Math Remark
Algebraic Structure

X

ElegantLaTeX Program

Update: April 14, 2025

Contents

1 Number System

Without talking some basic knowledge of Mathmatics logic, we generally define the object we want to study: Number System is a set of "number" and equipped by certain opreations. Here "number" is not necessary a real number like 1,2,3 we face daily in caculation, later we will aware that "number is actually a represent of a system, or using the language of the category, a normal system like $\mathbb{N}$ is just a represent object we choose in a category $Cat(\mathbb{N})$ (The collection of the system same as $\mathbb{N}$).

The main goal of this part is to construct the different number system begin from the natural number $\mathbb{N}$, the procedure often can be found in the textbook and the exercise, and the extension of distinct system inspire us to define the new algebra object.

1.1 From $\mathbb{N}$ to $\mathbb{Z}$

The common idea is to add a new element -1 to the system such that

$$1 + (-1) = 0$$

which refers to the completion of the unit of $\mathbb{N}$. We should notice that $\mathbb{Z}$ is a typical commutative ring with 1 identity, by comparison $(\mathbb{N}, +)$ is even not an abelian group, so by add a new element to the system we can clearly get the another "direction", which means $\{0, -1, -2, ...\}$ also forms a number system like $\mathbb{N}$ loosely speaking. we can caulate that $-2 = (-1) + (-1)$ by

$$2 + (-1) + (-1) = 1 + 1 + (-1) + (-1) = 0$$

so we can define that $-k$ is the sum of k same number -1.

Here we reconsider the negative number from the inspiration of the substraction, we can know that

$$-1 = 1 - 2 = 2 - 3 = 3 - 4 = ...$$

and

$$1 = 2 - 1 = 3 - 2 = 4 - 3 = ...$$

so we can define a binary relation on $\mathbb{N} \times \mathbb{N}$ by

$$(a, b) \sim (c, d) \Longleftrightarrow a + d = b + c$$

In fact we should notice that we want to write $a-b = c-d$, but we do not still define substraction formally, so we do the change. we can define that the relation is equivalent, which is easily to verify:

- **reflexivity:** $(a,b) \sim (a,b) \iff a+b=b+a$.
- **Symmetry:**

$$\begin{aligned}(a,b) \sim (c,d) &\iff a+d=b+c \\ &\iff c+b=b+c=a+d=d+a \\ &\iff (c,d) \sim (a,b)\end{aligned}$$

- **transitivity:**

$$\begin{aligned}(a,b) \sim (c,d) \wedge (c,d) \sim (e,f) &\iff a+d=b+c \wedge c+f=d+e \\ &\iff a+(d+c)+f=b+(c+d)+e \\ &\iff a+f=b+e \\ &\iff (a,b) \sim (e,f)\end{aligned}$$

Hence we can use this equiavlence relation to construct the intger.

Proposition 1.1 *Suppose $X=\mathbb{N}\times\mathbb{N}$, and we put $[a,b]$ to be the equiavlence class of the class containning $(a,b)\in X$, then following result can be verified:*
(1) the following operation is well-defined.

$$[a,b]+[c,d]=[a+c,b+d]$$

$$[a,b]\cdot[c,d]=[ac+bd,ad+bc]$$

(2) the system $(X/\sim,+,\cdot)$ form a commutative ring with multiplicative identity.
(3) The map $f:\mathbb{N}\to\mathbb{Z}, n\mapsto[n,0]$ is injective and additives

$$f(n+m)=f(n)+f(m)$$

(4) If $X_+=\{[n,0]:n\in\mathbb{N}\}$ and $X_-=\{[0,n]:n\in\mathbb{N}\}$, then

$$X/\sim = X_+ + X_-$$

Proof. (1) For any $(x,y)\in[a,b]$ and $(x',y')\in[c,d]$, we define the addition by

$$(x,y)+(x',y')=(x+x',y+y')$$

then we have

$$x+b=y+a\wedge x'+d=y'+c$$

add them togther we get

$$(x+y)+(b+d)=(x'+y')+(a+c)$$

which implies $(x+x', y+y') \sim (a+c, b+d)$, and then clearly $[a,b]+[c,d] \subset [a+c, b+d]$. The proof can be finished here because that the caculation will always be in the $[a+c, b+d]$, so we just need to check the corresponding caculation is really an injective then the definition will be well, but let us finish another direction, because it refers to the properties of natural number.

