# **Commutative Algebra**, Autumn, 2016 (ver. 2.00)

Masanori Ishida

## Intoroduction

This note is written for my lecture at Tohoku University. The main reference of this note is the book [AM] by Atiyah and MacDonald.

## 0 Preliminary comments

In this section, we recall some elementary words in commutative algebra. For the detail, see textbooks such as [AM] and [L].

**Commutative rings** A *ring* is an additive group $R$ with multiplications satisfying the following.
(1) $(xy)z = x(yz)$ for $x, y, z \in R$.
(2) There exists $1 \in R$ with $1x = x1 = x$ for $x \in R$.
(3) $(x + y)z = xz + yz$ and $x(y + z) = xy + yz$ for $x, y, z \in R$.

For a ring $R$, the element 1 may be equal to 0 of the addition. In this case, $R = \{0\}$. A ring $R$ is said to be *commutative* if $xy = yx$ for all $x, y \in R$. In this note, we treat only commutative rings unless otherwise stated.

Let $R$ be a commutative ring with $1 \neq 0$. An element $u \in R$ is said to be *regular* if there exists $v \in R$ with $uv = 1$. In this case, $v$ is unique and denoted by $u^{-1}$. For any element $a \in R$, $au^{-1}$ is also denoted by $a/u$. Note that the symbol "$x/y$" is equal to $\dfrac{x}{y}$. So the commutativity of the multiplications in $R$ is necessary for this notation. $R$ is said to be a *field* if $1 \neq 0$ and every non-zero element is regular.

A *homomorphism* $f : R \to R'$ of rings is a map such that (1) $f(1) = 1$, (2) $f(x + y) = f(x) + f(y)$ and (3) $f(xy) = f(x)f(y)$. A bijective homomorphism is called an *isomorphism*. An additive subgroup $I$ of a commutative ring $R$ is said to be an *ideal* if $ax \in I$ for any $x \in I$ and $a \in R$. If $I \subset R$ is an ideal, then the quotient module $R/I$ has a structure of commutative ring. There exists a natural surjective homomorphism $\phi : R \to R/I$. An additive subgroup $S$ of a commutative ring $R$ is a *subring* if $1 \in S$ and $xy \in S$ for $x, y \in S$. In this case, $S$ is a commutative ring, and the inclusion map is a homomorphism to $R$.

If $f : R \to R'$ is a homomorphism of commutative rings, then the *kernel* $\operatorname{Ker} f = \{x \in R \, ; \, f(x) = 0\}$ is an ideal of $R$, and the *image* $\operatorname{Im} f = \{f(x) \, ; \, x \in R\}$ is a subring of $R'$.

An element $a$ of a commutative ring $R$ with $1 \neq 0$ is said to be a *zero divisor* if there exists a non-zero element $b$ with $ab = 0$. A commutative ring $R$ is an *integral domain* if $1 \neq 0$ and 0 is the unique zero divisor of $R$. A field is an integral domain.

**Prime ideals** An ideal $P$ of a commutative ring $R$ is said to be a *prime ideal* if $P \neq R$ and $xy \in P$ implies $x \in P$ or $y \in P$. The set of ideals of $R$ has the order with respect to inclusions. An ideal $P$ is said to be *maximal* if it is maximal in the set of ideals not equal to $R$. An ideal $P$ is prime if and only if $R/P$ is an integral domain, and is maximal if and only if $R/P$ is a field. In particular, maximal ideals are prime.

**Modules over a ring** Let $R$ be a ring which is not necessarily commutative. An additive group $M$ is said to be an $R$-module if the multiplication $R \times M \to M$ denoted by $(a, x) \mapsto ax$ is defined and satisfies (1) $1x = x$ for $1 \in R$ and $x \in M$, (2) $a(bx) = (ab)x$ for $a, b \in R$ and $x \in M$, (3) $a(x + y) = ax + ay$ for $a \in R$ and $x, y \in M$, and (4) $(a + b)x = ax + bx$ for $a, b \in R$ and $x \in M$.

Any additive group is a $\mathbf{Z}$-module for the ring $\mathbf{Z}$ of rational integers. When $R$ is a field $k$, then "$k$-module" and "$k$-vector space" have the same meaning.

An additive subgroup $N$ of an $R$-module is an *$R$-submodule* if $ax \in N$ for $a \in R$ and $x \in N$. If $N \subset M$ is an $R$-submodule, then $N$ and $M/N$ are $R$-modules. For any subset $G \subset M$, there exists the smallest $R$-submodule $N$ of $M$ containing $G$. Actually, $N$ is the set of elements $x \in M$ such that there exist $s \geqq 0$, $x_1, \ldots, x_s \in G$ and $a_1, \ldots, a_s \in R$ with

$$x = a_1 x_1 + \cdots + a_s x_s \ .$$

In this case, $G$ is said to be a set of generators of $N$, and $N$ is said to be the $R$-submodule generated by $G$. When $G$ is a finite set, $N$ is said to be *finitely generated*. Note that the $R$-submodule generated by the empty set is $\{0\}$.

A ring $R$ itself is an $R$-module, and the $R$-submodules of $R$ are the ideals of $R$ if $R$ is commutative. For elements $x_1, \ldots, x_s$ in $R$, we denote by $(x_1, \ldots, x_s)$ the ideal generated by $\{x_1, \ldots, x_s\}$. In particular, $(x) = Rx$ for $x \in R$.

Assume that $R$ is commutative. If $I$ is an ideal of $R$ and $M$ is an $R$-module, then $IM = \{a_1 m_1 + \cdots + a_n m_n \ ; \ n \geqq 0, a_1, \ldots, a_n \in I, m_1, \ldots, m_n \in M\}$ is an $R$-submodule of $M$. If $I = (b_1, \ldots, b_s)$, then any element $z \in IM$ is expressed as $z = b_1 y_1 + \cdots + b_s y_s$ with $y_1, \ldots, y_s \in M$. On the other hand, if $M$ is generated by $x_1, \ldots, x_t \in M$, then any element $z \in IM$ is expressed as $z = a_1 x_1 + \cdots + a_t x_t$ with $a_1, \ldots, a_t \in I$.

**Homomorphisms of modules** A map $f : M \to N$ of $R$-modules is said to be an *$R$-homomorphism* or simply a homomorphism if $f(x + y) = f(x) + f(y)$ and $f(ax) = af(x)$ for any $a \in R$ and $x, y \in M$. An *isomorphism* is a bijective homomorphism. The set of $R$-homomorphisms is denoted by $\mathrm{Hom}_R(M, N)$, which has a structure of additive group by defining $(f + g)(x) = f(x) + g(x)$ for $f, g \in \mathrm{Hom}_R(M, N)$ and $x \in M$. When $R$ is commutative, it is also an $R$-module by defining $(af)(x) = a(f(x))$ for $a \in R$ and $f \in \mathrm{Hom}_R(M, N)$.

Let $L$, $M$, $N$ be $R$-modules. A map $g : L \times M \to N$ is said to be an *$R$-bilinear map* if $g(x + x', y) = g(x, y) + g(x', y)$, $g(x, y + y') = g(x, y) + g(x, y')$, $g(ax, y) = ag(x, y)$, and $g(x, by) = bg(x, y)$ for any $a, b \in R$, $x, x' \in L$, and $y, y' \in M$.

When $R$ is commutative, for $R$-modules $M$, $N$, $P$, the map

$$\mathrm{Hom}_R(M,N) \times \mathrm{Hom}_R(N,P) \to \mathrm{Hom}_R(M,P)$$

defined by $(f,g) \mapsto g \cdot f$ is $R$-bilinear.

**Direct sum and direct product of modules** For a family of $R$-modules $\{M_\lambda \, ; \, \lambda \in \Lambda\}$, the *direct product* $M = \prod_{\lambda\in\Lambda} M_\lambda$ has a natural structure of $R$-module. Namely,

$$(x_\lambda) + (y_\lambda) = (x_\lambda + y_\lambda) \ , \quad a(x_\lambda) = (ax_\lambda)$$

for $(x_\lambda), (y_\lambda) \in M$ and $a \in R$. The *direct sum* $\oplus_{\lambda\in\Lambda} M_\lambda$ is the $R$-submodule of $M$ consisting of the elements $(x_\lambda) \in M$ such that $\{\lambda \in \Lambda \, ; \, x_\lambda \neq 0\}$ is finite. The direct sum is equal to the direct product if $\Lambda$ is finite.

The direct sum of two $R$-modules $M, N$ is denoted by $M \oplus N$. The each of the $R$-submodules $M$ and $N$ of the direct sum is called the *direct summand* of $M \oplus N$.

**Noetherian rings** *The ascending chain condition* of an $R$-module $M$ is, if $N_1 \subset N_2 \subset N_3 \subset \cdots$ is an ascending chain of $R$-submodules of $M$, then there exists $m \geqq 1$ with $N_m = N_{m+1} = \cdots$. A commutative ring $R$ satisfying the ascending chain condition in ideals is called a *Noetherian* ring. This condition is equivalent to the condition that all ideals of $R$ are finitely generated, and also to the maximal condition of ideals, i.e., any non-empty set of ideals of $R$ has a maximal element.

The quotient of a Noetherian ring by an ideal is Noetherian. If $R$ is an Noetherian ring, then the Hilbert basis theorem says that the polynomial ring $R[x_1, \ldots, x_n]$ of any finite variables is Noetherian. This implies that any ring $R'$ finitely generated over $R$, i.e., $R' \simeq R[x_1, \ldots, x_n]/I$ for an ideal $I \subset R[x_1, \ldots, x_n]$, is Noetherian. If $R$ is Noetherian, then an $R$-module $M$ satisfies the ascending chain condition on $R$-submodules if and only if $M$ is finitely generated.

**Radical of an ideal** Let $I$ be an ideal of a commutative ring $R$. Then the *radical* $\sqrt{I}$ of $I$ is defined by

$$\sqrt{I} = \{x \in R \, ; \, x^n \in I \text{ for an integer } n > 0\} \ .$$

Here, note that $x^n$ is the $n$-th power of $x$ and $x^0 = 1$ in $R$. $\sqrt{I}$ is an ideal containing $I$. For the zero ideal $(0)$, the radical $\sqrt{(0)}$ is the set of nilpotent elements of $R$.

# 1 Primary decompositions

An ideal $I$ of a commutative ring $R$ is said to be *irreducible* if $I \neq R$ and is not equal to the intersection $J \cap K$ of strictly larger ideals $J, K$ of $R$.

An ideal $I \neq R$ is said to be *primary* if $x, y \in R$ and $xy \in I$ imply $x \in I$ or $y^n \in I$ for some $n > 0$. If $I$ is primary, then the radical $\sqrt{I}$ is a prime ideal.

For ideals $I, J$ of $R$, we define $I : J = \{a \in R \, ; \, aJ \subset I\}$. $I : J$ is an ideal of $R$. It is clear that $I_1 : J \subset I_2 : J$ if $I_1 \subset I_2$ and $I : J_2 \subset I : J_1$ if $J_1 \subset J_2$.

**Theorem 1.1** *Let $R$ be a Noetherian ring. If an ideal $I$ of $R$ is irreducible, then $I$ is primary.*

Proof Let $I$ be an irreducible ideal. It suffices to show that if $x, y \in R$, $xy \in I$ and $x \notin I$, then a power $y$ is contained in $I$.

If this does not hold, then $\{1, y, y^2, y^3, \ldots\} \cap I = \emptyset$. Then

$$I : (1) \ , \quad I : (y) \ , \quad I : (y^2) \ , \quad I : (y^3) \ , \ldots$$

is an ascending chain of ideals, and there exists $n \geqq 0$ with $I : (y^n) = I : (y^{n+1})$ since $R$ is Noetherian. We will show that

$$I = (I + (x)) \cap (I + (y^n)) \ . \tag{1}$$

It is clear that $I$ is contained in the righthand. Let $z$ be an element of the righthand, i.e., there exist $u, v \in I$ and $a, b \in R$ with

$$z = u + ax = v + by^n \ .$$

Then $zy = uy + axy$ is in $I$ since $u, xy \in I$. Hence $by^{n+1} = zy - vy \in I$ and $b \in I : (y^{n+1})$. We have $b \in I : (y^n)$ by the choice of $n$. Hence $by^n \in I$ and $z = v + by^n \in I$. Thus we get the equality (1). The ideals $I + (x)$ and $I + (y^n)$ are strictly larger than $I$, and this contradicts that $I$ is irreducible. Hence a power of $y$ is in $I$. QED

**Theorem 1.2** *Let $R$ be a Noetherian ring. Then any ideal $I$ of $R$ is the intersection of a finite number of irreducible ideals. Here we understand that $R$ is the intersection of zero irreducible ideals, and an irreducible ideal is that of one irreducible ideal.*

Proof Suppose that there was an ideal which is not written as the intersection of a finite number of irreducible ideals. We denote by $X$ the set of such ideals. Since $R$ is Noetherian, it satisfies the maximal condition and there exists a maximal element $I$ in $X$. Since any irreducible ideal is not in $X$, $I$ is not irreducible, i.e., $I = J \cap K$ for some strictly larger ideals $J, K \subset R$. Since $I$ is maximal, $J$ and $K$ are not in $X$. Hence there exist finite numbers irreducible ideals $J_1, \ldots, J_s$ and $K_1, \ldots, K_t$ of $R$ such that

$$J = J_1 \cap \cdots \cap J_s \ , \quad K = K_1 \cap \cdots \cap K_t \ .$$

Then $I$ is the intersection of irreducible ideals

$$I = J_1 \cap \cdots \cap J_s \cap K_1 \cap \cdots \cap K_t \ ,$$

which contradicts the assumption $I \in X$. QED

By Theorems 1.1 and 1.2, we get the following.

**Theorem 1.3** *Any ideal $I$ of a Noetherian ring $R$ is written as the intersection of a finite number of primary ideals.*

For a primary ideal $Q$, the radical $P = \sqrt{Q}$ is a prime ideal. If $Q$, $Q'$ are primary ideal with the radical $P$, then $Q \cap Q'$ is also a primary ideal with the radical $P$. In the primary ideal decomposition

$$I = Q_1 \cap \cdots \cap Q_n$$

of an ideal $I$, we may arrange the decomposition so that $P_i = \sqrt{Q_i}$ are all different, and $I \neq \bigcap_{j \neq i} Q_j$ for every $i$, i.e., *irredundant* decomposition. Each $P_i$ is called the *associated prime ideal* of $I$.

The irredundant primary ideal decomposition is not unique in general. However, it has the following uniqueness in a restricted sense.

**Theorem 1.4** *The set of prime ideals $\{P_1, \ldots, P_n\}$ does not depend on the choice of the decomposition. Furthermore, every $Q_i$ for minimal $P_i$ is unique.*

**Lemma 1.5** *Let $I$ be a primary ideal of a commutative ring $R$. If $x$ is in $R \setminus I$, then $I : x$ is a primary ideal with $\sqrt{I : x} = \sqrt{I}$, where $I : x = I : (x)$.*

Proof Since $x \notin I$, $I : x$ is not equal to $R$. Let $P = \sqrt{I}$, which is a prime ideal of $R$. If $xy \in I$, then $y \in P$ since $I$ is primary and $x$ is outside $I$. Hence $I : x$ is contained in $P$. Since $I \subset I : x$, we have $\sqrt{I : x} = \sqrt{I} = P$. If $yz \in I : x$, then $xyz \in I$ by definition. If $z$ is outside $P$, then $xy \in I$ since $I$ is primary, i.e., $y \in I : x$. Hence $I : x$ is primary. QED

Theorem 1.4 follows from the next lemmas. For the localizations, see Section 3.

**Lemma 1.6** *Let $I = I_1 \cap \cdots \cap I_n$ be an irredundant primary decomposition of an ideal $I$ of a Noetherian ring $R$. Let $P_i = \sqrt{I_i}$ for each $i$. Then a prime ideal $P$ is one of $P_1, \ldots, P_n$ if and only if there exists $x \in R \setminus I$ with $P = I : x$.*

Proof Assume that $P$ is in $\{P_1, \ldots, P_n\}$. We will find $x$ with $P = I : x$. We may assume that $P = P_1$. Since the decomposition is irredundant, $I_2 \cap \cdots \cap I_n$ is strictly larger than $I$. Since some power of $P$ is in $I_1$, there exists an integer $m \geqq 0$ with $P^m \cap I_2 \cap \cdots \cap I_n \not\subset I$ and $P^{m+1} \cap I_2 \cap \cdots \cap I_n \subset I$. Take an element $x \in P^m \cap I_2 \cap \cdots \cap I_n \setminus I$. Then $I_1 : x$ is a primary ideal with the radical $P$ by Lemma 1.5. Since $Px \subset P^{m+1}$, we have $I_1 : x = P$. Since $I : x \subset I_1 : x$ and $xy \in I_1$ implies $xy \in I$ by the choice of $x$, we have $I_1 : x = I : x$. Hence $I : x = P$.

Assume that there exists $x \in R \setminus I$ such that $P = I : x$ is prime and is none of $P_1, \ldots, P_n$. Then

$$P = I : x = I_1 : x \cap \cdots \cap I_n : x \ , \tag{2}$$

where $I_i : x = R$ if $x \in I_i$. Since $P \neq P_i$ for each $i$, $P$ is not equal to $I_i : x$ by Lemma 1.5 for $i$ with $x \notin I_i$. Take $y_i \in I_i : x \setminus I$ for each $i$. Then $y = y_1 \cdots y_n$ is in the righthand of (2), while $y$ is not in $P$ since $P$ is prime. This contradicts the equality (2). QED

**Lemma 1.7** *Let $I = I_1 \cap \cdots \cap I_n$ be an irredundant primary decomposition of an ideal $I$ of a commutative ring $R$, and $P_i = \sqrt{I_i}$ for each $i$. Let $S$ be a multiplicatively closed subset of $R$. Assume that $P_i \cap S = \emptyset$ for $i = 1, \ldots, m$ and $P_i \cap S \neq \emptyset$ for $i = m+1, \ldots, n$. Let $\phi_S : R \to S^{-1}R$ be the natural homomorphism. Then $\phi_S^{-1}(\phi_S(I)S^{-1}R) = I_1 \cap \cdots \cap I_m$.*

Proof We take an element $y_i \in P_i \cap S$ for $i = m+1, \ldots, n$, and set $y = y_{m+1} \cdots y_n$. Then $y^l \in I_{m+1} \cap \cdots \cap I_n$ for a positive integer $l$. Let $x$ be an arbitrary element of $I_1 \cap \cdots \cap I_m$. Then $x/1 = xy^l/y^l$ is in $\phi_S(I)S^{-1}R$. Hence $x$ is in $\phi_S^{-1}(\phi_S(I)S^{-1}R)$.

Let $x$ be an element of $\phi_S^{-1}(\phi_S(I)S^{-1}R)$. Then $x/1 \in \phi_S(I)S^{-1}R$ is equal to $z/s$ for some elements $z \in I$ and $s \in S$. Then there exists $t \in S$ with $t(sx - z) = 0$. Since $tsx = tz \in I \subset I_i$ and $ts \in S$ is not in $P_i$ for $i = 1, \ldots, m$, $x$ is in $I_i$ for such $i$ since $I_i$ is primary. Hence $x$ is in $I_1 \cap \cdots \cap I_m$. QED

The last assertion of Theorem 1.4 is proved as follows. If $P_i$ is minimal, we set $S = R \setminus P_i$. Then $P_j \cap S \neq \emptyset$ for $j \neq i$ since $P_j \not\subset P_i$. Hence $\phi_S^{-1}(\phi_S(I)S^{-1}R) = I_i$ by Lemma 1.7. This means that $I_i$ is uniquely determined by $I$.

**Lemma 1.8** *Let $P$ be a maximal ideal of a commutative ring $R$. If an ideal $I$ is contained in $P$ and contains $P^n$ for an integer $n \geqq 1$, then $I$ is primary.*

Proof Clearly, $I$ is not equal to $R$, and $\sqrt{I} = P$. Assume that $x, y \in R$ and $xy \in I$. It suffices to show that $x \in I$ if $y \notin P$. The radical $\sqrt{I + Ry}$ is equal to $R$ since it contains the maximal ideal $P$ and $y \notin P$. Hence $I + Ry = R$, and there exist $z \in I$ and $a \in R$ with $1 = z + ay$. Then $x = x(z + ay) = xz + axy \in I$. QED

**Example 1.9** Let $k$ be a field and $k[x, y]$ a polynomial ring with two variables. For any positive integers $l, m$, the ideal $(x^l, y^m)$ of $k[x, y]$ is irreducible. Actually, we can show that if an ideal $I$ is strictly larger than $(x^l, y^m)$, then $I$ contains $x^{l-1}y^{m-1}$, which is not in $(x^l, y^m)$. Hence the intersection of any strictly larger ideals contains $x^{l-1}y^{m-1}$, and is not equal to $(x^l, y^m)$.

