LaTeX Note Template

X

November 18, 2025

Github: *https://github.com/Baudelaireee/Notebook*

Contents

1 9/28 Notes for «Calculus on Manifolds» by Spivak

Problem. Can we derive the explicit formula from an equation with several variables? Here are two examples :

$$x^2 + y^2 - 1 = 0 \tag{1}$$

and

$$e^{xy} + \sin y + x^2 - 2 = 0 \tag{2}$$

In the first example, it is clearly that we can express y as a function of x in a certain interval. But in the second example, it seems that we can draw a picture to visualize the implicit curve.

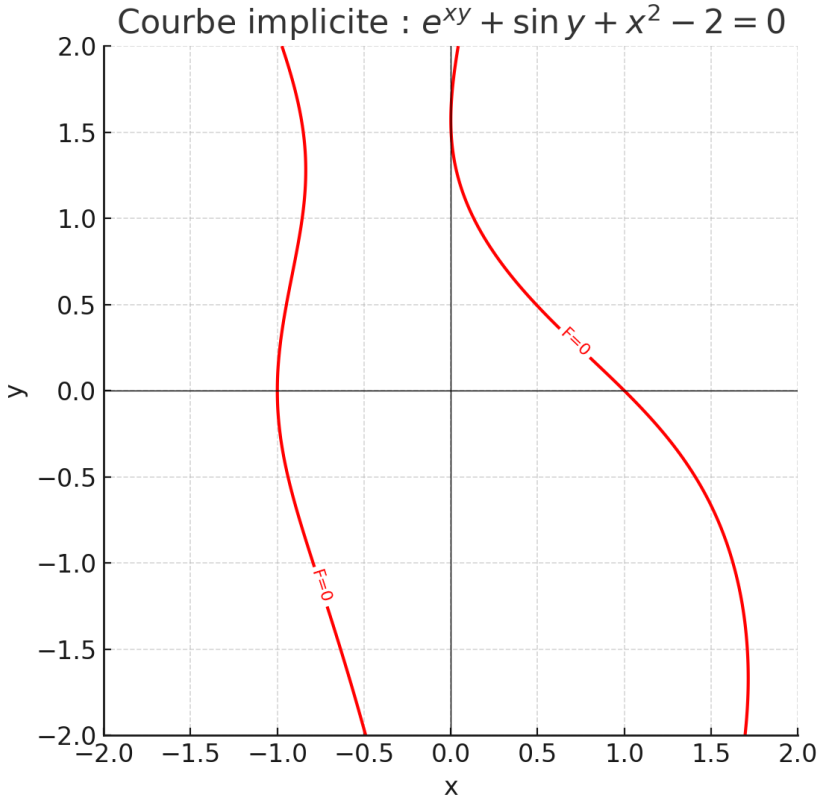


Figure 1: $e^{xy} + \sin y + x^2 - 2 = 0$

The curve here seems very smooth, so for example, at the point $(x_0, 0)$ in the curve we can express y as a function of x in the neighborhood, but it does not mean that we can write the function explicitly.

For thinking about this problem, we assume here we have a multivariable function $F(x, y)$ and we want to solve the equation $F(x, y) = 0$. Like equation (1), we can express it as $F(x, y) = x^2 + y^2 - 1$. Here we assume F is a smooth function, then we can get the total differential of F

$$df = \frac{\partial F}{\partial x}dx + \frac{\partial F}{\partial y}dy$$

If we assume the existence of the implicit function $y = f(x)$, then along the curve

$(G(x) = F(x, f(x)) = 0)$ we can get

$$0 = G'(x) = \frac{\partial F}{\partial x}(x, f(x)) + \frac{\partial F}{\partial y}(x, f(x)) \cdot f'(x)$$

hence we can get the derivative of the function f can be denoted by

$$f'(x) = -\frac{\frac{\partial F}{\partial x}(x, f(x))}{\frac{\partial F}{\partial y}(x, f(x))}$$

let us check some necessary condition here:
1. We try to restrict the function to be vanishing at some point, that means in the voisinage of the point, there exists something like a curve $F(x, y) = 0$ such that we can do the total differential like above, so here we need two conditions: locally, $F(a, b) = 0$ for some point (a, b) and a enough smooth function F.
2. We need to make sure the formula for $f'(x)$ makes sense, so locally $\frac{\partial F}{\partial y}(a, b) \neq 0$.

Actually, under these hypotheses, we can prove the existence of the implicit function $y = f(x)$ in the voisinage of the point (a, b) such that $F(x, f(x)) = 0$, which completes the implicit function theorem in the case of two variables.

Theorem 1.1 (Implicit Function Theorem in $\mathbb{R}^2$)**.** *Let F be a C^1 function defined on an open set containing the point (a, b). Assume that $F(a, b) = 0$ and $\frac{\partial F}{\partial y}(a, b) \neq 0$. Then there exists an open interval I containing a, an open interval J containing b, and a unique C^1 function $f : I \to J$ such that for all $x \in I$, $F(x, f(x)) = 0$. Moreover, the derivative of f is given by*

$$f'(x) = -\frac{\frac{\partial F}{\partial x}(x, f(x))}{\frac{\partial F}{\partial y}(x, f(x))}$$

Proof. here we just give a proof of the existence of the implicit function f, the propoerties have benn proved as above. The idea here is to construct a locally diffeomorphism and then use the inverse function theorem.

We take the map $\Phi(x, y) = (x, F(x, y))$, then we can compute the Jacobian matrix of Φ at the point (a, b)

$$D\Phi(x, y) = \begin{pmatrix} 1 & 0 \\ \frac{\partial F}{\partial x}(x, y) & \frac{\partial F}{\partial y}(x, y) \end{pmatrix}$$

The condition $\frac{\partial F}{\partial y}(a, b) \neq 0$ implies $\det D\Phi(a, b) \neq 0$ the Jacobian matrix is invertible, hence by the inverse function theorem, there exists an open set W containing (a, b) and an open set W' containing $\Phi(a, b) = (a, 0)$ such that $\Phi : W \to W'$ is a C^1 diffeomorphism.

Finally we can construct the implicit function: the inverse $\Phi^{-1}(x, y) = (x, g(x, y))$ for some C^1 smooth function g in W', so we define the implicit function on the domain $D = \{x \in \mathbb{R} | (x, 0) \in W'\}$ (**RMQ:** here D is the intersection of W' and the x-axis, notice that at least $(a, 0) \in W'$, so D is not empty and can be seen as an open interval conatining a)

$$f(x) = g(x, 0)$$

then

$$\Phi(x, f(x)) = \Phi(x, g(x, 0)) = \Phi \circ \Phi^{-1}(x, 0) = (x, 0)$$

by the definition of Φ we can conlude that $F(x, f(x)) = 0$ □

Let us back to the two examples above, if we apply the implicit function theorem here, we can get a clear ODE for the implicit function $y = f(x)$, that is an equivalent view of the implicit function theorem.

Example 1.1. See the equation (2), we want to find the express of y as a function of x, so see the whole equation as a curve $F(x, y) = e^{xy} + \sin y + x^2 - 2$, then by the implicit function theorem, we can conclude a new realtionship between x and y:

$$y' = f'(x) = -\frac{F_x(x, y)}{F_y(x, y)} = -\frac{ye^{xy} + 2x}{xe^{xy} + \cos y}$$

so finding the explicit formula of y is equivalent to solving above ODE to get a explicit solution. The information here is given by the differentail structure of the curve, and notice that the ODE conatins the original information about the curve. However, sometimes we can find the explicit formula of the implicit function, for example, in equation (1), we can express y as a function of x explicitly:

$$y = \pm\sqrt{1 - x^2}$$

and the corresponding ODE here is

$$y' = -\frac{x}{y}$$

It's a separable ODE, we can solve it easily to get the explicit formula of the $y = f(x)$.

2 CA: Some examples and technics

Example 2.1. We consider two algebraic number fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{5})$. and we can study the algebraic intger ring in two fields, then we can find that

$$K = \mathbb{Q}(\sqrt{2}), \qquad \mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$$

and

$$K = \mathbb{Q}(\sqrt{5}), \qquad \mathcal{O}_K = \mathbb{Z}[\frac{1 + \sqrt{5}}{2}]$$

here $X^2 + X + 1$ gives a monic polynomial with integer coefficients such that $\frac{1+\sqrt{5}}{2}$ is a root, that shows that $\frac{1+\sqrt{5}}{2}$ is an algebraic integer, so $\mathbb{Z}[\sqrt{5}] \subsetneq \mathcal{O}_K$.

It's a classic example about ring of algebraic integers, we can say more about quadratic fields

Theorem 2.1. *Let d be an integer without square factors, and let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field. Then the ring of integers $\mathcal{O}_K$ is given by*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2, 3 \mod 4, \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & \text{if } d \equiv 1 \mod 4. \end{cases}$$

Proof. One proof elementary is to use p-adic valuation, here is the outline:

- Prove the **main lemma**: $a + b\sqrt{d}$ is an algebraic integer if and only if $2a \in \mathbb{Z}$ and $a^2 - db^2 \in \mathbb{Z}$.
- Verify that if $a + b\sqrt{d}$ is an algebraic integer, then $v_p(a) \geq 0$ and $v_p(b) \geq 0$ for any odd prime p. (Notice that here is not sufficent to say $a, b \in \mathbb{Z}$)
- Consider the case of 2-adic valuation we can get the condition $v_2(a) \geq -1$ and $v_2(b) \geq -1$.
- Prove that $v_2(a) = -1$ and $v_2(b) = -1$ if and only if $d \equiv 1 \mod 4$, otherwise $v_2(a) \geq 0$ and $v_2(b) \geq 0$, then we can conclude the result.

□

Notice that it is not so easy to prove the similar result for cubic fields or higher degree fields, the concept of **integral basis** is useful here.

operatio of ideals: a useful techincs to compute the isomorphism.

