Math Remark
Algebraic Structure

X

ElegantLaTeX Program

Update: June 23, 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

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

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

$$\begin{aligned}0/1+a/b=0b+1a/1b=a/b\\ 1/1\cdot a/b=1a/1b=1/b\end{aligned}$$

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

$$\begin{aligned}f(n+m)&=n+m/1=n/1+m/1=f(n)+f(m)\\ f(nm)&=nm/1=n/1\cdot m/1=f(n)\cdot f(m)\end{aligned}$$

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 ε > 0, there exists an integer N   N such that for all n ≥ 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 $ker f = (X^2 + 1)$, 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 Classification

There are many types of ring, we do a general classification here for a clear implication.

Definition 2.1 *Let R be a domain, and then we define*

*- R is a **PID (Principal ideal domain)** if all the ideal is princiapl.*

*- R is a **UFD (Unique factorization domain)** if every non-zero and non-unit element can be wirtten as a finite product of irreducible elements, and the representation is unique up to the order: if p_i and q_j are all irreducible such that $q_1 \cdots q_n = p_1 \cdots p_m$, then $m = n$ and there exists a permutation $\sigma \in S_n$ such that $q_i = p_{\sigma(i)}$.*

*- R is a **ED (Euclidean domain)** if a domain having a division algorithm: there exists a degree function $N : R - \{0\} \to \mathbb{N}$ such that for all $f, g \in R$ with $f \neq 0$, we can conclude $q, r \in R$ satisifying*

$$g = qf + r$$

where either $r = 0$ or $N(r) < N(f)$.

Remark We must notice the relationship of the definition and the arithemtic properties:

Ring	**Arithmetic Property of $\mathbb{Z}$**
Euclidean Domain	Euclidean Algorithm
UFD	Fundamental Theorem of Arithmetic
PID	Bézout's Theorem

So there exists a baisc implication:

Proposition 2.1 *Let R be a domain*

$$\textit{ED} \implies \textit{PID} \implies \textit{UFD}$$

Proof. First implication: Let R be an euclidean domain and I be an non-zero ideal. Suppose that N is the degree function, then $S = \{N(x) | x \in I - \{0\}\} \subset \mathbb{N}$, by the well-ordering principle of natural number, we can conclude a minimal element $N(a) \in S$, then we will prove that $I = (a)$. For any $n \in I$ we can find $r, s \in R$ such that $n = sa + r$. Since I is an ideal, then $sa \in I$ and so immediately $r \in I$. Notice that $N(r) < N(a)$, by the minimal of a we can conclude that r must be zero, so $n \in (a)$, which implies $I \subset (a)$, and another direction is trival, so we finish the proof.

Second implication: We prove by contradiction. Suppose that R is a PID but not a UFD, then not each non-unit and non-zero element in R can be decomposed, so we can take an element $a \in R$ which is not irreducible, and there exists two non-zero and non-unit element a_1, b_1 such that $a = a_1 b_1$, so immediately $(a) \subset (a_1)$. Notice that if $(a) = (a_1)$, then b_1 must be a unit, so we must have $(a) \subsetneq (a_1)$. with the same procedure we have

$$a = a_1 b_1 = a_2 b_2 b_1 = a_3 b_3 b_2 b_1 = \ldots$$

which implies a **infinite strictly ascending chain** of ideals (Notice that it must be infinite, if the process ends in a finite step, then we get a finite product of non-irreducible element, then by definition a must be irreducible)

$$(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \ldots$$

Then we take $I = \cup_{n \geq 0} (a_n)$ with convention $a_0 = a$, we can verify that I is an ideal, so there exists $d \in I$ such that $I = (d)$ since R is a PID, then there exists $n \geq 0$ such that

$$I = (d) \subset (a_n) \subsetneq (a_{n+1}) \subsetneq I$$

which implies a contradiction. ■

2.2 Prime ideal and maximal ideal

There are two important ideals.