Mutually, if $(x,y) \in [a+c, b+d]$, then we have

$$x+b+d = y+a+c$$

By the choice of the element in class $[a,b]$, we can always find (i,j) such that $i \leq a$ and $j \leq b$, one thing should be pointed that we do not use substraction, usually we fix j such that $y+j \geq x$, which can be ensured by Archimedean Property , i.e. $\mathbb{N}$ is not bounded. and then i will be founded by **the properties of additive group**. hence here we can write down

$$(x,y) = (i,j) + (x_i, y_j)$$

we do not write $x_i = x - i$ and $y_j = y - j$ to prevent the abuse of the substraction. Finally, we can get two equation

$$i + x_i + b + d = j + y_j + a + c$$

$$i + b = j + a$$

then we can use the cancellation law of the group to get $(x_i, y_j) \sim (c,d)$, which finish our proof. ■

Remark We finish our definition, and formally we define the integer is such a ring which is an quotient set,

$$\mathbb{Z} = \mathbb{N} \times \mathbb{N} / \sim$$

and we denote $[0,0]$ by 0, denote $[1,0]$ by 1. And $[a,b]$ is called a positive number if $a > b$, and we denote it by $a-b$, which is the solution of $a = b + x$, otherwise we call $[a,n]$ a negiative number with the notation $-(a-b)$. More directly, if $n \in \mathbb{N} - \{0\}$, we have the simialrly notation in $\mathbb{Z}$ by

$$n = [n,0] \qquad -n = [0,n]$$

then we will have some basic properties as following

- $-(-a) = a$ or $a + (-a) = 0$
- $(-a)b = a(-b) = -ab$

By some verification, we can use these symbols to replace the equivalence class to refers the element in the integer ring, i.e. we finish the construction of the integer.

1.2 From $\mathbb{Z}$ to $\mathbb{Q}$: Fraction

Now the extension of the number system is about to extends a ring to be a field. Firstly, we consider the unit of the integer then we will find that $U(\mathbb{Z}) = \{\pm 1\}$, any other element do not have the multiplicative inverse. with the basic arithmetic opreaties of rational number we know that

$$\frac{a}{b} = \frac{c}{d} \iff ad = bc$$

So simialrly we can give a relation on $\mathbb{Z} \times \mathbb{Z} - \{0\}$ by

$$(p, q) \sim (m, n) \iff pn = qm$$

This relation is set up on multiplication, that is an imprtant point. and we can verify that this relation is equiavlent:

- **Reflexive:** $(p, q) \sim (p, q)$ since $pq = qp$.
- **Symmetric:** $(p, q) \sim (m, n) \implies pn = qm \implies mq = np \implies (m, n) \sim (p, q)$
- **Transitive:** $(p, q) \sim (m, n) \wedge (m, n) \sim (a, b) \implies pn = qm \wedge mb = na \implies mnpb = mnqa$. If $m = 0$, then $pn = na = 0$, so $p = a = 0$ by $n \neq 0$, immediately $pb = qa = 0$. If $m \neq 0$, then we can cancel mn to get $pb = qa$.

After this basic definition then we can rewrite the class of equivalence by

$$a/b = [(a, b)]$$

This is the symbol of fraction, so we usually call the field with the same method of extension from a ring, **field of fraction**.

Proposition 1.2 *Suppose $\mathbb{Q} = \mathbb{Z} \times \mathbb{Z} - \{0\}/\sim$, and use a/b to denote the element, then following:*
(1) The opreations below is well-defined

$$a/b + c/d = (ad + bc)/bd$$
$$a/b \cdot c/d = ac/bd$$

(2) With the opreations defined above, $\mathbb{Q}$ is a field.
(3) There exists an embedding from $\mathbb{Z}$ to $\mathbb{Q}$ by $k \mapsto k/1$, so we identify integr k with $k/1$ in $\mathbb{Q}$.
(4) For any $a, b \in \mathbb{Z} - \{0\}$, there exists a unique positive co-prime pair (p, q) such that $a/b = p/q \vee -p/q$.