Proposition 2.2. *Let M be a A-module, I be an ideal of A and N be a submodule of M, then we have the isomorphism:*

$$I(M/N) \cong (IM + N)/N$$

In particular, when $M = A$ and $N = J$ is a ideal, then we have

$$I(A/J) \cong (I + J)/J$$

Proof. we consider the natural map $\pi : M \to M/N$. We can verify that $I(M/N)$ is a submodule of M/N, then by correspondence theorem, there exists a submodule in M:

$$\begin{aligned} \pi^{-1}(I(M/N)) &= \pi^{-1}\{\sum_{\text{finite}} a_k \cdot (m_k + N) \mid a_k \in I, m_k \in M\} \\ &= \pi^{-1}\{\sum_{\text{finite}} a_k m_k + N \mid a_k \in I, m_k \in M\} \\ &= IM + N \end{aligned}$$

Then again by the image of natural map we can match

$$I(M/N) = (IM + N)/N$$

□

Proposition 2.3. *If $I \subset R$ as a ideal, $a \in I$ and $b \notin I$, then*

$$a + b \notin I$$

Proof. If $a + b \in I$, then $b = (a + b) - a \in I$, which is a contradiction. □

3 Infinite products

The form of infinite products is important in complex analysis to study the poles and zeros of functions, here is the definition:

Definition 3.1. Let $(a_n)_{n=1}^{\infty}$ be a sequence of complex numbers. The infinite product $\prod_{n=1}^{\infty} a_n$ is said to converge if there exists $N \in \mathbb{N}$ such that:
(1) $a_n \neq 0$ for all $n \geq N$
(2) the sequence of partial products$(\prod_{k=n}^{N} a_k)_{n \geq N}$ converges to a non-zero limit as $n \to \infty$.
If the limit is zero, we say the product **diverges to zero**. If the limit does not exist, we say the product diverges.

we avoid the case that some terms are zero, because it will make the product zero, which is not interesting; and we notice that if the sequence (a_n) converges to zero, then the product will tend to zero trivally, so we need to avoid this case too. Anyway, the definition here is delicated enough to avoid any trival case.

Proposition 3.1 (The properties of convergence)**.** *Let $(a_n)_{n=1}^{\infty}$ be a sequence of complex numbers such that the infinite product $\prod_{n=1}^{\infty} a_n$ converges, then:*
(1) $\lim_{n\to\infty} a_n = 1$
(2-LOG) If $a_n \in \mathbb{C} - \mathbb{R}_-$ for sufficent large n, then we have equivalent conidtion for the convergence of the product: the series $\sum_{n=1}^{\infty} \operatorname{Log} a_n$ converges.
(3-CVA) If $\sum_{n\in\mathbb{N}} |a_n| < \infty$, then the product $\prod_{n=1}^{\infty} 1 + a_n$ converges or diverges to zero.

Proof. (1) is immediate form $a_n = (\prod_{k=1}^{n} a_k / \prod_{k=1}^{n-1} a_k)$ for $n \geq 2$.
(2) By the convergence of (1), for sufficent large n, a_n stays near 1, hence we can choose the principal branch such that for sufficent large N

$$\operatorname{Log} \prod_{n \geq N} a_n = \sum_{n \geq N} \operatorname{Log} a_n$$

(3) If $\sum_{n\in\mathbb{N}} |a_n| < \infty$, so a_n converges to zero so we can expend

$$\operatorname{Log}(1 + a_n) = a_n - \frac{a_n^2}{2} + o(a_n^3)$$

Then by (2), the series $\sum_{n\in\mathbb{N}} \operatorname{Log}(1 + a_n)$ converges absolutely, hence the product converges or diverges to zero.

□

With the basic technics, we can study the products of fuctions, that's the core to construct some important functions like gamma function.

Definition 3.1 (Convergence of product of functions)**.**
Let $(f_n)_{n\in\mathbb{N}}$ be a sequence of continous function on a open set U
- The product $\prod_{n\in\mathbb{N}} f_n$ converges pointwise to F on U if for each $z \in U$, the product $\prod_{n\in\mathbb{N}} f_n(z)$ converges to $F(z)$.
- The product $\prod_{n\in\mathbb{N}} f_n$ converges uniformly to F on U if there exists $N \in \mathbb{N}$ such that for

all $n \geq N$, f_n does not vanish on U and the sequence of partial products $(\prod_{k=n}^{N} f_k)_{n\geq N}$ converges uniformly to F on U.

Here is the definition following above definition, the zero of the functions in sequence may cause some problems, so there are some difficult in definition. Another clear definition is from **Henri Cartan's book**, here we give as a lemma:

Lemma 3.2. *In above definition, let $K \subset U$ as a subset, then the product $\prod_{n\in\mathbb{N}} f_n$ converges uniformly on K if f_n satisfies the following condition:*
(1) $(f_n)_{n\in\mathbb{N}}$ coverges uniformly to 1 on K.
(2) The series $\sum_{n\in\mathbb{N}} \operatorname{Log} f_n$ converges normally on K.

Proof. By (1), for sufficent large N, we have $|f_N - 1| < 1/2$, so for all $n \geq N$, $\operatorname{Log} f_n$ is well defined and f_n does not vanish on K. so for any $z \in K$

$$\operatorname{Log} \prod_{k=n}^{N} |f_k| = \sum_{k=n}^{N} |\operatorname{Log} f_k| \leq \sum_{k=n}^{N} \|\operatorname{Log} f_k\|_K$$

it implies that the sequence of partial products converges uniformlly on K by weierstrass M-test. □

Infinite products is a strong tool to construct function with certain zeros, for example we can constryct a function with zeros at all integers like following:

$$z \prod_{n\geq 1} (1 - \frac{z^2}{n^2})$$

It is not difficult to verify that he product converges locally uniformlly to a holomorphic function, and one holomorphic function sharing the propoerties is **sine function**, actually we can prove that they are equally up to a constant factor, which is a famous result called **Euler's sine product formula**. With the following proposition, we can completely prove the formula:

$$\sin(\pi z) = \pi z \prod_{n\geq 1} (1 - \frac{z^2}{n^2})$$

The proof can be found in [Stein 2, page 142].

Proposition 3.3. *Let $(f_n)_{n\in\mathbb{N}}$ be a sequence of holomorphic functions on an open set $\Omega \subset \mathbb{C}$, and suppose that the product $\prod_{n\in\mathbb{N}} f_n$ converges Ω to a function f locally uniformly, then*
(1) f is holomorphic on Ω
(2) The zeros and multiplicities of f follows from the sequence:

$$Z(f) = \bigcup_{n\in\mathbb{N}} Z(f_n) \qquad m_f(z) = \sum_{n\in\mathbb{N}} m_{f_n}(z)$$

(3) If f_n does not vanish on Ω for any n, then the series of meromorphic functions $\sum_{n\in\mathbb{N}} f_n'/f_n$ converges locally uniformly on $\Omega - Z(f)$ to f'/f.

Proof. It's the result of locally uniformlly convergence on the inifinite product, notice that the proof of (3) is referred to a idenetity:

$$\frac{(\prod_{k=1}^{n} f_k)'}{\prod_{k=1}^{n} f_k} = \sum_{k=1}^{n} \frac{f_k'}{f_k}$$

which can be proved by induction. Another point is that the proof of (2) needs that the multiplicities of zeros are finite, i.e. for any $a \in \Omega$ we have

$$\#\{n \in \mathbb{N} | f_n(a) = 0\} < \infty$$

Which is ensured by the definition of convergence of infinite product. □

There are two natural question arsing from Euler's formula, one is that if we find another entire function with zeros at all integers, whether the function is same with sine function up to coefficients or anything else? The other is that if there exists a general method to construct entire function with given finite or infinite zeros? The answer is from **Weierstrass's** construction.

Firstly, the zeros of holomorphic is isolated or discrete, so we the given zeros can not have any limit point in $\mathbb{C}$, hence the problem is limited to discrete set of points. **For finite zeros, we can use the fundamental theorem of algebra to construct a polynomial with given zeros**, so the problem is limited to infinite zeros. By Borel-Weierstrass theorem, we can deuduce that the set of zeros must be unbounded.

Another point about zero is that the multiplicity of zeros must be finite. Suppose that f is an non-zero entire function, then by propoerty of analytic function, f can be expended at any point z_0 as a Taylor series

$$f(z) = \sum_{n=0}^{\infty} \frac{f^{(n)}(z_0)}{n!}(z - z_0)^n$$

If z_0 is a zero with inifinite multiplicity, then $f^{(n)}(z_0) = 0$ for all $n \in \mathbb{N}$, hence $f \equiv 0$ in the neighborhood of z_0, which implies $f \equiv 0$ in $\mathbb{C}$ by analytic countiuation, it is absurd. Together with the above statement, if $(a_n)_{n\in\mathbb{N}}$ is the sequence of zeros, then the zeros must satisfy $\lim_{n\to\infty} |a_n| = \infty$.

With the basic analysis of zeros, now we can consrtuct the entire function by given zeros. Notice that we can not simply combine the zeros together by linear terms

$$\prod_{n\in\mathbb{N}} (z - a_n)$$

The product diverges for infinite unbounded zeros, so we can copy the idea of Euler's formula, i.e.

$$\prod_{n\in\mathbb{N}} (1 - \frac{z}{a_n})$$

However, we can not ensure the convergence of the product, for example we take zeros as all positive integers. To ensure the convergence we need to add some extra terms in each factor, that is called **Weierstrass's canonical factors**.

Lemma 3.4. *We define the weierstrass's canonical factor of the degree p as*

$$E_p(z) := \begin{cases} (1-z) & p = 0 \\ (1-z)e^{(z+\frac{z^2}{2}+\cdots+\frac{z^p}{p})} & p \in \mathbb{N} \end{cases}$$

then the factor has the following propoerties:
(1) It is an entire function with a simple zero at $z = 1$ and no other zeros.
(2) It is a function of finite order $p + 1$.
(3) For $|z| \leq r < 1$, we have the estimate

$$|E_p(z) - 1| \leq C_r|z|^{p+1}$$

for some constant $C_r > 0$. That means the larger the p is, the convergence of $E_p(z)$ to 1 is faster.

Proof. (1) and (2) is clear, we prove (3).

$$\begin{aligned} \log(E_p(z)) &= \log(1-z) + z + \frac{z^2}{2} + \cdots + \frac{z^p}{p} \\ &= -\sum_{n=1}^{\infty} \frac{z^n}{n} + (z + \frac{z^2}{2} + \cdots + \frac{z^p}{p}) \\ &= -\sum_{n=p+1}^{\infty} \frac{z^n}{n} = O(|z|^{p+1}) \end{aligned}$$

the expansion here is ensured by $|z| < 1$, hence

$$E_p(z) = \exp(\log E_p(z)) = 1 + O(|z|^{p+1})$$

by expansion of expoential function $e^z = 1 + z + o(z^2)$, so we can conlude the result. □

So we can response the original question by collecting the above ideas:

Theorem 3.5 (Weierstrass's Factorization Theorem)**.**
Let $(a_n)_{n\in\mathbb{N}}$ be a sequence of complex numbers such that $\lim_{n\to\infty} |a_n| = \infty$, and we make convention that $E_n(\frac{z}{0}) := z$, then the infinite product

$$f(z) = \prod_{n=1}^{\infty} E_n(\frac{z}{a_n})$$

converges locally uniformly in $\mathbb{C}$ to an entire function f whose zeros are precisely the points a_n, with multiplicities by counting. Moreover, if g is any other entire function with the same zeros and multiplicities, then there exists an entire function h such that

$$g(z) = f(z)e^{h(z)}$$

for all $z \in \mathbb{C}$.