Here we prove it. Let $f(x, y)$ be an element of $I \setminus (x^l, y^m)$. Then there exists a monomial $x^i y^j$ of $f$ with non-zero coefficient such that $i < l$ and $j < m$. Let $s$ be the minimum of $i$ for such monomials of $f$. Then $x^{l-1-s}f$ is still in $I \setminus (x^l, y^m)$ since it has monomials $x^{l-1}y^j$ with non-zero coefficient and $j < m$. Let $t$ be the minimum of $j$ for such monomials in $x^{l-1-s}f$. Then the coefficient of $x^{l-1}y^{m-1}$ in $x^{l-1-s}y^{m-1-t}f \in I$ is not zero, and all the other monomials of $x^{l-1-s}y^{m-1-t}f$ are in $(x^l, y^m)$. Hence $x^{l-1}y^{m-1}$ is in $I$ since $(x^l, y^m) \subset I$.

For any $n \geqq 2$, $P^n = (x^n, x^{n-1}y, \ldots, xy^{n-1}, y^n)$ is a primary ideal by Lemma 1.8. However, it is not irreducible. Actually, we have

$$(x^n, x^{n-1}y, \ldots, xy^{n-1}, y^n) = (x^n, y) \cap (x^{n-1}, y^2) \cap \cdots \cap (x^2, y^{n-1}) \cap (x, y^n) \ ,$$

where the righthand is the intersection of irreducible ideals.

# 2 Modules on a ring

Let $R$ be a commutative ring. In this section, we assume that $R \neq \{0\}$, i.e., $1 \neq 0$. For a positive integer $n$, we denote by $R^n$ the set of column vectors

$$x = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \tag{3}$$

of elements of $R$. For $a \in R$ and $x, y \in R^n$, we define

$$ax = \begin{bmatrix} ax_1 \\ \vdots \\ ax_n \end{bmatrix}, \quad x + y = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} + \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{bmatrix}.$$

Then $R^n$ has a structure of $R$-module. This is a free $R$-module with the basis

$$e_1 = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \quad e_2 = \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix}, \quad \dots, \quad e_n = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}.$$

The following facts are similar to the case of vector spaces over a field.

**Proposition 2.1** *The set of $R$-homomorphisms from $R^n$ to $R^m$ has natural one-to-one correspondences with the set $M_{m,n}(R)$ of $m \times n$ matrices of elements of $R$. The composite of the $R$-homomorphisms $A$ from $R^n$ to $R^m$ and $B$ from $R^m$ to $R^r$ is represented by the product $r \times n$ matrix $BA$.*

**Proposition 2.2** *$M_n(R) = M_{n,n}(R)$ is a non-commutative ring for $n \geqq 2$. $R^n$ is a left $M_n(R)$-module, and $A \in M_n(R)$ is an isomorphism of $R^n$ if and only if the matrix $A$ is invertible.*

The determinant of a matrix $A = [a_{ij}] \in M_n(R)$ over a commutative ring $R$ is defined as an element of $R$ by the same formula

$$\det A = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)}$$

as the case of a field. It has similar properties. Namely, the determinant does not change if one adds to a column (resp. a row) some multiple of another column (resp. another row), and the determinant is multiplied by $c$ if a column or a row is multiplied by $c$. The determinant is zero if two columns or two rows are equal. The determinant of the identity matrix $I$ is 1, and the equality $\det AB = (\det A)(\det B)$ holds for any $A, B \in M_n(R)$.

**Proposition 2.3** *The $R$-homomorphism $A : R^n \to R^n$ defined by a matrix $A$ is an isomorphism if and only if* $\det A$ *is a regular element of $R$.*

Proof If the $R$-homomorphism is an isomorphism, then it has inverse and is defined by a matrix $B$. Then $BA = E$ and $\det A$ is regular since $(\det B)(\det A) = \det BA = \det E = 1$.

On the other hand, if $\det A$ is regular, then the cofactor matrix multiplied by $(\det A)^{-1}$ is the inverse matrix of $A$ and defines the inverse $R$-homomorphism. QED

For an $R$-homomorphism $A : R^n \to R^m$, $\mathrm{Ker}\, A = \{x \in R^n \ ; \ Ax = 0\}$ is an $R$-submodule of $R^n$, and $\mathrm{Im}\, A = \{Ax \ ; \ x \in R^n\}$ is an $R$-submodule of $R^m$. However, the rank of $A$ can not be defined in a simple sense contrary to the case of a field.

A square matrix $A$ with regular $\det A$ is called a *regular* matrix. Note that $\det A \neq 0$ is not the condition for a regular matrix. In particular, for the ring $\mathbf{Z}$ of rational integers, $A \in M_n(\mathbf{Z})$ is regular if and only if $\det A = \pm 1$.

For arbitrary elements $u_1, \ldots, u_m$ of an $R$-module $M$, an $R$-homomorphism $\phi : R^m \to M$ is defined by $y \mapsto y_1u_1 + \cdots + y_mu_m$. Furthermore, for $A \in M_{m,n}(R)$, the $R$-homomorphism $\phi_A : R^n \to M$ is defined by

$$\phi_A(x) = \sum_{i=1}^{m}(\sum_{j=1}^{n} a_{ij}x_j)u_i$$

with respect to the expression (3). This is the composite of $A$ and $\phi$.

**Theorem 2.4** *If $A : R^n \to R^m$ defined by $A \in M_{m,n}(R)$ is an isomorphism, then $m = n$.*

Proof Let $P$ be a maximal ideal of $R \neq \{0\}$. By taking the image of the entries of the matrix $A$ in $R/P$, we get the matrix $\overline{A}$ in $M_{m,n}(R/P)$ which defines the isomorphism $(R/P)^n \to (R/P)^m$ of $(R/P)$-vector spaces. Since these are vector spaces of dimensions $n$ and $m$, we have $m = n$ by the uniqueness of the dimension. QED

Note that $M/IM$ is an $R/I$-module for an $R$-module $M$ and an ideal $I$. If $f : M \to N$ is an $R$-homomorphism, then we have an $R/I$-homomorphism $\bar{f} : M/IM \to N/IN$, and if $f$ is an isomorphism then so is $\bar{f}$.

When $\phi : R^n \to F$ defined by $y \mapsto y_1u_1 + \cdots + y_mu_m$ is an isomorphism, we say $F$ a *free $R$-module* with the basis $\{u_1, \ldots, u_m\}$. We can also consider a free $R$-module $F = \bigoplus_{\lambda \in \Lambda} Ru_\lambda$ with an infinite basis $\{u_\lambda \ ; \ \lambda \in \Lambda\}$. For any $R$-module $M$ and a set of elements $\{x_\lambda \ ; \ \lambda \in \Lambda\}$, there exists a unique $R$-homomorphism $\phi : F \to M$ such that $\phi(u_\lambda) = x_\lambda$ for every $\lambda \in \Lambda$.

For any $R$-module $M$, there exists a surjective $R$-homomorphism from a free $R$-module. Namely, it is enough to set $\Lambda = M$ and $x_\lambda = \lambda$ for $\lambda \in M$.

# 3 Tensor products and localizations

Let $M, N$ be $R$-modules over a commutative ring $R$. Then the tensor product $M \otimes_R N$ is the $R$-module enjoying the following properties, where (3) with the existence of the

bilinear map $\phi : M \times N \to M \otimes_R N$ is the functorial characterization of the tensor product.

(1) For $x \in M$ and $y \in N$, there exists an element $x \otimes y \in M \otimes_R N$, and the map $\phi : M \times N \to M \otimes_R N$ defined by $(x, y) \mapsto x \otimes y$ is $R$-bilinear.

(2) Every element $z$ of $M \otimes_R N$ is written as $z = x_1 \otimes y_1 + \cdots + x_s \otimes y_s$ for an $s \geqq 0$, $x_1, \ldots, x_s \in M$ and $y_1, \ldots, y_s \in N$.

(3) If $f : M \times N \to L$ is an $R$-bilinear map to an $R$-module $L$, then there exists a unique $R$-homomorphism $g : M \otimes_R N \to L$ with $f = g \cdot \phi$.

(4) Let $L, M, N$ be $R$-modules. Then there exists a natural isomorphism

$$\mathrm{Hom}_R(M, \mathrm{Hom}_R(N, L)) \simeq \mathrm{Hom}_R(M \otimes_R N, L)$$

of $R$-modules.

(5) $M \otimes_R R = M$, $M \otimes_R N = N \otimes_R M$, $L \otimes_R (M \otimes_R N) = (L \otimes_R M) \otimes_R N$.

The tensor product $M \otimes_R N$ is constructed as follows. Let $F(M, N)$ be the free $R$ module with the basis $M \times N$, and $K(M, N)$ the $R$-submodule of $F(M, N)$ generated by elements

$$\begin{array}{ll} (u + u', v) - (u, v) - (u', v)\ , & (u, v + v') - (u, v) - (u, v')\ , \\ (au, v) - a(u, v)\ , & (u, bv) - b(u, v) \end{array}$$

for $a, b \in R$, $u, u' \in M$ and $v, v' \in N$. Then $M \otimes_R N$ is defined to be the quotient $R$-module $F(M, N)/K(M, N)$. For $u \in M$ and $v \in N$, the element $u \otimes v$ is the image of $(u, v) \in F(M, N)$ in $M \otimes_R N$.

If a homomorphism $\lambda : A \to B$ of commutative rings is given, the $A$-module structure of $B$ is defined by $ab = \lambda(a)b$ for $a \in A$ and $b \in B$. Furthermore, if $N$ is a $B$-module, then the $A$-module structure of $N$ is defined by $ax = \lambda(a)x$ for $a \in A$ and $x \in N$.

When a homomorphism $\lambda : A \to B$ is fixed, $B$ is called an $A$-*algebra*. If $B$ is an $A$-algebra, we have the following.

1. For an $A$-module $M$ and a $B$-module $N$, $M \otimes_A N$ is a $B$-module.

   For $u \in M \otimes_A N$ and $b \in B$, $bu \in M \otimes_A N$ is defined as follows. It is easy to see that map $f_b : M \times N \to M \otimes_A N$ defined by $f_b(x, y) = x \otimes by$ is $A$-bilinear. For example, $f_b(x, ay) = x \otimes b(ay) = x \otimes a(by) = a(x \otimes by)$ for $a \in A$. Hence, there exists an $A$-homomorphism $g_b : M \otimes_A N \to M \otimes_A N$ with $f_b = g_b \cdot \phi$. Then we define $bu = g_b(u)$.

2. For an $A$-module $M$ and a $B$-module $P$, $\mathrm{Hom}_A(M, P)$ is a $B$-module by defining $(bf)(x) = b(f(x))$ for $b \in B$, $f \in \mathrm{Hom}_A(M, P)$ and $x \in M$, and is isomorphic to $\mathrm{Hom}_B(M \otimes_A B, P)$.

   For an $A$-homomorphism $f : M \to P$, the $A$-bilinear map $g : M \times B \to P$ defined by $g(x, b) = bf(x)$ defines the $A$-homomorphism $f_B : M \otimes_A B \to P$ which is also a $B$-homomorphism. If $g : M \otimes_A B \to P$ is a $B$-homomorphism, then $g = f_B$ for the $A$-homomorphism $f : M \to P$ defined by $f(x) = g(x \otimes 1)$.

3. For an $A$-module $M$ and a $B$-modules $P, Q$, we have $(M \otimes_A P) \otimes_B Q = M \otimes_A (P \otimes_B Q)$.

4. For $A$-modules $M, N$, we have $(M \otimes_A N) \otimes_A B = (M \otimes_A B) \otimes_B (N \otimes_A B)$.

The third equality is generalized for rings $A, B$ which are not necessarily commutative, right $A$-module $M$, left-right $(A, B)$-module $P$ and left $B$-module $Q$.

A non-empty subset $S$ of a commutative ring $R$ is said to be *multiplicatively closed* if $st \in S$ for $s, t \in S$. For a multiplicatively closed subset $S$, we always assume $1 \in S$.

For any element $y \in R$, $\{1, y, y^2, y^3, \ldots\}$ is a multiplicatively closed subset. Note that an ideal $I$ intersects this set if and only if $y$ is in the radical $\sqrt{I}$. If $I$ is an ideal of $R$, the complement $R \setminus I$ is a multiplicatively closed subset if and only if $I$ is prime. If $H$ is a union of prime ideals in $R$, then $R \setminus H$ is multiplicatively closed.

Let $R$ be a commutative ring and $S$ a multiplicatively closed subset with $1 \in S$. For an $R$-module $M$, the localization $S^{-1}M$ is defined as the quotient of $M \times S$ by the equivalence relation

$$(x, s) \sim (x', s') \Leftrightarrow \exists u \in S, u(s'x - sx') = 0 \ .$$

The equivalence class including $(x, s)$ is denoted by $x/s$. In the case $M = R$, $S^{-1}R$ has a ring structure defined by

$$\frac{a}{s} + \frac{b}{t} = \frac{ta + sb}{st} \ , \quad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st} \ .$$

For general $R$-module $M$, $S^{-1}M$ is the $S^{-1}R$-module defined by

$$\frac{x}{s} + \frac{y}{t} = \frac{tx + sy}{st} \ , \quad \frac{a}{u} \cdot \frac{x}{s} = \frac{ax}{us}$$

for $x/s, y/t \in S^{-1}M$ and $a/u \in S^{-1}R$.

**Lemma 3.1** *We have the following.*
(1) *If $N$ is an $R$-submodule, then $S^{-1}N$ is an $S^{-1}R$-submodule of $S^{-1}M$.*
(2) *$S^{-1}M$ is naturally isomorphic to $M \otimes_R S^{-1}R$.*

Proof (1) For $x, y \in N$ and $s, t \in S$, $x/s = y/t$ in $S^{-1}N$ if and only if there exists $u \in S$ with $u(tx - sy) = 0$ by definition. Since this is equivalent to the condition for $x/s = y/t$ in $S^{-1}M$, the map $S^{-1}N \to S^{-1}M$ defined by $x/s \mapsto x/s$ is an inclusion.

(2) It is easy to see that the map $S^{-1}M \to M \otimes_R S^{-1}R$ defined by $x/s \mapsto x \otimes (1/s)$ is well defined. The bilinear map $M \times S^{-1}R \to S^{-1}M$ defined by $(x, a/s) \mapsto ax/s$ defines an $S^{-1}R$-homomorphism $M \otimes_R S^{-1}R \to S^{-1}M$, which is clearly the inverse of the above map. QED

By this lemma, $N \otimes_R S^{-1}R \to M \otimes_R S^{-1}R$ can be regarded as an inclusion map if $N \subset M$.

An $R$-module $M$ is said to be *$R$-flat* if $L \otimes_R M \to P \otimes_R M$ is injective for every injective $R$-homomorphism $L \to P$. If an $A$-algebra $B$ is $A$-flat as $A$-module, it is called a flat $A$-algebra.

**Theorem 3.2** *For a multiplicatively closed subset $1 \in S \subset R$, $S^{-1}R$ is a flat $A$-algebra.*

Proof Let $L \to P$ be an injective $R$-homomorphism. Let $N$ be the image of $L$. Then, by the injectivity, $L$ is isomorphic to $N$ and hence $L \otimes_R S^{-1}R \to N \otimes_R S^{-1}R$ is isomorphic. Since $N \otimes_R S^{-1}R$ is a submodule of $P \otimes_R S^{-1}R$ by Lemma 3.1, $L \otimes_R S^{-1}R \to P \otimes_R S^{-1}R$ is an isomorphism to a submodule, namely injective. QED

Let $B, C$ be $A$-algebras. Since these are $A$-modules, the tensor product $B \otimes_A C$ is defined. The tensor product is defined as the quotient of $F(B,C)$ by the submodule $K(B,C)$. The free $A$-module $F(B,C)$ has an $A$-algebra structure defined by $(b,c)(b',c') = (bb',cc')$ for $b, b' \in B$ and $c, c' \in C$. Since

$$\begin{aligned}
(b,c)\{(u+u',v)-(u,v)-(u',v)\} &= (bu+bu',cv)-(bu,cv)-(bu',cv)\\
(b,c)\{(u,v+v')-(u,v)-(u,v')\} &= (bu,cv+cv')-(bu,cv)-(bu,cv')\\
(b,c)\{(au,v)-a(u,v)\} &= (abu,cv)-a(bu,cv)\\
(b,c)\{(u,a'v)-a'(u,v)\} &= (bu,a'cv)-a'(bu,cv)
\end{aligned}$$

are in $K(B,C)$ for $a, a' \in A$, $b, u \in B$ and $c, v \in C$, we know that $K(B,C)$ is an ideal of $F(B,C)$. It follows that $B \otimes_A C$ is an $A$-algebra. The map $b \mapsto b \otimes 1$ for $b \in B$ defines a ring homomorphism $B \to B \otimes_A C$, while $c \mapsto 1 \otimes c$ for $c \in C$ defines $C \to B \otimes_A C$.

**Proposition 3.3** *We have the following.*
(1) *If $M$ is a flat $A$-module and $B$ an $A$-algebra, then $M \otimes_A B$ is a flat $B$-module.*
(2) *If $B$ is a flat $A$-algebra and $P$ is a flat $B$-module then $P$ is a flat $A$-module.*
(3) *If both $B$ and $C$ are flat $A$-algebra, then $B \otimes_A C$ is a flat $A$-algebra.*

Proof (1) Let $L \to P$ be an injective $B$-homomorphism. It suffices to show that the $B$-homomorphism $(M \otimes_A B) \otimes_B L \to (M \otimes_A B) \otimes_B P$ is injective. Since $(M \otimes_A B) \otimes_B L = M \otimes_A (B \otimes_B L) = M \otimes_A L$ and $(M \otimes_A B) \otimes_B P = M \otimes_A (B \otimes_B L) = M \otimes_A P$, this is equal to $M \otimes_A L \to M \otimes_A P$, which is injective since $M$ is $A$-flat.

(2) Let $L \to M$ be an injective $B$-homomorphism. Then $L \otimes_A B \to M \otimes_A B$ is injective since $B$ is $A$-flat. Since this is an injective $B$-homomorphism and $P$ is $B$-flat, $(L \otimes_A B) \otimes_B P \to (M \otimes_A B) \otimes_B P$ is injective. Since this homomorphism is $L \otimes_A P \to M \otimes_A P$, $P$ is $A$-flat.

(3) Since $C$ is $A$-flat, $B \otimes_A C$ is $B$-flat by (1). Since $B$ is $A$-flat, $P = B \otimes_A C$ is $A$-flat by (2). QED

**Lemma 3.4** *If the homomorphism $L \otimes_R M \to P \otimes_R M$ is injective for every injective $R$-homomorphism $L \to P$ of finitely generated $R$-modules, then $M$ is $R$-flat.*

Proof If $M$ is not flat, there exists an injective homomorphism $f : L \to P$ such that $f \otimes 1_M : L \otimes_R M \to P \otimes_R M$ is not injective. Hence, there exists a non-zero element $x_1 \otimes z_1 + \cdots + x_n \otimes z_n \in L \otimes_R M$ such that $f(x_1) \otimes z_1 + \cdots + f(x_n) \otimes z_n = 0$.

It suffices to show that there exist finitely generated $R$-submodules $L_0 \subset L$ and $P_0 \subset P$ such that $x_1, \ldots, x_n \in L_0$, $f(L_0) \subset P_0$ and $f(x_1) \otimes z_1 + \cdots + f(x_n) \otimes z_n = 0$ in $P_0 \otimes_R M$. By the assumption, $(f(x_1)\, z_1) + \cdots + (f(x_n), z_n)$ is in $K(P, M)$. Clearly, there exists a finitely generated $R$-submodule $P_0 \subset P$ such that the element is in $K(P_0, M)$ and $f(x_1), \ldots, f(x_n) \in P_0$. Let $L_0 \subset L$ be the $R$-submodule generated by $x_1, \ldots, x_n$. Then $L_0$ and $P_0$ satisfy the condition. QED

# 4 Exact sequences

Let $R$ be a commutative ring and $\phi : M' \to M$ a homomorphism of $R$-modules. For an $R$-module $L$, we denote by $\phi_*$ the map $\mathrm{Hom}_R(L, M') \to \mathrm{Hom}_R(L, M)$ defined by $\phi_*(f) = \phi \cdot f$. Also, for an $R$-module $N$, we denote by $\phi^*$ the map $\mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M', N)$ defined by $\phi^*(g) = g \cdot \phi$. It is easy to see that $\phi_*$ and $\phi^*$ are $R$-homomorphisms if $R$ is commutative. These are typical examples of covariant and contravariant functors in the category theory.