Definition 2.2 *Let R be a commutative ring and $I \subsetneq R$ is a proper ideal, then*

*- I is an **prime ideal** if $ab \in I$ implies $a \in R$ or $b \in R$. Simialrly, we define a non-zero and non-unit element $a \in R$ as a **prime element** if $a|bc$ implies $a|b$ or $a|c$.*

*- I is an **maximal ideal** if there is no ideal J such that $I \subsetneq J \subsetneq R$.*

The definition of prime element usually be rstricted in a **domain**, and notice that prime ideal and prime element means an object satisfying **Euclid's Lemma**, under domain a good thing by definition is that

$$p \text{ prime element} \iff (p) \text{ prime ideal}$$

So it is easy to describe prime ideal in a ring like PID, later we will see that prime element will be like a real prime we want in UFD. Following are the equiavlent statement of this two ideals by the language of homomorphism.

Proposition 2.2 *Let $I \subsetneq R$ an ideal of a commutative ring.*

- I is a prime ideal if and only if R/I is a integral domain.

- I is a maximal ideal if and only if R/I is a field.

Proof. Notice that R/I is firstly a well-defined quotient ring, then we verify the extra properties. If I is a prime ideal, then for any classes $a+I$ and $b+I$ satisfies

$$ab + I = (a+I)(b+I) = \bar{0}$$

we have $ab \in I$, then by prime ideal $a \in I$ or $b \in I$, so $a + I = \bar{0}$ or $b + I = \bar{0}$. Conversely, if R/I is a domain, then for any $\bar{ab} = \bar{0}$ we must have $\bar{a} = \bar{0}$ or $\bar{b} = \bar{0}$, that is the implication we hope by $\bar{a} = \bar{0} \iff a \in I$.

If I is a maximal ideal, we need a **lemma** that K is a field if and only if $\{0\}$ is a maximal ideal in K: anyother non-zero element is unit and any ideal containing unit equals to K.

Then we consider $K = R/I$. We consider the natural map $\pi : R \to R/I$ and then any ideal J of ring R/I, by correspondence theorem $\pi^{-1}(J)$ must be an ideal of ring R containing I, but I is the maxiaml one, so there exists only two ideals in R/I: $\{0\}$ and R/I. ■

An immediate result is that **a maximal ideal must be a prime ideal** since a field is surely a domain, conversely a prime ideal is not necessary a maximal ideal unless the ring has a good properties. To describe the relationship clearly, we review that ”prime number” in $\mathbb{Z}$ is a number that can not be decomposed and satisfies the Euclid’s lemma, so it is natural to consider irreducible element here, a fundament unit in ring, and we consider a general implication and later we refine the realtionship.

Proposition 2.3 *Let $a \in R$ an non-unit element in a domain R, then*

$$\begin{tikzcd}
a \textit{ irreducible} \arrow[r, Leftarrow] & a \textit{ prime} \arrow[d, Leftrightarrow] \\
(a) \textit{ maximal ideal} \arrow[u, Rightarrow] \arrow[r, Rightarrow] & (a) \textit{ prime ideal}
\end{tikzcd}$$

Proof. If a is a prime element, then if $a = bc$ in R, then $a|bc$ clearly, so immediately $a|b$ or $a|c$ by prime element. What’s more, $b|a$ and $c|a$, so that implies $a = b$ or $a = c$, then b is a unit or c is a unit, so a is irreducible.

If (a) is maximal, we suppose that a is not irreducible, then $a = bc$ with b, c non-unit and non=zero, it implies $(a) \subsetneq (b)$, it is absurd since (a) is maximal, so a must be irreducible. ■

Remark It shows that prime elements is a good irreducible element satisfying good arithemtic properties. For a p-adic number system, we must have p is a prime since

$$\cdots \subsetneq p^3\mathbb{Z} \subsetneq p^2\mathbb{Z} \subsetneq p\mathbb{Z} \subsetneq \mathbb{Z}$$

In a projection system we need $p\mathbb{Z}$ to be a maximal ideal to construct a field, so p must be a irreducible element in $\mathbb{Z}$.