Another better theorem is given by **Hadamard**, it shows the growth of the entire function will influence the construction of the function by given zeros.

Theorem 3.6 (Hadamard's Factorization Theorem)**.**
Suppose that f is an entire function of finite order ρ with zeros $(a_n)_{n\in\mathbb{N}}$ (counting multiplicities), then there exists a polynomial P of degree at most $k = \lfloor \rho \rfloor$ such that

$$f(z) = e^{P(z)} \prod_{n=1}^{\infty} E_n(\frac{z}{a_n})$$

4 Ideal

Ideal is something like normal subgroups in group theory, it is important to reflect the structure and relationship of rings. Here is the definition:

Definition 4.1. Let R be a commutative ring, a subset $I \subset R$ is called a ideal of R if the following conditions are satisfied:
(1) I is an additive subgroup of R, that is for any $a, b \in I$, we have $a - b \in I$.
(2) For any $r \in R$ and any $a \in I$, we have $ra \in I$ and $ar \in I$.

Remark 4.1. Here is something to add as the properties, proof is not diffcult:

(1) Ideal $I \subset R$ can be seen as an R-submodule of R, roughly speaking, it can be seen as a "vector subspace". (The union of ideals is not necassary an ideal)

(2) An ideal generated by a subset $S \subset R$ is defined by

$$\langle S \rangle := \bigcap_{I \text{ ideal}, S \subset I} I$$

it is the smallest ideal containing S, and we can verify that

$$\langle S \rangle = \{ \sum_{\text{finite}} r_i s_i \mid r_i \in R, s_i \in S \}$$

In particular, a **principal ideal** is an ideal of the form $(a) = \langle \{a\} \rangle$, i.e a ideal generated by a single element (or it is a cyclic R-module).

(3) A useful statement: If a unit $r \in I$, then $I = R$.

(4) The operation of ideal: $IJ \subset I \cap J \subset I \subset \langle I \cup J \rangle$

5 Module

5.1 Generaltisation and Universal Properties

Definition 5.1. *Let R be a ring, an R-module M is an abelian group $(M, +)$ together with an operation of R on M:*

$$\cdot : R \times M \to M$$

satisfying the following axioms for all $r, s \in R$ and $m, n \in M$:
(1) $r \cdot (m + n) = r \cdot m + r \cdot n$
(2) $(r + s) \cdot m = r \cdot m + s \cdot m$
(3) $(rs) \cdot m = r \cdot (s \cdot m)$
(4) $1_R \cdot m = m$

- A R-module induces a natural ring homomorphism

  $$\phi : R \to \mathrm{End}(M), \quad r \mapsto \phi_r$$

  with $\phi_r(m) = r \cdot m$. Here axiom (1) ensures ϕ is well-defined (i.e. ϕ_r is an endomorphism of the group), axiom (2)(3)(4) ensures ϕ is a ring homomorphism.

  Conversely, any ring homomorphism $\phi : R \to \mathrm{End}(M)$ induces a R-module structure on M by defining

  $$r \cdot m := \phi_r(m)$$

  Hence we can conclude a correspondence:

  $$\{R\text{-module structures on } M\} \leftrightarrow \{\text{Ring homomorphisms } R \to \mathrm{End}(M)\}$$

- Similarly we can define the morphism between modules, if M, N are two R-modules, then a group homomorphism $f : M \to N$ is a **R-module homomorphism (or R-linear)** if two condition s are satisfied:
  (1) $f(m_1 + m_2) = f(m_1) + f(m_2)$ for all $m_1, m_2 \in M$
  (2) $f(r \cdot m) = r \cdot f(m)$ for all $r \in R$ and $m \in M$

Example 5.1. Here are some important example of modules:
(1) Any vector space can be seen as a k-module, here k is a field.

(2) Any abelian group can be seen as a $\mathbb{Z}$-module.

(3) Any ideal I of a ring R can be seen as a R-module.

(4) Any $k[x]$-module can be seen as a pair (V, T) where V is a k-vector space and $T : V \to V$ is a linear transformation. The module structure is given by

$$(\sum_{i=0}^{n} a_i x^i) \cdot v := \sum_{i=0}^{n} a_i T^i(v)$$

In the another view, it refers a morphism of polynomial rings:

$$\phi : k[x] \to \mathrm{End}(V), \quad x \mapsto T$$

Another important example is algebra, it always appears in the theory of field extension.

Definition 5.2. *Let R and A be two rings with a ring homomorphism $\varphi : R \to A$, then we say (A, φ) is a R-algebra, and we can define a R-module structure on A by*

$$r \cdot a := \varphi(r)a$$

Remark 5.1. In particular, an R-module is not necessary a R-algebra, because the multiplication in A may not be defined in M. For example, an ideal $I \subset R$ is a R-module, but it is not a R-algebra unless $I = R$.

There are some properties about algebras:

(1) If M is a A-module with (A, φ) a R-algebra, then M is also a R-module. It is clearl by

$$R \longrightarrow A \longrightarrow \mathrm{End}(M)$$

(2) If M and N are two A-modules with (A, φ) a R-algebra, then any A-module homomorphism $f : M \to N$ is also a R-module homomorphism, i.e.

$$\mathrm{Hom}_A(M, N) \subset \mathrm{Hom}_R(M, N)$$

In particular, we can take equality if φ is surjective.

Similar with vector spaces, we can define the submodule annd quotient module as following:

Definition 5.3. *Let M be a R-module, a subset $N \subset M$.*

- *N is called a submodule of M if N is also a R-module with the induced operations from M. Equivalently, N satisfies the following conditions:*
  (1) N is an additive subgroup of M.
  (2) For any $r \in R$ and any $n \in N$, we have $r \cdot n \in N$.

- *Let N be a submodule of M, then there exists a natural quotient group homomorphism $\pi : M \to M/N$, if we add the condition that π is a R-module homomorphism, then we can naturally get the multiplication on M/N by*

  $$r \cdot \bar{m} := r \cdot \pi(m) = \pi(rm) = r\bar{m}$$

  Then M/N is called the quotient module of M by N.

- *the R-module homomorphism $\pi : M \to M/N$ is called the quotient map or **canonical projection**. It induced a correspondence:*

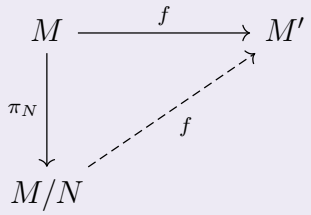
  $$\{\textit{submodules of } M \textit{containing } N\} \leftrightarrow \{\textit{submodules of } M/N\}$$

Now we conlude the isomorphism theorems for modules, the results are similar with groups and vector spaces, so we just give the statements here without proof.

Theorem 5.1 (UPQ-Module)**.**
Let $f : M \to M'$ be a R-module homomorphism, and N be a submodule of M such that $N \subset \ker f$, then there exists a unique R-module homomorphism

$$\bar{f} : M/N \to f$$

such that the following diagram commutes:



The results of the universal properties are three important isomoprhism for modules:

Theorem 5.2 (Isomorphism Theorems for Modules)**.**
Let M be a R-module, and let N, P be two submodules of M, then:
(1) (First Isomorphism Theorem) If $f : M \to N$ is a R-module homomorphism, then we have the isomorphism:

$$M/\ker f \cong f(M)$$

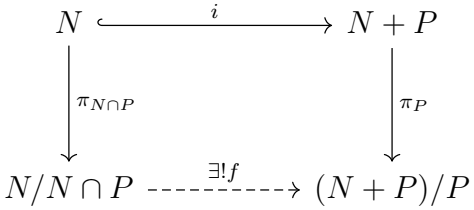
(2) (Second Isomorphism Theorem) We have the isomorphism:

$$(N + P)/P \cong N/(N \cap P)$$

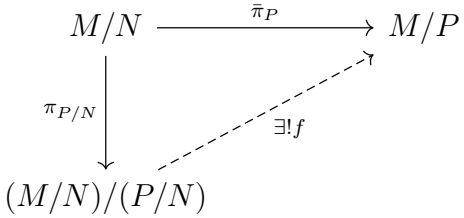
(3) (Third Isomorphism Theorem) If $P \subset N$, then we have the isomorphism:

$$(M/P)/(N/P) \cong M/N$$

Proof. Proof for (1) is directly from UPQ-Module when $N = \ker f$. For (2), we consider diagram:



Here we just need to verify that $\ker(\pi_P \circ i) = N \cap P$ and $pi_P \circ i$ is surjective, then by UPQ-Module we can get the isomorphism. For (3), we consider diagram:



□

where $\bar{\pi}_P$ is induced by the natural quotient map $\pi_P : M \to M/P$. We just need to verify that $\ker \bar{\pi}_P = P/N$ and $\bar{\pi}_P$ is surjective, then by (1) we can get the isomorphism.

5.2 Finite generated module

Like vector spaces, we also hope to find some elemnts to generate the whole module, here is some vacabulary:

Definition 5.4. *Let M be a R-module, let $(m_i)_{i\in I}$ be a family of elements in M, then:*

*(1) The family is **a generate set** of M if any element of M can be written as a **finite** linear combination of elements in the family, i.e. for any $m \in M$, there exists a finite subset $J \subset I$ and $c_j \in R$, $j \in J$, such that*

$$m = \sum_{j\in J} c_j m_j$$

*(2) The family is **linearly independent** if for any finite subset $J \subset I$ and $c_j \in R$, $j \in J$, the condition $\sum_{j\in J} c_j m_j = 0$ implies that $c_j = 0$ for all $j \in J$.*

*(3) The family is a **basis** of M if it is a generate set and linearly independent.*

*(4) The module M is called **finitely generated** if there exists a finite generate set of M.*

*(5) The module M is called **free** if it has a basis.*

Remark 5.2. Remember that "a free module is a lucky accident", not all modules are free, and even finitely generatd modules are not necessarily free. Here are some examples for clarification:

(a) Any vector space is a free module, but the proof is not trival, it is something about **Zorn's lemma (Axiom of choice.)**. In particular, we have implication

$$\{ \begin{array}{c}\text{finite generated}\\ k\text{-module}\end{array} \} = \{\text{finite dimensional vector space}\} \implies \text{free}$$

(b) An example that a finitely generated module is not free: let $R = \mathbb{Z}$, $M = \mathbb{Z}/2\mathbb{Z}$ as a $\mathbb{Z}$-module, then M is finitely generated by $\{1 + 2\mathbb{Z}\}$, but it is not free since it is not a base by

$$2 \cdot \bar{1} = \bar{2} = \bar{0}$$

here 2 is non-zero.