A sequence of $R$-homomorphisms

$$M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} \cdots \xrightarrow{f_{n-2}} M_{n-1} \xrightarrow{f_{n-1}} M_n$$

of $R$-modules is called a *complex* if $f_{i+1} \cdot f_i = 0$ for $i = 1, 2, \ldots, n-2$. It includes the case that this sequence extends infinitely to left or right, or both. A sequence is said to be *exact* if $\mathrm{Im}\, f_{i-1} = \mathrm{Ker}\, f_i$ for $i = 2, 3, \ldots, n-1$.

For example,

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

is exact if $f$ is injective, $g$ is surjective and $\mathrm{Ker}\, g = \mathrm{Im}\, f$.

In the following, we assume that $R$ is a commutative ring.

**Proposition 4.1** (1) *A sequence of $R$-modules $0 \to N' \xrightarrow{f} N \xrightarrow{g} N''$ is exact if and only if*

$$0 \to \mathrm{Hom}_R(L, N') \xrightarrow{f_*} \mathrm{Hom}_R(L, N) \xrightarrow{g_*} \mathrm{Hom}_R(L, N'')$$

*is exact for every $R$-module $L$.*

(2) *A sequence of $R$-modules $M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ is exact if and only if*

$$0 \to \mathrm{Hom}_R(M'', P) \xrightarrow{g^*} \mathrm{Hom}_R(M, P) \xrightarrow{f^*} \mathrm{Hom}_R(M', P)$$

*is exact for every $R$-module $P$.*

Proof (1) Easy. (2) Assume that the first sequence is exact. We prove only the part $\mathrm{Ker}\, f^* = \mathrm{Im}\, g^*$ since the others are easy. The inclusion $\mathrm{Im}\, g^* \subset \mathrm{Ker}\, f^*$ is clear. If $u : M \to P$ satisfies $f^*(u) = u \cdot f = 0$, then $u$ is zero on $\mathrm{Im}\, f$. Hence $f$ factors

$M \to M/\operatorname{Im} f \to P$. Since $M/\operatorname{Im} f \simeq M''$, $u$ factors $M \to M'' \to P$, and hence $u \in \operatorname{Im} g^*$.

Next, assume that the second sequence is exact for every $P$. Set $P = M''/\operatorname{Im} g$ and let $p : M'' \to P$ be the natural surjection. Then $g^*(p) = p \cdot g = 0$. Since $g^*$ is injective, we have $p = 0$. Since $p$ is surjective, $P$ must be zero, i.e., $g$ is surjective. For the inclusion $\operatorname{Im} f \subset \operatorname{Ker} g$, set $P = M''$. Then $g \cdot f = f^*(g^*(1_P)) = 0$, which implies the inclusion. Finally, set $P = M/\operatorname{Im} f$ and consider the natural surjection $p : M \to P$. Since $f^*(p) = p \cdot f = 0$ and $\operatorname{Im} g^* = \operatorname{Ker} f^*$, there exists $q : M'' \to P$ with $g^*(q) = q \cdot g = p$. Hence $p(\operatorname{Ker} g) = q(g(\operatorname{Ker} g)) = q(0) = 0$. This implies that $\operatorname{Ker} g \subset M$ is included in $\operatorname{Im} f$. Hence $\operatorname{Im} f = \operatorname{Ker} g$. QED

**Proposition 4.2** *For any exact sequence $M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ of $R$-modules and and an $R$-module $L$, the sequence*

$$L \otimes_R M' \xrightarrow{1_L \otimes f} L \otimes_R M \xrightarrow{1_L \otimes g} L \otimes_R M'' \longrightarrow 0$$

*is exact.*

Proof By Proposition 4.1 (2), it suffices to show that

$$0 \to \operatorname{Hom}_R(L \otimes_R M'', P) \to \operatorname{Hom}_R(L \otimes_R M, P) \to \operatorname{Hom}_R(L \otimes_R M', P) \tag{4}$$

is exact for every $R$-module $P$. By Proposition 4.1 (2),

$$0 \to \operatorname{Hom}_R(M'', P) \xrightarrow{g^*} \operatorname{Hom}_R(M, P) \xrightarrow{f^*} \operatorname{Hom}_R(M', P)$$

is exact. Then by applying Proposition 4.1 (1) to this exact sequence and $L$, we know

$$0 \to \operatorname{Hom}_R(L, \operatorname{Hom}_R(M'', P)) \xrightarrow{(g^*)^*} \operatorname{Hom}_R(L, \operatorname{Hom}_R(M, P)) \xrightarrow{(f^*)^*} \operatorname{Hom}_R(L, \operatorname{Hom}_R(M', P))$$

is exact. Since the substitutions $\operatorname{Hom}_R(L, \operatorname{Hom}_R(N, P)) = \operatorname{Hom}_R(L \otimes_R N, P)$ are possible for $N = M, M', M''$, we know the sequence (4) is exact. QED

This theorem implies that if $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ is exact and $L$ is a flat $R$-module, then

$$0 \longrightarrow L \otimes_R M' \xrightarrow{1_L \otimes f} L \otimes_R M \xrightarrow{1_L \otimes g} L \otimes_R M'' \longrightarrow 0$$

is exact.

**Exercise 4.3** Prove that, if $M' \xrightarrow{f} M \xrightarrow{g} M''$ is exact and $L$ is flat, then $L \otimes_R M' \to L \otimes_R M \to L \otimes_R M''$ is exact.

**Theorem 4.4** *If the two rows in the commutative diagram*

$$\begin{array}{ccccccccc} 0 & \to & M' & \to & M & \stackrel{\lambda}{\to} & M'' & \to & 0 \\ & & {\scriptstyle f'}\downarrow & & {\scriptstyle f}\downarrow & & {\scriptstyle f''}\downarrow & & \\ 0 & \to & N' & \stackrel{\mu}{\to} & N & \to & N'' & \to & 0 \end{array}$$

*are exact, then there exists* $\delta : \mathrm{Ker}\, f'' \to \mathrm{Coker}\, f'$ *which defines the exact sequence*

$$0 \to \mathrm{Ker}\, f' \to \mathrm{Ker}\, f \to \mathrm{Ker}\, f'' \stackrel{\delta}{\to} \mathrm{Coker}\, f' \to \mathrm{Coker}\, f \to \mathrm{Coker}\, f' \to 0\ .$$

Proof $\delta$ is defined as follows. For $x \in M''$ with $f''(x) = 0$, we can take $y \in M$ such that $\lambda(y) = x$ by the surjectivity of $\lambda$. Then there exists $z \in N'$ with $\mu(z) = f(y)$ since $f(y) \in \mathrm{Im}\, \mu$ by the exactness of the lower row. We define $\delta(x)$ as the image of $z$ in $\mathrm{Coker}\, f'$. It is easy to see that this does not depend on the choice of $y$. The exactness of the sequence is checked by chasing the diagram (cf. Theorem 7.1). QED

$\delta$ in the above theorem is called a connecting homomorphism. See Section 7 for the detail.

A *category* $\mathcal{C}$ consists of a class $\mathrm{Obj}(\mathcal{C})$ of *objects* and a set $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ of *morphisms* for each pair $(X, Y)$ of objects in $\mathrm{Obj}(\mathcal{C})$. An element of $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ is denoted as $u : X \to Y$ or simply $u$. For morphisms $u : X \to Y$ and $v : Y \to Z$, the *composite* $vu : X \to Z$ is defined, and the following conditions are satisfied.

(1) For each object $X$, there exists an element $1_X : X \to X$ such that $1_X t = t$ for any object $W$ and $t : W \to X$, and $u1_X = u$ for any object $Y$ and $u : X \to Y$.

(2) For any $t : W \to X$, $u : X \to Y$ and $v : Y \to Z$, the equality $(vu)t = v(ut)$ holds.

$u : X \to Y$ is said to be an isomorphism if there exists $v : Y \to X$ such that $vu = 1_X$ and $uv = 1_Y$. A *small* category is a category such that the class of objets is a set. It is common to consider a sufficiently large set as a *universe*, and do every mathematical operations inside this set. In this case, all categories are small.

**Example 4.5** In the category **Set** of sets, $\mathrm{Obj}(\mathbf{Set})$ is the class of sets and the morphisms are maps. In the category **Top** of topological spaces, the morphisms are continuous maps. In the category **Gr** of groups, the morphisms are group homomorphisms.

**Example 4.6** Let $R$ be a commutative ring. The objects of the category $R$-**Mod** are $R$-modules, and the morphisms are $R$-homomorphisms. For $R$-modules $M$ and $N$, $\mathrm{Hom}_{R\text{-}\mathbf{Mod}}(M, N)$ is $\mathrm{Hom}_R(M, N)$.

Let $\mathcal{C}$ and $\mathcal{C}'$ be categories. A *covariant functor* $F : \mathcal{C} \to \mathcal{C}'$ consists of a mapping $X \mapsto F(X)$ from $\mathrm{Obj}(\mathcal{C})$ to $\mathrm{Obj}(\mathcal{C}')$ and a mapping $(u : X \to Y) \mapsto (F(u) : F(X) \to F(Y))$ from $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ to $\mathrm{Hom}_{\mathcal{C}'}(F(X), F(Y))$ for each $(X, Y)$, such that $F(1_X) = 1_{F(X)}$ for each $X$, and $F(vu) = F(v)F(u)$ for $u : X \to Y$ and $v : Y \to Z$. A *contravariant*

*functor* $F$ is defined similarly but $(u : X \to Y) \mapsto (F(u) : F(Y) \to F(X))$ and $F(vu) = F(u)F(v)$.

Let $F$ and $G$ be functors from $\mathcal{C}$ to $\mathcal{C}'$. A *homomorphism* $f : F \to G$ of covariant functors is a class of morphisms $f(X) : F(X) \to G(X)$ in $\mathcal{C}'$ for all objects $X$ of $\mathcal{C}$ such that the diagram

$$\begin{array}{ccc} F(X) & \overset{F(u)}{\to} & F(Y) \\ {\scriptstyle f(X)}\downarrow & & {\scriptstyle f(Y)}\downarrow \\ G(X) & \overset{G(u)}{\to} & G(Y) \end{array}$$

is commutative for every morphism $u : X \to Y$. The composite of homomorphisms of functors is defined naturally. If $\mathcal{C}$ and $\mathcal{C}'$ are small categories, then functors from $\mathcal{C}$ to $\mathcal{C}'$ and their homomorphisms form a small category. We denote this category by $\mathrm{Hom}(\mathcal{C}, \mathcal{C}')$.

The *opposite category* $\mathcal{C}^\circ$ of a category $\mathcal{C}$ is defined by $\mathrm{Obj}(\mathcal{C}^\circ) = \mathrm{Obj}(\mathcal{C})$ and $\mathrm{Hom}_{\mathcal{C}^\circ}(X, Y) = \mathrm{Hom}_{\mathcal{C}}(Y, X)$. A contravariant functor $F$ from $\mathcal{C}$ to $\mathcal{C}'$ is regarded as a covariant functor from $\mathcal{C}^\circ$ to $\mathcal{C}'$.

Let $\mathcal{C}$ be a small category. For each object $X$, the contravariant functor $h_X : \mathcal{C} \to \mathbf{Set}$ is defined by $h_X(W) = \mathrm{Hom}(W, X)$. For $v : W' \to W$, the map $h_X(v) : h_X(W) \to h_X(W')$ is defined by $f \mapsto fv$. If $u : X \to Y$ is a morphism in $\mathcal{C}$, then the homomorphism $u_* : h_X \to h_Y$ of functors is defined naturally. Namely, for any object $W$, $u_*(W) : h_X(W) \to h_Y(W)$ is defined by $u_*(W)(f) = uf$. Thus we get a covariant functor $h : \mathcal{C} \to \mathrm{Hom}(\mathcal{C}^\circ, \mathbf{Set})$. It is known that $h$ is *fully faithful*, i.e., the natural map

$$\mathrm{Hom}_{\mathcal{C}}(X, Y) \longrightarrow \mathrm{Hom}_{\mathcal{C}}(h_X, h_Y)$$

is bijective for any objects $X, Y$ in $\mathcal{C}$. A contravariant functor $p : \mathcal{C} \to \mathbf{Set}$ is said to be *representable* if $p$ is isomorphic to $h_X$ for an object $X$ in $\mathcal{C}$.

**Example 4.7** For two objects $X, Y$ in $\mathcal{C}$, the *direct product* $h_X \times h_Y$ in $\mathrm{Hom}(\mathcal{C}^\circ, \mathbf{Set})$ is defined by $h_X \times h_Y(W) = h_X(W) \times h_Y(W)$, where the righthand side is the direct product as the sets. If this functor is represented by an object $Z$ in $\mathcal{C}$, then $Z$ is called the *direct product* of $X$ and $Y$, and is usually denoted by $X \times Y$. In the category $R$-**Mod**, the direct product of $R$-modules $M$ and $N$ is the direct sum $M \oplus N$.

We can also define the covariant functor $h'_X : \mathcal{C} \to \mathbf{Set}$ by $h'_X(V) = \mathrm{Hom}(X, V)$. In this case, we get a fully faithful covariant functor $h' : \mathcal{C}^\circ \to \mathrm{Hom}(\mathcal{C}, \mathbf{Set})$. The representability with respect to this functor is defined similarly.

**Example 4.8** The direct product $h'_X \times h'_Y$ of $h'_X$ and $h'_Y$ in $\mathrm{Hom}(\mathcal{C}, \mathbf{Set})$ is defined by $h'_X \times h'_Y(V) = h'_X(V) \times h'_Y(V)$. If this functor is represented by an object $Z$ in $\mathcal{C}$, then $Z$ is called the *direct sum* of $X$ and $Y$. In the category $R$-**Mod**, the $R$-module $M \oplus N$ is the direct sum in this sense. Actually, we identify $M$ and $N$ with the $R$-submodules $M \times \{0\}$ and $\{0\} \times N$ in $M \oplus N$, respectively. Then, the map $\mathrm{Hom}_R(M \oplus N, P) \to \mathrm{Hom}_R(M, P) \times \mathrm{Hom}_R(N, P)$ defined by $f \mapsto (f|M, f|N)$ is bijective for any $R$-module $P$.

An *additive category* $\mathcal{A}$ is a category such that $\mathrm{Hom}_{\mathcal{A}}(X,Y)$ is an additive group for any $X, Y$. It is required to satisfy the following conditions.

(1) For $X, Y, Z$ in $\mathcal{A}$, the map of compositions $\mathrm{Hom}_{\mathcal{A}}(Y,Z) \times \mathrm{Hom}_{\mathcal{A}}(X,Y) \to \mathrm{Hom}_{\mathcal{A}}(X,Z)$ is bilinear.

(2) There exists an object $\mathbf{0}$ in $\mathcal{A}$ with $\mathrm{Hom}_{\mathcal{A}}(X,\mathbf{0}) = \{0\}$ and $\mathrm{Hom}_{\mathcal{A}}(\mathbf{0},X) = \{0\}$ for any object $X$.

(3) The direct product and the direct sum exist for any $X, Y$ in $\mathcal{A}$.

It follows that the direct product and the direct sum are isomorphic in an additive category. We identify them and denote it by $X \oplus Y$. A covariant functor $F : \mathcal{A} \to \mathcal{A}'$ between additive categories is called *additive* if the map $\mathrm{Hom}_{\mathcal{A}}(X,Y) \to \mathrm{Hom}_{\mathcal{A}'}(X,Y)$ defined by $u \mapsto F(u)$ is a homomorphism. If $F$ is additive, then $F(\mathbf{0})$ is the zero of $\mathcal{A}'$ since $1_{F(\mathbf{0})} = F(1_{\mathbf{0}}) = 0$.

Let $\mathcal{A}$ be an additive category. For a morphism $f : X \to Y$ in $\mathcal{A}$, if the functor $W \mapsto \mathrm{Ker}[f_*(W) : \mathrm{Hom}(W,X) \to \mathrm{Hom}(W,Y)]$ is represented by an object $U$, we call it the *kernel* of $f$ and denote it by $\mathrm{Ker}\, f$. There exists a morphism $i_{U/X} \in \mathrm{Ker}(f_*(U))$ corresponding to $1_U \in \mathrm{Hom}(U,U)$. If $s : W \to X$ satisfies $fs = 0$, then there exists a unique $s' : W \to U$ with $i_{U/X}s' = s$.

The *cokernel* $\mathrm{Coker}\, f$ is an object $V$, if exists, which represents the functor $Z \mapsto \mathrm{Ker}[f^*(Z) : \mathrm{Hom}(Y,Z) \to \mathrm{Hom}(X,Z)]$. There exists a morphism $p_{Y/V} \in \mathrm{Ker}(f^*(V))$ corresponding to $1_V \in \mathrm{Hom}(V,V)$. If $t : Y \to Z$ satisfies $tf = 0$, then there exists a unique $t' : V \to Z$ with $t'p_{Y/V} = t$. The *coimage* and the *image* of $f$ is defined by $\mathrm{Coim}\, f = \mathrm{Coker}\, i_{U/X}$ and $\mathrm{Im}\, f = \mathrm{Ker}\, p_{Y/V}$, respectively.

Assume that $\mathrm{Coim}\, f$ and $\mathrm{Im}\, f$ exist for $f$. Since $fi_{U/X} = 0$, there exists $w : \mathrm{Coim}\, f \to Y$ which factors $f$. Then $p_{Y/V}w = 0$ since $p_{Y/V}f = 0$ and the map $\mathrm{Hom}(\mathrm{Coim}\, f, V) \to \mathrm{Hom}(X,V)$ is injective. Thus we get a natural morphism $\mathrm{Coim}\, f \to \mathrm{Im}\, f$ which makes the following diagram commutative.

$$\begin{array}{ccccccc} \mathrm{Ker}\, f & \stackrel{i_{U/X}}{\longrightarrow} & X & \stackrel{f}{\longrightarrow} & Y & \stackrel{p_{Y/V}}{\longrightarrow} & \mathrm{Coker}\, f \\ & & \downarrow & & \downarrow & & \\ & & \mathrm{Coim}\, f & \longrightarrow & \mathrm{Im}\, f & & \end{array}$$

An *abelian category* is an additive category $\mathcal{A}$ such that
(1) the kernel and the cokernel exist for every morphism in $\mathcal{A}$, and
(2) the natural morphism $\mathrm{Coim}\, f \to \mathrm{Im}\, f$ is an isomorphism for every morphism $f$.
In an abelian category, the image and the coimage of a morphism are identified.

Let $\mathcal{A}$ be an abelian category. If

$$L \stackrel{f}{\longrightarrow} M \stackrel{g}{\longrightarrow} N$$

is a sequence of morphisms in $\mathcal{A}$ such that $gf = 0$, then the object $\mathrm{Ker}\, g/\mathrm{Im}\, f$ is defined. Actually, this is equal to $\mathrm{Coker}(L \to \mathrm{Ker}\, g)$ and $\mathrm{Ker}(\mathrm{Coker}\, f \to N)$. This is also equal to $\mathrm{Coim}\, \phi = \mathrm{Im}\, \phi$ of the induced morphism $\phi : \mathrm{Ker}\, g \to \mathrm{Coker}\, f$. This sequence is said to be *exact* if $\mathrm{Ker}\, g/\mathrm{Im}\, f$ is the zero $\mathbf{0}$.

A sequence, which may be bounded, of morphisms

$$M^\bullet : \quad \cdots \overset{d^{m-1}}{\to} M^m \overset{d^m}{\to} M_{m+1} \overset{d^{m+1}}{\to} \cdots \overset{d^{n-2}}{\to} M^{n-1} \overset{d^{n-1}}{\to} M^n \overset{d^n}{\to} \cdots$$

in $\mathcal{A}$ with $d^{i+1} \cdot d^i = 0$ for all $i$ is called a *complex*. The cohomology object $H^i(M^\bullet) = \mathrm{Ker}(d^i)/\mathrm{Im}(d^{i-1})$ is defined for all $i$ such that $d^{i-1}$ and $d^i$ exist.

