uniqueness and we are done.

Definiton 1.1.13. Let R be a ring. Let $e \in R$ be an idempotent, i.e. $e^2 = e$ then Re is a ring with e as multiplication unit, but Re is not a subring unless $e = 1$.

Let $e' := 1 - e$, then e' is idempotent and $ee' = 0$ and we call them complementary idempotents.

Denote $\mathrm{Idem}(R)$ the set of all idempotents, which is close under a ring homomorphism.

Proposition 1.1.6. If $e_1, e_2 \in R$ such that $e_1 + e_2 = 1$ and $e_1e_2 = 0$, then they are complementary idempotents.

Definiton 1.1.14. Let $R : R' \times R''$ be a product of two rings with componentwise operations.

Proposition 1.1.7. Let R be a ring and e', e'' complementary idempotents. Set $R' := Re'$ and $R'' = Re''$. Define $\phi : R \to R' \times R''$ by $\phi(x) = (xe', xe'')$ and then ϕ is a ring isomorphism. $R' = R/Re''$ and $R'' = R/Re'$.

Proof.

Check ϕ is surjective and injective.

There is a natrual isomorphism between $I = \{(0, xe'')\} \subset R' \times R''$ and R'', and consider the diagram

$$\begin{tikzcd} R \arrow[r, leftrightarrow] \arrow[d] & R' \times R'' \arrow[d] \\ R/R'' & R' \times R''/I \end{tikzcd}$$

and use the UMP.

1.2 Prime Ideals

Definiton 1.2.1. (Zerodivisors)

Let R be a ring. An element x iscalled a zerodivisor if there is a nonzero y such that $xy = 0$; otherwise, x is called a nonzerodivisor. Denote the set of zerodivisors by $\text{z.div}(R)$ and the nonzerodivisors by S_0.

Definiton 1.2.2. (Multiplicative subsets, prime ideals)

Let R be a ring. A subset S is called multipliccative if $1 \in S$ and $x, y \in S$ implies $xy \in S$.

An ideal P is called prime if its complement $R - p$ is multiplicative, or equivalentely, if $1 \neq P$ and $xy \in P$ implies $x \in P$ or $y \in P$.

Definiton 1.2.3. (Fields,domains)

A ring is called a field if $1 \neq 0$ and if every nonzero element is a unit.

A ring is called an integral domain, or a domain if $\langle 0 \rangle$ or equivalently, if R is nonzero and has no nonzero zerodivisors.

Every domain R is a subring of its fraction field $\text{Frac}(R) := \{x/y, x, y \in R \text{ and } y \neq 0\}$.

Proposition 1.2.1. Any subring R of a field K is a domain, and for a domain R, $\text{Frac}(R)$ has the UMP: the inclusion of R into any field L extends uniquely to an inclusion of $\text{Frac}(R)$ into L.

Proof.

For any subring R of a field, $a, b \in R$, if $ab = 0$, and a nonzero, then $b = 0$ and we are done.

If $\phi : R \hookrightarrow L$, then $\phi(x/y) = \phi(x)\phi(y)^{-1}$ is well-defined and obviously a ring homomorphism and we are done.

Definiton 1.2.4. (Polynomials over a domain)

Let R be a domain, X a set of variable. $P := R[X]$ and then P is a domain, and $\text{Frac}(P)$ is called the rational functions.

Definiton 1.2.5. (Unique factorization)

Let R be a domain, p a nonzero nonunit. We call p prime if $p|xy$ implies $p|x$ or $p|y$, which is equivalent with $\langle p \rangle$ is prime.

For $x, y \in R$, we call $d \in R$ their gcd if $d|x$ and $d|y$ and if $c|x, c|y$ then $c|d$.

p is irreducible if $p = yz$ implies y or z is a unit. We call R is a UFG if every nonzero nonunit factors into a product of irreducibles and the facrtotization is unique to order and units.

Proposition 1.2.2. If every nonzero nonunit factors have a factorization of a product of irreducible elements, then the factorization is unique up to order and units iff every irreducible element is prime.

Proof.

Lemma 1.2.3. Let $\phi : R \to R'$ be a ring homomorphism, and $T \subset R'$ a subset. If T is multiplicative, then $\phi^{-1}T$ is multiplicative; the converse holds if ϕ is surjective.

Proof.