(c) In a R-module M, we define the **torsion** to be the element $m \in M$ such that

$$r \cdot m = 0 \quad \text{for some } r \in R - \{0\}$$

The torsion elements will obstruct the module to be free, in example (2) we can see that $\bar{1}$ is a torsion element.

(d) An submodule of a finitely generated module is not necessarily finitely generated, for example, let $R = k[x_1, x_2, \cdots]$ be the polynomial ring of infinite variables over a field k, then R is a finitely generated module over itself, but the ideal $I = \langle x_1, x_2, \cdots \rangle$ is not finitely generated.

Some basic properties about finitely generated modules is useful, because we always need to claim whether a module is finitely generated or not.

Proposition 5.3. *Let M be a R-module, and $N \subset M$ be a submodule:*
(1) If M is finitely generated, then quotient module M/N is also finitely generated.

(2) If N and M/N are finitely generated, then M is also finitely generated.

(3) If M_i is finitely generated R-modules for all $i = 1, 2, \cdots, n$, then the product module $\prod_{i=1}^{n} M_i$ is also finitely generated.

(4) Let M be A-module, and (A, ϕ) be a R-algebra, then if M is finitely generated as a R-module, then M is also finitely generated as a A-module.

Proof. (1) Let $(m_1, m_2, \cdots, m_n)$ be a finite generate set of M, then we claim that $(\bar{m_1}, \bar{m_2}, \cdots, \bar{m_n})$ is a finite generate set of M/N. For any $\bar{m} \in M/N$, there exists $c_i \in R$ such that

$$m = \sum_{i=1}^{n} c_i m_i$$

hence

$$\bar{m} = \sum_{i=1}^{n} c_i \bar{m_i}$$

it implies the result.
(2) Let $(n_1, n_2, \cdots, n_k)$ be a finite generate set of N, and let $(\bar{m_1}, \bar{m_2}, \cdots, \bar{m_l})$ be a finite generate set of M/N. We claim that $(n_1, n_2, \cdots, n_k, m_1, m_2, \cdots, m_l)$ is a finite generate set of M. For any $m \in M$, there exists $c_j \in R$ such that

$$\bar{m} = \sum_{j=1}^{l} c_j \bar{m_j}$$

hence

$$m - \sum_{j=1}^{l} c_j m_j \in N$$

so there exists $d_i \in R$ such that

$$m - \sum_{j=1}^{l} c_j m_j = \sum_{i=1}^{k} d_i n_i$$

it implies that

$$m = \sum_{i=1}^{k} d_i n_i + \sum_{j=1}^{l} c_j m_j$$

hence the result.

(3) Let $(m_{i1}, m_{i2}, \cdots, m_{in_i})$ be a finite generate set of M_i for each $i = 1, 2, \cdots, r$, then the finite set (order is $n_1 + \cdots + n_r$)

$$\{(0, \cdots, 0, m_{ij}, 0, \cdots, 0) \mid i = 1, 2, \cdots, r; j = 1, 2, \cdots, n_i\}$$

is a generate set of $\prod_{i=1}^{r} M_i$.

(4) Let $(m_1, m_2, \cdots, m_n)$ be a finite generate set of M as a R-module, then for any $m \in M$, there exists $c_i \in R$ such that

$$m = \sum_{i=1}^{n} c_i \cdot m_i = \sum_{i=1}^{n} \phi(c_i) m_i$$

□

The statement (2) can be generalized to a exact sequence as following:

Corollary 5.4. *Let $0 \to N \to M \to P \to 0$ be an exact sequence of R-modules, then*

$$\{N, P\} \textit{ finitely generated} \implies M \textit{ finitely generated}$$

However, we can not say more about the implication because the submodule of a finitely generated module is not necessarily finitely generated. We should make some restriction on the module such that some good properties can be ensured, that is called **Noetherian module**.

Definition 5.5. *A R-module M is called a **Noetherian module** if it satisfies the following equivalent conditions:*
(1) Any submodule of M is finitely generated.
(2) Any ascending chain of submodules of M

$$N_1 \subset N_2 \subset N_3 \subset \cdots$$

stabilizes, i.e. there exists $k \in \mathbb{N}$ such that for all $n \geq k$, $N_n = N_k$.
(3) Any non-empty set of submodules of M has a maximal element with respect to inclusion.

The equivalent of the conditions need a proof here for clarification.

Proof. □

Immediate with the definition, we can get some properties of Noetherian modules like proposition 5.3:

- Let $0 \to N \to M \to P \to 0$ be an exact sequence of R-modules, then

  $$\{N, P\} \text{ Noetherian} \iff M \text{ Noetherian}$$

  in particular, let N be a submodule of M, then

  $$M \text{ Noetherian} \iff \{N, M/N\} \text{ Noetherian}$$

- Let M_i be Noetherian R-modules for all $i = 1, 2, \cdots, n$, then the product module $\prod_{i=1}^{n} M_i$ is also Noetherian.

- Let M be a A-module, and (A, ϕ) be a R-algebra, then M is Noetherian as a A-module if it is Noetherian as a R-module.

Noetherian condition is very important in commutative algebra, because it ensures that many bad situations will not happen. For example, in a locally ring (R, m), we only have one chain of ideals

$$\cdots I_2 \subset I_1 \subset m$$

so which ensures the maximal ideal m is finitely generated, and other ideals will be generated by part of the generators of m.

Definition 5.1. Let R be a commutative ring, R is called a **Noetherian ring** if it is Noetherian as a R-module, i.e. it satisfies one of the following equivalent conditions:
(1) Any ideal of R is finitely generated.
(2) A.C.C condition on ideals.
(3) Any non-empty set of ideals has a maximal element with respect to inclusion.

Remark 5.3. Many rings we meet are Noetherian rings:

(a) Any field k is a Noetherian ring, because the only ideals are $\{0\}$ and k.

(b) Any principal ideal domain (PID) is a Noetherian ring, because any ideal is generated by a single element.

(c) The extension of $\mathbb{Z}$ is a Noetherian ring, for example $\mathbb{Z}[\sqrt{2}]$ and $\mathbb{Z}[i]$. The result can be generalized to the following proposition.

Proposition 5.5. *Let R be a Noetherian ring, and M is a finitely generated R-algebra, then M is also a Noetherian ring.*

Proof. Let $\{m_1, \ldots, m_n\}$ be a set of generators of M as a R-module, then define $R^n := \prod_{i=1}^n R$ to be the product R-module. It is clear that R^n is a Noetherian module since R is a Noetherian module as a R-module, then we can define a natural surjection of R-modules by

$$\varphi : R^n \to M, \quad (a_1, ..., a_n) \mapsto \sum_{i=1}^{n} a_i m_i$$

It is actually a R-module homomorphism, so by the first isomorphism can conclude that $A^n/\ker\varphi \cong M$, then the quotient module of the Noetherian module R^n is also Noetherian, hence M is a Noetherian ring. □

The idea of the proof is important, In the proof we try to construct a module isomorphic to M, so we define a natural object R^n and a natural morphism φ to M, we can find that the propoerty of R^n is so nice that we can transfer the property to M by the isomorphism theorem, i.e. R^n is a free object.

The statement without the finiteness condition is not correct, for example we consider rational number $\mathbb{Q}$, it is not finitely generated as a $\mathbb{Z}$-module, and it is not a noetheriam ring since we can find a chain of ideals:

$$\mathbb{Z} \subset \frac{1}{2}\mathbb{Z} \subset \cdots \subset \frac{1}{2^n}\mathbb{Z} \subset \cdots$$

it will not stop, so $\mathbb{Q}$ is not a Noetherian ring.

5.3 direct sum and product, free module

With the basic knowledge of modules, we can define the the category of modules

$$\mathbf{Mod_R} \;\Big|\; \begin{array}{l}\text{objects: } R\text{-modules}\\ \text{morphisms: } R\text{-module homomorphisms}\end{array}$$

We define the product of modules as following:

Definition 5.6. *Let $(M_i)_{i\in I}$ be a family of R-modules, then the* ***product module*** *is defined by*

$$\prod_{i\in I} M_i := \{(m_i)_{i\in I} \mid m_i \in M_i\}$$

with the operations defined by

$$(m_i)_{i\in I} + (n_i)_{i\in I} := (m_i + n_i)_{i\in I}$$

and

$$r \cdot (m_i)_{i\in I} := (r \cdot m_i)_{i\in I}$$

for any $r \in R$.

There exists a natural projection (a R-module homomorphism)

$$\pi : \prod_{i\in I} M_i \to M_i, \quad \pi((m_i)_{i\in I}) = m_j \text{ for some fixed } j \in I$$

We can conclude that the product of modules satisfies the universal property of product in category $\mathbf{Mod_R}$.

Proposition 5.6. *Let $f : N \to \prod_{i\in I} M_i$ be a R-module homomorphism, then there exists a unique R-module homomorphism $\tilde{f} : N \to M_i$ such that $\pi_i \circ f = \tilde{f}$ for all $i \in I$. Equivalently, we have a natural isomoprhism*

$$\mathrm{Hom}_R(N, \prod_{i\in I} M_i) \cong \prod_{i\in I} \mathrm{Hom}_R(N, M_i)$$

Proof. □

Moreover, we can define the dual sturcture of product, that is the direct sum of modules.

Definition 5.7. *Let $(M_i)_{i\in I}$ be a family of R-modules, then the* ***direct sum module*** *is defined by*

$$\bigoplus_{i\in I} M_i := \{(m_i)_{i\in I} \mid m_i \in M_i, \text{ and } m_i \neq 0 \text{ for finitely many } i\}$$

with the operations defined by

$$(m_i)_{i\in I} + (n_i)_{i\in I} := (m_i + n_i)_{i\in I}$$

and

$$r \cdot (m_i)_{i\in I} := (r \cdot m_i)_{i\in I}$$

for any $r \in R$.

Remark 5.4.

(1) $\bigoplus_{i\in I} M_i$ is a submodule of $\prod_{i\in I} M_i$. In particular, if the index set is finite, then they are same.

(2) There exists a projection (a R-module homomorphism)

$$\pi : \bigoplus_{i\in I} M_i \to M_i, \quad \pi((m_i)_{i\in I}) = m_j \text{ for some fixed } j \in I$$

However, the projection is not natural in general, because it does not satisfy the universal property of product. For example we consider $I = \mathbb{N}$ and $M_i = M = \mathbb{Z}$, if we decide the application in component by $f_i : \mathbb{Z} \to \mathbb{Z}, \quad z \mapsto z$, then by universal property we can get a application f such that $\pi_i \circ f = f_i$ for all i. But f is not well-defined in direct sum since the image of $1 \in \mathbb{Z}$ is $(1, 1, 1, \cdots)$ which is not in $\bigoplus_{i\in I} M_i$.