To refine the result, the ring will be added more properties. Firstly we suppose that ring R is a PID.

Proposition 2.4 *If $a \in R$ is an irreducible element of a PID R, then (a) is a maximal ideal and a is a prime element.*

Proof. Supposet that J is an ideal containing (a), then by PID there exists $d \in J$ such that $(a) \subset (d)$, so there exists $l \in R$ such that $a = dl$. Since a is irreducible, so d is a unit or l is a unit. If d is a unit, then $J = R$; If l is a unit, then $d = l^{-1}a$ implies $(d) \subset (a)$, so $J = (a)$. Notice that a is not a unit, so $(a) \subsetneq R$, so it must be a maximal ideal. Then clearly, (a) is a prime ideal so a is a prime by proposition 2.3. ■

By this proposition we get a completion of implication in PID as following

$$\begin{tikzcd}
a \text{ irreducible} \arrow[r, Leftrightarrow] \arrow[d, Leftrightarrow] & a \text{ prime} \arrow[d, Leftrightarrow] \\
(a) \text{ maximal ideal} \arrow[r, Leftrightarrow] & (a) \text{ prime ideal}
\end{tikzcd}$$

In particular, $\mathbb{Z}$ is a PID so in any PID we can identify irreducible element as a prime element, that is why in a polynomial ring over a field $k[x]$, we have Euclid's lemma for the irreducible polynomial (like thm 3.37 in Rotman old version). and we can see a example showing PID is the most lowest condition for above good implication.

Example 2.1 *Consider UFD but not PID $\mathbb{Z}[X]$, (X) is a prime ideal since $\mathbb{Z}/(X) \cong \mathbb{Z}$ a domain; (X) is not a maixmal ideal since $(X) \subset (X, 2)$, and $\mathbb{Z}/(X, 2) \cong \mathbb{Z}/2\mathbb{Z}$ a field , so $(X, 2)$ a maximal ideal which means $(X) \subsetneq (X, 2)$.*

Review that UFD is the ring that element can be decomposed to be the form of the product of irreducible elements, in that case irreducible element must be prime element, similar reason is that we can prove Euclid's lemma by fundamental theorem of arithemtic.

Theorem 2.5 *R is a UFD if and only if the ring satisfies two condition:*

(1) R is a factorization domain, that means each non-unit and non-zero element can be decomposed to the product of irreducible elements.

(2) Each irreducible element is a prime element.

Proof. If R is a UFD, then it is trivally a factroization domain. For any irreducible $p \in R$ with $p|ab$, there exists $r \in R$ such that $ab = rp$, by factorization of a and b, a or b contain the irreducible element p, so $a \in (p)$ or $b \in (p)$, that means $p|a$ or $p|b$, so p is prime.

Conversely, the proof is similar to the proof of the fundamental theorem of arithemtic, we need to prove the uniqueness of factorization. We suppose that

$$p_1 \cdots p_m = q_1 \cdots q_n$$

for irreducible elements p_i and q_j. Then we will prove that $m = n$ and there exists permutation giving the index a correspondence. Without loss of generality, set $m \geq n$, then for q_1 we have $q_1 | p_1 \cdots p_m$ by equality, (2) properties implies $k_1 \in \{1, .., m\}$ such that $q_1 = p_{k_1} u_1$ with $k_i \in \{1, ..., m\}$ and u_1 a unit, and then we plug it into the equality to cancellation

$$u_1 p_1 \cdots p_m / q_{k_1} = q_2 \cdots q_n q_n$$

repeating above process we can conclude n correspondences $q_i = p_{k_i} u_i$ with u_i a unit, take them in the equality we can get the follwoing equality by cancellation

$$u_1 ... u_n x = 1$$

where x is the product of the rest irreducibles q_j, $j \notin \{k_i | i = 1, ..., n\}$ which means $x = 1$, so $m = n$ otherwise 1 is a irreducible. The permutation here is clearly defined by $\sigma(i) = k_i$

$$q_1 \cdots q_n = p_{\sigma(1)} \cdots p_{\sigma(n)}$$

so we prove the uniqueness of factorization. ■

Remark It gives us the idea that how to prove a PID is a UFD: Firsly in PID each irreducible element is a prime ideal, then we need to prove that PID is a fractorization, and that is the difficult of the proof, it refers to the chain of ideal.