Proposition 1.2.4. Let $\phi : R \to R'$ be a ring map, and $J \subset R'$ an ideal. Set $I := \phi^{-1}J$. If J is prime, then I is prime; the converse holds if ϕ is surjective.

Corollary 1.2.5. Let R be a ring, I an ideal. Then I is prime iff R/I is a domain.

Proof.

Consider

$$\kappa : R \to R/I$$

the quotient map and I prime implies $\langle 0 \rangle$ is prime in R/I and hence R/I is a domain.

Definiton 1.2.6. (Maximal ideal)

Let R be a ring. An ideal I is sai to be maximal if I is proper and there is no proper ideal J such that $I \subset J, I \neq J$.

Proposition 1.2.6. A ring R is a field iff $\langle 0 \rangle$ is a maximal ideal.

Corollary 1.2.7. Let R be a ring, I an ideal. Then I is maximal iff R/I is a field.

Proof.

Only need to check $\langle 0 \rangle$ is maximal in R/I.

Corollary 1.2.8. In a ring, every maximal ideal is prime.

Definiton 1.2.7. (Coprime)

Let R be a ring, and $x, y \in R$. We say x and y are coprime if their ideals $\langle x \rangle$ and $\langle y$ are comaximal.

x and y are coprime if and only if there are $a, b \in R$ such that $ax + by = 1$.

Definiton 1.2.8. A domain R is called a Principal Ideal Domain if every ideal is principal. A PID is a UFD.

Theorem 1.2.9. Let R be a PID. Let $P := R[X]$ be the polynomial ring in one variable X, and I a nonzero prime ideal of P. Then $P = \langle F \rangle$ with F prime, or P is maximal. Assume P is maximal. Then either $P = \langle F \rangle$ with F prime, or $P = \langle p, G \rangle$ with $p \in R$ prime, $pR = P \cap R$ and $G \in P$ prime with iamge $G' \in (R/pR)[X]$ prime.

Theorem 1.2.10. Every proper ideal I is contained in some maximal ideal.

Corollary 1.2.11. Let R be a ring, $x \in R$. Then x is a unit iff x belongs to non maximal ideal.

1.3 Radicals

Definiton 1.3.1. (Radical)

Let R be a ring. Its radical $\mathrm{rad}(R)$ is defined to be the intersection of all its maximal ideals.

Proposition 1.3.1. Let R be a ring, I an ideal, $x \in R$ and $u \in R^\times$. Then $x \in \mathrm{rad}(R)$ iff $u - xy \in R^\times$ for all $y \in R$. In particular, the sum of an element of $\mathrm{rad}(R)$ and a unit is a unit, and $I \subset \mathrm{rad}(R)$ if $1 - I \subset R^\times$.

Proof.

For a maximal ideal J, if $u - xy \in J$, then $u \in J$ which is a contradiction and hence $u - xy$ is a unit. Conversely, if there exists J maximal such that $x \in J$, then $\langle x \rangle + J = R$ and hence there exists $m \in J$ such that $u - xy = m$ for some unit u, which is a contradiction.

Corollary 1.3.2. Let R be a ring, I an ideal, $\kappa : R \to R/I$ the quotient map. Assume $I \subset \mathrm{rad}(R)$, then κ is injective on $\mathrm{Idem}(R)$.

Proof.

For $e, e' \in \mathrm{Idem}(R)$ and $x = e - e'$, if $\kappa(x) = 0$, then $x^3 = x$ and hence $x(1 - x^2) = 0$, so $1 - x^2$ is a unit and hence x is 0 and we are done.

Definiton 1.3.2. (Local ring)

A ring is called local if it has exactly one maximal ideal, and semilocal if it has at least one and at most finitely many.

By the residue field of a local ring A, we mean the field A/M where M is the maximal ideal of A.

Lemma 1.3.3. Let A be a ring, N the set of nonunits. Then A is local iff N is an ideal, if so, then N is the maximal idal.

Proof.

Only need to check the sufficiency, if A is local, then we know M is contained in N, and if there is $y \in M - N$, then $\langle y \rangle$ is a proper ideal and hence $y \in N$, which is a contradiction and hence $M = N$ and we are done.

Proposition 1.3.4. Let R be a ring, S a multiplicative subset, and I an ideal with $I \cap S = \emptyset$. Set $\mathcal{S} := \{J, J \supset I, J \cap S = \emptyset\}$, then $\mathcal{S}$ has a maximal element P and every such P is prime.

Proof.