Proof. (1) Given $a'/b' = a/b$ and $c'/d' = c/d$, then

$$a'/b' + c'/d' = a'd' + b'c'/b'd'$$
$$a'/b' \cdot c'/d' = a'c'/b'd'$$

Notice that

$$(a'd' + b'c')bd = (a'b)(d'd) + (c'd)(b'b) = b'ad'd + d'cb'b = (ad + bc)b'd'$$

which implies $a'd' + b'c'/b'd' = ad + bc/bd$. Simialrly,

$$a'c'bd = (a'b)(c'd) = (b'a)(d'c) = acb'd'$$

Which meams $a'c'/b'd' = ac/bd$.

(2) Firstly the operations are clearly commutative, associative and distributive, which inherits the properties of $\mathbb{Z}$. For any $a/b \in \mathbb{Q}$, we have

$$0/1 + a/b = 0b + 1a/1b = a/b$$
$$1/1 \cdot a/b = 1a/1b = 1/b$$

so $0/1$ is a addtive identity and $1/1$ is a multiplicative identity. and a/b has an additive inverse $-a/b$ since

$$a/b + (-a/b) = ab + b(-a)/b = 0/b = 0/1$$

And if $a \neq 0$, then a/b has an multiplicative inverse b/a since

$$a/b \cdot b/a = ab/ba = 1/1$$

(3) Denote $f(k) = k/1$, then $f(1) = 1/1 = 1_{\mathbb{Q}}$, and by

$$f(n + m) = n + m/1 = n/1 + m/1 = f(n) + f(m)$$
$$f(nm) = nm/1 = n/1 \cdot m/1 = f(n) \cdot f(m)$$

So clearly f is a field homomorphism, and it is injective since

$$f(n) = f(m) \implies n/1 = m/1 \implies n/1 \sim m/1 \implies n = m$$

So it is a embedding in $\mathbb{Q}$.

(4) Suppose that $d = gcd(a, b)$, then $gac(\frac{a}{d}, \frac{b}{d}) = 1$ and $(\frac{a}{d})/\frac{b}{d} = a/b$, so we prove the existence. If (p', q') is another pair satisfying the condition, we can conclude that

$$aq' = bp' \wedge aq = bp \implies p'q = pq'$$

Then By Guass's Lemma, $p|p'q$ and $gcd(p, q) = 1$, then $p|p'$; Simialrly, we can get $q|q'$, then we let $p' = lp$ and $q' = tq$ and mbn

we can conlude that $1 = gcd(q', p') = gcd(lp, tq) = gcd(l, q)$, again by $p'/q' = p/q$ we get that $l = t$ so the unique case is that $l = t = 1$, which implies the uniqueness. ■

We can generalize the usual construction of the field in the ring theory, and notice that key properties of $\mathbb{Z}$ is that **its multiplication satisfying cancellation law**, that refers to the integer domain.

Definition 1.1 *A ring $(R, +, \cdot)$ is called an integer domain if it does not conatain any zero divisor, that means for any $a, b \in \mathbb{Z} - \{0\}$, we have $ab \neq 0$.*

Another equivalent definition is that the ring satisfying cancellation law, which is easy to prove. If we take $a, b, c \in R$ such that $ab = ac$, and we suppose that $a \neq 0$, then $a(b - c) = 0$ by distributive law, and immediately we know that $b - c$ must be zero, so they are equal. With the key properties of intger domain we can conlude the theorem below.

Theorem 1.3 (field of fraction) *If $(R, +, \cdot)$ is an integer domain, then there exists a field F containning R as a subring by given the relation on $R \times R - \{0\}$:*

$$(a, b) \sim (c, d) \iff a \cdot d = b \cdot c$$

Moreover, this field is the smallest field conatinnig R, and usually we denote $F = Frac(Q)$.