(3) There exists a natural injection (a R-module homomorphism)

$$\iota : M_j \to \bigoplus_{i\in I} M_i, \quad i(m) = (0, \cdots, 0, m, 0, \cdots) \text{ for some fixed } j \in I$$

We can conclude that the direct sum of modules satisfies the universal property of **co-product** in category $\mathbf{Mod_R}$.

Proposition 5.7. *Let $f_i : M_i \to N$ be a R-module homomorphism for all $i \in I$, then there exists a unique R-module homomorphism $\tilde{f} : \bigoplus_{i\in I} M_i \to N$ such that $\tilde{f} \circ \iota_i = f_i$ for all $i \in I$. Equivalently, we have a natural isomoprhism*

$$\mathrm{Hom}_R(\bigoplus_{i\in I} M_i, N) \cong \prod_{i\in I} \mathrm{Hom}_R(M_i, N)$$

Proof. We can define $\tilde{f}$ by

$$\tilde{f}((m_i)_{i\in I}) = \sum_{i\in I} f_i(m_i)$$

for all $(m_i)_{i\in I} \in \bigoplus_{i\in I} M_i$. It is easy to see that $\tilde{f}$ is well-defined (direct sum supports on finitely many non-zero components) and R-linear. Moreover, we have

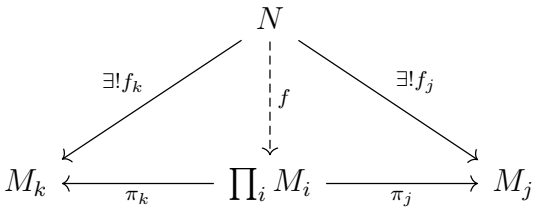
$$\tilde{f} \circ \iota_i(m) = \tilde{f}((0, \cdots, 0, m, 0, \cdots)) = f_i(m)$$

for all $m \in M_i$, which shows $\tilde{f}$ is a desired homomorphism. For the uniqueness, if there exists another solution f, then $(\tilde{f} - f) \circ \iota_i = 0$ for each $i \in I$, hence for any $(m_i)_{i\in I} \in \bigoplus_{i\in I} M_i$, we have

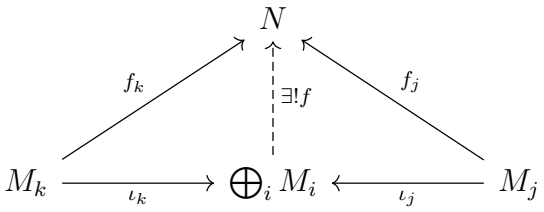
$$(\tilde{f} - f)((m_i)_{i\in I}) = (\tilde{f} - f)(\sum_{i\in I} \iota_i(m_i)) = \sum_{i\in I} (\tilde{f} - f) \circ \iota_i(m_i) = 0$$

it implies $\tilde{f} = f$. □

The properties of direct sum and product can be concludes by the diagram as following:
–product:



and
–direct sum (coproduct):



Sum of modules

Let M be a R-module, and let $E \subset M$ be a subset, then we can define the module generated by E as following:

$$M(E) := \{a_1e_1 + \cdots + a_ne_n \mid n \in \mathbb{N}, a_i \in R, e_i \in M\}$$

in particular, if $E = \{a\}$, then we denote $Ra := M(E)$ to be the **cyclic module** generated by a. Hence $M(E)$ is actually the finite sum of linear combinations of elements in E, so we can define the sum of modules as following:

Definition 5.8. *Let $(M_i)_{i\in I}$ be a family of submodules of a R-module M, then the **sum** of modules is defined as the generated module by the union of the submodules $(M_i)_{i\in I}$, i.e.*

$$\sum_{i\in I} M_i := \{\sum_{i\in J} m_i \mid J \subset I \text{ finite}, m_i \in M_i\}$$

Naturally, we consider the inclusion map $\phi : M_i \hookrightarrow M_i$ for each $i \in I$, then by the universal properties of direct sum, there exists a unique R-module homomorphism

$$\Phi : \bigoplus_{i\in I} M_i \to M, \quad (m_i)_{i\in I} \mapsto \sum_{i\in I} m_i$$

Then we can conclude that the image of Φ is exactly the sum of modules $\sum_{i\in I} M_i$:

$$\sum_{i\in I} M_i = \operatorname{Im}\Phi$$

Definition 5.2. A sum of modules $\sum_{i\in I} M_i$ is called a **(internal) direct sum**, if the homomorphism $\Phi : \bigoplus_{i\in I} M_i \to M$ above is injective. In this case, an

isomoprhism is induced:

$$\sum_{i\in I} M_i \cong \bigoplus_{i\in I} M_i$$

Remark 5.5. Equivalently, the family of submodules $(M_i)_{i\in I}$ is a direct sum if for any finite subset $J \subset I$, the following condition holds:

$$\sum_{i\in J} m_i = 0 \implies m_i = 0 \text{ for all } i \in J, m_i \in M_i$$

In particular, if I is **finite**, then the sum $\sum_{i=1}^{n} M_i$ is a direct sum if and only if

$$M_i \cap \sum_{j\neq i} M_j = \{0\} \quad \text{for all } i = 1, 2, \cdots, n$$

The definition of external direct sum is actually the direct sum defined at first, i.e. let $(M_i)_{i\in I}$ be a family of R-modules, then the direct sum $\bigoplus_{i\in I} M_i$ is the **(external) direct sum** of the submodules. If we choose exactly the subomodules of the same modules, then the external direct sum will be reduced to the internal direct sum.

A question raised here is that: for a module M, if we take a submodule N, can we find another submodule P such that $M = N \oplus P$ such that M has a good decomposition? The answer is not always true, and we define that the submodule N is **direct summand** if such P exists.

Example 5.2.
(1) $\mathbb{Z}$ is a module over itself, and let $2\mathbb{Z}$ be the submodule of $\mathbb{Z}$, then we can find that $2\mathbb{Z}$ is not direct summand. (Reason: any submodule of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for some $n \in \mathbb{N}$, then $2\mathbb{Z} \cap n\mathbb{Z}$=$\{0\}$ iff $n = 0$.)

(2) Any subspace of a **vector space** is direct summand, because any vector space has a basis. If V is a vector space with a basis $\{v_i\}_{i\in I}$, and let $W \subset V$ be a subspace with $W = \text{Span}(\{v_i\}_{i\in J})$ with $J \subset I$, then we can define the complement subspace by $U = \text{Span}(\{v_i\}_{i\in I-J})$.

(3) Simarly with (2), any submodule of a **free module** is direct summand.

An condition can be given here to determine whether a submodule is direct summand or not.

Proposition 5.8. *Let M be a R-module, and let $N \subset M$ be a submodule, then the following conditions are equivalent:*
(1) N is direct summand of M
(2) M/N is isomorphic to a submodule of M.
*(3) There exists a homomorphism (**section**) $s : M/N \to M$ such that $\pi \circ s = \text{id}_{M/N}$, where $\pi : M \to M/N$ is the canonical projection.*
*(4) There exists a homomorphism (**retraction**) $\rho : M \to N$ such that $\rho(x) = x$ for all $x \in N$.*

Proof. (1) $\implies$ (2): Let P be a submodule such that $M = N \oplus P$, then by the second isomorphism theorem we have

$$M/N = (P + M)/N \cong P/(P \cap N) \cong P$$

since direct sum ensures that $P \cap N = \{0\}$.

(2) $\implies$ (3): Let $P \subset M$ be a submodule such that $M/N \cong P$, then the canonical projection $\pi : M \to M/N$ restricts to an isomorphism $\pi|_P : P \to M/N$, hence we can define the section $s : M/N \to M$ by $s^{-1} = (\pi|_P)^{-1}$, and immediately we have $\pi \circ s = \mathrm{id}_{M/N}$.

(3) $\implies$ (1): Let $s : M/N \to M$ be a section, then we can define a homomorphism $\rho : M \to M$ by $\rho = \mathrm{id}_M - s \circ \pi$, then we will show that it is a retraction onto N. For any $m \in M$, we have

$$\pi \circ \rho(m) = \pi(m) - \pi \circ s \circ \pi(m) = \pi(m) - \pi(m) = \bar{0}$$

which implies that $\operatorname{Im} \rho \subset N$. Moreover, for any $x \in N$, we have $\rho(x) = n - s \circ \pi(x) = n - s(\bar{0}) = n$ hence we finish the proof.

(4) $\implies$ (1): Let $\rho : M \to N$ be a retraction, then we will prove that $M = N \oplus \ker \rho$. For any $m \in M$, we have

$$m = m - \rho(m) + \rho(m)$$

where m-$\rho(m) \in \ker \rho$ and $\rho(m) \in N$, hence $M = N + \ker \rho$. Moreover, we can caclulate the intersection to prove the dierectness:

$$N \oplus \ker \rho = \{x \in N | \rho(x) = 0\} = \{0\}$$

□

Remark 5.6. It is a motivation to consider the decomposition of the exact sequence. Let

$$0 \longrightarrow N \xrightarrow{f} M \xrightarrow{g} P \longrightarrow 0$$

be a short exact sequence of R-modules, then the following conditions are equivalent:
(1) There exists an isomorphism $M \cong N \oplus P$.
(2) There exists a section $s : P \to M$ such that $g \circ s = \mathrm{id}_P$.
(3) There exists a retraction $r : M \to N$ such that $r \circ f = \mathrm{id}_N$.
If one of the condition holds, then the s.q.e is called **split**. The proof is similar with the previous proposition, we just need to notice that f is injective and g is surjective in a s.e.q.

Free module

For the convience of notation, we define the product of copies of a commutative ring A as following:

$$A^I := \prod_{i \in I} A \quad \text{and} \quad A^{(I)} := \bigoplus_{i \in I} A$$

for any index set I. In particular, if $I = \{1, 2, \cdots, n\}$ is finite, then $A^I = A^{(I)} = A^n$.

Remark 5.7. Recall that a module is free if it has a basis, i.e. a linearly independent generate set.

(1) $A^{(I)}$ is a free A-module with the standard basis as following:

$$e_k := (\delta_{k,i})_{i\in I} = (\dots, 0, \underset{k\text{-th}}{1}, 0, \dots)$$

for all $(a_i)_{i\in I} \in A^{(I)}$, we have

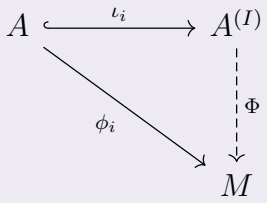
$$(a_i)_{i\in I} = \sum_{i\in I} a_i e_i = \sum_{i\in J} a_i e_i$$

where J is the finite subset of I such that $a_i \neq 0$, so the family is a set of generators. Moreover, if $\sum_{i\in J} a_i e_i = 0$, then $a_i = 0$ for all $i \in J$, so the family is linearly independent.