By Zorn's lemma, their is a maximal element P in S, for $x, y \in R - P$, there exists $p, q \in P, a, b \in R$ such that $p + ax \in S, q + by \in S$ and hence $pq + pby + qax + abxy \in S$, and hence $xy \notin P$ and we are done.

Definiton 1.3.3. (Saturated multiplicative subsets)

Let R be a ring, and S a multiplicative subset. We say S is saturated if for $x, y \in R, xy \in S$, then $x, y \in S$.

Lemma 1.3.5. Let R be a ring, I a subset of R that is stable under addition and multiplication, and $P_1, \cdots, P_n$ ideals such that $P_3, \cdots, P_n$ are prime. If I is not contained in P_j for all j, then there is an $x \in I$ such that $x \in P_j$ for j or equivalently, if $I \subset \bigcup_{i=1}^n P_i$, then $I \subset I_i$ for some i.

Proof.

If $n = 1$ then we are done. We may use the induction, assume that $n \geq 2$, then by induction, for each i, there is $x_i \in I$ such that x_i is not in $P_j, i \neq j$ and $x_i \in P_i$, so then $x_1 + x_2 \notin P_2$ if $n = 2$. For other n, we will know $(x_1 \cdots, x_{n-1}) \notin P_j$ for all j.

Definiton 1.3.4. Let R be a ring, S a subset, its radical $\sqrt{S}$ is the set

$$\sqrt{S} := \{x \in R | x^n \in S \text{ for some } n\}$$

If I is an ideal and $I = \sqrt{I}$, then call I to be radical.

We call $\sqrt{0}$ is the nilradical and denoted as $\mathrm{nil}(R)$. We call $x \in R$ nilpotent if $x \in \mathrm{nil}(0)$, we call an ideal I nilpotent if $a^n = 0$ for some $n \geq 1$.

Theorem 1.3.6. Let R be a ring, I an ideal, then

$$\sqrt{I} = \cap_{P \supset I, P \text{ prime}} P$$

Proof.

For $x \notin \sqrt{I}$, let S contains all the expotents of x and S is multiplicative, then $I \cap S = \emptyset$ and then there is an P prime containing I with not containing x and hence $\sqrt{a}$ contains the union.

Converse direction is easy.

Proposition 1.3.7. Let R be a ring, I an ideal. Then $\sqrt{I}$ is an ideal.

Definiton 1.3.5. (Minimal primes)

Let R be a ring, I an ideal and P prime. We call P a minimal prime of I if P is minimal in the set of primes containing I, we all P a minimal prime of R if P is a minimal prime of $\langle 0 \rangle$.

Proposition 1.3.8. A ring R is reduced, i.e. 0 is the only nilpotent, and has only one minial prime iff R is a domain.

Proof.

Converse direction is obvious. If 0 is the only nilpotent elements, Q is a minimal prime ideal, then $Q = 0$ since 0 is the intersection of all the minimal primes, and we are done.

1.4 Modules

Definiton 1.4.1. (Modules)

Let R be a ring. An R-module M is an abelian group with a scalar multiplication $R \times M \to M$ which is

- $x(m+n) = xm + xn$ and $(x+y)m = xm + ym$
- $x(ym) = (xy)m$
- $1m = m$

A submodule N of M closed under scalar multiplication.

Given $m \in M$, its annihilator

$$\mathrm{Ann}(m) := \{x \in R | xm = 0\}$$

and the annilhilator of M is

$$\mathrm{Ann}(M) := \{x \in R | xm = 0 \text{ for all } m \in M\}$$

We call the intersection of all maximal ideals containing $Ann(M)$ the radical of M, denoted as $\mathrm{rad}(M)$.

Proposition 1.4.1. There is a bijection between the maximal ideals containing $\mathrm{Ann}(M)$ and the maximal ideals of $R/\mathrm{Ann}(M)$, and hence

$$\mathrm{rad}(R/\mathrm{Ann}(M)) = \mathrm{rad}(M)/\mathrm{Ann}(M)$$

Proposition 1.4.2. Given a submodule N of M, and then $\mathrm{Ann}(M) \subset \mathrm{Ann}(N)$ and we also have $\mathrm{Ann}(M) \subset \mathrm{Ann}(M/N)$.

Definiton 1.4.2. (Semilocal)

We call M semilocal if there are only finitely many maximal ideals containing $\text{Ann}(M)$. If R is semilocal, so is M and we will know M is semilocal iff $R/\text{Ann}(M)$ is a semilocal ring.