It is possible to define homomorphisms of complexes and short exact sequences of complexes. For a short exact sequence, we get a long exact sequence similarly as in Section 7. However, since we can not take an *element* of an object of an abelian category as the case of modules, it has some difficulties in the proof.

# 5 Nakayama's Lemma

**Theorem 5.1 (Nakayama's Lemma)** *Let $R$ be a commutative ring and $I$ an ideal included in every maximal ideal of $R$. If a finitely generated $R$-module $M$ and an $R$-submodule $N$ satisfy*

$$M = N + IM \ ,$$

*then $N = M$.*

Proof Since $M$ is finitely generated, there exist $x_1, \ldots, x_n \in M$ with

$$M = Rx_1 + \cdots + Rx_n \ .$$

For every $i$, the condition implies $x_i \in N + IM$ and there exist $a_{i1}, \ldots, a_{in} \in I$ and $y_i \in N$ with

$$x_i = a_{i1}x_1 + \cdots + a_{in}x_n + y_i \ .$$

If we consider the matrix $A = [a_{ij}]$ and the identity matrix $E = [\delta_{ij}]$, we have

$$(E - A) \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} \ .$$

Since $\det(E - A) \in 1 + I$ is a regular element in $R$, the matrix $E - A$ has the inverse $B$. Namely, we have

$$\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = B \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} \ .$$

This implies that each $x_i$ is in $N$. Since $x_1, \ldots, x_n$ generate $M$, we have $M \subset N$. Since $N$ is a submodule of $M$, we have $N = M$. QED

Remark. In the above proof, the fact that "if $a$ is contained in every maximal ideal of $R$ then $1 + a$ is regular" is used. This is proved easily. If $1 + a$ is not regular, it is

contained in a maximal ideal $P$. Since $a$ is contained in $P$, we have $1 = (1+a) - a \in P$, which contradicts $P \neq R$.

A commutative ring $R$ with only one maximal ideal is called a *local ring*. If $P$ is the maximal ideal, we also write the local ring as the pair $(R, P)$. In some books, local rings are defined to be Noetherian. However, we do not assume it here.

Let $(R, P)$ be a local ring and $M$ a finitely generated $R$-module. Since $R/P$ is a field, $M/PM$ is an $(R/P)$-vector space of finite dimension. Note that the condition of Nakayama's Lemma is satisfied for $I = P$.

**Lemma 5.2** *Let $M$ be a finitely generated $R$-module over a local ring $(R, P)$. Elements $x_1, \ldots, x_s \in M$ generates $M$ if and only if the images $\bar{x}_1, \ldots, \bar{x}_s$ of these elements in $M/PM$ generate this vector space.*

*Furthermore, if $M$ is a free $R$-module of rank $s$, $\{x_1, \ldots, x_s\}$ is a basis of $M$ if and only if $\{\bar{x}_1, \ldots, \bar{x}_s\}$ is a basis of $M/PM$.*

Proof It is clear that the condition is necessary.

Assume that $\bar{x}_1, \ldots, \bar{x}_s$ generate $M/PM$. Let $N$ be the $R$-submodule of $M$ generated by $x_1, \ldots, x_s$. Since the image of $N$ in $M/PM$ is $(N+PM)/PM$ and contains $\bar{x}_1, \ldots, \bar{x}_s$, the image is equal to $M/PM$, and hence $M = N + PM$. By Nakayama's Lemma, we have $N = M$.

When $M$ is a free $R$-module of rank $s$, let $\{u_1, \ldots, u_s\}$ be a basis of $M$. Then each $x_i$ is written as $x_i = \sum_{j=1}^{s} c_{ij} u_j$. If $\{\bar{x}_1, \ldots, \bar{x}_s\}$ is a basis of $M/PM$, then $(\det[c_{ij}] \bmod P) = \det[\bar{c}_{ij}] \neq 0$. Hence $\det[c_{ij}]$ is regular, and $\{x_1, \ldots, x_s\}$ is a basis of $M$. QED

**Theorem 5.3** *Let $(R, P)$ be a Noetherian local ring. If a finitely generated $R$-module $M$ is $R$-flat, then $M$ is free.*

Proof Assume that the dimension of the vector space $M/PM$ is $n$, and the images of $x_1, \ldots, x_n \in M$ form a basis of $M/PM$. We define the $R$-homomorphism from the free $R$-module $F = Re_1 \oplus \cdots \oplus Re_n$ to $M$ by $a_1 e_1 + \cdots + a_n e_n \mapsto a_1 x_1 + \cdots + a_n x_n$. This is surjective by Lemma 5.2. Let $K$ be the kernel of this $R$-homomorphism, which is finitely generated since $R$ is Noetherian. Then we get the exact sequence

$$0 \longrightarrow K \longrightarrow F \longrightarrow M \longrightarrow 0\ .$$

For $k = R/P$, the exact sequence $0 \to P \to R \to k \to 0$ induces the diagram

$$\begin{array}{ccccccccc}
 & & & & 0 & & 0 & & \\
 & & & & \downarrow & & \downarrow & & \\
 & & K \otimes_R P & \stackrel{\nu}{\to} & F \otimes_R P & \stackrel{\rho}{\to} & M \otimes_R P & \to & 0 \\
 & & {\scriptstyle\delta}\downarrow & & {\scriptstyle\beta}\downarrow & & {\scriptstyle\alpha}\downarrow & & \\
0 & \to & K \otimes_R R & \stackrel{\eta}{\to} & F \otimes_R R & \stackrel{\kappa}{\to} & M \otimes_R R & \to & 0 \\
 & & {\scriptstyle\epsilon}\downarrow & & {\scriptstyle\gamma}\downarrow & & \downarrow & & \\
 & & K \otimes_R k & \stackrel{\lambda}{\to} & F \otimes_R k & \stackrel{\mu}{\to} & M \otimes_R k & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & & .
\end{array}$$

in which the rows and the columns are exact. Note that the last column is exact since $M$ is $R$-flat. We will show that $\lambda$ is injective. Let $z$ be an element of $\mathrm{Ker}\,\lambda$. Since $\epsilon$ is surjective, there exists $y \in K \otimes_R R$ with $\epsilon(y) = z$. Then, since $\gamma(\eta(y)) = \lambda(\epsilon(y)) = \lambda(z) = 0$, $\eta(y)$ is in $\mathrm{Ker}\,\gamma = \mathrm{Im}\,\beta$. Hence, there exists $u \in F \otimes_R P$ with $\beta(u) = \eta(y)$. Then, $\rho(u) = 0$ since $\alpha(\rho(u)) = \kappa(\beta(u)) = \kappa(\eta(y)) = 0$ and $\alpha$ is injective. Hence $u$ is in $\mathrm{Ker}\,\rho = \mathrm{Im}\,\nu$, i.e., there exists $x \in K \otimes_R P$ with $\nu(x) = u$. Then $\eta(\delta(x)) = \beta(\nu(x)) = \beta(u) = \eta(y)$, and $\delta(x) = y$ since $\eta$ is injective. Thus $z = \epsilon(y) = \epsilon(\delta(x)) = 0$, which implies that $\lambda$ is injective. Namely, if $z$ is in the kernel of $\lambda$, we can show that $z$ is the image of an element $x \in K \otimes_R P$ in the first column, i.e., $z = 0$. In this diagram chase, the injectivity of $\alpha$ is important.

Since $\mu$ is an isomorphism, $K \otimes_R k = 0$ and hence $K = PK$. Since $R$ is Noetherian, $K$ is finitely generated, and $K = 0$ by Nakayama's Lemma. Hence $M$ is a free $R$-module isomorphic to $F$. QED

# 6 Projective modules and injective modules

Although we assume that $R$ is a commutative ring, most of the results in this section hold for non-commutative rings.

An $R$-module $P$ is said to be *projective* if the sequence

$$0 \to \mathrm{Hom}_R(P, N') \xrightarrow{f_*} \mathrm{Hom}_R(P, N) \xrightarrow{g_*} \mathrm{Hom}_R(P, N'') \to 0$$

is exact for every exact sequence $0 \to N' \xrightarrow{f} N \xrightarrow{g} N'' \to 0$ of $R$-modules. Note that the above sequence is exact except the surjectivity of $g_*$ by Proposition 4.1 (1). Hence, $P$ is projective if, for any surjective homomorphism $f : M \to N$ and any homomorphism $g : P \to N$, there exists a homomorphism $h : P \to M$ with $g = f \cdot h$.

**Lemma 6.1** *Any free module is projective.*

Proof Let $F$ be a free $R$-module and $\{u_\lambda \ ; \ \lambda \in \Lambda\}$ a basis. Let $f : M \to N$ be a surjective $R$-homomorphism. For an $R$-homomorphism $g : F \to N$, there exists $x_\lambda \in M$ with $f(x_\lambda) = g(u_\lambda)$ for each $u_\lambda$ since $f$ is surjective. If we define an $R$-homomorphism $h : F \to M$ by $h(u_\lambda) = x_\lambda$ for $\lambda \in \Lambda$, then $g = f \cdot h$. Hence $F$ is projective. QED

**Lemma 6.2** *For any $R$-module $M$, there exists a surjective $R$-homomorphism from a projective $R$-module. If $M$ is finitely generated, then there exists a surjective $R$-homomorphism from a finitely generated projective $R$-module.*

Proof We consider the free $R$-module $F$ which has a basis bijective to a set of generators of $M$. Since there exists a surjection $F \to M$, the lemma follows from Lemma 6.1. QED

**Theorem 6.3** *An $R$-module $P$ is projective if and only if it is a direct summand of a free $R$-module.*

Proof Assume that $P$ is projective. Let $f : F \to P$ be a surjective $R$-morphism from a free $R$-module. Since $P$ is projective, there exists $g : P \to F$ with $f \cdot g = 1_P$. Then $F = \operatorname{Ker} f \oplus \operatorname{Im} g$ and $\operatorname{Im} g \simeq P$. Hence we may consider $P$ a direct summand of $F$ by identifying with $g(P)$.

Assume that $P \oplus Q$ is a free $R$-module. Let $f : M \to N$ be a surjective $R$-homomorphism and $g : P \to N$ an $R$-homomorphism. For $(x, y) \in P \oplus Q$, we define $g'((x, y)) = g(x)$. Since this is an $R$-homomorphism from a free $R$-module $P \oplus Q$ to $N$, it can be lifted to $h' : P \oplus Q \to M$ by the projectivity of $P \oplus Q$. If we define $h$ to be the restriction of $h'$ to $P$, we have $g = f \cdot h$. Hence $P$ is projective. QED

Remark. If $R$ is the polynomial ring of $n$ variables over a field, then any finitely generated projective $R$-module is free. This is a famous Serre Conjecture proved by D. Quillen and A. Suslin, independently. We can find a proof of it in [L, Chap.21].

An $R$-module $I$ is said to be *injective* if

$$0 \to \operatorname{Hom}_R(M'', I) \xrightarrow{g^*} \operatorname{Hom}_R(M, I) \xrightarrow{f^*} \operatorname{Hom}_R(M', I) \to 0$$

is exact for every exact sequence $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$. The exactness except the surjectivity of $f^*$ follows from Proposition 4.1 (2). Hence, an $R$-module $I$ is injective if, for any injection $f : L \to M$ and any homomorphism $g : L \to I$, there exists a homomorphism $h : M \to I$ with $g = h \cdot f$.

A $\mathbf{Z}$-module $D$ is said to be *divisible* if for any $x \in I$ and a positive integer $n$, there exists $y \in D$ with $ny = x$.

**Lemma 6.4** *A $\mathbf{Z}$-module $I$ is injective if and only if it is divisible.*

Proof Let $I$ be an injective $\mathbf{Z}$-module, $x \in I$ an arbitrary element, and $n$ a positive integer. For the injection $n\mathbf{Z} \to \mathbf{Z}$ and the homomorphism $g : n\mathbf{Z} \to I$ defined by $g(an) = ax$, there exists an extension $g' : \mathbf{Z} \to I$ of $g$ by the injectivity of $I$. Then $x = g(n) = g'(n) = ng(1)$. Hence $x = ny$ for $y = g'(1)$, i.e., $I$ is divisible.

Now assume that $I$ is divisible. Let $f : L \to M$ be an injection and $g : L \to I$ a homomorphism. We may assume that $f$ is an inclusion map. Consider the set of pairs $(N, p)$ of a submodule $N \subset M$ which contains $L$ and an extension $p : N \to I$ of $g$. Clearly, $(L, g)$ is in this set. It is easy to see that this is a non-empty ordered set such that any totally ordered subset has an upper bound. Hence there exists a maximal element $(N, p)$ by Zorn's Lemma. Assume that $N \neq M$. Let $z$ be an element of $M \setminus N$. If we can extend $p$ to $p' : N + \mathbf{Z}z \to N$, it contradicts that $(N, p)$ is maximal. If there exist no $n > 0$ with $nz \in N$, we define $p'(y + az) = p(y)$ for $y \in N$ and $a \in \mathbf{Z}$. If $nz \in N$ for an $n > 0$, then we take minimal such $n$ and choose $u \in I$ with $nu = p(nz)$ by the divisibility of $I$. Then we can extend $p$ by $p'(y + az) = p(y) + au$. QED

**Example 6.5** The $\mathbf{Z}$-modules $\mathbf{Q}$ and $\mathbf{Q}/\mathbf{Z}$ are injective since these are divisible.

**Lemma 6.6** (1) *For any $R$-module $M$, $M^\wedge = \mathrm{Hom}_{\mathbf{Z}}(M, \mathbf{Q}/\mathbf{Z})$ has a structure of an $R$-module.* (2) *There exists a natural injective $R$-homomorphism $M \to M^{\wedge\wedge} = (M^\wedge)^\wedge$.* (3) *If $\phi : M \to N$ is a surjective $R$-homomorphism, then the induced $R$-homomorphism $\phi^* : N^\wedge \to M^\wedge$ is an injection.* (4) *If $F$ is a free $R$-module, then $F^\wedge$ is an injective $R$-module.*

Proof (1) In general, if $S \to R$ is a homomorphism of commutative rings, $M$ an $R$-module and $N$ an $S$-module, then $\mathrm{Hom}_S(M, N)$ has a structure of an $R$-module by defining $(af)(x) = f(ax)$ for $f \in \mathrm{Hom}_S(M, N)$, $a \in R$ and $x \in M$.

(2) $\lambda : M \to M^{\wedge\wedge}$ is defined by $\lambda(x)(f) = f(x)$ for $x \in M$ and $f \in M^\wedge$. For any nonzero element $x \in M$, there exists a nonzero homomorphism $f_0 : \mathbf{Z}x \to \mathbf{Q}/\mathbf{Z}$. Since $\mathbf{Q}/\mathbf{Z}$ is injective, $f_0$ extends to a $\mathbf{Z}$-homomorphism $f : M \to \mathbf{Q}/\mathbf{Z}$. Since $\lambda(x)(f) = f_0(x) \neq 0$, $\lambda(x)$ is not zero. Hence $\lambda$ is an injection.

(3) If $f \in N^\wedge$ is nonzero, then $\phi^*(f) = f \cdot \phi$ is not zero since $\phi$ is surjective.

(4) Since a free $R$-module is isomorphic to a direct sum of copies of $R$, the $R$-module $F^\wedge$ is isomorphic to a direct product of copies of $R^\wedge = \mathrm{Hom}_{\mathbf{Z}}(R, \mathbf{Q}/\mathbf{Z})$. Hence, it suffices to prove that $R^\wedge$ is an injective $R$-module. Here, note that the direct product of injective modules is injective, while the direct sum of projective modules is projective.

Let $L \to M$ be an inclusion map of $R$-modules, and $\lambda : L \to R^\wedge$ a homomorphism. Then, a $\mathbf{Z}$-homomorphism $\bar{\lambda} : L \to \mathbf{Q}/\mathbf{Z}$ is defined by $\bar{\lambda}(x) = \lambda(x)(1)$. Since $\mathbf{Q}/\mathbf{Z}$ is injective, $\bar{\lambda}$ extends to a $\mathbf{Z}$-homomorphism $\bar{\lambda}' : M \to \mathbf{Q}/\mathbf{Z}$. We define $\lambda' : M \to R^\wedge$ by $\lambda'(y)(a) = \bar{\lambda}'(ay)$. Then $\lambda'$ is an $R$-homomorphism extending $\lambda$. Hence $R^\wedge$ is an injective $R$-module. QED

**Theorem 6.7** *Every $R$-module $M$ can be embedded in an injective $R$-module.*

Proof Take a surjection $F \to M^\wedge$ from a free $R$-module $F$. Then the composite $M \to M^{\wedge\wedge} \to F^\wedge$ is an embedding of $M$ to the injective $R$-module $F^\wedge$ by Lemma 6.6. QED

For any $R$-module $M$, there exists a minimal injective $R$-module $E_R(M)$ which contains $M$. $E_R(M)$ is called the *injective hull* of $M$. When $R$ is Noetherian, every injective module is a direct sum of injective modules each of which is isomorphic to $E_R(R/P)$ for a prime ideal $P$ of $R$ (cf. [H]).

An extension $M \subset P$ of $R$-module $M$ is said to be *essential* if any non-zero $R$-submodule $N \subset P$ has a nontrivial intersection $M \cap N$. Clearly, $M$ itself is an essential extension of $M$.

Let $M$ be an $R$-module. Take an injective $R$-module $I$ with $M \subset I$. Then, any essential extension $M \subset P$ of $M$ can be embedded in $I$. Actually, since $I$ is injective, there exists an $R$-homomorphism $\phi : P \to I$ which extends the inclusion map $M \subset I$. Then $\mathrm{Ker}\,\phi \cap M = \{0\}$ since $\phi(x) = x$ for $x \in M$. Since $P$ is an essential extension of $M$, $\mathrm{Ker}\,\phi = \{0\}$, i.e., $\phi$ is an injection.

The set of $R$-submodules $P$ of $I$ which are essential extensions of $M$ is inductive, and has a maximal element $E$ by Zorn's Theorem. This $E$ has no essential extension other than $E$. Namely, if $E \subset E'$ is an essential extension, then $E'$ is an essential extension of $M$ and is embedded in $I$. Then $E' = E$ by the maximality of $E$.

**Lemma 6.8** *The maximal essential extension $E$ is injective.*

Proof The set of $R$-submodules $Q$ of $I$ with $Q \cap E = \{0\}$ is inductive. Hence, there exists a maximal element $F$ by Zorn's Theorem. If $E + F \neq I$, then the natural $R$-homomorphism $\lambda : E \to I/F$ is injective since $E \cap F = \{0\}$, and not surjective since the cokernel is $I/(E+F)$. Then $E \simeq \lambda(E) \subset I/F$ is not an essential extension by the above remark. Hence, there exists a nontrivial $R$-submodule $N \subset I/F$ with $\lambda(E) \cap N = \{0\}$. Then the pull-back $F'$ of $N$ is a nontrivial extension of $F$ with $E \cap F' = \{0\}$, which contradicts the maximality of $F$. Hence $E + F = I$, and $E$ is injective since it is a direct summand of the injective module $I$. QED

**Lemma 6.9** *Let $M \subset E'$ be a maximal essential extension in an embedding $M \subset I'$ to an injective $R$-module. Then $E'$ is isomorphic to $E$ as extensions of $M$.*

Proof Since $E'$ is injective by Lemma 6.8, there exists an $R$-homomorphism $\phi : E \to E'$ with $\phi(x) = x$ for $x \in M$. Then $\operatorname{Ker} \phi = \{0\}$ since the extension $M \subset E$ is essential. Hence $\phi$ is an injection, and $E'$ is the direct sum $\phi(E) \oplus F$ for an $R$-submodule $F \subset E'$ since $\phi(E)$ is injective. Then $F \cap M \subset F \cap \phi(E) = \{0\}$, which implies $F = \{0\}$ since the extension $M \subset E'$ is essential. Hence $E \simeq \phi(E) = E'$. QED

This $E$ is called the *injective hull* or the *injective envelope* of $M$.

# 7 Cohomology group

When an $R$-module $M$ has an $R$-endomorphism $d$ with $d \cdot d = 0$, we call $(M, d)$ or simply $M$ a $d$-module. Although the symbol $d$ for the endomorphism may change as $d'$, $d_M$, etc., we always call it a $d$-module.