2.3 Polynomial

Polynomial is an important algebra structure, formal polynoimal is different with the function we meet, it can be seen as a vector space over a ring or a field.

Proposition 2.6 (Universal property) *Let R and A be two rings, let $\phi : R \to A$ a ring homomorphism. Then for any $a \in A$, there exists a unique ring homomorphism*

$$\Phi : R[X] \to A$$

such that $\Phi(X) = b$ and $\Phi(c) = \phi(c)$ for any $c \in R$.

$$\begin{tikzcd}
R \arrow[r, "\phi"] \arrow[d, hook, "i"'] & A \\
R[X] \arrow[ur, dotted, "\Phi"] &
\end{tikzcd}$$

Proof. ■

Remark This result can be generalize to a multvariable polynomial ring $R[X_1, ..., X_n]$, for any $a_1, ..., a_n \in R$ we can uniquely define a homomorphism. The proposition naturally shows that the polynomial ring over R is a **free commutative R-algebra** generated by the indeterminates.

Now if we take $A = R$ and ϕ is a identity map, then naturally we can obtain a ring homomorphism: **evaluation map** of an element $a \in R$

$$e_a : R[X] \to R, \quad P \mapsto P(a)$$

It is interesting to study the kernel of the morphism

$$\ker e_a = \{P \in R[X] : P(a) = 0_R\}$$

That means the set of polynomials having a root a. We are used to do the decompoistion of polynomial in according to the root: in $\mathbb{Z}[X]$, we can decompose

$$X^2 - 3X + 2 = (X - 2)(X - 1)$$

because 2 and 1 are the roots of the polynomial $X^2 - 3X + 2$ in R.

Proposition 2.7 *Let $P \in R[X]$ be a polynomial on a ring R, then a is a root of P if and only if $X - a$ divides $P(X)$ in $R[X]$, equiavlently*

$$\ker e_a = (X - a)$$

Proof. Two method, one is by divison of polynomial and it is very classic; theother is by homomorphism, here we use the second method to show that the structure is independent of divsion with remainder. If $X - a$ divides P, the result is trival.

Convserly, if P have a root a, then $\deg P \geq 1$ and

$$\begin{aligned} P(X) - P(a) &= \sum_{k \geq 1} c_k (X^k - a^k) \\ &= (X - a) \sum_{k \geq 1} c_K (X^{k-1} + ... + a^{k-1}) \end{aligned}$$

that means $X - a$ divides $P(X) - P(a) = P(X)$ ■

Corollary (Number of the root)
The polynomial on a ring with the degree n has at most n distinct roots

Corollary *Natural structure for a ring R and $a \in R$*

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

It is natural to study the arithemtic properties of polynomial ring, the beginning of the number theory is divison with reminder (Euclidean divison), simialrly we get the same result.

Theorem 2.8 (Euclidean Algorithm)
Suppose that R is a commutative ring (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 $\deg r < \deg f$ *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:

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

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 divison with remainder is well-defined on it, furthermore it will satisfy all arithemtic properties in $\mathbb{Z}$, in brief, it is a Euclidean domain with degree as its euclidean function

quotient ring as a k-algebra

In this section, we will talk about $K[X]$ a polynoimals ring on a field, so we can see it as a vector space over the field K, and clearly it is infinite-dimensional, simialrly ideal (P) can be seen as a subspace of $K[X]$, so quotient ring $K[X]/(P)$ can be seen as a quotient vector space.

Proposition 2.9 *Let $p \in K[X]$ a polynoimal with degree $n \geq 1$, then*

(1) $K[X]/(p)$ is a K-algebra with a base $\{\bar{1}, \bar{X}, ..., \bar{X}^{n-1}\}$.