Definiton 1.4.3. (Polynomials)

The sets of polynomials

$$M[X] := \{\sum_{i=0}^{n} m_i M_i, M_i \text{ monomials}\}$$

and then $M[X]$ is an $R[X]-module$.

Definiton 1.4.4. (Homomorphisms)

Let R be aring, M and N modules. A R-linear map is a map $\alpha : M \to N$ such that

$$\alpha(xm + yn) = x\alpha m + y\alpha n$$

Let $\iota : \ker\alpha \to M$ be the inclusion and then $\ker\alpha$ has the UMP: $\alpha\iota = 0$ and for a homomorphism $\beta : K \to M$ with $\alpha\beta = 0$, there is a unique homomorphism $\gamma : K \to \ker\alpha$ with $\iota\gamma = \gamma$ as shown below

$$\begin{tikzcd}
\ker\alpha \arrow[r, "\iota"] & M \arrow[r, "\alpha"] & N \\
& K \arrow[ul, "\gamma"] \arrow[u, "\beta"] \arrow[ur, "0"'] &
\end{tikzcd}$$

Definiton 1.4.5. (Endomorphism)

An endomorphism of M a self-homomorphism denoted as $\text{End}_R(M) \subset \text{End}_{\mathbb{Z}}(M)$.

For $x \in R$, let μ_x the self map of multiplication by x and then $x \mapsto \mu_x$ denoted as

$$\mu_R : R \to \text{End}_R(M)$$

and note that $\ker\mu_R = \text{Ann}(M)$. We call M faithful if μ_R is injective.

Definiton 1.4.6. For two rings R and R', suppose R' is an R-algebra and M' an R'-module, then M' is also an R-module by $xm := \phi(x)m$.

A subalgebra R'' of R' is a subring such that the structure map owning image in R''. The subalgebra generated by $x_\lambda \in R'$ for $\lambda \in \Lambda$ is the smallest R-subalgebra containing x_λ and we denote it by $R[\{x_\lambda\}]$ and we call x_λ the generators.

We say R' is a finitely generated R-algebra if there exists $x_i, 1 \le i \le n$ such that $R' = R[x_1, \cdots, x_n]$.

Definiton 1.4.7. (Residue modules)

Let R be a ring, Ma module and $M' \subset M$ a submodule. Then

$$M/M' := \{m + M' | m \in M\}$$

which is the residue module or M modulo M', form the quotien map

$$\kappa : M \to M/M', \quad m \mapsto m + M'$$

Definiton 1.4.8. (Cyclic Modules)

Let R be a ring. A module M is said to be cyclic if there exists $m \in M$ such that $m = Rm$, then $\alpha : x \mapsto xm$ induces an isomorphism $R/\mathrm{Ann}(m) \cong M$.

Definiton 1.4.9. (Noether Isomorphisms)

Let R be a ring, N a module, and L and M submodules.

Assume $L \subset M$, and

$$\alpha : N \to N/L \to (N/L)/(M/L)$$

and we may know $\ker \alpha = M$. then α factors through the isomorphism β in $N \to N/M \to (N/L)/(M/L)$ since α is surjective and $\ker \alpha = M$, so

$$\begin{tikzcd} N \arrow[r] \arrow[d] & N/M \arrow[d, "\beta"] \\ N/L \arrow[r] & (N/L)/(M/L) \end{tikzcd}$$

Assume L not in M and

$$L + M := \{l + m, l \in L, m \in M\}$$

and it will be a submodule, then similarly

$$\begin{tikzcd} L \arrow[r] \arrow[d] & L/(L \cap M) \arrow[d, "\beta"] \\ L + M \arrow[r] & (L+M)/M \end{tikzcd}$$

Definiton 1.4.10. (Cokernels, coimages)

Let R be a ring, $\alpha : M \to N$ linear. Associated to α there are its cokernel and its coimage

$$\mathrm{Coker}(\alpha) := N/\mathrm{Im}(\alpha) \quad \mathrm{Coim}(\alpha) := M/\ker \alpha$$

Definiton 1.4.11. (Generators, free modules)

Let R be a ring, M a module. Given some submodules N_λ, by the sum $\sum N_\lambda$, we mean the set of all finite linear combinations $\sum x_\lambda m_\lambda, m_\lambda \in N_\lambda$.