Proof. With the same method above we can construction a new field $Q = R \times R - \{0\}/\sim$, and we notice that F can be embedded in Q, so conversely we choose so that, for each $x \in F$, there exists $a, b \in R$ and $b \neq 0_R$ such that $ab^{-1} \in F$. Then Q and F and naturally isomorphic since

$$ab^{-1} = cd^{-1} \iff ad = bc$$

And we suppose that the field F' is a field containning R, then any $a \in R^*$ we have $a^{-1} \in F'$, so any form of ra^{-1} will be in F', which means $F \subset F'$, so F is the smallest field. ■

1.3 From $\mathbb{Q}$ to $\mathbb{R}$: Completion

In this section we will talk about the construction of real number, there are many equivalent ways to define real number, they are all same we will see that later. The flaw of the rational number is that it is not complet, or intuitively it can be seen as a line with too many holes in it. Convergence and limit theory is the core of the analysis, we are interested in what value a sequence convergs to, for example:

$$\lim_{n\to\infty} (1 + \frac{1}{n})^n = e$$

clearly, it is a sequence of $\mathbb{Q}$ but it converges to an irrational number. Moreover, we can consider Fibonacci number given by recurrence $F_{n+2} = F_{n+1} + F_n$, then we define s sequnece in $\mathbb{Q}$ by $a_n = \frac{F_{n+1}}{F_n}$, then it will converges to the golden ratio $\frac{1+\sqrt{5}}{2}$. Although the two example gives

the limit of the seqence, but the fact is that we do not have the number in the rational number system we had! Hence some problem confuse the people in the time when the axiomatic system of number fields or even the real number system had not yet been established.

Now Let us construct the real number from the point of view: **any sequence of $\mathbb{Q}$ with the good characteristic of convergence can find a limit in the system.** Here the sequence is just **Cauchy sequence**.

Definition 1.2 *A sequence (x_n) in $\mathbb{Q}$ is called a **Cauchy sequence** if for every rational $\varepsilon > 0$, there exists an integer $N \in \mathbb{N}$ such that for all $m, n \geq N$, we have*

$$|x_n - x_m| < \varepsilon.$$

Moreover, it is called to converges to L in $\mathbb{Q}$ if for every rational $\varepsilon > 0$, there exists an integer N N such that for all $n \geq N$, we have

$$|x_n - L| < \varepsilon$$

This is a type of sequence which tends to level off at the tail, so has a good feature to be convergent to some value. Now we denote the set of all sequence of $\mathbb{Q}$ be Q, then we can define a relation in it by

$$(a_n)_{n\in\mathbb{N}} \sim (b_n)_{n\in\mathbb{N}} \iff (a_n - b_n)_{n\in\mathbb{N}} \text{ converges to } 0$$

The relation is clearly equiavlent, the transitivity is given by the triangle inequality, that nuaturally the properties of absolute value (generally a norm). We use $[a_n]$ denote the class of equivalence of the sequnece $(a_n)_{n\in\mathbb{N}}$, now we need to define the algebra operation in it, respectively we define:

$$[a_n] + [b_n] := [a_n + b_n]$$
$$[a_n] \cdot [b_n] := [a_n \cdot b_n]$$

where the opreations in bracket is the operation we defined in Q, so $a_n + b_n$ and $a_n \cdot b_n$ is again a sequnce of $\mathbb{Q}$. The definition is well-defined, on the one hand, sum of two cauchy sequence is still cauchy, so $a_n + b_n$ is exactly in some class of equivalence, and we just choose it to be the represent. on the other hand, the product is not very clear, we notice that

$$|a_n b_n - a_m b_m| = \frac{1}{2}|(a_n - a_m)(b_n + b_m) + (a_n + a_m)(b_n - b_m)|$$

easily we can know that cauchy sequence must be bounded, so there exists M, M' such that

$$|a_n b_n - a_m b_m| \leq M|a_n - a_m| + M'|b_n - b_m|$$

so we can just choose $n, m \geq \max\{N_a, N_b\}$, which is implied by two cauchy sequence, and simialrly we choose $a_n \cdot b_n$ to be the represent.