For a $d$-module $(M, d)$, we set $Z(M) = \operatorname{Ker} d$ and $B(M) = \operatorname{Im} d$. We have $B(M) \subset Z(M)$ by the assumption $d \cdot d = 0$. We call $\mathrm{H}(M) := Z(M)/B(M)$ the *cohomology group* of $M$. The cohomology group $\mathrm{H}(M)$ is an $R$-module. For $x \in Z(M)$, the equivalence class $[x]$ in $\mathrm{H}(M)$ is called the *cohomology class* of $x$.

It is often the case that $R$ here is just $\mathbf{Z}$ or a field $k$, and $M$ is an $R'$-module over a bigger ring or a $k$-algebra $R'$.

For $d$-modules $(M, d_M)$, $(N, d_N)$, a *homomorphism $f : M \to N$ of $d$-modules* is an $R$-homomorphism satisfying $d_N \cdot f = f \cdot d_M$. In this case, by the commutative diagram

$$\begin{array}{ccc} M & \xrightarrow{d_M} & M \\ {\scriptstyle f}\downarrow & & {\scriptstyle f}\downarrow \\ N & \xrightarrow{d_N} & N \end{array},$$

we have $f(Z(M)) \subset Z(N)$, $f(B(M)) \subset B(N)$ and the homomorphism $\mathrm{H}(f) : \mathrm{H}(M) \to \mathrm{H}(N)$ of cohomology groups is defined by $[x] \mapsto [f(x)]$.

Let $(M, d)$ be a $d$-module. If $M' \subset M$ is an $R$-submodule with $d(M') \subset M'$, then $(M', d')$ is a $d$-module for $d' = d|M'$, and $M' \subset M$ is a homomorphism of $d$-modules. Furthermore, if we set $M'' := M/M'$, then $d$ induces a homomorphism $d'' : M'' \to M''$, and $(M'', d'')$ is also a $d$-module. We denote by $\bar{x}$ the equivalence class of $x$ in $M''$. The natural surjection $M \to M''$ is a homomorphism of $d$-modules. Hence we get a sequence of cohomology groups

$$\mathrm{H}(M') \xrightarrow{\alpha} \mathrm{H}(M) \xrightarrow{\beta} \mathrm{H}(M'') \ .$$

The *connecting homomorphism* $\delta : \mathrm{H}(M'') \to \mathrm{H}(M')$ is defined as follows.

If $\bar{x} \in Z(M'')$, then $d(x) \in M'$ and $d(x) \in Z(M')$ by $d \cdot d(x) = 0$. We define $\delta([\bar{x}])$ to be the cohomology class of $d(x)$ in $\mathrm{H}(M')$. We will show that this class does not depend on the choice of $x$. Assume $[\bar{x}']'' = [\bar{x}]''$ for $x, x' \in M$. Then there exists $y \in M$ with $\bar{x}' - \bar{x} = d''(\bar{y})$. This means $x' - x = d(y) + z$ for a $z \in M'$. Then we have $[d(x')]' = [d(x)]'$ by

$$d(x') - d(x) = d^2(y) + d(z) = d(z) \in d'(M') \ .$$

Hence $\delta([\bar{x}]'') = [d(x)]'$ is well defined. It is easy to see that $\delta$ is an $R$-homomorphism.

**Theorem 7.1** *Let $M, M', M''$ be given as above, then the sequence of modules*

$$\mathrm{H}(M') \xrightarrow{\alpha} \mathrm{H}(M) \xrightarrow{\beta} \mathrm{H}(M'') \xrightarrow{\delta} \mathrm{H}(M') \xrightarrow{\alpha} \mathrm{H}(M)$$

*is exact.*

Proof First, we show the exactness at $\mathrm{H}(M)$. We have $\beta \cdot \alpha = 0$ since $\beta \cdot \alpha([x]') = [\bar{x}]''$ and $\bar{x} = 0$ for $x \in Z(M') \subset M'$. If the cohomology class $[x]$ satisfies $\beta([x]) = 0$, then there exists $y \in M$ with $d''(\bar{y}) = \bar{x}$. Hence $x = d(y) + z$ for an element $z \in M'$. This means that the cohomology class $[z]'$ of $z$ in $\mathrm{H}(M')$ is mapped to $[z] = [x]$ by $\alpha$. Hence $\mathrm{Ker}\, \beta = \mathrm{Im}\, \alpha$.

Next we show the exactness at $\mathrm{H}(M'')$. For $[x] \in \mathrm{H}(M)$ represented by $x \in Z(M)$, $\beta([x])$ is $[\bar{x}]''$. By the definition of $\delta$, $\delta([\bar{x}]'')$ is $[d(x)]'$, which is zero since $x \in Z(M)$. Hence $\mathrm{Im}\, \beta \subset \mathrm{Ker}\, \delta$. If $[\bar{x}]'' \in \mathrm{H}(M'')$ with $x \in M$ is contained in $\mathrm{Ker}\, \delta$, then there exists $z \in M'$ with $d(x) = d(z)$. Since $d(x - z) = 0$ and $\bar{z} = 0$, the cohomology class $[x - z] \in \mathrm{H}(M)$ is defined, and the image of this class by $\beta$ is $[\bar{x}]''$. Hence $\mathrm{Ker}\, \delta = \mathrm{Im}\, \beta$.

Finally, we will see the exactness at $\mathrm{H}(M')$. If $\bar{x} \in Z(M'')$ for $x \in M$, then $d''(\bar{x}) = 0$ and $d(x) \in M'$. Then $\delta([\bar{x}]'')$ is the cohomology class $[d(x)]'$ of $d(x)$ in $\mathrm{H}(M')$, which is mapped to $[d(x)] = 0$ by $\alpha$. Hence $\alpha \cdot \delta = 0$. If $[z] \in \mathrm{H}(M)$ is 0 for $z \in Z(M')$, then there exists $x \in M$ with $z = d(x)$. In this case, $\delta([\bar{x}]'')$ is equal to the cohomology class $[z]'$ of $z$ in $\mathrm{H}(M')$. Hence $\mathrm{Ker}\, \alpha = \mathrm{Im}\, \delta$. QED

Let $R$ be a ring. A sequence of $R$-homomorphisms

$$\cdots \longrightarrow M^{k-1} \xrightarrow{d^{k-1}} M^k \xrightarrow{d^k} M^{k+1} \xrightarrow{d^{k+1}} M^{k+2} \xrightarrow{d^{k+2}} \cdots$$

satisfying $d^{i+1} \cdot d^i = 0$ for every $i \in \mathbf{Z}$ is called a *cochain complex* and denoted by $(M^\bullet, \{d^i\})$ or simply $M^\bullet$. The each morphism $d^i$ or the collection $\{d^i \, ; \, i \in \mathbf{Z}\}$ is called the *coboundary map* of this complex.

Let $M^\bullet$ be a cochain complex. Then $\operatorname{Im} d^{k-1} \subset \operatorname{Ker} d^k$ for every integer $k$. We write the quotient $R$-module $\operatorname{Ker} d^k / \operatorname{Im} d^{k-1}$ by $\mathrm{H}^k(M^\bullet)$ and call it the $k$-th cohomology group of $M^\bullet$. If we set $M = \bigoplus_{k \in \mathbf{Z}} M_k$ and $d : M \to M$ the direct sum of $d^i$'s, then $(M, d)$ is a $d$-module and

$$Z(M) = \bigoplus_{k \in \mathbf{Z}} \operatorname{Ker} d^k \ , \quad B(M) = \bigoplus_{k \in \mathbf{Z}} \operatorname{Im} d^{k-1} \ .$$

Hence $\mathrm{H}(M)$ is equal to $\bigoplus_{k \in \mathbf{Z}} \mathrm{H}^k(M^\bullet)$.

When $M'^\bullet$ is a subcomplex of $M^\bullet$ and $M''^\bullet$ is the quotient $M^\bullet / M'^\bullet$, then the connecting homomorphism $\delta : \mathrm{H}(M''^\bullet) \to \mathrm{H}(M'^\bullet)$ is decomposed to the direct sum of $\delta^i : \mathrm{H}(M''^\bullet)^i \to \mathrm{H}(M'^\bullet)^{i+1}$ for $i \in \mathbf{Z}$. The $R$-homomorphism $\delta^i$ is also called a *connecting homomorphism*. By Theorem 7.1, we have the *long exact sequence*

$$\cdots \xrightarrow{\beta^{i-1}} \mathrm{H}^{i-1}(M'') \xrightarrow{\delta^{i-1}} \mathrm{H}^i(M') \xrightarrow{\alpha^i} \mathrm{H}^i(M) \xrightarrow{\beta^i} \mathrm{H}^i(M'') \xrightarrow{\delta^i} \mathrm{H}^{i+1}(M') \xrightarrow{\alpha^{i+1}} \cdots \ .$$

# 8 Tor group

Let $R$ be a commutative ring and $N$ an $R$-module. Assume a sequence of $R$-homomorphisms

$$\cdots \xrightarrow{d_3} P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\epsilon} N$$

satisfies the following conditions.

(1) Each $P_i$ ($i \geqq 0$) is a projective $R$-module, and $\operatorname{Im} d_{i+1} = \operatorname{Ker} d_i$ for every $i > 0$.

(2) $\operatorname{Im} d_1 = \operatorname{Ker} \epsilon$ and $\epsilon$ is surjective.

In this case, we call the pair $(P_\bullet, \epsilon)$ a *projective resolution* of $N$.

For any $R$-module $N$, there exists a projective resolution. Actually, there exist a projective module $P_0$ and a surjection $\epsilon$ by Lemma 6.2. Then, by applying Lemma 6.2 again for $\operatorname{Ker} \epsilon$, there exists a surjection $P_1 \to \operatorname{Ker} \epsilon$ from a projective $R$-module $P_1$, and $d_1$ is defined to be the composite of this map with the inclusion $\operatorname{Ker} \epsilon \subset P_0$. In this way, projective modules $P_1, P_2, \ldots$ and homomorphisms $d_1, d_2, \ldots$ are defined inductively by using Lemma 6.2.

Let $M, N$ be $R$-modules. Then for each non-negative integer $n$, the Tor group $\operatorname{Tor}_n^R(M, N)$ of degree $n$ is defined as follows.

Let $(P_\bullet, \epsilon)$ be a projective resolution of $N$. We consider the sequence of $R$-modules and $R$-homomorphisms

$$\cdots \xrightarrow{1_M \otimes d_3} M \otimes_R P_2 \xrightarrow{1_M \otimes d_2} M \otimes_R P_1 \xrightarrow{1_M \otimes d_1} M \otimes_R P_0 \xrightarrow{1_M \otimes d_0} 0 \ ,$$

where $d_0$ is the zero map $P_0 \to 0$. It is clear that this is a complex, and we denote it by $M \otimes_R P_\bullet$. For each non-negative integer $n$, we define

$$\operatorname{Tor}_n^R(M, N) := \mathrm{H}_n(M \otimes_R P_\bullet) = \operatorname{Ker}(1_M \otimes d_n) / \operatorname{Im}(1_M \otimes d_{n+1}) \ .$$

It can be shown that this definition does not depend on the choice of the resolution. The homotopy equivalence of the resolutions is used for the proof. We have the equality $\mathrm{Tor}_0^R(M,N) = M \otimes_R N$ by Proposition 4.2. Here, note that we sometimes identify functors which give canonically isomorphic objects. Namely, the correspondences $M \mapsto \mathrm{Tor}_n^R(M,N)$ is a *derived functor* define for $N$ for each $n \geqq 0$. However, the case $n = 0$ is not new since $\mathrm{Tor}_0^R(M,N)$ is canonically isomorphic to $M \otimes_R N$. Hence $\mathrm{Tor}_0^R(M,N)$ is identified with $M \otimes_R N$.

**Proposition 8.1** *Let $M, N$ be $R$-modules and $(P_\bullet, \epsilon)$ a projective resolution of $N$. For a positive integer $k$, let $N_k := \mathrm{Im}\, d_k \subset P_{k-1}$. Then $\mathrm{Tor}_n^A(M,N)$ is equal to $\mathrm{Tor}_{n-k}^A(M,N_k)$ for every $n > k$.*

Proof We set $Q_i := P_{i+k}$ for $i \geqq 0$, and define $\epsilon' = d_k : Q_0 \to N_k$ and $d'_i = d_{i+k} : Q_i \to Q_{i-1}$ for $i \geqq 1$. Then $(Q_\bullet, \epsilon')$ is a projective resolution of $N_k$. Hence

$$\begin{aligned} & \mathrm{Tor}_n^R(M,N) \\ &= \mathrm{Ker}(1_M \otimes d_n)/\,\mathrm{Im}(1_M \otimes d_{n+1}) \\ &= \mathrm{Ker}(1_M \otimes d'_{n-k})/\,\mathrm{Im}(1_M \otimes d'_{n-k+1}) \\ &= \mathrm{Tor}_{n-k}^R(M,N_k) \end{aligned}$$

for every $n > k$. QED

**Theorem 8.2** *Let $M, N$ be $R$-modules. Then $\mathrm{Tor}_k^R(M,N) \simeq \mathrm{Tor}_k^R(N,M)$ for every non-negative integer $k$.*

Proof If $k = 0$, then

$$\mathrm{Tor}_0^R(M,N) = M \otimes_R N \simeq N \otimes_R M = \mathrm{Tor}_0^R(N,M)\ .$$

We prove the theorem for $k = 1$. Let $(Q_\bullet, \epsilon')$ be a projective resolution of $M$, and let $M_1 := \mathrm{Ker}\,\epsilon'$. Then

$$0 \longrightarrow M_1 \longrightarrow Q_0 \longrightarrow M \longrightarrow 0$$

is exact. Since $Q_0$ is projective, it is flat and $Q_0 \otimes_R P_\bullet$ is exact for a projective resolution $P_\bullet$ of $N$. Hence $\mathrm{Tor}_1^R(Q_0,N) = 0$, and

$$0 \longrightarrow \mathrm{Tor}_1^R(M,N) \xrightarrow{\delta_1} \mathrm{Tor}_0^R(M_1,N) \longrightarrow \mathrm{Tor}_0^R(Q_0,N)$$

is exact by the long exact sequence. Hence we have isomorphisms

$$\begin{aligned} \mathrm{Tor}_1^R(M,N) &\simeq \mathrm{Ker}(M_1 \otimes_R N \to Q_0 \otimes_R N) \\ &\simeq \mathrm{Ker}(N \otimes_R M_1 \to N \otimes_R Q_0)\ . \end{aligned}$$

Set $E := \mathrm{Ker}(N \otimes_R M_1 \to N \otimes_R Q_0)$. Then, since

$$N \otimes_R Q_2 \longrightarrow N \otimes_R Q_1 \xrightarrow{\rho} N \otimes_R M_1 \longrightarrow 0$$

is exact, we have

$$E \simeq \rho^{-1}(E)/\operatorname{Ker}\rho = \mathrm{Ker}(N \otimes_R Q_1 \to N \otimes_R Q_0)/\operatorname{Im}(N \otimes_R Q_2 \to N \otimes_R Q_1)\ ,$$

which is equal to $\mathrm{Tor}_1^R(N, M)$ by definition.

We prove the case $k > 1$ by induction. By $\mathrm{Tor}_k^R(Q_0, N) = \mathrm{Tor}_{k-1}^R(Q_0, N) = 0$ and the long exact sequence

$$\cdots \longrightarrow \mathrm{Tor}_k^R(Q_0, N) \longrightarrow \mathrm{Tor}_k^R(M, N) \longrightarrow \mathrm{Tor}_{k-1}^R(M_1, N) \longrightarrow \mathrm{Tor}_{k-1}^R(Q_0, N) \longrightarrow \cdots\ ,$$

we have $\mathrm{Tor}_k^R(M, N) \simeq \mathrm{Tor}_{k-1}^R(M_1, N)$. Since $\mathrm{Tor}_{k-1}^R(M_1, N) \simeq \mathrm{Tor}_{k-1}^R(N, M_1)$ by the assumption of the induction and $\mathrm{Tor}_{k-1}^R(N, M_1)$ is equal to $\mathrm{Tor}_k^R(N, M)$ by Proposition 8.1, we have $\mathrm{Tor}_k^R(M, N) \simeq \mathrm{Tor}_k^R(N, M)$. QED

# 9 Ext group

Let $R$ be a commutative ring. The *injective resolution* $(I^\bullet, \epsilon)$ of an $R$-module $M$ is a pair of a complex $I^\bullet = (I^i, d^i\ ; i \geqq 0)$ of injective $R$-modules and an injection $\epsilon : M \to I^0$ such that

$$0 \longrightarrow M \xrightarrow{\epsilon} I^0 \xrightarrow{d^0} I^1 \xrightarrow{d^1} I^2 \xrightarrow{d^2} \cdots$$

is exact. An injective resolution of $M$ is constructed as follows.

First, by Theorem 6.7, we take an embedding $\epsilon : M \to I^0$ to an injective $R$-module. Then we take also an embedding $I^0/\operatorname{Im}\epsilon \to I^1$ to an injective $R$-module, and let $d^0 : I^0 \to I^1$ be the composite from $I^0$. In this way, we continue to define $d^i : I^i \to I^{i+1}$ as the composite of of the surjection $I^i \to I^i/\operatorname{Im} d^{i-1}$ and an embedding $I^i/\operatorname{Im} d^{i-1} \to I^{i+1}$ to an injective $R$-module $I^{i+1}$. Then we get an injective resolution of $N$.

For $R$-modules $M, N$ and non-negative integer $n$, the Ext group $\mathrm{Ext}_R^n(M, N)$ of degree $n$ is defined as follows.

Let $(I^\bullet, \epsilon)$ be an injective resolution of $N$. We denote the cochain complex

$$0 \longrightarrow \mathrm{Hom}_R(M, I^0) \xrightarrow{d_*^0} \mathrm{Hom}_R(M, I^1) \xrightarrow{d_*^1} \mathrm{Hom}_R(M, I^2) \xrightarrow{d_*^2} \cdots$$

by $\mathrm{Hom}_R(M, I^\bullet)$. We define $\mathrm{Ext}_R^n(M, N)$ to be the $n$-th cohomology of this complex, i.e., $\operatorname{Ker} d_*^n/\operatorname{Im} d_*^{n-1}$ if $n > 0$ and $\operatorname{Ker} d_*^0$ if $n = 0$. Note that we can not exchange $M$ and $N$ here.

For the exact sequence $0 \to N \to I^0 \to I^1$,

$$0 \longrightarrow \mathrm{Hom}_R(M, N) \longrightarrow \mathrm{Hom}_R(M, I^0) \longrightarrow \mathrm{Hom}_R(M, I^1)$$

is exact by Proposition 4.1 (1). Hence $\mathrm{Ext}_R^0(M, N) \simeq \mathrm{Hom}_R(M, N)$, and these are identified.

**Lemma 9.1** *Let $M_1, M_2, N$ be $R$-modules. Then*

$$\mathrm{Ext}^n_R(M_1 \oplus M_2, N) = \mathrm{Ext}^n_R(M_1, N) \oplus \mathrm{Ext}^n_R(M_2, N)$$

*for every $n \geqq 0$.*

Proof Since the complex $\mathrm{Hom}_R(M_1 \oplus M_2, I^\bullet)$ is the direct sum of $\mathrm{Hom}_R(M_1, I^\bullet)$ and $\mathrm{Hom}_R(M_2, I^\bullet)$, the cohomology is also the direct sum. QED

If $M$ is a free $R$-module and isomorphic to $R^{\oplus r}$, the each component of $\mathrm{Hom}_R(M, I^\bullet)$ is the $r$-times direct sum of the component of $I^\bullet$. Hence $\mathrm{Ext}^i_R(M, N) = 0$ for $i > 0$. When $M$ is a free $R$-module of infinite rank, we also have $\mathrm{Ext}^i_R(M, N) = 0$ for $i > 0$, although the component $\mathrm{Hom}_R(M, I^i)$ of $\mathrm{Hom}_R(M, I^\bullet)$ becomes an infinite direct product of $I^i$.