Elements m_λ are said to be free of linearly independent if the linear combination equals to zero implies zero coefficients. If m_λ are said to be form a (free) basis of M, then they are free and generate M and we say M is free on m_λ.

We say M is finitely generated if it has a finite set of generators and M is free if it has a free basis.

Theorem 1.4.3. Let R be a PID, E a free module with e_λ a basis, and F a submodule, then F is free and has a basis indexed by a subset of λ.

Definiton 1.4.12. Let R be a ring, Λ a set, M_λ a module for $\lambda \in \Lambda$. The direct product of M_λ is the set of any vectors

$$\prod M_\lambda := \{(m_{m_\lambda})\}$$

which is a module under componentwise addition and scalar multiplication.

The direct sum of M_λ is the subset of restricted vectors:

$$\bigoplus M_\lambda := \{(m_\lambda), m_\lambda \text{ nonzero for only finite elements}\}$$

Proposition 1.4.4. $\prod M_\lambda$ has the UMP, for R-homomorphism $\alpha_\kappa : L \to M_\kappa$, there is a unique R-homomorphism $L \to \prod M_\lambda$ such that $\pi_\kappa \alpha = \alpha_\kappa$, in other words, π_λ induce a bijection of

$$\mathrm{Hom}(L, \prod M_\lambda) \cong \prod \mathrm{Hom}(L, M_\lambda)$$

Similarly, the direct sum comes equipped with injections

$$\iota_\kappa \to \bigoplus M_\lambda$$

and it has the UMP: given $\beta_\kappa : M_\kappa \to N$, there is a unique R-homomorphism $\beta : \bigoplus M_\lambda \to N$ such that $\beta\iota_\kappa = \beta_\kappa$ and ι_κ induce the bijection:

$$\mathrm{Hom}(\bigoplus, N) \to \bigoplus \mathrm{Hom}(M_{\lambda,N})$$

1.5 Exact Sequences

Definiton 1.5.1. (Exact)

A sequence of module homomorphisms

$$\cdots \to M_{k-1} \xrightarrow{\alpha_{k-1}} M_k \xrightarrow{\alpha_k} M_{k+1} \to \cdots$$

is said to be exact at M_k if $\ker \alpha_k = \mathrm{Im}(\alpha_k)$. The sequence is said to be exact if it is exact at every M_k, except an initial source of final target.

Definiton 1.5.2. (Short exact sequences)

A sequence $0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$ is exact if and only if α is injective and $N \cong \mathrm{Coker}\alpha$ or dually if and only if β is surjective and $L = \ker \beta$. Then the sequence is called short exact and we often regard L as a submodule of M and N the quotient M/L.

Proof.

Proposition 1.5.1. For $\lambda \in \Lambda$, let $M'_\lambda \to M_\lambda \to M''_\lambda$ be sequence of module homomorphisms. If every sequence is exact, then so are the two induced sequences

$$\bigoplus M'_\lambda \to \bigoplus M_\lambda \to \bigoplus M''_\lambda, \quad \prod M'_\lambda \to \prod M_\lambda \to \prod M''_\lambda$$

Conversely, if either induced sequence is exact then so is every original one.

Proof.

Proposition 1.5.2. Let $0 \to M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$ be a short exact sequence, and $N \subset M$ a submodule. Set $N' := \alpha^{-1}(N)$ and $N'' := \beta(N)$. Then the induced sequence $0 \to N' \to N \to N'' \to 0$ is short exact.

Definiton 1.5.3. (Retraction, section, splits)

A linear map $\rho : M \to M'$ is a retraction of another $\alpha : M' \to M$ if $\rho\alpha = 1_{M'}$, then α is injective and ρ is surjective.

Dually, we call $\sigma : M'' \to M$ a section of another $\beta : M \to M''$ if $\beta\sigma = 1_{M''}$, then β is surjective and σ is injective.

We call a 3-term exact sequence $M' \xrightarrow{\alpha} M \xrightarrow{\beta} M''$ splits if there is an isomorphism $\phi : M \cong M' \oplus M''$ with $\phi\alpha = \iota_{M'}$ and $\beta = \pi_{M''}\phi$.

Proposition 1.5.3. Let $M' \xrightarrow{\alpha} M \xrightarrow{\beta} M''$ be a 3-term exact sequence. Then the following conditions are equivalent

- The sequence splits
- There exists a retraction $\rho : M \to M'$ of α and β is surjective.
- There exists a section $\sigma : M'' \to M$ of β and α is injective

Proof.