(2) A^I is not a free A-module if I is infinite. For example, let $I = \mathbb{N}$, then consider the element $(1, 1, 1, \cdots) \in A^I$, it can not be expressed as a finite combination of the standard basis elements above. However, the proof is not trival here, we will do it later.

As we have constructed, $A^{(I)}$ is a **standard model** as a free module, it refers to the following universal property:

Proposition 5.9 (UP-Free module)**.**
Let M be a free A-module with a family of elements $\{m_i\}_{i\in I}$, there exists a unique morphism of A-modules $\Phi : A^{(I)} \to M$ such that $\Phi(e_i) = m_i$ for all $i \in I$.



Equivalently, it induces a natural isomoprhism by $\Phi \mapsto (\phi(e_i))_{i\in I}$

$$\mathrm{Hom}_A(A^{(I)}, M) \cong \prod_{i\in I} M$$

Proof. The proof is similar to the properties of linear map **(the choice of images of basis determines a unique linear map)**. For any $(a_i)_{i\in I} \in A^{(I)}$, we can define

$$\Phi((a_i)_{i\in I}) = \sum_{i\in I} a_i m_i$$

It is easy to verify that Φ is well-defined (direct sum supports on finitely many non-zero components) and A-linear. For the uniqueness, if there exists another morphism $\Psi : A^{(I)} \to M$ such that $\Psi(e_i) = m_i$ for all $i \in I$, then for any $(a_i)_{i\in I} \in A^{(I)}$, we have

$$\Psi((a_i)_{i\in I}) = \Psi(\sum_{i\in I} a_i e_i) = \sum_{i\in I} a_i \Psi(e_i) = \sum_{i\in I} a_i m_i = \Phi((a_i)_{i\in I})$$

hence $\Psi = \Phi$. Hence we can conclude that the two A-linear maps are the same if and only if they have the same images of the basis elements, which implies the natural isomorphism. □

Hence we can generalize the statement of the generating set and basis by the language of morphisms.

Corollary 5.10. *Let M be an A-module, and let I be an index set, then*
(1) M is generated by $\{m_i\}_{i\in I}$ if and only if the morphism $\Phi : A^{(I)} \to M$ defined by $\Phi(e_i) = m_i$ for all $i \in I$ is surjective.
(2) $\{m_i\}_{i\in I}$ is linearly independent set of M if and only if the morphism $\Phi : A^{(I)} \to M$ defined by $\Phi(e_i) = m_i$ for all $i \in I$ is an injective.
(3) $\{m_i\}_{i\in I}$ is a basis of M if and only if the morphism $\Phi : A^{(I)} \to M$ defined by $\Phi(e_i) = m_i$ for all $i \in I$ is an isomorphism.
(4) M is a finitely generated A-module if and only if there exists a surjective morphism $\Phi : A^n \to M$ for some $n \in \mathbb{N}$.

If M is a free A-module and finitely generated, then we can define "dimension" of M by proving the following statement:

Lemma 5.9. *Let M be a free A-module, and let $\{m_1, \cdots, m_n\}$ and $\{n_1, \cdots, n_k\}$ be two bases of M, then $n = k$.*

Proof. □

5.4 Construction of polynomial and series

As we know that a polynomial can be defined as following:

$$\mathbb{Z}[X] = \{a_n x^n + \cdots + a_1 x + a_0 \mid a_i \in \mathbb{Z}\}$$

It is clearly a free $\mathbb{Z}$-module with basis $\{x^n \mid n \in \mathbb{N}\}$, that means $\mathbb{Z}^{(\mathbb{N})} \cong \mathbb{Z}[X]$ as modules. Moreover, we notice that the polynomial is furthermore a ring, so it is a $\mathbb{Z}$-algebra, hence the operations should be extended here to generalize the definition of polynomial ring.

Definition 5.3. Let $A^{(\mathbb{N})}$ be a free $A-module$ with basis $(e_i)_{i\in\mathbb{N}} = (\delta_j, i)_{i\in\mathbb{N}}$, then we can define a multiplication on it by make conservation:

$$e_n \cdot e_m = e_{n+m} \quad \text{for all } n, m \in \mathbb{N}$$

and develop it for any elements

$$(a_i)_{i\in\mathbb{N}} \cdot (b_i)_{i\in\mathbb{N}} = (c_i)_{i\in\mathbb{N}} \quad \text{with} \quad c_i = \sum_{l+k=i} a_l b_k$$

Then $A^{(\mathbb{N})}$ is a A-algebra with ring homomorphism

$$\varphi : A \to A^{(\mathbb{N})}, \quad a \mapsto ae_0 = (a, 0, 0, \ldots)$$

Remark 5.8.

(1) It is easy to verify that the multiplication is well-defined, i.e. the result is still in $A^{(\mathbb{N})}$ since only finitely many a_i and b_i are non-zero.

(2) The multiplicative identity is e_0, since for any $(a_i)_{i\in\mathbb{N}} \in A^{(\mathbb{N})}$, we have

$$e_0 \cdot \sum_{i\in\mathbb{N}} a_i e_i = \sum_{i\in\mathbb{N}} a_i(e_0 \cdot e_i) = \sum_{i\in\mathbb{N}} a_i e_i = (a_i)_{i\in\mathbb{N}}$$

(3) The multiplication is associative, commutative and distributive with respect to addition, which can be verified by direct calculation.

with the work of (1)(2)(3), we can conclude that $A^{(\mathbb{N})}$ is a commutative ring with unity, hence it is a A-algebra.

Then we can construct the polynomial ring as following:

Definition 5.4. Let $A^{(\mathbb{N})}$ be the A-algebra defined above, we identify it as the **polynomial ring** $A[X]$ over A by making the following notation:
- basis: $X^n :\equiv e_n$ for all $n \in \mathbb{N}$ with $1_A = X^0 :\equiv e_0$.
- elements: $f(X) = \sum_{i\in\mathbb{N}} a_i X^i :\equiv (a_i)_{i\in\mathbb{N}}$ for all $(a_i)_{i\in\mathbb{N}} \in A^{(\mathbb{N})}$.
- addition: $\sum_n a_n X^n + \sum_n b_n X^n = \sum_n (a_n + b_n) X^n$.
- multiplication: $(\sum_n a_n X^n) \cdot (\sum_n b_n X^n) = \sum_n c_n X^n$ with $c_n = \sum_{l+k=n} a_l b_k$.

Or equivalently, if we define the polynomial ring as what we usually do, then we can get the isomorphism $A[X] \cong A^{(\mathbb{N})}$ by sending X^n to e_n for all $n \in \mathbb{N}$.

More generally, we can define the polynomial ring with multiple variables, it is similarlt with what we have done just now, we need to extend the the multiplication of free-module on any reasonable index set.

Definition 5.10. *Let $(N, +, 0)$ be an associative monoid with identity, we can define a multiplication on the free A-module $A^{(N)}$ with basis $(e_n)_{n\in N} = (\delta_{k,n})_{n\in N}$ by*

$$e_u \cdot e_v = e_{u+v} \quad \textit{for all } u, v \in N$$

and develop it for any elements

$$(a_n)_{n\in N} \cdot (b_n)_{n\in N} = (c_n)_{n\in N} \quad \textit{with} \quad c_n = \sum_{u+v=n} a_u b_v$$

Then $A^{(N)}$ is a A-algebra with ring homomorphism

$$\varphi : A \to A^{(N)}, \quad a \mapsto a e_0$$

*and we call it the **polynomial ring** over A with index monoid N, denoted by $A[N]$.*

In particular, if we take $N = \mathbb{N}$ we can get the polynomial ring in one variable $A[X]$. If we take $N = \mathbb{N}^n$ with the component-wise addition, then we can get the polynomial ring in n variables $A[X_1, \cdots, X_n]$ by identifying the basis element $e_{(k_1,\cdots,k_n)}$ with $X_1^{k_1} X_2^{k_2} \cdots X_n^{k_n}$ for all $(k_1, \cdots, k_n) \in \mathbb{N}^n$, then we can get the algebra of polynomial as following:
- elements:

$$f(X_1, ..., X_n) = \sum_{(k_1,...,k_n)\in\mathbb{N}^n} a_{(k_1,...,k_n)} X_1^{k_1} X_2^{k_2} \cdots X_n^{k_n} = \sum_{\kappa\in\mathbb{N}} a_\kappa X^\kappa$$

where only finitely many a_κ are non-zero.

- addition:

$$(\sum_{\kappa\in\mathbb{N}} a_\kappa X^\kappa) + (\sum_{\kappa\in\mathbb{N}} b_\kappa X^\kappa) = \sum_{\kappa\in\mathbb{N}} (a_\kappa + b_\kappa) X^\kappa$$

- multiplication:

$$(\sum_{\kappa\in\mathbb{N}} a_\kappa X^\kappa) \cdot (\sum_{\kappa\in\mathbb{N}} b_\kappa X^\kappa) = \sum_{\kappa\in\mathbb{N}} c_\kappa X^\kappa \quad \text{with } c_\kappa = \sum_{\lambda+\mu=\kappa} a_\lambda b_\mu$$

where the addition $\lambda + \mu$ is defined by component-wise addition in $\mathbb{N}^n$. The verification here is omitted for brevity, the process is similar to the one-variable case.

Polynomial is a natural object in algebra, in a certainn vacabulary, we say that polynomial ring $A[X]$ is a free commutative A-algebra, it refers to the following universal properties:

Proposition 5.11 (UP-Poly)**.**
For any A-algebra B with elements $b_1, ..., b_n$, there exists a unique morphism of A-algebras $\Phi : A[X_1, ..., X_n] \to B$ such that $\Phi(X_i) = b_i$ for all $i = 1, 2, ..., n$.
Or equivalently, it induces a natural bijection by $\Phi \mapsto (\Phi(X_1), ..., \Phi(X_n))$

$$\mathrm{Hom}_{A\text{-}alg}(A[X_1, ..., X_n], B) \cong B^n$$

The inverse is given by evaluation map $(b_1, \ldots, b_n) \mapsto \mathrm{ev}_{(b_1,...,b_n)}$, where $\mathrm{ev}_{(b_1,...,b_n)} : A[X_1, ..., X_n] \to B$ is defined by $ev_{(b_1,...,b_n)(f)} = f(b_1, \ldots, b_n)$.