**Proposition 9.2** *Let $P$ be a projective $R$-module. Then $\mathrm{Ext}^n_R(P, N) = 0$ for any $R$-module $N$ and positive integer $n$.*

Proof Since $P$ is projective, there exists an $R$-module $Q$ such that $F = P \oplus Q$ is a free $R$-module. Then $\mathrm{Ext}^n_R(F, N) = 0$ for $n > 0$ as we remarked above. Since $\mathrm{Ext}^n_R(P, N)$ is a direct summand of $\mathrm{Ext}^n_R(F, N)$ by Lemma 9.1, it is also 0. QED

Let $M, N$ be $R$-modules, $(I^\bullet, \epsilon)$ an injective resolution of $N$ and $(P_\bullet, \epsilon')$ the projective resolution of $M$. The following theorem shows that $\mathrm{Ext}^i_R(M, N)$ can also be calculated by the projective resolution of $M$. Here $\mathrm{Hom}_R(P_\bullet, N)$ is the cochain complex whose $i$-th component is $E^i = \mathrm{Hom}_R(P_i, N)$ and $d^i : E^i \to E^{i+1}$ is $(d^P_{i+1})_*$.

**Theorem 9.3** *In above notation, we have $\mathrm{H}^k(\mathrm{Hom}_R(P_\bullet, N)) \simeq \mathrm{Ext}^k_R(M, N)$ for every integer $k \geqq 0$.*

Proof We prove the theorem by induction on $k$. When $k = 0$, $\mathrm{H}^0(\mathrm{Hom}_R(P_\bullet, N))$ is isomorphic to $\mathrm{Hom}_R(M, N)$ by Proposition 4.1 (2) applied for the exact sequence $P_1 \to P_0 \xrightarrow{\epsilon'} M \to 0$ and $N$.

Assume $k = 1$. We set $M_1 := \mathrm{Ker}\, \epsilon'$. Then the short exact sequence

$$0 \longrightarrow M_1 \longrightarrow P_0 \longrightarrow M \longrightarrow 0$$

induces a long exact sequence

$$\mathrm{Hom}(P_0, N) \longrightarrow \mathrm{Hom}_R(M_1, N) \longrightarrow \mathrm{Ext}^1_R(M, N) \longrightarrow \mathrm{Ext}^1_R(P_0, N)\ ,$$

and we have

$$\mathrm{Ext}^1_R(M, N) \simeq \mathrm{Coker}(\mathrm{Hom}(P_0, N) \to \mathrm{Hom}_R(M_1, N))\ ,$$

since $\mathrm{Ext}^1_R(P_0, N) = 0$ by Proposition 9.2. Since $\mathrm{Hom}_R(M_1, N) = \mathrm{Ker}(\mathrm{Hom}(P_1, N) \to \mathrm{Hom}(P_2, N))$ by the exact sequence $P_2 \longrightarrow P_1 \longrightarrow M_1 \longrightarrow 0$, the righthand is equal to the cohomology group $\mathrm{H}^1(\mathrm{Hom}_R(P_\bullet, N))$. Hence we get the theorem for $k = 1$.

We prove the case $k > 1$ by induction. We have $\mathrm{Ext}_R^{k-1}(P_0, N) = \mathrm{Ext}_R^k(P_0, N) = 0$ by Proposition 9.2 since $P$ is projective. Hence by the long exact sequence

$$\mathrm{Ext}_R^{k-1}(P_0, N) \longrightarrow \mathrm{Ext}_R^{k-1}(M_1, N) \longrightarrow \mathrm{Ext}_R^k(M, N) \longrightarrow \mathrm{Ext}_R^k(P_0, N) \ ,$$

we have

$$\mathrm{Ext}_R^{k-1}(M_1, N) \simeq \mathrm{Ext}_R^k(M, N) \ .$$

The lefthand is isomorphic to $\mathrm{H}^k(\mathrm{Hom}_R(P_\bullet, N))$ by the assumption of the induction.
QED

Let $(M^\bullet, d_M)$ and $(N^\bullet, d_N)$ be complexes of $R$-modules. A homomorphism $f : M^\bullet \to N^\bullet$ of complexes is a collection $(f_i)_{i \in \mathbf{Z}}$ of $R$-homomorphisms $f_i : M^i \to N^i$ such that $d_N^i f_i = f_{i+1} d_M^i$ for every $i \in \mathbf{Z}$. If there exists such homomorphism $f$, then we get the homomorphism $H^i(f) : H^i(M^\bullet) \to H^i(N^\bullet)$ of the cohomology groups for every $i \in \mathbf{Z}$.

We say that two homomorphisms $f, g : M^\bullet \to N^\bullet$ are *homotopic* if there exists a collection $(h^i)_{i \in \mathbf{Z}}$ of homomorphisms $h^i : M^i \to N^{i-1}$ such that

$$f_i - g_i = d_N^{i-1} h^i + h^{i+1} d_M^i \tag{5}$$

for every $i \in \mathbf{Z}$.

**Lemma 9.4** *If $f$ and $g$ are homotopic, then $H^i(f) = H^i(g)$ for every $i \in \mathbf{Z}$.*

Proof Let $x$ be an element of $Z(M^i)$ and $[x] \in \mathrm{H}^i(M^\bullet)$ the cohomology class. Then $H^i(f)([x])$ and $H^i(g)([x])$ are represented by $f_i(x)$ and $g_i(x)$, respectively. By the equality (5), we have

$$f_i(x) - g_i(x) = d_N^{i-1} h^i(x) + h^{i+1} d_M^i(x) = d_N^{i-1} h^i(x) \in B(N^i)$$

since $d_M^i(x) = 0$. Hence $f_i(x)$ and $g_i(x)$ define the same cohomology class in $\mathrm{H}^i(N^\bullet)$.
QED

**Lemma 9.5** *Let $(P_\bullet, \epsilon_M)$ and $(Q_\bullet, \epsilon_N)$ be projective resolutions of $M$ and $N$, respectively. Then, any $R$-homomorphism $\phi : M \to N$ can be lifted to a homomorphism $P_\bullet \to Q_\bullet$ of the resolutions, and any two liftings are homotopic. Similarly, for any injective resolutions $(I^\bullet, \epsilon'_M)$ and $(J^\bullet, \epsilon'_N)$, there exists a homomorphism $I^\bullet \to J^\bullet$ extending the homomorphism $\phi$, and any two extensions are homotopic.*

Proof We will give $\lambda_0$ and $\lambda_1$ of the commutative diagram

$$\begin{array}{ccccccccccc}
\to & P_2 & \stackrel{d_2^M}{\to} & P_1 & \stackrel{d_1^M}{\to} & P_0 & \stackrel{\epsilon_M}{\to} & M & \to & 0 \\
 & {\scriptstyle \lambda_2}\downarrow & & {\scriptstyle \lambda_1}\downarrow & & {\scriptstyle \lambda_0}\downarrow & & {\scriptstyle \phi}\downarrow & & \\
\to & Q_2 & \stackrel{d_2^N}{\to} & Q_1 & \stackrel{d_1^N}{\to} & Q_0 & \stackrel{\epsilon_N}{\to} & N & \to & 0 \ .
\end{array}$$

Then $\lambda_i$ for $i \geqq 2$ are defined similarly as $\lambda_1$. Since $\epsilon_N$ is surjective and $P_0$ is projective, there exists $\lambda_0 : P_0 \to Q_0$ such that $\phi \cdot \epsilon_M = \epsilon_N \cdot \lambda_0$. Since $\epsilon_N \cdot \lambda_0 \cdot d_1^M = \phi \cdot \epsilon_M \cdot d_1^M = 0$, the image of $\lambda_0 \cdot d_1^M$ is contained in $\mathrm{Ker}(\epsilon_N) = \mathrm{Im}(d_1^N)$. Since $P_1$ is projective and $d_1^N$ is surjective to its image, there exists $\lambda_1 : P_1 \to Q_1$ with $\lambda_0 \cdot d_1^M = d_1^N \cdot \lambda_1$.

Assume that there exists another set $\{\lambda'_i \ ; \ i = 0, 1, 2, \ldots\}$ of $R$-homomorphisms making this diagram commutative. First, we define $h_0 : P_0 \to Q_1$. Since

$$\epsilon_N \cdot (\lambda_0 - \lambda'_0) = \epsilon_N \cdot \lambda_0 - \epsilon_N \cdot \lambda'_0 = \phi \cdot \epsilon_M - \phi \cdot \epsilon_M = 0 \ ,$$

$\mathrm{Im}(\lambda_0 - \lambda'_0)$ is in $\mathrm{Ker}(\epsilon_N) = \mathrm{Im}(d_1^N)$, and there exists $h_0 : P_0 \to Q_1$ with $d_1^N \cdot h_0 = \lambda_0 - \lambda'_0$ since $P_0$ is projective. Next, we define $h_1 : P_1 \to Q_2$. Since

$$d_1^N \cdot (\lambda_1 - \lambda'_1 - h_0 \cdot d_1^M) = d_1^N \cdot (\lambda_1 - \lambda'_1) - (\lambda_0 - \lambda'_0) \cdot d_1^M = 0 \ ,$$

$\mathrm{Im}(\lambda_1 - \lambda'_1 - h_0 \cdot d_1^M)$ is in $\mathrm{Ker}(d_1^N) = \mathrm{Im}(d_2^N)$. Hence there exists $h_1 : P_1 \to Q_2$ with $d_2^N \cdot h_1 = \lambda_1 - \lambda'_1 - h_0 \cdot d_1^M$ since $P_1$ is projective. For $i > 1$, assume that $h_{i-1}$ and $h_{i-2}$ are defined. Then

$$d_i^N \cdot (\lambda_i - \lambda'_i) = (\lambda_{i-1} - \lambda'_{i-1}) \cdot d_i^M = (d_i^N \cdot h_{i-1} + h_{i-2} \cdot d_{i-1}^M) \cdot d_i^M = d_i^N \cdot h_{i-1} \cdot d_i^M$$

since $d_{i-1}^M \cdot d_i^M = 0$. Hence $d_i^N \cdot (\lambda_i - \lambda'_i - h_{i-1} \cdot d_i^M) = 0$, and the image of $\lambda_i - \lambda'_i - h_{i-1} \cdot d_i^M$ is in $\mathrm{Im}(d_{i+1}^N)$. Then there exists $h_i : P_i \to Q_{i+1}$ with $d_{i+1}^N \cdot h_i = \lambda_i - \lambda'_i - h_{i-1} \cdot d_i^M$. Hence these two homomorphisms of complexes are homotopic.

The assertions for injective resolutions are proved similarly. QED

Consider the case where $M = N$ and $\phi$ is the identity map. Then there is also a set $\{\mu_i \ ; \ i = 0, 1, 2, \ldots\}$ of $R$-homomoprhisms $\mu_i : Q_i \to P_i$ which makes a similar diagram commutative.

Let $F$ be a covariant additive functor from $R$-**Mod** to an abelian category $\mathcal{A}$. Then $F(P_\bullet)$ and $F(Q_\bullet)$ are complexes, and $F(\lambda)$ and $F(\mu)$ define homomorphisms of homology groups $H_i(F(\lambda))$ and $H_i(F(\mu))$ (objects of $\mathcal{A}$). The composite of the homomorphisms $H_i(F(\mu)) \cdot H_i(F(\lambda))$ is equal to $H_i(F(\mu \cdot \lambda))$. Since the identity map of $F(P_\bullet)$ is also a lifting of $1_F(N)$, $F(\mu \cdot \lambda)$ is homotopic to the identity map, here note that homotopy relations are preserved by the functor $F$. Hence $H_i(F(\mu \cdot \lambda))$ is the identity map for every $i \geqq 0$. Similarly, $H_i(F(\lambda \cdot \mu))$ is also the identity map for every $i \geqq 0$.

Since $\mathrm{Tor}_i^R(M, N) = H_i(F(P_\bullet))$ for the additive functor $M \mapsto M \otimes_R N$, the definition of $\mathrm{Tor}_i^R(M, N)$ does not depend on the choice of the projective resolution $P_\bullet$. Similarly, the definition of $\mathrm{Ext}_R^i(M, N)$ does not depend on the choice of the injective resolution $I^\bullet$ of $N$.

# 10 Artin-Rees

A commutative ring $R$ is said to be *graded* if it is a direct sum $\bigoplus_{i=0}^{\infty} R_i$ of submodules and $R_i R_j \subset R_{i+j}$ for any $i, j \geqq 0$. For each $i \geqq 0$, an element of $R_i$ is said to be *homogeneous*. An $R$-module $M$ is called a *graded $R$-module* if it is a direct sum $\bigoplus_{i \in \mathbf{Z}} M_i$

such that $R_iM_j \subset M_{i+j}$ for any $i \geqq 0$ and $j \in \mathbf{Z}$. An ideal $I$ of a graded ring $R$ is called a *homogeneous ideal* if $I$ is generated by a set of homogeneous elements.

The quotient of a graded ring $R$ by a homogeneous ideal $I$ is a graded ring. Namely, we can write as $I = \bigoplus_{i=0}^{\infty} I_i$ for $I_i = I \cap R_I$, $i = 0, 1, 2, \ldots$, and $R/I = \bigoplus_{i=0}^{\infty} R_i/I_i$

**Example 10.1** (1) For a commutative ring $R$, the polynomial ring $R[x]$ is a graded ring by considering the direct sum $\bigoplus_{i=0}^{\infty} Rx^i$. The polynomial ring $R[x_1, \ldots, x_n]$ of $n$ variables has a structure of a graded ring by setting a non-negative degree $a_i$ for each variable. Namely, the degree of a monomial $f = x_1^{e_1} \cdots x_n^{e_n}$ is defined to be $e_1a_1 + \cdots + e_na_n$. It is standard to set $a_1 = \cdots = a_n = 1$.

(2) For an ideal $J$ of $R$, $\bigoplus_{i=0}^{\infty} J^it^i \subset R[t]$ is a graded ring. This graded ring is called the *Rees algebra* of $J$ and denoted by $\mathrm{Rees}_R(J)$.

(3) If $I$ is an ideal of a commutative ring $R$, then $R = I^0 \supset I^1 \supset I^2 \supset \cdots$ is a descending chain of ideals. For every $i \geqq 0$, $I^i/I^{i+1}$ is an $(R/I)$-module, and there exists a multiplication map $(I^i/I^{i+1}) \times (I^j/I^{j+1}) \to (I^{i+j}/I^{i+j+1})$ for each pair $(i, j)$. By these maps, the graded ring $\mathrm{Gr}_I(R) = \bigoplus_{i=0}^{\infty} I^i/I^{i+1}$ is defined. $\mathrm{Gr}_I(R)$ is an $(R/I)$-algebra generated by $\mathrm{Gr}_I(R)_1 = I/I^2$. This graded ring is used in the dimension theory of rings (cf. Section 12).

**Proposition 10.2** *Let $R = \bigoplus_{k=0}^{\infty} R_i$ be a graded ring. Then, the following conditions are equivalent.*
(1) *$R$ is Noetherian.*
(2) *The subring $R_0$ is Noetherian, and $R$ is finitely generated over $R_0$.*

Proof (2) implies (1) by the Hilbert Basis Theorem.

We assume (1). Since $I = \bigoplus_{k=1}^{\infty} R_i$ is an ideal of the Noetherian ring $R$, it is finitely generated. Let $\{x_1, \ldots, x_s\}$ be a set of generators of the homogeneous ideal $I$. We may assume that all $x_i$ are homogeneous elements of positive degrees. We will show that $R = R_0[x_1, \ldots, x_s]$. It suffices to show that any homogeneous element $f$ of $R$ is contained in the righthand. If $\deg f = 0$, then $f \in R_0 \subset R_0[x_1, \ldots, x_s]$. If $d = \deg f > 0$, then $f \in I$ and there exist elements $g_1, \ldots, g_s \in R$ with $f = g_1x_1 + \cdots + g_sx_s$. We may assume that $g_i$'s are homogeneous and $\deg g_i = d - \deg x_i < d$ if $g_i \neq 0$. By induction on $d$, we may assume $g_1, \ldots, g_s \in R_0[x_1, \ldots, x_s]$. Then clearly $f$ is in the righthand. QED

**Theorem 10.3 (Artin-Rees)** *Let $I$ be an ideal of a Noetherian ring $R$, $M$ a finitely generated $R$-module and $N \subset M$ an $R$-submodule. Then there exists a non-negative integer $r$ such that $I^nM \cap N = I^{n-r}(I^rM \cap N)$ for every $n \geqq r$.*

Proof It is clear that $I^{n-r}(I^rM \cap N) \subset I^nM \cap N$ for any $r$ and $n$ with $n \geqq r \geqq 0$.

Consider the Rees algebra $\mathrm{Rees}_R(I) = \bigoplus_{k=0}^{\infty} I^kt^k$ which is a graded Noetherian ring. The $R$-submodule $\widetilde{N} = \bigoplus_{k=0}^{\infty}(I^kM \cap N)t^k$ of $\widetilde{M} = \bigoplus_{k=0}^{\infty}(I^kM)t^k$ is a graded $\mathrm{Rees}_R(I)$-module since

$$I^it^i\widetilde{N}_j = I^it^i(I^jM \cap N)t^j \subset (I^{i+j}M \cap N)t^{i+j} = \widetilde{N}_{i+j} .$$

Since $M$ is finitely generated, so is the $\mathrm{Rees}_R(I)$-module $\widetilde{M}$. Hence the $\mathrm{Rees}_R(I)$-submodule $\widetilde{N}$ is also finitely generated. Assume that homogeneous elements $x_1, \ldots, x_s$ generate $\widetilde{N}$. Let $r$ be the maximum of $d_1 = \deg x_1, \ldots, d_s = \deg x_s$. Since

$$\widetilde{N} = \mathrm{Rees}_R(I)x_1 + \cdots + \mathrm{Rees}_R(I)x_s \ ,$$

we have

$$I^n M \cap N = \widetilde{N}_n = I^{n-d_1}x_1 + \cdots + I^{n-d_s}x_s \tag{6}$$

for every $n \geqq r$, where we omit the symbol $t$. Since $x_i \in I^{d_i}M \cap N$ and

$$I^{r-d_i}(I^{d_i}M \cap N) \subset I^r M \cap N \ ,$$

we have $I^{n-d_i}x_i \subset I^{n-r}(I^r M \cap N)$ for each $i$. Hence $I^n M \cap N \subset I^{n-r}(I^r M \cap N)$ by (6). QED

**Theorem 10.4** *Let $R$ be a Noetherian ring and $M$ a finitely generated $R$-module. If an ideal $I$ is contained in every maximal ideal of $R$, then $\bigcap_{i=0}^{\infty} I^i M = 0$.*

Proof We set $N = \bigcap_{i=0}^{\infty} I^i M$. By Artin-Rees, there exists $r$ such that

$$N = I^{r+1}M \cap N = I(I^r M \cap N) = IN \ .$$

Since $N$ is an $R$-submodule of $M$, $N$ is finitely generated. Hence $N = 0$ by Nakayama's Lemma. QED

**Corollary 10.5** *Let $(R, P)$ be a Noetherian local ring. For any ideal $I$ contained in $P$, we have $\bigcap_{i=0}^{\infty} I^i = 0$. In particular, $\bigcap_{i=0}^{\infty} P^i = 0$.*

Let $R$ be a commutative ring and $I$ an ideal. The *$I$-adic topology* of $M$ is defined by setting $\{I^i M\}$ a fundamental system of neighborhoods of 0. Namely, a subset $U$ of $M$ is open if, for any $x \in U$, there exists $i \geqq 0$ with $x + I^i M \subset U$.

**Lemma 10.6** *Let $R$ be a Noetherian ring, $M$ a finitely generated $R$-module and $N$ an $R$-submodule of $M$. Then the $I$-adic topology of $N$ is equal to the relative topology of the $I$-adic topology of $M$.*

Proof Since $I^i N \subset I^i M$ for every $i \geqq 0$, a subset of $N$ is open if it is open for the relative topology. On the other hand, by Artin-Rees, there exists $r$ with $I^n M \cap N = I^{n-r}(I^r M \cap N) \subset I^{n-r}N$ for $n \geqq r$. Hence if a subset $U \subset N$ is open, then it is open for the relative topology. QED

# 11 Completions

Let $R$ be a commutative ring and $M$ an $R$-module. An infinite sequence

$$M = M_0 \supset M_1 \supset M_2 \supset M_3 \supset \cdots$$

of descending $R$-submodules is called a *filtration* of $M$. If a filtration is given, then the completion $\hat{M}$ is defined by the projective limit

$$\hat{M} = \varprojlim M/M_i \ .$$

An element of $\hat{M}$ is described by a sequence $(x_n)$ of elements $x_n \in M/M_n$ such that the image of $x_{n+1}$ in $M/M_n$ is equal to $x_n$ for every $n \geqq 0$.