Assume the sequence is splits, then we have the commuting diagram

$$\begin{tikzcd}
M' \arrow[r, "\alpha"] \arrow[dr, "\iota_{M'}"'] & M \arrow[r, "\beta"] \arrow[d, "\phi(\cong)"] & M'' \\
& M' \oplus M'' \arrow[ur, "\pi_{M''}"'] &
\end{tikzcd}$$

then let $\rho = \pi_{M'}\phi$, then $\rho\alpha = \pi_{M'}\phi\phi^{-1}\iota_{M'} = 1_{M'}$. Let $\sigma = \phi^{-1}\iota_{M''}$ and then $\beta\sigma = \pi_{M''}\phi\phi^{-1}\iota_{M''} = 1_{M''}$ and then β is surjective and α is injective.

Now assume there is such a retraction ρ and β is surjective, then define $\sigma = 1_M - \alpha\rho$ and $\phi : M \to M' \oplus M''$ by $m \mapsto (\rho(m), \beta\sigma(m))$., if $\phi(m) = 0$, then $\rho(m) = 0$ and $\sigma(m) = m$, which means $\beta(m) = 0$. There exists $a \in M'$ such that $m = \alpha(a)$ and hence $a = 0$ which means $m = 0$, so $\ker\phi = 0$. For $(a, b) \in M' \oplus M''$, assume $\beta(m) = b$, then $\phi(\alpha(a) + \sigma(m)) = (a + \rho(m - \alpha\rho(m)), \beta(\alpha(a)) + \beta(\sigma(m))) = (a, b)$ and hence ϕ is surjective. And $\phi\alpha(a) = (a, \beta\sigma\alpha(a)) = (a, 0)$ and $\pi_{M''}\phi(m) = \beta(\sigma(m)) = \beta(m)$ and we are done.

Lemma 1.5.4. Consider this commutative diagram with exact rows:

$$\begin{tikzcd}
& M' \arrow[r, "\alpha"] \arrow[d, "\gamma'"] & M \arrow[r, "\beta"] \arrow[d, "\gamma"] & M'' \arrow[r] \arrow[d, "\gamma''"] & 0 \\
0 \arrow[r] & N' \arrow[r, "\alpha'"] & N \arrow[r, "\beta'"] & N'' &
\end{tikzcd}$$

It yields the following exact sequence:

$$\ker\gamma' \xrightarrow{\varphi} \ker\gamma \xrightarrow{\psi} \ker\gamma'' \xrightarrow{\partial} \mathrm{coker}\gamma' \xrightarrow{\varphi'} \mathrm{coker}\gamma \xrightarrow{\psi'} \mathrm{coker}\gamma''$$

Moreover, if α is injective, then so is φ; dually, if β' is surjective, then so is ψ'.

Proof.

Notice $\alpha'\gamma' = \gamma\alpha, \beta'\gamma = \gamma''\beta$ and let $\varphi = \alpha|_{\ker\gamma'}, \psi = \beta|_{\ker\gamma}$ and we know $\varphi(\ker\gamma') \subset \ker\gamma, \psi(\ker\gamma) \subset \ker\gamma''$. Obviously, $\mathrm{Im}(\varphi) \subset \ker\psi$ and for any $b \in \ker\psi$, it is in $\ker\gamma \cap \mathrm{Im}\alpha$, since α' is injective and hence its preimage has to be contained in $\ker\gamma'$ and hence it is in $\mathrm{Im}(\varphi)$.

α', β' will induce natural φ', ψ' on $\mathrm{coker}\gamma', \mathrm{coker}\gamma$ by defining $n' + \mathrm{Im}\gamma' \mapsto \alpha'(n') + \mathrm{Im}\gamma, n + \mathrm{Im}\gamma \mapsto \beta'(n) + \mathrm{Im}\gamma''$, which is well-defined since $\alpha'(\mathrm{Im}\gamma') \subset \mathrm{Im}\gamma, \beta'(\mathrm{Im}\gamma) \subset \mathrm{Im}\gamma''$ and the exactness is similarly checked.