Proposition 1.4 *Let $\mathbb{R} = Q/\sim$, under above definition, $(\mathbb{R}, +, \cdot)$ is a field.*

Proof. It is just the boring verification, you can choose to do it or just trust the result, here I do it.

we let the class $[0]$ denote the sequence $a_n = 0$ for any n, then it will be the additive identity and it denote all sequence converging to zero, since for any sequence $(b_n)_{n\in\mathbb{N}}$, we have $b_n + 0 = b_n$, so it has an inverse $-b_n$. And the multiplicative identity is $[1]$, it is the class of the sequence with 1 as all element, it will denote all sequence convering to 1. Then for any sequence $(b_n)_{n\in\mathbb{N}}$ not in $[0]$, we have $b_n \cdot 1 = b_n$, so $[b_n] \cdot [1] = [b_n]$, and the existence of its multiplicative inverse is a little complex since not necessary all b_n are not zero. We firstly prove a properties of the cauchy sequence:

Lemma 1.5 *For any cauchy sequence not converging to zero, there exists at most finite term having the different sign with the other term. and we call a cauchy sequence is poistive (negiative) if almost term is positive (negative).*

For a cauchy sequence $(a_n)_{n\in\mathbb{N}}$, $\epsilon_1 > 0$ implies an integer N_1 such that $|a_n - a_m| < \epsilon_1$ for any $n, m \geq N_1$. It is not converges to zero, then there exists a lower bound $c > 0$ which implies an intger N_2 such that any $n_0 \geq N_2$, $|a_{n_0}| > c$. so we just take $N_2 = N_1$ such that for any $n \geq N_1$

$$||a_n| - |a_{n_0}|| \leq |a_n - a_{n_0}| < \epsilon_1$$

and then

$$|a_n| \geq -\epsilon_1 + |a_{n_0}| > c - \epsilon_1 > 0$$

so we just take $\epsilon_1 = c/2$, which finish the proof of the lemma.

so we just need to construct a new sequence $(\bar{a}_n)$, for any $n \geq N_1$, $\bar{a}_n = a_n$ and for any $n < N_1$, $\bar{a}_n = a_{N_1}$, then $a_n \neq 0$ for any integer, so the sequence will be equiavlent to (a_n) and then sure $[a_n] = [\bar{a}_n]$, so the multiplicative inverse will be $[\frac{1}{\bar{a}_n}]$.

Finally notice that associative law and distributive law is inherit the rational number, so we finish our proof. ■

Now we will consider the representative of the field to simplify the notation. We firstly notice that if a sequence converges to some q in $\mathbb{Q}$, then the sequence will clearly be equiavlent to a constant sequence $(q)_{n\in\mathbb{N}}$, so we just embed $\mathbb{Q}$ in $\mathbb{R}$ by $q = [q]$. But for the representative for irrational number, sometimes we really can choose a algebra symbol like $\pi, e, \sqrt{2}\ldots$, but these symbol actually refer to a non-constant sequence in $\mathbb{Q}$, or we say that we use rational number to apporximate it. When n really be ∞, something changes and the apporixmation will really be thought as a new number which is not contained in the original system of rational number.

The process we often call it the **completion of the metric space**, hence we give it a conclusion generally.

1.4 From $\mathbb{R}$ to $\mathbb{C}$: Extension

The construction of complex number refers to add element, the classic valuation operates on $\mathbb{C}$ is a morphism

$$f : \mathbb{R}[X] \to \mathbb{C}, \quad P \mapsto P(i)$$

with the basic knowledge about the complex number and ring theory, we can conlude that $kerf = (X^2 + 1)$, the principal ideal of polynomial $X^2 + 1$, hence we can get an isomorphism as following

$$\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}$$

That is a very simple thought. we know that $x^2 + 1 = 0$ can not have a solution in $\mathbb{C}$, so we hope to find a lager field containning $\mathbb{R}$ such that the algebraic equation indeedly has a solution, and we denote the solution by i, then how will the field forms? All algebraic operations we do in equation is just addition and multiplication, so with a little inspiration we know that the new field we hope is the form of linear combination

$$R[i] = \{a + bi | a, b \in \mathbb{R}, i^2 = -1\}$$

here we get a $\mathbb{R}$-vector space really containning the solution of the equation. and then we can easily conclude the new addition and multiplication in the field

$$(a + bi) + (c + di) = (a + c) + (b + d)i$$
$$(a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i$$