Proof. For any $f(X_1, ..., X_n) = \sum_{\kappa\in\mathbb{N}^n} a_\kappa X^\kappa \in A[X_1, ..., X_n]$, we can define

$$\Phi(f) = \sum_{\kappa\in\mathbb{N}^n} a_\kappa b^\kappa \in B$$

where $b^\kappa = b_1^{k_1} b_2^{k_2} \cdots b_n^{k_n}$ for $\kappa = (k_1, ..., k_n) \in \mathbb{N}^n$. It is easy to verify that Φ is well-defined (only finitely many a_κ are non-zero) and a morphism of A-algebras. Moreover, we have

$$\Phi(X_i) = \Phi(e_{(0,...,1,...,0)}) = b_i$$

for all $i = 1, 2, ..., n$, which shows that Φ is a desired morphism. For the uniqueness, if there exists another solution Ψ, then for any $f(X_1, ..., X_n) = \sum_{\kappa\in\mathbb{N}^n} a_\kappa X^\kappa \in A[X_1, ..., X_n]$, we have

$$\Psi(f) = \Psi(\sum_{\kappa\in\mathbb{N}^n} a_\kappa X^\kappa) = \sum_{\kappa\in\mathbb{N}^n} a_\kappa \Psi(X^\kappa) = \sum_{\kappa\in\mathbb{N}^n} a_\kappa b^\kappa = \Phi(f)$$

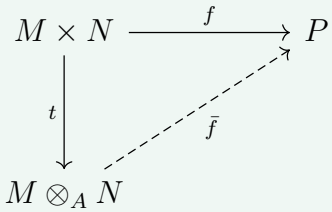
hence we finish the proof. □

5.5 Tensor product

Definition 5.5. Let M and N be two A-modules, the **tensor product** of M and N over A is an A-module $M \otimes_A N$ together with a bilinear map

$$t : M \times N \to M \otimes_A N, \quad (m, n) \mapsto m \otimes n$$

such that the following Unniversal properties (UPQ-TENSOR) holds:



for any A-module P and any bilinear map $f : M \times N \to P$, there exists a unique A-linear $\bar{f} : M \otimes_A N \to P$ such that $f = \bar{f} \circ t$, i.e. $\bar{f}(a \otimes b) = f(a, b)$.

Remark 5.9. The definition is concluded by some work to give a good construction

(1) The existence of tensor product can be constructed by taking the free module $A^{(M\times N)}$ and its submodule R generated by the following elements:

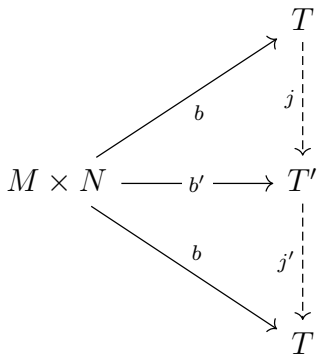
$$\begin{cases} e_{m+m',n} - e_{m,n} - e_{m',n} \\ e_{m,n+n'} - e_{m,n} - e_{m,n'} \\ e_{am,n} - ae_{m,n}, \\ e_{m,an} - ae_{m,n} \end{cases}$$

where $m, m' \in M, n, n' \in N, a \in A$, and $(e_{m,n})_{(m,n)\in M\times N}$ is the standard basis of $A^{(M\times N)}$. Then we can define

$$M \otimes_A N := A^{(M\times N)}/R$$

with $m \otimes n := \overline{e_{m,n}}$. then some verification needs here to show that the construction satisfies the universal property.

(2) The tensor product is unique up to isomorphism, i.e. if (T, t) and (T', t') are two tensor products of M and N, then the universal properties induce two morphism $j : T \to T'$ and $j' : T' \to T$ with the following diagram:



then $j \circ j' : T \to T$ a morpshim satisfying $b = (j \circ j') \circ b$, by the uniqueness of universal property we have $j \circ j' = \mathrm{id}_T$. Similarly, we can get $j' \circ j = \mathrm{id}_{T'}$, hence $T \cong T'$.

(3) The concret construction of tensor product is not important, the nice universal property allows us to treat a multilinear map as a linear map, usually we call $M \otimes_A N$ as «tensor», and $m \otimes n \in M \otimes_A N$ as «tensor element».

Some basic algebraic properties of tensor product can be concluded as following:

Lemma 5.11. *The letter we use are A-modules, then we have the following isomorphisms of A-modules:*

(1) $A \otimes_A M \cong M$ *with the isomoprhism* $a \otimes m \mapsto am$.

(2) $M \otimes_A N \cong N \otimes_A M$ *with the isomorphism* $m \otimes n \mapsto n \otimes m$.

(3) $(M \otimes_A N) \otimes_A P \cong M \otimes_A (N \otimes_A P)$ *with the isomoprhism* $(m \otimes n) \otimes p \mapsto m \otimes (n \otimes p)$.

(4) $M \otimes_A (N \oplus P) \cong (M \otimes_A N) \oplus (M \otimes_A P)$ *with the isomoprhism* $m \otimes (n, p) \mapsto (m \otimes n, m \otimes p)$

Remark 5.10. Pay attention to the abuse of the equality, sometimes we write $=$ instead of $\cong$ to simplify the notation.
(1) the first result can be generalized to $A^n \otimes_A M \cong M^n$.
(2) the last result can be generalized to

$$M \otimes_A (\bigotimes_{i \in I} M_i) \cong \bigotimes_{i \in I} (M \otimes_A M_i)$$

where I is any index set, with the isomorphism we can conclude that tensor product can preserve the free module structure by isomoprhism

$$A^{(I)} \otimes_A M \cong M^{(I)}$$

which covers the first remark.
(3) In general, by above result we can conclude in category: $\mathbf{Mod_A}$ with tensor product $\otimes_A$ forms a monoidal category.

Definition. A monoidal category contains following data:
(1) a category $\mathcal{C}$.
(2) a bifunctor $\otimes : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$.
(3) an unit object $I \in \mathcal{C}$ *having two natural isomorphisms.*

$$I \otimes X \cong X \cong X \otimes I$$

(4) a natural isomorphism (associator)

$$X \otimes Y \otimes Z \cong X \otimes (Y \otimes Z)$$

(5) These ismoprhism satisfy the Maclane axiom and triangle axiom.

We can generalize the universal property to construct the correspondence between multilinear maps and linear maps from the tensor product as following:

Proposition 5.12 (UPQ-MULTI-TENSOR)**.**
Let $M_1, \ldots, M_k$ *be A-modules, then for any A-module* P*, there exists a natural*

isomorphism

$$\mathrm{Hom}_A(M_1 \otimes_A \cdots \otimes_A M_k, P) \cong \mathrm{Mult}_A(M_1 \times \cdots \times M_k, P)$$

with the bijection $f \mapsto f(- \otimes - \cdots - \otimes -)$

The tensor product of two module is a larger module containg both information of two object in parallel way, hence the morphism of two tensor product is similarly a "product" of morphisms of two modules, which is the tensor product of morphisms:

Proposition 5.13. *Let* $f : M \to M'$ *and* $g : N \to N'$ *be two morphisms of* A*-modules, then there exists a unique morphism of* A*-modules*

$$f \otimes g : M \otimes_A N \to M' \otimes_A N', \quad m \otimes n \mapsto f(m) \otimes g(n)$$

6 Commutative Ring

6.1 Noetherian ring

Theorem 6.1 (Hilbert's Basis Theorem)**.** *If A is a Noetherian ring, then the polynomial ring $A[X]$ is also Noetherian.*

6.2 UFD

In this section we will study the commutative ring with nice factorization properties, which allows us to define arithemtic sturcture as what we have done in $\mathbb{Z}$.

Definition 6.1. *An integral domain A is called* ***unique factorization domain (UFD)*** *if it satisfies the following conditions:*

(Ex): A is a factorization ring: any non-unit element $a \in A - \{0\}$ can be written as a finite product of irreducible elements.

(Un): The factorization is unique up to order and unit factors, i.e. if

$$x = p_1 p_2 \dots p_r = p_1' p_2' \dots p_{r'}'$$

Then $r = r'$ and there exists a permutation $\sigma \in S_r$ such that p_i and $p'_{\sigma(i)}$ are ***associate*** *(equal up to a unit) for all $i = 1, 2, \cdots, r$.*

Remark 6.1. Here is some example of UFD:

(1) $\mathbb{Z}$ is a UFD by the fundamental theorem of arithmetic.

(2) $\mathbb{Z}[\sqrt{-5}]$ is not a UFD since

$$6 = (1 - \sqrt{-5}) \times (1 + \sqrt{-5}) = 2 \times 3$$

where $2, 3, 1 \pm \sqrt{-5}$ are irreducible elements. pay attention that many algebraic number rings are not UFDs.

(3) The elementary number theory is based on the division with remainder, with that we can develop the fundamental theorem of arithmetic in $\mathbb{Z}$, similarly we can define the division with remainder in the polynomial ring over a field $K[X]$, which allows us to conclude that $K[X]$ is a UFD. This is an informal proof, we will talk about it later in Euclidean domains.

(4) An interesting example is $\mathcal{O}(\mathbb{C})$, the ring of all entire function on $\mathbb{C}$, in complex analysis we have Euler's formula

$$\sin(\pi z) = \pi z \prod_{n \geq 1} (1 - \frac{z^2}{n^2})$$

where $\sin(\pi z)$ is not a unit but it can write as an infinite product of irreducible elements, hence $\mathcal{O}(\mathbb{C})$ is not a UFD.

Review the example (2) above, we notice here is a difference betweenn prime elemennts annd irreducible elements:

$$2 \mid 6 \nRightarrow 2 \mid 1+\sqrt{-5}$$

Hence 2 is not a prime elements. However, in $\mathbb{Z}$ all irreducible elements are essentially prime elements, which leads to the proof of FTA according to the properties of prime numbers (Euclid's lemma). This motivates us to redefine UFD in another way:

Proposition 6.2. *If A is a FD (factorization domain), then the following conditions are equivalent:*
(1) A is a UFD.
(2) Euclid's lemma holds in A: irreducible elements are prime elements.
(3) Gauss's lemma holds in A: $(a \mid bc \quad \wedge \quad gcd(a,b)=1) \implies (a \mid c)$

Valuation

Valuation is a useful too to study the local properties of commutative rings, in $\mathbb{Z}$ it relects the divisbility of integers by prime numbers, which is a fundamental tool in number theory, we define it on UFD, but the definition can be generalized to FD although some good properties may not hold.

Definition 6.2. *Let A be a UFD, and let $p \in A$ be an irreducible (prime) element, then we define the p-adic valuation a function $v_p : A - \{0\} \to \mathbb{N}$ by*

$$v_p(a) = \max\{n : p^n \mid a\}$$

and we make convention that $v_p(0) = +\infty$.