Define ∂ by the following, if $\gamma'' m'' = 0$, consider m is one of preimage of m'' and let a to be the preimage of $\gamma(m)$, then let $\partial m'' = a + \mathrm{Im}\gamma'$. It is well-defined since if $\beta m = \beta n = m''$, then $m - n \in \ker \beta$, which means the preiamges of $\gamma m, \gamma n$ are in the same coset. For $m \in \ker \gamma$, $\partial(\psi(m)) = \alpha'^{-1}\gamma(m) + \mathrm{Im}\gamma' = 0$ and if $\partial(m'') = 0$, then assume $\beta m = m''$ and we know $\alpha^{-1}\gamma(m) \in \mathrm{Im}\gamma'$ and hence there exists $x \in M'$ such that $\gamma\alpha x = \gamma m$ and we know $\beta(m - \alpha(x)) = m''$ and $\gamma(m - \alpha x) = 0$, which means $\ker \partial = \mathrm{Im}\psi$. If $a = \alpha'^{-1}(\gamma(m))$ with $m'' = \beta m \in \ker \gamma''$, then $\varphi'(a + \mathrm{Im}(\gamma')) = \alpha' a + \mathrm{Im}\gamma = 0$ and if $\varphi'(a + \mathrm{Im}(\gamma')) = 0$, then there exists m such that $\alpha'(a) = \gamma m$ and then $\partial(\beta(m)) = a + \mathrm{Im}\gamma'$ and we are done.

Theorem 1.5.5. (Left exactness of Hom)

- Let $M' \to M \to M'' \to 0$ be a sequence of linear maps. Then it is exact iff for all modules N, the following induced sequence is exact

$$0 \to \hom(M'', N) \to \hom(M, N) \to \hom(M', N)$$

- Let $0 \to N' \to N \to N''$ be as sequence of linear maps. Then it is exact iff for all modules M, the following induced sequence is exact.

$$0 \to \hom(M, N') \to \hom(M, N) \to \hom(M, N'')$$

Proof.

Assume $M' \overset{\phi}{\to} M \overset{\psi}{\to} M''$ and then the induced map will be $\tilde{\psi} : f \mapsto f \circ \psi$ and $\tilde{\phi} : g \mapsto g \circ \phi$. If ψ is surjective, then $\tilde{\psi}$ will be an injective since $f \circ \psi = 0$ implies $f = 0$, and if $g \circ \phi = 0$, then $\ker \psi = \mathrm{Im}\phi \subset \ker g$ and hence there will be $g' : M'' \cong M / \ker \psi \to N$ such that $g'\psi = g$ by the UMP and we are done. We know for $g : M \to N, g \circ \phi = 0$, equivalently $\mathrm{Im}\phi \subset \ker g$ iff there exists unique $g' : M'' \to N$ such that $g' \circ \psi = g$, which means $M'' \cong \mathrm{coker}\phi$ and the diagram

$$\begin{tikzcd}
M' \arrow[r, "\phi"] & M \arrow[r, "\psi"] \arrow[dr, "\kappa"'] & M'' \arrow[r] \arrow[d, leftrightarrow] & 0 \\
& & \mathrm{coker}\phi \arrow[ur] &
\end{tikzcd}$$

commutes and we are done.

Similarly assume that $N' \overset{\phi}{\to} N \overset{\psi}{\to} N''$, then $\tilde{\phi} : f \mapsto \phi \circ f$ and $\tilde{\psi} : g \mapsto \psi \circ g$, which means $\ker \psi = N' \hookrightarrow N$. It is easy to check $\ker \tilde{\phi} = 0$ and $\mathrm{Im}\tilde{\phi} \subset \ker \tilde{\psi}$. For $g \in \ker \tilde{\psi}$, since $\mathrm{Im}g \subset \ker \psi = \mathrm{Im}\phi$, then let $g' = g|_N$ will satisfy that $\phi \circ g' = g$. For the converse direction, we know for any $g : M \to N$, $\mathrm{Im}g \subset \ker \psi$ iff there exists a unique $g' : M \to N'$ such that

$\phi \circ g' = g$, then we may, which is

$$\begin{tikzcd}
0 \arrow[r] \arrow[dr] & N' \arrow[r, "\phi"] & N \arrow[r, "\psi"] & N'' \\
& \ker \psi \arrow[ur, hook] & &
\end{tikzcd}$$

Definiton 1.5.4. (Presentation)

A (free) presentation of a module M is an exact sequence

$$G \to F \to M \to 0$$

with G and F free. If G and F are free of finite rank, then the presentation is called finite. If M has a finite presentation, then call M finitely presented.