(2) $K[X]/(p)$ is a field if and only if p is irreducible.

Proof. (2) The quotient ring is a field if and only if (p) is a maximal ideal, and $K[X]$ is a PID, by proposition 2.4 we can conlude the result. ■

This proposition is very fundamental and important, it shows many things, and the description is very elegant from my view, it gives a good beginning for field theory.

It is used to decomposed the vector space by direct sum, here we can simialrly do that by observing that $K[X]/(p)$ is a quotient ring at the same time.

Theorem 2.10 (Chinese reminder theorem)
Let $p_1, ..., p_n \in K[X]$ be polynomials pairwise coprime, then we have structure

$$K[X]/(p_1...p_n) \cong K[X]/(p_1) \times \cdots \times K[X]/(p_n)$$

Proof. It is immediately ■

2.3.1 primitive

Lemma 2.11 *If R is a UFD, then for any finite set $\{a_1, ..., a_n\}$ of R, their gcd (greatest common divisor) exists.*

Proof. ■

With above lemma, we can talk about one type of polynomial, which will be useful for us to determine the irreducibility of the polynoimal. In this section, any notation R denotes a UFD.

Definition 2.3 *Let $f \in R[X]$ a polynomial with the form*

$$f(X) = a_n x^n + \cdots + a_1 x + a_0$$

*where $a_0, ..., a_n \in R$, f is called **primitive** if $\gcd(a_0, a_1, ..., a_n)$ is a unit (or we can say that gcd associates with 1).*

usually we let $c(f) = \gcd(a_0, ..., a_n)$ be the **cotent** of polynoimal f. A natural decomposition of the polynoimal here is

$$f(x) = c(f)f'(x)$$

where f' is called adjoint polynoimal, and f' is primitive.

Proposition 2.12 *Let $f, g \in R[X]$, then $c(fg) = c(f)c(g)$ up to associate.*

Proof. ■

a classic result about irreducible polynomial in $\mathbb{Z}$ is to see it in $\mathbb{Q}$, i.e. see the polynoimal in the fraction field. For any UFD R, we make convent here $K = \text{Frac}(R)$, and then we can extend the properties of primitive polynoimal.

For any polynoimal $f \in K[X]$, there exists non-zero element $n \in R$ such that $nf \in R[X]$, then we can define the cotent of polynoimal in $K[X]$

$$c(f) := \frac{1}{n} c(nf)$$

the definition is independent of the choice of the n: for any two non-zero elements $m, n \in R$ such that $mf, nf \in R[X]$, we have

$$\frac{c(nf)}{n} = \frac{mc(nf)}{mn} = \frac{c(m)c(nf)}{mn} = \frac{c(nmf)}{nm} = \frac{c(mf)}{m}$$

which ensures the defniition of the cotent effective, so we can obtain the same propoerties in $K[X]$: $c(fg) = c(f)c(g)$ for any two polynoimals.

$$c(f)c(g) = \frac{c(n_1 f)}{n_1}\frac{c(n_2 g)}{n_2} = \frac{c(n_1 n_2 fg)}{n_1 n_2} = c(fg)$$

Then we can conclude some important properties.

Proposition 2.13 *in $K = Frac(R)$*

(1) polynoimals $p \in K[X]$ can be seen in $R[X]$ if and only if $c(f) \in R$.

(2) Let $f, g \in R[X]$ and $f|g$ in $K[X]$. If f is primitive, then $f|g$ in $R[X]$.

(3) non-constant polynomial f is irreducible in $R[X]$ if and only if f is irreducible in $K[X]$ and $f \in R[X]$ is primitive.

Proof. (1) For any $f \in K[X]$, we have decomposition $nf = c(nf)f'$ with f' a primitive polynoimal in $R[X]$, then we have a better form of decomposition

$$f = \frac{c(nf)}{n} f'$$

hence $f \in R[X]$ if and only if $\frac{c(nf)}{n} \in R[X]$, and we can prove the result by contradiction.