Remark 6.2. The following statement can be seen as a lemma for the definition, we suppose that A is just a FD here, and p is a prime element:

(1) For any $a \in A - \{0\}$, the set $E = \{n : p^n \mid a\} \subset \mathbb{N}$ is finite, esure the existence of the maximum such that $v_p(a)$ is well-defined.

(2) If $v_p(a) = n$ the maximum of E above, then there exists a unique element $b \in A - \{0\}$ such that $a = p^n b$ and $p \nmid b$.

The valuation has some nice properties as following, pay attention that the proof is independent of the UFD property:

Proposition 6.3. *Let v_p be a p-adic valuation on a UFD A, then for any $a, b \in A$, the following conditions hold:*
(1) $v_p(ab) = v_p(a) + v_p(b)$
(2) $v_p(a+b) \geq \min\{v_p(a), v_p(b)\}$, with equality if $v_p(a) \neq v_p(b)$

with the help of valuation, we can give some characterizations of elements in UFD, sometimes it rewrites the definitions of some concepts we meet in elementary number theory.

Proposition 6.4. *Let A be a UFD*

(1) an element $a \in A$ is a ***unit*** *if and only if $v_p(a) = 0$ for all irreducible elements $p \in A$.*

(2) an element $a \in A$ is an ***irreducible*** *element if and only if there exists an irreducible element $p \in A$ such that $v_p(a) = 1$ and $v_q(a) = 0$ for all irreducible elements $q \neq p$.*

(3) two elements $a, b \in A$ are ***associate*** *if and only if $v_p(a) = v_p(b)$ for all irreducible elements $p \in A$.*

(4) two elements $a, b \in A$, the ***divisibility*** *$a \mid b$ if and only if $v_p(a) \leq v_p(b)$ for all irreducible elements $p \in A$.*

(5) an element $a \in A$ with factorization $a = p_1 p_2 \dots p_r$ into irreducible elements, then $v_p(a)$ is the number of factors p_i that are associate to p.

(6) Let P be the set of representatives of the associate classes of irreducible elements in A, then for any $a \in A - \{0\}$ there exists a unique unit $u \in A$ such that

$$a = u \prod_{p \in P} p^{v_p(a)}$$

(7) The ***greatest common divisor*** *of two elements $a, b \in A$ is given by*

$$\gcd(a, b) = \prod_{p \in P} p^{\min(v_p(a), v_p(b))}$$

(8) The ***least common multiple*** *of two elements $a, b \in A$ is given by*

$$\operatorname{lcm}(a, b) = \prod_{p \in P} p^{\max(v_p(a), v_p(b))}$$

Proof. □

Remark 6.3. In a noetherian intger or a FD, none of the above properties may hold true, that is the reason why we restrict our discussion about valuation techinic on UFD. For example we consider the ring $\mathbb{Z}[\sqrt{-5}]$ again, then some counterexample will happenn:

- take $a = 2(1 + \sqrt{-5})$ and $b = 6$, then (4) fails since $v_2(a) = 1$ but $v_2(b) = 2$, however $a \nmid b$.

- take $6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, then (5) fails since $v_2(6) = 1$ but there is only one factor 2 in the factorization of 6.

- take $a = 6$, then (6) fails so that (7) and (8) also fail, since

$$\prod_{p \in P} p^{v_p(a)} = 2 \times 3 \times (1 + \sqrt{-5}) \times (1 - \sqrt{-5}) = 36 \neq 6$$

As the consequence of the valuation tool, we prove the transfert theorem of UFD, the traditional proof is based on the study of primitive polynomial, and it is a bit complicated.

Theorem 6.3 (Guass's Theorem)**.**
If A is a UFD, then the polynomial ring $A[X]$ is also a UFD.

Proof. □

6.3 Localization

Localization is a technique to extend a commutative ring by inverting some elements, such that we can study the local properties of the original ring. For example, we want to view 2 as a unit in some algebraic ring, it is natural to consider $\mathbb{Z}[\frac{1}{2}]$ such that $2^{-1} = \frac{1}{2}$.

Definition 6.5. *Let A be a ring, a subset $S \subset A - \{0\}$ is called a* ***multiplicative subset*** *if $1 \in S$ and for any $s, t \in S$, we have $st \in S$.*

with the multiplicative subset, we choose the elements we want to invert, then we can construct the localization of the ring as following:

Lemma 6.4. *Let A be a ring and S be a multiplicative subset of A.*

- We define a equivalent realtion $\sim$ on $A \times S$ by

$$(a, s) \sim (a', s') \iff \exists t \in S, t(as' - a's) = 0$$

it induces a quotient set denoted by $S^{-1}A = (A \times S)/\sim$.

(1-addition) we can define an addition on $S^{-1}A$ by

$$\frac{a}{s} + \frac{a'}{s'} := \frac{as' + a's}{ss'}$$

with a additive identity $\frac{0}{1}$.

(2-multiplication) we can define a multiplication on $S^{-1}A$ by

$$\frac{a}{s} \cdot \frac{a'}{s'} := \frac{aa'}{ss'}$$

with a multiplicative identity $\frac{1}{1}$.

Then $S^{-1}A$ is a ring with the operations above, called the ***localization*** *of A at S.*

Proof. □

Remark 6.4. There exists a natural ring homomorphism onto any localization of A:

$$\ell : A \to S^{-1}A, \quad a \mapsto \frac{a}{1}$$

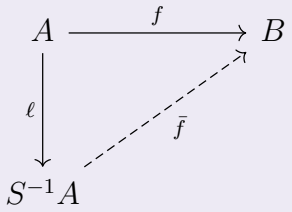
which shows that any localization of A is a A-algebra. And we can verify the kernel of ℓ is given by

$$\ker \ell = \{a \in A \mid \exists s \in S, sa = 0\}$$

it is actually some zero divisors of A "killed" by some elements in S. Hence if A is an **integral domain**, then ℓ is injective, and $\frac{a}{s} = 0$ if and only if $a = 0$.

As a A-algebra object, the localization satisfies the universal properties a little like "analytic continuation" in complex analysis, it refers to extend the morphism to a larger initial object:

Proposition 6.5 (UP-Localization)**.**
Let $S^{-1}A$ be the localization of a ring A, then for any A-algebra (B, f) such that $f(S) \subset B^\times$, then there exist a unique morphism of A-algebras $\bar{f} : S^{-1}A \to B$ such that the $\bar{f} \circ \ell = f$.



Proof. □

Remark 6.5. There are some consequennces of the universal property above:

(1) For a A-module M, if we consider $B = \mathrm{End}(M)$ and f is the structure morphism of M, then UP induces a natural morphsim $\bar{f}$ if any element in S acts as an automorphism on M, i.e. for any $s \in S$, the map $f(s) : M \to M$ is bijective. Hence M can be viewed as a $S^{-1}A$-module by defining

$$\frac{a}{s} \cdot m := f(a) \circ f(s)^{-1}(m)$$

for any $\frac{a}{s} \in S^{-1}A$ and $m \in M$.

(2) Conversely, any $S^{-1}A$-module can be trivally viewed as a A-module since $S^{-1}A$ is a A-algebra. Hence a correspondence about morphisms of module can be concluded here if the condition in (1) hols:

$$\mathrm{Hom}_A(M, N) = \mathrm{Hom}_{S^{-1}A}(M, N)$$

(3) If we set $B = S^{-1}A$ itself, then the UP implies that the uniqueness of the endomorphism of localization, i.e.

$$\mathrm{End}_{A\text{-alg}}(S^{-1}A) = \{\mathrm{id}\}$$

which shows that the localization in a cononcial construction.

Another important respects of localization is about correspondence of ideals, which allows us to identify the ideals in the localization, it is the base of the study of local rings.

Let $S^{-1}A$ be the localization of a ring A at a multiplicative subset S, then there exists two maps

$$\begin{aligned} \{I \subset A \text{ ideal} \mid I \cap S = \emptyset\} &\longleftrightarrow \{J \subset S^{-1}A \text{ ideal}\} \\ I &\longmapsto S^{-1}I := \{\frac{a}{s} \mid a \in I, s \in S\} \\ \ell^{-1}(J) &\longleftarrow J \end{aligned}$$

Proof. □

However, the correspondence above may not be a bijection, so it is not nice to do some identificaion:

$$\ell^{-1}(S^{-1}I) = \{a \in A \mid \frac{a}{1} \in S^{-1}I\} = \{a \in A \mid \exists t \in S, ta \in I\}$$

If the ideal here is prime, then we can get a better result that $\ell^{-1}(S^{-1}I) = I$, hence we can conlude a good corresponence as following:

Proposition 6.6. *Let $S^{-1}A$ be the localization of A, and define*

$$D(S) := \{p \in \mathrm{Spec}(A) \mid p \cap S = \emptyset\}$$

then there exists a bijection

$$\mathrm{Spec}(S^{-1}A) \to D(S), \quad \mathfrak{p} \mapsto \ell^{-1}(\mathfrak{p})$$

Remark 6.6.

(1) $D(S)$ is not empty if $S^{-1}A \neq 0$ (which map happen if $o \in S$, but we aviod it by definition), the reason is that any ring has at least one maximal ideal by Zorn's lemma, hence by bijection we can at least find one element in $D(S)$.

(2) The statement (1) can be concluded to be a techinic lemma to prove the existence of prime ideals in any ring, which is a fundamental result in commutative algebra:

Lemma. Let S be a multiplicative subset of a ring A, if $I \subsetneq A$ is an ideal such that $I \cap S = \emptyset$, then there exists a prime ideal $p \subset A$ such that $I \subset p$ and $p \cap S = \emptyset$.

The quotient of localization is another basic question as a object of ring. Here we make some remarks to avoid talk too much in the proof of main propoition below, and it gives a clear motivation to the construction:

Let I be a ideal of A such that $I \cap S = \emptyset$ disjoint, then by above correspondence we can know that $S^{-1}I$ is actually an ideal of localization $S^{-1}A$, so it makes sense to define the quotient ring $S^{-1}A/S^{-1}I$.

On the other hand, we consider natural morphism $\pi : A \to A/I$, then $\bar{S} = \pi(S)$ is a multiplicative subset (verify) of A/I if $I \cap S = \emptyset$, then we can do localization on A/I at $\bar{S}$ to get the ring $\bar{S}^{-1}(A/I)$.

So a immediate question is that the two objects above are isomorphic or not? It is essentially that the quoitent of localization is again a localization, and it is the localization of the quotient of initial ring.

Proposition 6.7 (UPQ-Localization)**.** *Let $S^{-1}A$ be a localization of a ring A, and I is a ideal of A such that $I \cap S = \emptyset$, then there exists a natural isomorphism of rings*

$$\bar{S}^{-1}(A/I) \cong S^{-1}A/S^{-1}I$$