Proposition 1.5.6. Let R be a ring, M a module, m_λ generators. Then there is an exact sequence $0 \to K \to R^{\oplus \Lambda} \xrightarrow{\alpha} M \to 0$ with $\alpha e_\lambda = m_\lambda$ where e_λ the standard basis and there is a presentation.

Remark.

Choose $K = \ker \alpha$ and $k_\sigma, \sigma \in \Sigma$ to be generators of K, then

$$R^{\oplus \Sigma} \to R^{\oplus \Lambda} \to M \to 0$$

is a presentation.

Definiton 1.5.5. (Projective Module)

A module P is called projective if given any surjective linear map $\beta : M \to N$, every linear map $\alpha : P \to N$ lifts to one $\gamma : P \to M$, i.e. $\alpha = \beta\gamma$.

Theorem 1.5.7. The following conditions on an R-module P are equivalent

- The module P is projective
- Every short exact sequence $0 \to K \to M \to P \to 0$ splits
- There is a module K such that $K \oplus P$ is free
- Every exact sequence $N' \to N \to N''$ induces an exact sequence

$$\hom(P, N) \to \hom(P, N) \to \hom(P, N'')$$

- Every surjective homomophism $\beta : M \to N$ induces a surjection

$$\hom(P, \beta) : \hom(P, M) \to \hom(P, N)$$

Proof.

By considering the $P \cong M/\ker \phi$ it will induce a section of $\psi : M \to P$ and obviously $\phi : K \to M$ is injective and we are done for (1) implies (2). Use proposition 1.5.6. and we will know there exists K such that $K \oplus P \cong R^{\oplus \Lambda}$ which is free, which is for (2) implies (3).

Assume (3), then there exists Λ such that $K \oplus P \cong R^{\oplus \Lambda}$. Also notice that we will have

$$\prod N'_\lambda \to \prod N_\lambda \to \prod N''_\lambda$$

is exact, which implies that

$$\hom(R^{\oplus\Lambda}, N') \to \hom(R^{\oplus\Lambda}, N) \to \hom(R^{\oplus\Lambda}, N'')$$

is exact since $\hom(R^{\oplus\Lambda}, N) \cong \prod N_\lambda$ and hence

$$\hom(K \oplus P, N') \to \hom(K \oplus P, N) \to \hom(K \oplus P, N'')$$

which implies

$$\hom(K, N') \oplus \hom(P, N') \to \hom(K, N) \oplus \hom(P, N) \to \hom(K, N'') \oplus \hom(P, N'')$$

by isomorphism and hence the conclusion goes.

Assume (4), we know $M \to N \to 0$ is exact and we are done.

Assume (5), which is exactly the definition of projective module.

Lemma 1.5.8. (Schanuel)

Any two short exact sequences

$$0 \to L \xrightarrow{i} P \xrightarrow{\alpha} M \to 0, \quad 0 \to L' \xrightarrow{i'} P' \xrightarrow{\alpha'} M \to 0$$

with P and P' projective are essentially isomorphic; i.e. there is the following commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & L \oplus P' \arrow[r, "i \oplus 1_{P'}"] \arrow[d, "\cong\ \beta"] & P \oplus P' \arrow[r, "\alpha \oplus 0"] \arrow[d, "\cong\ \gamma"] & M \arrow[r] \arrow[d, "="] & 0 \\
0 \arrow[r] & P \oplus L' \arrow[r, "1_P \oplus i'"] & P \oplus P' \arrow[r, "0 \oplus \alpha'"] & M \arrow[r] & 0
\end{tikzcd}$$

Proof.

Firstly, it is easy to check the two exact sequences are exact. Then consider

$$0 \to K := \ker(\alpha \oplus \alpha') \to P \oplus P' \to M \to 0$$

which is exact, there exists $\pi : P' \to P$ such that $\alpha\pi = \alpha'$, so we may define $\phi : P \oplus P' \to P \oplus P'$ by $\begin{pmatrix} 1_P & \pi \\ 0 & 1'_P \end{pmatrix}$ which means $(p, p') \mapsto (p + \pi p', p')$ and then $\alpha p + \alpha' p' = (\alpha \oplus 0)\phi(p, p') = (\alpha \oplus \alpha')(p, p')$ where the inverse of ϕ will be $\begin{pmatrix} 1_P & -\pi \\ 0 & 1'_P \end{pmatrix}$ and hence ϕ is an automorphism.