(2) If there exists $h \in K[X]$ such that $fh = g$, then $c(h) = c(f)c(h) = c(g) \in R$, by (1) $h \in R[X]$, so we finish the proof since $fh = g$ holds in $R[X]$.

(3) If f is irreducible in $R[X]$, then f must be primitive, otherwise $f = c(f)f'$ shows that f is not irreducible since $c(f)$ is not a unit. Then we suppose that f is not irreducible in $K[X]$, that means there exists $g, h \in K[X]$ with degree ≥ 1 such that $f = gh$, notice that (1) implies a unit $c(f) \in R$, then we can get a decomposition in $R[X]$

$$f = c(g)c(h)g'h' = c(f)g' \cdot h'$$

That means f is not irreducible in $R[X]$, contradiction with the assumption. Conversely, it is easy to see that f reducible in $R[X]$ implies f reducible in $K[X]$. ■

Remark Notice that primitive here is necessary, we can see the example that $f(X) = 2X + 2$, it is irreducible in $\mathbb{Q}[X]$ but not in $\mathbb{Z}[X]$ since $f(X) = 2(X + 1)$ and 2 is a irreducible in $\mathbb{Z}$.

Notice that $K[X]$ is a K-algebra, then it is surely a UFD, and each element in it can be uniquely decompoistion. However, we have seen that the irreducible element in $R[X]$ is similar to that in $K[X]$, so a good structure we can obtain.

Theorem 2.14 (Theorem of Transfert)
If R is a UFD, then $R[X]$ is a UFD, and the irreducible elements is one of two following possible:

- primitive polynoimals which is irreducible in $K[X] = Frac(R)[X]$.

- irreducible elements in R.

Proof. The irreducible elements is immediately from above propoerties (3). For any $P \in R[X]$, since $K[X]$ is a UFD, then there exists a unique fractorization

$$P = f_1 \cdots f_n$$

with irreducibles $f_i \in K[X]$, then there exists a primitive $f_i' \in R[X]$ such that $f_i = c(f_i)f_i'$, and f_i' is irreducible in $R[X]$ since $f_i/c(f_i)$ is still irreducible in $K[X]$. so we can have a decompoistion

$$P = c(P)f_1' \cdots f_n'$$

with $c(P) \in R$ by above propoerties (1), the decomposition is uniquely up to a unit in $K[X]$, when we review it in $R[X]$ the decompoistion is still uniquely: If P is primitive i.e. $c(P)$ is unit, then P is the product of irreducibles $f_1', ..., f_n'$ uniquely up to a unit; If P is not primitive i.e. $c(P)$ is not unit, UFD ring R implies a unique decompoistion $c(P) = p_1, ..., p_n$ with p_i the irreducibles in R, so P is the product of irreducibles $p_1, ..., p_n, f_1', ..., f_n'$ uniquely up to a unit. ■

2.3.2 Irreducibility

It is difficult topic to determine whether a polynoimal is irreducibile or not, there are many different methods to determine that, in this section we collect them and focus on the specific examples, in this section we make convention that **"polynoimals" means non-constant polynoimals.**

One method is to consider the root of the polynoimal, this method is very effective for low degree polynoimal.

Proposition 2.15 (Root and irreducibile)
Let $f \in R[X]$ be a polynoimal, then

- If f having a root $a \in R$, then f is not irreducibile.

- Let R be a field and $\deg f \leq 3$, then f is irreducible if and only if f has no root in R.

Proof. ■

we give a counterexample to reflects the restriction of the method.

Example 2.2 *Consider $f(X) = X^4 + 2X^2 + 1 \in \mathbb{Q}[X]$, notice that*

$$f(X) = (X^2 + 1)^2$$

so $f(X)$ has no root in $\mathbb{Q}$ and $\deg f > 3$. It is a good example show that the method of root is not complete, usually we really know what exactly what the root is (in $\mathbb{C}$), but we do not know the polynoimal is irreducibile or not.

About the root of the polynoimals, we have a useful technic to determine the form of rational root.