A filtration $\{M_i\}$ of $M$ defines a structure of topological group on $M$. If another filtration $\{M_i'\}$ gives the same topology on $M$, then the completions of $M$ by these filtrations are equal.

If $I$ is an ideal of $R$, the $I$-adic topology of $M$ is given by the filtration $\{I^n M\}$. The completion of $M$ by this filtration is called the *$I$-adic* completion.

**Theorem 11.1** *Let $R$ be a Noetherian ring and $0 \to M' \to M \to M'' \to 0$ a short exact sequence of finitely generated $R$-modules. An ideal $I$ of $R$ defines $I$-adic topologies on these $R$-modules. Then the obtained sequence of completions*

$$0 \to \hat{M}' \to \hat{M} \to \hat{M}'' \to 0$$

*is an exact sequence of $R$-modules.*

Proof By Lemma 10.6, the $I$-adic completion of $M'$ is defined by the filtration $\{M' \cap I^n M\}$. Hence the sequence is the projective limit of the exact sequence

$$0 \longrightarrow M'/(M' \cap I^n M) \longrightarrow M/I^n M \longrightarrow M''/I^n M'' \longrightarrow 0 \ .$$

The exactness of the part $0 \to \hat{M}' \to \hat{M} \to \hat{M}''$ is proved easily from this exact sequence.

Now, its enough to show that any element $(x_n')$ in $\hat{M}''$ can be lifted to an element $(x_n)$ in $\hat{M}$. First, $x_0$ is defined to be the trivial element of $M/I^0 M = 0$. Suppose we have already defined $x_0, \ldots, x_n$ properly. We will define $x_{n+1}$. We consider the diagram

$$\begin{array}{ccccccccc} 0 & \to & M'/(M' \cap I^{n+1}M) & \stackrel{\alpha'}{\to} & M/I^{n+1}M & \stackrel{\beta'}{\to} & M''/I^{n+1}M'' & \to & 0 \\ & & \rho \downarrow & & \mu \downarrow & & \nu \downarrow & & \\ 0 & \to & M'/(M' \cap I^n M) & \stackrel{\alpha}{\to} & M/I^n M & \stackrel{\beta}{\to} & M''/I^n M'' & \to & 0 \ , \end{array}$$

whose two rows are exact. Take $y \in M/I^{n+1}M$ with $\beta'(y) = x_{n+1}'$. Then since $\beta(\mu(y)) = \nu(\beta'(y)) = \nu(x_{n+1}') = x_n' = \beta(x_n)$, we have $\beta(x_n - \mu(y)) = 0$, and there exists $z \in M'/(M' \cap I^n M)$ with $\alpha(z) = x_n - \mu(y)$. Since $\rho$ is surjective, we take $w \in M'/(M' \cap I^{n+1}M)$ with $\rho(w) = z$. We set $x_{n+1} = y + \alpha'(w)$. Then $\beta'(x_{n+1}) = \beta'(y) = x_{n+1}'$ and $\mu(x_{n+1}) = \mu(y) + \alpha(\rho(w)) = \mu(y) + (x_n - \mu(y)) = x_n$. Hence the sequence is extended to $n+1$. QED

The $I$-adic completion $\hat{R}$ of $R$ is a commutative ring since it is a projective limit of commutative rings. There is a natural homomorphism $R \to \hat{R}$. For an $R$-module $M$, the natural $R$-homomorphisms $\lambda_n : M \to M/I^n M$ define the $R$-homomorphism $\lambda : M \to \hat{M}$ by $\lambda(x) = (\lambda_n(x))$.

The $I$-adic completion $\hat{M}$ has a structure of an $\hat{R}$-module. Namely, for $(a_n) \in \hat{R}$ and $(x_n) \in \hat{M}$, we define $(a_n)(x_n) = (a_n x_n)$. This $\hat{R}$-module structure is compatible with the $R$-module structure through the homomorphism $R \to \hat{R}$ of rings. In particular, there exists an $\hat{R}$-homomorphism $\phi : M \otimes_R \hat{R} \to \hat{M}$.

**Theorem 11.2** *Let $R$ be a Noetherian ring, $M$ a finitely generated $R$-module and $I$ an ideal of $R$. Then, for the $I$-adic completions $\hat{R}$ and $\hat{M}$, the morphism $\phi : M \otimes_R \hat{R} \to \hat{M}$ is isomorphic.*

Proof By taking a surjection $\beta : F \to M$ from a free $R$-module $F$ of finite rank, we get a short exact sequence $0 \to N \xrightarrow{\alpha} F \xrightarrow{\beta} M \to 0$, where $N = \operatorname{Ker}\beta$. Since $R$ is Noetherian, $N$ is finitely generated. By Theorem 11.1, we have a diagram

$$\begin{array}{ccccccccc} & & N \otimes_R \hat{R} & \xrightarrow{\alpha'} & F \otimes_R \hat{R} & \xrightarrow{\beta'} & M \otimes_R \hat{R} & \to & 0 \\ & & \rho \downarrow & & \mu \downarrow & & \nu \downarrow & & \\ 0 & \to & \hat{N} & \xrightarrow{\alpha''} & \hat{F} & \xrightarrow{\beta''} & \hat{M} & \to & 0\,, \end{array}$$

where the two rows are exact. Since $\mu$ is isomorphic and $\beta''$ is surjective, $\nu$ is surjective. If we replace $M$ by $N$, we know $\rho$ is surjective by the same reason. By a diagram chase, or by Theorem 4.4, we know $\nu$ is injective and hence $\nu$ is an isomorphism. QED

Let $R$ be a Noetherian ring and $I$ an ideal. If $L \to M$ is an injection of finitely generated $R$-modules, then by Theorems 11.1 and 11.2, $L \otimes_R \hat{R} \to M \otimes_R \hat{R}$ is injective. Hence $\hat{R}$ is $R$-flat by Lemma 3.4.

A flat $R$-module $N$ is said to be *faithfully flat* if the injectivity of $L \otimes_R N \to M \otimes_R N$ implies that of $L \to M$. This is equivalent to the condition that $E \otimes_R N \neq 0$ for every $R$-module $E \neq 0$.

**Lemma 11.3** *Let $(R, P)$ and $(S, Q)$ be local rings and $f : R \to S$ a local homomorphism, i.e., $f(P) \subset Q$. If $S$ is $R$-flat, then it is faithfully flat.*

Proof Since $PS \subset Q$, $(R/P) \otimes_R S = S/PS \neq 0$. Let $I$ is an ideal of $R$ with $I \neq R$. Then, since there exists a surjection $(R/I) \otimes_R S \to (R/P) \otimes_R S$, we have $(R/I) \otimes_R S \neq 0$. For any $R$-module $E \neq 0$, take a non-zero element $x$ of $E$ and define $I = \{a \in R \,;\, ax = 0\}$. Then there is an injection $R/I \to E$ defined by $\bar{a} \mapsto ax$ for $a \in R$. By the flatness of $S$, we get an injection $(R/I) \otimes_R S \to E \otimes_R S$. This implies $E \otimes_R S \neq 0$. QED

**Theorem 11.4** *Let $(R, P)$ be a Noetherian local ring. Then the $P$-adic completion $\hat{R}$ is a local ring with the maximal ideal $P\hat{R}$, and is a faithfully flat $R$-algebra.*

# 12 Dimension theory

An integer valued function $f(n)$ is said to be *a polynomial for large* $n$, if there exists a polynomial $g(x)$ with rational coefficients and an integer $n_0$ such that $f(n) = g(n)$ for every integer $n \geqq n_0$.

**Lemma 12.1** *If $f(n)$ is a polynomial of degree $d \geqq 0$ for large $n$, then $F(n) = \sum_{k=0}^{n-1} f(k)$ is a polynomial of degree $d+1$ for large $n$.*

Proof We use the fact that $\sum_{k=0}^{n-1} k^l$ is a polynomial of degree $l+1$ of $n$ for every $l \geqq 0$. This is known as Faulhaber's formula, and the coefficients of the polynomial are written by Bernoulli numbers. Assume that $f(n) = g(n)$ for $n \geqq n_0$ and $g(x) = \sum_{i=0}^{d} a_i x^i$ with $a_d \neq 0$. Then, for $n \geqq n_0$, we have

$$F(n) = \sum_{i=0}^{d} a_i \left\{ \sum_{k=0}^{n-1} k^i \right\} + \sum_{k=0}^{n_0-1} (f(k) - g(k)) \ .$$

Since the second term of the righthand is a constant, this is a polynomial of degree $d+1$ since $a_d \neq 0$. QED

Let $R$ be a commutative ring and $M$ an $R$-module. A sequence

$$M = M_0 \supset M_1 \supset \cdots \supset M_{s-1} \supset M_s = 0 \tag{7}$$

of $R$-modules is called a *maximal chain* if there exist no $R$-submodule $N$ with $M_{i-1} \supsetneq N \supsetneq M_i$ for any $i = 1, \ldots, s$. If there exists a maximal chain for $M$, the number $s$ does not depend on the choice of the maximal sequence (see the comment after Lemma 12.5). The number $s$ is called the *length* of $M$ and denoted by $l(M)$. When $M$ has no maximal chain, we define the length to be infinity. If $0 \to M' \to M \to M'' \to 0$ is an exact sequence of $R$-modules, then we have equality $l(M) = l(M') + l(M'')$ (cf. Lemma 12.5).

If a Noetherian ring $R$ has only one prime ideal $P$, then $\{0\}$ is a primary ideal with the radical $P$ by Theorem 1.3. Hence $P^n = \{0\}$ for an integer $n > 0$, and $R$ is of finite length as an $R$-module. Such an ring $R$ is called an *Artin local ring*, and any finitely generated $R$-module is of finite length. Note that any field is an Artin local ring.

**Lemma 12.2** *Let $R = \bigoplus_{i=0}^{\infty} R_i$ be a graded ring and $M = \bigoplus_{i=0}^{\infty} M_i$ a finitely generated graded $R$-module. We assume $R_0$ is an Artin local ring and $R = R_0[x_1, \ldots, x_s]$ for a finite number of elements $x_1, \ldots, x_s \in R_1$. Then each $M_i$ is a finitely generated $R_0$-module, and $f_M(n) = l(M_n)$ is a polynomial of degree at most $s-1$ for large $n$, where we understand the polynomial $0$ is of degree $-1$.*

Proof We prove the lemma by induction on $s$. If $s = 0$, then $R = R_0$ and $f_M(n) = 0$ for large $n$ since $M$ is finitely generated.

Assume that $s > 0$ and the lemma is true for $s-1$. Let $\mu : M \to M$ be the map of multiplications by $x_s$, and set $K = \operatorname{Ker} \mu$ and $L = \operatorname{Coker} \mu$. Then we get an exact sequence

$$0 \longrightarrow K \longrightarrow M \xrightarrow{x_s} M \longrightarrow L \longrightarrow 0$$

of finitely generated $R$-modules. Since $x_nK = x_nL = 0$, $K$ and $L$ are $R_0[x_1, \ldots, x_{s-1}]$-modules. By the assumption of the induction, $f_K(n)$ and $f_L(n)$ are polynomials of degrees at most $s-2$ for large $n$. Since $x_n$ is a homogeneous element of degree 1, we know that this complex is the direct sum of the exact sequences

$$0 \to K_n \to M_n \to M_{n+1} \to L_{n+1} \to 0 \tag{8}$$

for $n \in \mathbf{Z}$. From the exact sequence (8) of $R_0$-modules, we have the equality $f_K(n) - f_M(n) + f_M(n+1) - f_L(n+1) = 0$ for each $n$. Hence $f_M(k+1) - f_M(k) = f_L(k+1) - f_K(k)$, and

$$f_M(n) = \sum_{k=0}^{n-1} \{f_L(k+1) - f_K(k)\} + f_M(0)$$

is a polynomial of degree at most $s-1$ for large $n$ by Lemma 12.1. QED

**Lemma 12.3** *Let $(R, P)$ be a Noetherian local ring, $I = (x_1, \ldots, x_d)$ an ideal satisfying $\sqrt{I} = P$. Then, for a finitely generated $R$-module $M$, $\chi_{I,M}(n) = l(M/I^nM)$ is a polynomial of degree at most $d$ for large $n$.*

Proof We define the graded ring $G_I(R) = \bigoplus_{i=0}^{\infty} I^i/I^{i+1}$ and the graded $G_I(R)$-module $G_I(M) = \bigoplus_{i=0}^{\infty} I^iM/I^{i+1}M$. Then $G_I(R)_0 = R/I$ is an Artin local ring, and $G_I(R) = (R/I)[\bar{x}_1, \ldots, \bar{x}_d]$ for the images $\bar{x}_1, \ldots, \bar{x}_d$ of $x_1, \ldots, x_d$ in $I/I^2$. By Lemma 12.2, $f(n) = l(I^nM/I^{n+1}M)$ is a polynomial of degree at most $d-1$ for large $n$. Since

$$\chi_{I,M}(n) = l(M/I^nM) = \sum_{i=0}^{n-1} l(I^iM/I^{i+1}M) = \sum_{i=0}^{n-1} f(i) \ ,$$

$\chi_{I,M}(n)$ is a polynomial of degree at most $d$ for large $n$. QED

Let $I$ be an ideal of a Noetherian local ring $(R, P)$ contained in $P$. Then $\sqrt{I}$ is equal to $P$ if and only if some power of $P$ is contained in $I$, and if and only if $I$ is $P$-primary. We denote by $\delta(A)$ the minimum of the number $n \geqq 0$ such that there exist $x_1, \ldots, x_n \in P$ with $P = \sqrt{(x_1, \ldots, x_n)}$.

The number $d(R)$ is defined to be the polynomial degree of $\chi_{I,R}(n) = l(R/I^n)$, which is the case of $M = R$ in Lemma 12.3. This definition does not depend on the choice of the $P$-primary ideal $I$. Namely, since $\chi_{P^e,R}(n) = \chi_{P,R}(en)$ for $e > 1$, the degree of this polynomial is equal to that of $\chi_{P,R}(n)$. For general $P$-primary $I$, there exists $e \geqq 1$ with $P \supset I \supset P^e$. Then $\chi_{P,R}(n) \leqq \chi_{I,R}(n) \leqq \chi_{P^e,R}(n)$, and we know the degrees of these functions in $n$ are equal by comparing the growths.

The *length* of a sequence $P_0 \subset P_1 \subset \cdots \subset P_{t-1} \subset P_t$ of distinct prime ideals of $R$ is defined to be $t$. The maximum of the lengths of such sequences of prime ideals of a commutative ring $R$ is called the *dimension* of $R$, and denoted by $\dim R$.

**Theorem 12.4** *Let $(R, P)$ be a Noetherian local ring. Then the equalities*

$$\dim R = d(R) = \delta(R)$$

*hold. If $R$ is the localization at a maximal ideal of an integral domain which is finitely generated over a field $k$, then this number is equal to the transcendence degree over $k$ of the quotient field.*

Proof We will show in the order (1) $d(R) \leqq \delta(R)$, (2) $\delta(R) \leqq \dim R$, (3) $\dim R \leqq d(R)$. We omit the proof the last statement. We will give some comments in Section 13.

(1) $d(R)$ is equal to the degree of $\chi_{I,R}(n)$, which is the case $M = R$ in Lemma 12.3. Since this is less than or equal to the number of generators of $I$ by the lemma, it is less than or equal to the minimum $\delta(R)$.

(2) Every minimal prime ideal of a Noetherian ring is an associated ideal of the zero ideal (0). In particular, $R$ has only a finite number of minimal prime ideals, and we can take an element $x_1$ outside these prime ideals if $P$ is not minimal. Then $\dim R/(x_1) \leqq d-1$ for $d = \dim R$. Repeating this process, we can take less than or equal to $d$ elements $x_1, \ldots, x_s$ with $\dim R/(x_1 \ldots, x_s) = 0$. Then $(x_1 \ldots, x_s)$ is a primary ideal whose radical is the maximal ideal of $R$, and we have $\delta(R) \leqq s \leqq \dim R$.

(3) We prove by induction on $d = \dim R$. The assertion is clear for $d = 0$.

Assume $d > 0$, and let $P_0 \subset P_1 \subset \cdots \subset P_{d-1} \subset P_d$ be a sequence of prime ideals of $R$. We can consider the induced sequence on $R/P_0$, and we may assume that $R$ is an integral domain by replacing $R$ by $R/P_0$ since $d(R) \geqq d(R/P_0)$.

Let $x \in P_1$ be a non-zero element, and set $N = xR$. We consider a short exact sequence $0 \to N \to R \to R/xR \to 0$. Let $P$ be the maximal ideal of $R$, and set $f(n) = l(R/P^n)$. By Artin-Rees, there exists $r > 0$ such that $P^n N \subset N \cap P^n = P^{n-r}(N \cap P^r) \subset P^{n-r}N$ for every $n \geqq r$. Since $N \simeq R$, we have

$$f(n) = l(N/P^n N) \geqq l(N/N \cap P^n) = l(N/P^{n-r}(N \cap P^r)) \geqq l(N/P^{n-r}N) = f(n-r) \ .$$

By the exact sequence $0 \to N/N \cap P^n \to R/P^n \to (R/xR)/P^n(R/xR) \to 0$, we have

$$l((R/xR)/P^n(R/xR)) = f(n) - l(N/N \cap P^n) \leqq f(n) - f(n-r) \ ,$$

where the righthand is of degree at most $d(R) - 1$. Hence $d(R/xR) \leqq d(R) - 1$. Since $\dim R/xR = d - 1$, we have $d - 1 \leqq d(R/xR) \leqq d(R) - 1$ by the assumption of the induction, and hence $\dim R \leqq d(R)$. QED

**Lemma 12.5** *We define $l(M)$ to be the minimum of $s$ in (7) if an $R$-module $M$ has a maximal chain. If $N$ is an $R$-submodule of $M$, then $N$ and $M/N$ have maximal chains, and the equality $l(M) = l(N) + l(M/N)$ holds.*

Proof We prove the lemma by induction on $l(M)$. If $l(M) = 0$, then the assertion is trivially true. If $l(M) = 1$, then $M$ is a simple $R$-module, i.e., an $R$-submodule of $M$ is either $M$ or $\{0\}$, and the lemma is true. Assume that $l(M) > 1$ and $N \neq M, \{0\}$. Then the inequality $l(M) \leqq l(N) + l(M/N)$ holds if the righthand is defined. Let (7) be a maximal chain with $s = l(M)$. Then $l(M_1) = s - 1$ by the minimality of $s$.

If $N \subset M_1$, then $l(N)$ and $l(M_1/N)$ are defined and $l(M_1) = l(N) + l(M_1/N)$ by the assumption of the induction. Since $l(M/N) \leqq l(M/M_1) + l(M_1/N) = 1 + l(M_1/N)$ holds,

we have $s-1 = l(M_1) \geqq I(N) + I(M/N) - 1$, which implies $l(M) \geqq l(N) + l(M/N)$. Hence $l(M) = l(N) + l(M/N)$.

If $N \not\subset M_1$, then set $N_1 = N \cap M_1$. If $N_1 = \{0\}$, then $N \simeq M/M_1$ and $l(N) = 1$ as well as $M/N \simeq M_1$ and $l(M/N) = s-1$. Hence $l(N)+l(M/N) = s$. If $N_1 \neq \{0\}$, then we have $l(M) = l(N_1) + l(M/N_1)$ by the previous part. Since the lemma holds for $N_1 \subset N$ and $N/N_1 \subset M/N_1$ by the assumption of the induction, we have $l(N) = l(N_1) + 1$ and $l(M/N) = l(M/N_1) - 1$. Hence $l(N) + l(M/N) = l(N_1) + l(M/N_1) = l(M)$. QED

For the maximal chain (7), $l(M_{i-1}/M_i) = 1$ for $i = 1, 2, \ldots, s$. Hence, this lemma implies $l(M) = s$, i.e., it does not depend on the choice of the maximal chain.

# 13 Integral extensions of rings

Let $A$ be a subring of a commutative ring $B$. An element $x$ in $B$ is said to be *integral* over $A$, if there exist an integer $n$ and elements $a_1, a_2, \ldots, a_n \in A$ with

$$x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n = 0 \, .$$

$B$ is said to be integral over $A$ if all elements in $B$ are integral over $A$. An integral domain $A$ is said to be *integrally closed* if, for the quotient field $K$ of $A$, no element of $K \setminus A$ is integral over $A$.