By some verification we can know that the set we construct is a field. Hence from the view of $\mathbb{R}-$Algebra, $\mathbb{C} \cong \mathbb{R}^2$ makes sense and it brings many amazing results at the same time. The simple description given here refers to the **algebraic extension**,

We notice that $\mathbb{C}$ is equipped with the metric and Hermite inner product is based on $\mathbb{C}$, so here we give it a beautiful correspondence by matrix algebra. The most important information about complex field is the conjuation, so we just define

$$\mathbb{C} = \{\begin{pmatrix} a & -b \\ b & a \end{pmatrix} | a, b \in \mathbb{R}\}$$

Which is a subspace of $M_2(\mathbb{R})$, and claerly it has dimension of 2 with two base

$$e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad i = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

Proposition 1.6 *By the identification above we have*
(1) $\mathbb{C}$ *is a field with* e *as the multiplicative identity.*
(2) $Vect(e)$ *has an isomorphism* φ *with* $\mathbb{R}$ *by* $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mapsto 1$ *and if we identify* $e \equiv 1$*, then any* $z \in \mathbb{C}$*, it has the form linear combination* $z = a + bi$*.*
(3) For any $z = a + bi$*, it has a conguation* $\overline{z} = a - bi = z^T$*.*
(4) Define the modulo $|\cdot| : \mathbb{C} \to \mathbb{R}^+$ *via* $z \mapsto \varphi(z\overline{z})$ *it gives a norm of* $\mathbb{C}$*.*
(5) The equiavlent definition of (4) is via $|z| = \sqrt{det(z)}$*.*

Proof. Just verify ■

Another imprtant form of complex number is polar form, so the structure of the disc deserves a look. We define

$$\mathbb{U} = \{z \in \mathbb{C} || z| = 1\}$$

With the multiplication, then it is isomorphic to the orthognal group $SO_2(\mathbb{R})$, by the reduction of the matrix we know that it has the form

$$z = \begin{pmatrix} cosa & -sina \\ sina & cosa \end{pmatrix} = cosa + \mathbf{i}sina$$

which means the details of $\mathbb{U}$ depends on a parmeter with the period 2π, which gives a connection with the **Euler's formula**:

$$e^{i\theta} = cos\theta + \mathbf{i}sin\theta$$

then the polar form is given by the isomorphism

$$\mathbb{R}^* \times \mathbb{R}/2\pi\mathbb{Z} \xrightarrow{\sim} \mathbb{C}^*, \quad (r, \theta) \mapsto re^{i\theta}$$

Moreover, the expontial structure is derived from the matrix expontial

$$exp : M_2(\mathbb{R}) \to GL_2(\mathbb{R}), \quad A \mapsto \sum_{\mathbb{N} \in \mathbb{N}} \frac{A^n}{n!}$$

Notice that in finite-dimensional vector space with norm, any its subspace must be closed, so $\mathbb{C}$ is a closed subspace of $M_2(\mathbb{R})$, which ensures that the series will always converge inside $\mathbb{C}$ such that we can restrict the exponti

2 Commutative ring

2.1 Polynomial

2.1.1 arithmetic of polynoimal

In this section we will discuss the arithemtic properties of polynoimal under a commutative ring R, The proof of properties is nearly same with the proof of arithemtic properties of intger.

Theorem 2.1 (Euclidean Algorithm)
Suppose that R is a domain and $f, g \in R[X]$ with f a monic polynomial, then there exists unique polynoimals $r, s \in R[X]$ such that

$$g = sf + r$$

with $\deg r < degf$ *or* $\deg r = 0$

Proof. **Existence:** If $\deg g < \deg f$, simply set $s = 0$, $r = g$. Then $g = sf + r$ and $\deg r < \deg f$, as required. Suppose $\deg g \geq \deg f$. Let

$$g = a_n X^n + \cdots + a_0, \quad f = X^d + ... + b_0.$$

Let $n = \deg g$, $d = \deg f$. Then define

$$s_1 = a_n X^{n-d}$$

Then the degree of $r_1 = g - s_1 f$ will be less than n, if the degree is still larger than d, we do the same procedure till some integer k:

$$\begin{aligned} r_1 &= g - s_1 f \\ r_2 &= r_1 - s_2 f \\ &... \\ r_k &= r_{k-1} - s_k f \end{aligned}$$

where $s_i = a_i X^{m_i}$ with a_i the leading cofficient of r_{i-1} and $m_i = \deg r_{i-1} - d$. k satisfies

$$\deg r_1 > \deg r_2 > ... > \deg r_{k-1} \geq d = degf > \deg r_k$$

Finally, adding them togther we get

$$r = r_k, s = s_1 + s_2 + ... + s_k$$

Uniqueness: Suppose there exist two such decompositions:

$$g = s_1 f + r_1 = s_2 f + r_2.$$

Then:

$$(s_1 - s_2) f = r_2 - r_1.$$

The left-hand side is divisible by f if $s_1 \neq s_2$, and the right-hand side has degree strictly less than $\deg f$, unless it is zero. Since R is an integral domain, this implies $r_1 = r_2$ and thus $s_1 = s_2$. Hence the decomposition is unique. ■

Remark For a field K, $K[X]$ will be an excellent object to study (we call it K**-algebra**) since it satisfies Euclidean Algorithm, Furthermore it will satisfy all arithemtic properties in $\mathbb{Z}$, in brief, it is a Euclidean ring with degree as its euclidean function

3 Field Theory

3.1 Field extension

For the beginning, notice a trival isomorphism:

$$\mathbb{R}[X]/(X-a) \cong \mathbb{R}$$

For any $a \in \mathbb{R}$, and we review the isomorphism given in complex number field:

$$\mathbb{R}[X]/(X^2+1) \cong \mathbb{C}$$

Clearly, $\mathbb{C}$ is a larger field containning $\mathbb{R}$, but we wonder how we can get it from the algebra structure. Here it motivates us to consider the question from the polynoimal structure defined on a field.

Firstly we need some lemma

Lemma 3.1 *If K a field and $p \in K[X]$, then p is irreducible if and only if $K[X]/(p)$ is a field.*

Lemma 3.2 *Let L be a field containning K as a subfield, then L is a vector space over K.*

Proposition 3.3 *Let K be a field and I be a principl ideal generated by a monic irreducible polynoimal $p \in K[X]$ of degree d, Let $L = K[X]/I$, then*
(1) L is a field and K can be embedded in L , so K can be identified as a subfield of L.
(2) p has a root β in L, exactly $\beta = X + I \in L$
(3) If $g \in K[X]$ and β is a root of g in L, then $p|g$.
(4) p is the unique monic irreducible polynoimal in $K[X]$ having β as a root in L.
(5) L can be viewed as a K-vector space with the basis $\{1, \beta, ..., \beta^{d-1}\}$.

Proof. (1) L is a field by above Lemma, and we consider an embedding $i(a) = a + I$ for any $a \in K$, clearly it is injective and actually it is $\pi|_K$, where π is the canoncial map from $K[x]$ to $K[x]/I$.

(2) Suppose $p(x) = a_0 + ... + a_d x^d$, then in L, we have

$$\begin{aligned} p(\beta) &= a_0 + a_1\beta + ... + a_d\beta^d \\ &= a_0 + a_1(X+I) + ... + a_d(X+I)^d \\ &= a_0 + a_1(X+I) + ... + a_d(X^d+I) \\ &= p(X) + I = I \end{aligned}$$

Here $p(X) \in I$ and I is the zero element in L.

(3) If p does not divide g, then $gcd(p, g) = 1$ since p is irreducible, so there exists r, t in $K[X]$ such that

$$1 = s(x)p(x) + t(x)g(x)$$

put $x = \beta$ in L, then $1 = 0$ leads to a contradiction.