Proposition 2.16 (Rational root)
Let $f(X) = a_0 + a_1 X + \cdots + a_n X^n \subset \mathbb{Q}[X]$ with intger coefficient, then

-If $\dfrac{p}{q}$ is a rational root of f with p, q coprime, then $p|a_0$ and $q|a_n$.

-If f is monic ($a_n = 1$), then all rational roots must integers.

Proof. Take $X = p/q$, then we can rewrite

$$-a_n p^n = q(a_0 q^{n-1} + a_1 q^{n-2} p + ... + a_{n-1} p^{n-1})$$

then $q| - a_n p^n$ with p a prime number, by Euclid's lemma we get $q|a_n$. Simialrly, p divides right term, which implies $p|a_0$. ■

Example 2.3 *Let $f(X) = 6x^3 - 11x^2 - 3x + 2 \in \mathbb{Q}[X]$. By rational root, if p/q is a root of f, then possible choices of p are ± 1 or ± 2, the possible choices of q are ± 1, ± 2, ± 3 or ± 6, we try the integer root ± 1 and ± 2, then we can get $f(2) = 0$, so f is not irreducibile.*

Local methods is one type of important methods, determining reducibility from the definition involves traversing all possible combinations within an algebraic system, whereas local methods restrict the system to a relatively smaller algebraic structure, making the judgment easier.

Proposition 2.17 (Guass's Lemma)
Let $f \in \mathbb{Z}[X]$ be a prmitive polynoimal, then f is irreducibile in $\mathbb{Q}[X]$ if and only if f is irreducibile in $\mathbb{Z}[X]$.

Proof. Immediately from proposition 2.13. ■

Example 2.4 *$f(X) = X^4 + 1$ is irreducibile in $\mathbb{Q}[X]$. By Gauss's lemma, we just need to show that f is irreducibile in $\mathbb{Z}[X]$. Firsly, f has no real root, so there exists no linear term $X - a$ divides f in $\mathbb{Z}$, so the unique possible to factor is that*

$$X^4 + 1 = (X^2 + aX + b)(X^2 + cX + d)$$

then we can get $a + c = 0$, $d + ac + b = 0$, $ad + bc = 0$ and $bd = 1$. We solve it in $\mathbb{Z}$ then we can get $a^2 = \pm 2$, so f must be irreducibile in $\mathbb{Z}$.

Furthermore, a good local object is $\mathbb{F}_p$ finite field, in it caculation will be easier, so we can do more.

Proposition 2.18 *Let $f \in \mathbb{Z}[X]$ be a monic polynoimal, then f is irreducibile in $\mathbb{Z}[X]$ if $\bar{f}$ is irreducibile in $\mathbb{F}_p$.*

Proof. Suppose that f is not irreducibile in $\mathbb{Z}[X]$, then there exists two polynoimals $g, h \in \mathbb{Z}[X]$ with degree ≥ 1 such that $f = gh$, then mod p we can get $\bar{f} = \bar{g}\bar{h}$. Notice that monic polynoimal f ensures that $\bar{g}$ and $\bar{h}$ are the non-constant polynoimals in $\mathbb{F}_p[X]$, so $\bar{f}$ is not irreducible in $\mathbb{F}_p$, the original statement follows from the contrapositive. ■

In finite field, it is easy to classify the irreducible polynoimals by testing root or try decompoistion, then it reflects the different irreducible polynoimals in $\mathbb{Q}[X]$.

Example 2.5 *consider all irreducibles of low degree on* $\mathbb{F}_2[X]$

degree 2: $x^2 + x + 1.$
degree 3: $x^3 + x + 1; \quad x^3 + x^2 + 1.$
degree 4: $x^4 + x^3 + 1; \quad x^4 + x + 1; \quad x^4 + x^3 + x^2 + x + 1.$

according to that we can determine that polynoimal like $99x^2 + 37x + 3$ *is irreducible, it is quite easy by local method instead of compute roots. Notice in this case* $x^4 + x^2 + 1$ *is not irreducible, that is by* ***freshman's dream equation***

$$x^4 + x^2 + 1 = (x^2 + x + 1)^2$$

a general local method is Eisenstein criterion, the irreducible of a polynoimal under depends the behavior of coefficients in a finite field (local).