The last assertion of Theorem 12.4 is a consequence of the following theorems.

**Theorem 13.1 (Going up theorem)** *Let $B$ be integral over $A$, and let $P_0 \subset P_1 \subset \cdots \subset P_{d-1} \subset P_d$ be a sequence of distinct prime ideals of $A$. Then there exists a sequence $P'_0 \subset P'_1 \subset \cdots \subset P'_{d-1} \subset P'_d$ of prime ideals of $B$ such that $P'_i \cap A = P_i$ for all $i$.*

**Theorem 13.2 (Going down theorem)** *Let $B$ be an integral domain integral over an integrally closed subring $A$, and let $P_0 \subset P_1 \subset \cdots \subset P_{d-1} \subset P_d$ be a sequence of distinct prime ideals of $A$. Assume that there exists a prime ideal $P'_d \subset B$ with $P'_d \cap A = P_d$. Then there exists a sequence $P'_0 \subset P'_1 \subset \cdots \subset P'_{d-1} \subset P'_d$ of prime ideals of $B$ such that $P'_i \cap A = P_i$ for all $i$.*

For the proof of this theorem, [ZS, Ch. V, Theorem 6] seems better than [AM, Theorem 5.16].

**Theorem 13.3 (Normalization theorem)** *Let $k$ be a field and $R$ be an integral domain which is finitely generated over $k$. Then there exist a integer $d \geqq 0$ and $x_1, \ldots, x_d \in R$ such that $x_1, \ldots, x_d$ are algebraically independent over $k$ and $R$ is integral over $k[x_1, \ldots, x_d]$. In particular, $d$ is the transcendence degree of $R$ over $k$.*

**Proposition 13.4** *For a polynomial ring $R = k[x_1, \ldots, x_d]$, any maximal ideal $P \subset R$ is generated by $d$ elements and $\dim R_P = d$.*

# 14 Discrete valuation rings

Let $K$ be a field. Non-zero map $v : K \setminus \{0\} \to \mathbf{Z}$ is called a *discrete valuation* if the following conditions are satisfied, where we define $v(0) = \infty$.
(1) $v(xy) = v(x) + v(y)$
(2) $v(x+y) \geqq \min\{v(x), v(y)\}$ (We see later that the equality $v(x+y) = \min\{v(x), v(y)\}$ holds if $v(x) \neq v(y)$.)

If $v$ is a discrete valuation, then $R = \{x \in K \ ; \ v(x) \geqq 0\}$ is an integral domain contained in $K$. We call this integral domain a *discrete valuation ring*. For any $x \in K \setminus \{0\}$, either $x \in R$ or $x^{-1} \in R$ since $v(x) + v(x^{-1}) = v(1) = 0$. In particular, $K$ is the quotient field of $R$.

**Lemma 14.1** *Let $R$ be the discrete valuation ring by $v$. We take $p \in R$ such that $v(p)$ is the positive minimal value. Then any non-zero ideal $I$ of $R$ is written as $(p^n)$ for a non-negative integer $n$.*

Proof Let $v(p) = d$. Let $n \geqq 0$ be the maximal integer such that $nd \leqq v(x)$ for all $x \in I \setminus \{0\}$. Then $v(x/p^n) = v(x) - n \geqq 0$, and we have $x = (x/p^n)p^n \in (p^n)$ for every $x \in I$. On the other hand, if we take $u \in I$ with $nd \leqq v(u) < (n+1)d$, then $0 \leqq v(u/p^n) < d$ and $v(u/p^n) = 0$ by the choice of $p$. Hence the inverse $p^n/u$ is in $R$, and $p^n = (p^n/u)u \in I$. Hence $I = (p^n)$. QED

**Theorem 14.2** *Let $(R, P)$ be a Noetherian local integral domain. Then the following are equivalent.*
(1) *$R$ is a discrete valuation ring.*
(2) *$R$ is integrally closed and* $\dim R = 1$.
(3) *$P$ is a non-zero principal ideal.*

Proof (1) $\Rightarrow$ (2). Let $v$ be a discrete valuation of $K$. We may assume that there exists $p \in R$ with $v(p) = 1$. By Lemma 13.1, every non-zero ideal of $R$ is of the form $(p^n)$ with $n \geqq 0$, and it is not prime if $n > 1$. Of course $(p^0) = R$, and the remaining $(p)$ is the maximal ideal $P$. Hence prime ideals of $R$ are only $P$ and 0. We know $P \supset 0$ is the unique maximal sequence of prime ideals and $\dim A = 1$. Here, if $v(x) = n < v(y) = m$, then $x/p^n$ is invertible and $y/p^n \in (p)$. Hence $(x+y)/p^n$ is invertible since $R$ is a local ring. In particular, since $v((x+y)/p^n) = 0$, we have $v(x+y) = v((x+y)/p^n) + v(p^n) = n = \min\{v(x), v(y)\}$. This implies $v(x+y) = \min\{v(x), v(y)\}$ if $v(x) \neq v(y)$.

We will show that $R$ is integrally closed. If $x \in K \setminus R$, then $v(x) < 0$. Consider a polynomial

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

in $x$ with $a_1, \ldots, a_n \in R$. The valuations of the terms have unique minimum at $v(x^n) = nv(x)$. Hence by (2) of the definition of discrete valuation and the remark above, the valuation of this sum is $nv(x)$. Hence it is not zero, and $R$ is integrally closed.

(2) $\Rightarrow$ (3). $P \neq 0$ since $\dim R = 1$. Let $a \in P$ be a non-zero element. Since $(a)$ is not contained in a prime ideal other than $P$, $(a)$ is a $P$-primary ideal. Hence there exists

$n > 0$ with $P^n \subset (a)$. We take minimal such $n$. Since $P^{n-1} \not\subset (a)$, we take $b \in P^{n-1} \setminus (a)$ and set $y = b/a \in K$. Since $b \notin (a)$, $y$ is not in $R$. Since $bP \subset P^n$, we have $bP \subset (a)$ and $yP \subset R$. If $yP \subset P$, then $P$ is a $R[y]$-module finitely generated as an $R$-module. In this case, $y$ is integral over $R$, which contradicts the assumption that $R$ is integrally closed and $y \notin R$. Hence $yP$ is an ideal of $R$ which is not contained in the unique maximal ideal $P$, and $yP = R$. If we take $p \in P$ with $py = 1$, then $P = p(yP) = pR = (p)$.

(3) $\Rightarrow$ (1). Let $P = (p)$. Note that $U = R \setminus P$ is the set of regular elements of $R$ since $R$ is local. Hence $P^n \setminus P^{n+1} = p^n R \setminus p^n P = p^n U$ for any $n \geqq 0$. Since $\bigcap_{n=0}^{\infty} P^n = 0$, we have $R \setminus \{0\} = \bigcup_{n=0}^{\infty} p^n U$. If $x = p^m u$ and $y = p^n v$ for $m, n \in \mathbf{Z}$ and $u, v \in U$, then $x/y = p^{m-n}(u/v)$ with $u/v \in U$. Hence, for the quotient field $K$ of $R$, we have $K \setminus \{0\} = \bigcup_{n \in \mathbf{Z}} p^n U$. We define the valuation $v : K \setminus \{0\} \to \mathbf{Z}$ by $v(x) = n$ if $x = p^n u$ for $n \in \mathbf{Z}$ and $u \in U$. Then, we know that $R$ is a discrete valuation ring with respect to this valuation. QED

## Exercises

Give proofs or counterexamples to the following statements. $R$ is always a commutative ring.

☐ (1) Let $I$ be an ideal of $R$. Then the radical $\sqrt{I}$ defined by $\sqrt{I} = \{x \in R \, ; \, x^n \in I \text{ for an integer } n > 0\}$ is an ideal of $R$.

☐ (2) Let $I$ be an ideal of $R$, and $M$ an $R$-module. Then the natural homomorphism $\phi : M \otimes_R \hat{R} \to \hat{M}$ is an isomorphism, where $\hat{R}$ and $\hat{M}$ are $I$-adic completions.

☐ (3) Let $R$ be the set of polynomials $f(x) \in \mathbf{Q}[x]$ such that $f(0)$ is an integer, where $\mathbf{Q}$ is the field of rational numbers. Then $R$ is a noetherian ring.

☐ (4) If $P$ is a finitely generated projective $R$-module, then $P$ is $R$-flat.

☐ (5) Let $M = M_0 \supset M_1 \supset M_2 \supset \cdots$ be a filtration of an $R$-module $M$. Then the natural $R$-homomorphism $\phi : M \to \hat{M} = \varprojlim M/M_i$ is an injection if and only if $\bigcap_{i=0}^{\infty} M_i = 0$.

☐ (6) If $N$ is a flat $R$-module and $M$ is an $R$-module, then $\mathrm{Tor}_n^R(M, N) = 0$ for every $n > 0$.

☐ (7) For ideals $I, J$ of $R$, the ideal $I : J$ is defined to be $\{a \in R \, ; \, aJ \subset I\}$. If $R$ is an integral domain and $b \in R$ is a non-zero element, then $bI : J = b(I : J)$.

☐ (8) If an ideal $I \neq R$ satisfies the condition that, if $uv \in I$ then some power of $u$ or $v$ is in $I$, then $I$ is a primary ideal.

☐ (9) Assume that $R$ is a local ring and $F$ is a free $R$-module of rank $r$ generated by $\{x_1, \ldots, x_n\}$. Then there exists a subset $\{y_1, \ldots, y_r\} \subset \{x_1, \ldots, x_n\}$ which is a basis of $F$.

☐ (10) If $M$ and $N$ are $R$-modules, then $\mathrm{Ext}^1_R(M,N)$ is isomorphic to $\mathrm{Ext}^1_R(N,M)$.

☐ (11) If an element $a \in R$ is contained in every maximal ideal of $R$, then $1+a$ is regular, i.e., there exists $b \in R$ with $(1+a)b = 1$.

☐ (12) If $F$ is a free $R$-module of finite rank, then $F$ is projective.

☐ (13) For ideals $I, J$ of $R$, the ideal $I : J$ is defined to be $\{a \in R \,;\, aJ \subset I\}$. If $Q$ is a primary ideal and $x \in R$ is outside $Q$, then $Q : (x)$ is primary.

☐ (14) If $F$ is a free $R$-module of rank $r$ and generated by $\{x_1, \ldots, x_n\}$, then there exists a subset $\{y_1, \ldots, y_r\} \subset \{x_1, \ldots, x_n\}$ which is a basis of $F$.

☐ (15) If non of $R$ and $R$-algebras $A$, $B$ is a field, then the tensor product $A \otimes_R B$ is not a field.

( 1 ) True: It is enough to show that $x+y \in \sqrt{I}$ for $x, y \in \sqrt{I}$, and $ax \in \sqrt{I}$ for $x \in \sqrt{I}$ and $a \in R$. If $x, y \in \sqrt{I}$, then there exist positive integers $l, m$ such that $x^l, y^m \in I$. Then

$$(x+y)^n = x^n + nx^{n-1}y + \cdots + nxy^{n-1} + y^n$$

is in $I$ for $n = l+m-1$ since the each component ${}_n\mathrm{C}_k x^{n-k}y^k$ is in $I$. Namely, $x^{n-k} = x^{m-1-k}x^l \in I$ if $k \leqq m-1$, and $y^k = y^{k-m}y^m \in I$ if $k \geqq m$. Hence $x+y$ is in $\sqrt{I}$. If $x \in \sqrt{I}$ and $a \in R$, then there exists $l > 0$ with $x^l \in I$. Then $ax$ is in $\sqrt{I}$ since $(ax)^l = a^l x^l$ is in $I$. Hence $\sqrt{I}$ is an ideal of $R$.

( 2 ) False: Let $R = \mathbf{Z}$, $M = \mathbf{Q}$, and $I = (d)$ for an integer $d \geqq 2$. Then $\hat{M} = \varprojlim \mathbf{Q}/d^n\mathbf{Q} = 0$ since $d^n\mathbf{Q} = \mathbf{Q}$ for every $n \geqq 0$. On the other hand, $M \otimes_R \hat{R}$ contains $R \otimes_R \hat{R} = \hat{R} \neq 0$ since $\mathbf{Z} \subset \mathbf{Q}$ and $\hat{R}$ is $R$-flat. Hence, these are not isomorphic.

( 3 ) False: The ideal $(x) = x\mathbf{Q}[x]$ of $\mathbf{Q}[x]$ is contained in $R$ as an ideal. However, this ideal is not finitely generated. Namely, for any finite elements $xu_1(x), \ldots, xu_n(x)$ in $x\mathbf{Q}[x]$, there exists a positive integer $m$ such that the rational numbers $u_1(0), \ldots, u_n(0)$ are in $m^{-1}\mathbf{Z}$. Then for any elements $f_1(x), \ldots, f_n(x)$ in $R$, the coefficient of $x$ of the polynomial $f_1(x)u_1(x) + \cdots + f_n(x)u_n(x)$ is $f_1(0)u_1(0) + \cdots + f_n(0)u_n(0)$, which is in $m^{-1}\mathbf{Z}$ since $f_1(0), \ldots, f_n(0)$ are integers. Hence $(2m)^{-1}x \in x\mathbf{Q}[x]$ is not in the ideal generated by $xu_1(x), \ldots, xu_n(x)$.

( 4 ) True: Since $P$ is a finitely generated projective module, there exists an $R$-module $Q$ such that $F = P \oplus Q$ is a free $R$-module of finite rank. Let $L \to M$ be an injective $R$-homomorphism. Since $F$ is free, it is $R$-flat and $L \otimes_R F \to M \otimes_R F$ is an injection. Since this is the direct sum of $R$-homomorphisms $L \otimes_R P \to M \otimes_R P$ and $L \otimes_R Q \to M \otimes_R Q$, these are also injections. Hence $P$ is $R$-flat.

( 5 ) True: $\phi$ is defined by $\phi(x) = (x_n)$ where $x_n = (x \bmod M_n)$ for every $n$. Assume that $\bigcap_{i=0}^{\infty} M_i$ is 0. Then, if $x \neq 0$, there exists $m$ with $x \notin M_m$, and $\phi(x) \neq 0$ since

$x_m \neq 0$. Hence $\phi$ is an injection. Conversely, if $\bigcap_{i=0}^{\infty} M_i$ is not 0, there exists a non-zero element $x \in M$ in $\bigcap_{i=0}^{\infty} M_i$. Then $\phi(x) = 0$. Hence $\phi$ is not an injection.

( 6 ) True: Since $\mathrm{Tor}_n^R(M,N) = \mathrm{Tor}_n^R(N,M)$, it suffices to show that $\mathrm{Tor}_n^R(N,M) = 0$ for $n > 0$. Let $(P_\bullet, \epsilon)$ be a projective resolution of $M$. Then $\mathrm{Tor}_n^R(N,M)$ is the homology group $\mathrm{Ker}(1_N \otimes d_n)/\mathrm{Im}(1_N \otimes d_{n+1})$ of the complex

$$\cdots \xrightarrow{1_N \otimes d_3} N \otimes_R P_2 \xrightarrow{1_N \otimes d_2} N \otimes_R P_1 \xrightarrow{1_N \otimes d_1} N \otimes_R P_0 \xrightarrow{1_N \otimes d_0} 0 \,.$$

Since $N$ is $R$-flat, this complex is exact except at degree 0. Hence $\mathrm{Tor}_n^R(N,M) = 0$ for $n > 0$.

( 7 ) False: Note that $I : J = R$ if $J \subset I$ by definition. Let $R = k[x]$, i.e., a polynomial ring over a field $k$. If $I = R$ and $J = xR$, then both $I : J$ and $xI : J$ are equal to $R$ since $J$ is contained in $I$ and $xI = J$. Since $xI : J = R$ is not equal to $x(I : J) = xR$, $bI : J = b(I : J)$ is not true for $b = x$.

( 8 ) False: Let $R$ be the polynomial ring $k[x,y]$ over a field $k$, and $I$ the ideal $(x^2, xy)$. If $uv$ is in $I$, then since $I$ is contained in the ideal $(x)$, $u$ or $v$ is in the ideal $(x)$. Hence $u^2$ or $v^2$ is in $(x^2) \subset I$. However, although $xy \in I$, $x$ and any power of $y$ are all outside $I$. Hence $I$ is not primary.

( 9 ) True: Let $P$ be the maximal ideal of $R$. Since $F$ is generated by $\{x_1, \ldots, x_n\}$, the quotient $F/PF$ is generated by its image $\{\bar{x}_1, \ldots, \bar{x}_n\}$. Since $F/PF$ is an $R/P$-vector space of dimension $r$, there exists a subset $\{y_1, \ldots, y_r\}$ of $\{x_1, \ldots, x_n\}$ such that $\{\bar{y}_1, \ldots, \bar{y}_r\}$ is a basis of $F/PF$. Then $\{y_1, \ldots, y_r\}$ is a basis of $F$ by Lemma 5.2.

( 10 ) False: Let $R = k[x]$, $M = R$. Then $\mathrm{Ext}_R^i(M,N) = N$ for $i = 0$ and $\mathrm{Ext}_R^i(M,N) = 0$ for $i > 0$ for any $R$-module $N$. When $N = R/(x)$, there exists an exact sequence $R \xrightarrow{m_x} R \to N \to 0$, which is a projective resolution of $N$, where $m_x$ is the multiplication by $x$. Hence $\mathrm{Ext}_R^1(N,M)$ is the cokernel of the homomorphism $\mathrm{Hom}_R(R,M) \xrightarrow{m_x^*} \mathrm{Hom}_R(R,M)$. Since this homomorphism is equal to $R \xrightarrow{m_x} R$, we have $\mathrm{Ext}_R^1(N,M) = R/(x)$. Hence $\mathrm{Ext}_R^1(M,N)$ is not equal to $\mathrm{Ext}_R^1(N,M)$.

( 11 ) True: If $1 + a$ is not regular, the ideal $(1 + a)$ is not equal to $R$, hence is contained in a maximal ideal $P$. Since $a$ is also contained in $P$ by assumption, we have $1 = (1 + a) - a \in P$, which contradicts $P \neq R$. Hence $1 + a$ is regular.

( 12 ) True: We take a basis $\{u_1, \ldots, u_r\}$ of $F$. Let $f : M \to N$ be a surjective $R$-homomorphism. For an $R$-homomorphism $g : F \to N$, there exist $x_1, \ldots, x_r \in M$ such that $f(x_i) = g(u_i)$ for $i = 1, \ldots, r$ since $f$ is surjective. If we define an $R$-homomorphism $h : F \to M$ by $h(u_i) = x_i$ for all $i$, then $g = f \cdot h$. Hence $F$ is projective.

( 13 ) True: In order to prove that $Q : (x)$ is primary, we should show that, if $yz \in Q : (x)$ and $y \notin Q : (x)$ then some power of $z$ is in $Q : (x)$. Since $yz \in Q : (x)$, $(xy)z = x(yz)$ is in $Q$, while $xy$ is not in $Q$ since $y \notin Q : (x)$. Since $Q$ is primary, some power of $z$ is in $Q$, and hence in $Q : (x)$.

( 14 ) False: If $R$ is a polynomial ring $R$, $F = R$ is a free $R$-module of rank one. Although $F$ is generated by $\{x, 1-x\}$, neither $\{x\}$ nor $\{1-x\}$ is a basis of $F$ since $x, 1-x$ are not regular.

( 15 ) False: If $R = k[x, y]$, $A = R/(x)$ and $B = R/(y)$, then these are not field, while $A \otimes_R B = k[x, y]/(x, y) \simeq k$ is a field.

# References


[AM] M. F. Atiyah and I. G. MacDonald, Introduction to commutative algebra, Addison-Wesley, 1969.

[F] P. J. Freyd, Abelian categories, An introduction to the theory of functors, (Originally, Harper and Row, 1964), Reprints in Theory and Applications of Categories, No. 3, 2003. `http://www.tac.mta.ca/tac/`

[H] C. Huneke and Appendix 1 by A. Taylor, Lectures on local cohomology, `http://homepages.math.uic.edu/~bshipley/huneke.pdf`

[L] S. Lang, Algebra, Graduate Texts in Math. 211, Springer, 2002.

[ZS] O. Zariski and P. Samuel, Commutative Algebra II, Nostrand, Princeton, N.J., 1960, (Second printings) Graduate texts in mathematics **29**, Springer, 1979.