(4) immediately from (3). For (5) we use euclidean divison for polynoimal, any $f \in K[X]$, there exists $q, r \in K[X]$ with $\deg r < d$ such that $f(x) = q(x)p(x) + r(x)$, then $f + I = r + I$ in L, and if $r(x) = b_0 + ... + b_k x^k$, $k < d$, by opreations of ideal

$$r + I = b_0 + b_1\beta + ... + b_k\beta^k$$

so $\{1, \beta, ..., \beta^{d-1}\}$ spans L. They are linearly independent because if we assume they are linearly dependent, that means there exists a polynoimal $h \in K[X]$ of degree $< d$ such that h has β as the root, but by (3) we know that $p|h$, which leads to a contradiction since $d = \deg p \leq \deg h$. ■

Another ways to consider the field extension is to adjoin new element, that means adding a certain algebra element into the field to get a larger field, it is easy to see that $\mathbb{C} = R[i]$, so the complex number can be seen as the field by adjoining i which satisfies $i^2 + 1 = 0$.

Proposition 3.4 *Let K be a field and $f \in K[X]$ irreducible, adjoin element $c \notin K$ such that c is a root of f, then $K[c]$ is a field containning K as a subfield, so it can be written as $K(c)$.*

$$K(c) = \{a_0 + a_1 c + ... + a_k c^k | a_1, ..., a_k \in K, k = \deg f - 1\}$$

Proof. $K[c]$ naturally is a ring with same identity with K, so we just need to find the inverse. For any polynoimal $p \in K[X]$ with degree less than $\deg f$, it is co-prime with f since f is irreducible, so by Bezout's theorem for polynoimal, there exists $r, t \in K[X]$ such that

$$p(x)r(x) + t(x)f(x) = 1$$

hence we take $x = c$ then immediately $p(c)r(c) = 1$, so in $K[c]$ we find the inverse of $p(c)$. and notice that $K[c]$ is a field garantee any rational polynoimal can have the form of polynoimal, so $K[c] = K(c)$ evidently. ■

Here we find two method to extension the field, the first method is to embed K into a larger fild, the second is to adjoin element, we will see that they actually is the same.

Before doing that we can now define some vocabulary without without abruptness.

Definition 3.1 *If L is a field containing K as a subfield.*

- *L/K denotes a **field extension** of K, and for finite extension $[L : K]$ denotes the dimension of L.*

- *For $a \in L$, it is **algebraic** (over K) if there is some nonzero polynoimal of $K[X]$ having a as a root. L/K is a **algebraic extension** if any element in L is algebraic.*
- *For $a \in L$, it is transcendental if it is not algebraic.*
- *A field is **algebraically closed** if FTA holds in it. L is an **algebraic closure** of K if the extension is algebraic and L is algebraically closed.*

Theorem 3.5 (Structure of field extension)

Let L/K be field extension of K and $a \in L$ is algebraic, then

*(1) There exists a unique monic irreducible polynoimal in $K[X]$ having a as a root. Formally we call it **minimal polynoimal** of a over K, and denote it by $\pi_{a,K}$.*

(2) If $I = (\pi_{a,K})$, then there exists an isomorphism

$$\phi : K[X]/I \to K(a)$$

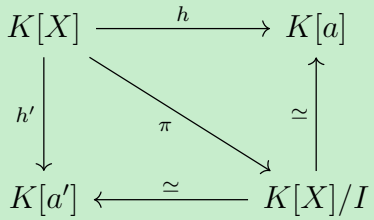
with $X + I \mapsto a$ and $c + I \mapsto c$ for all $c \in K$.

(3) If a' is another root of $\pi_{a,K}$, then there is an isomorphism

$$\theta : K(a) \to K(a')$$

with $a \mapsto a'$ and $c \mapsto c$ for all $c \in K$.

Proof. It needs to consider the **valuation map**, we define $h : K[X] \to L$ by $p \mapsto p(a)$, then clearly $\ker h$ contains all polynoimals having a as a root, then notice that $K[X]$ is a principal ideal ring, so $\ker h$ must be the form (p) with monic $p \in K[X]$. By first isomorphism theorem, we know that $K[X]/I \cong K(a)$, then by Lemma 3.1 p must be irreducible. hence we prove (1), and we can draw commtue diagram to finish.



where $h'(p) = p(a')$, and π is the canoncial map.

3.1.1 splitting field

■