Theorem 2.19 (Eisenstein criterion)
Let $f(X) = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Z}[X]$ *be a polynoimal, if the cofficients satisfy*

- $a_n \neq 0 \bmod p$

- $a_i = 0 \bmod p$ *for any* $i < n$

- $a_0 \neq 0 \bmod p^2$

where p *is a prime, then* f *is irreducibile in* $\mathbb{Q}[X]$.

Proof. By Gauss's lemma and local method, we just need to prove that f is irreducible in $\mathbb{F}_p[X]$. We suppose that f is not irreducible in $\mathbb{Q}[X]$, then there exists two polynoimals $g, h \in \mathbb{Z}[X]$ with degree ≥ 1 such that $f = gh$, then mod p we have

$$\bar{g}\bar{h} = \bar{f} = \bar{a_n}X^n$$

that means $\bar{f}$ is not irreducible in $\mathbb{F}_p[X]$, so the reasonable factorization is $\bar{g} = \bar{a_n}X^k$ and $\bar{h} = X^l$ with $k + l = n$ and $k, l > 0$. We let

$$g(X) = a_nX^k + b_{k-1}X^{k-1} + \cdots + b_0$$
$$h(X) = X^l + c_{l-1}X^{l-1} + \cdots + c_0$$

with b_j, c_j equal to zero mod p, then observe that the constant term of gh is $a_0 = b_0c_0 \equiv 0 \mod p^2$, which contradicts with the condition, so the only possible decompoistion is $\bar{g} = a_n$ and $\bar{h} = X^n$ which leads to that $\bar{f}$ is irreducible, contradiction happens. ■

3 Field Theory

To study the structure of the field, consider a natural map: Let K be a field

$$\phi : \mathbb{Z} \to K, \quad 1 \mapsto 1_K$$

It is a well-defined homomorphism, which invites a ideal of $\mathbb{Z}$

$$\ker \phi = \{n \in Z | n \cdot 1_k = 0_k\}$$

By the structure of $\mathbb{Z}$, so there exists a integer $p \in \mathbb{Z}$ such that $\ker \phi = p\mathbb{Z}$,which gives the definition of the characteristic of the field.

Definition 3.1 *For any field K, we define $\mathrm{char}(K)$ be the characteristic of the field: either 0 or the smallest integer $n \in \mathbb{N}$ such that $n \cdot 1_k = 0$, by the natural map equivalently*

$$\begin{cases} \mathrm{char}(K) = 0 \iff \mathrm{im}\phi \cong \mathbb{Z} \\ \mathrm{char}(K) = p \iff \mathrm{im}\phi \cong \mathbb{Z}/p\mathbb{Z} \end{cases}$$

The characteristic of a field is either zero or a prime number. Suppose that $\mathrm{char}(K) = p \neq 0$, if $p = ab$ is not a prime, then we will get two zero divisor $a \cdot 1_K$ and $b \cdot 1_K$, but a field can not conatain any zero divisor, so p must be prime. An amazing thing in a field (or ring) with non-zero characteristic p is that we can write a equation

$$(x + y)^p = x^p + y^p$$

it has an interesting name: **freshman's dream**, this is an equality that would be written by someone who has studied very little mathematics or is just beginning to learn it.

Another natural map is **Frobenius endomorphism**, let K be a field with non-zero characteristic p, then we define

$$\sigma : K \to K, \quad x \mapsto x^p$$

It is a well-defined injective field homomorphism, so it is a endomorphism, but it is not necessary surjective.

Example 3.1 *Consier $K = \mathbb{F}_p(x)$ a field of rational functions. $\mathrm{char}(K) = p$ since $\mathrm{im}\phi = \mathbb{F}_p$, and it is easy to observe that there exists no $f \in \mathbb{F}_p(x)$ such that $f^p(x) = x$, so the Frobenius map here is not surjective.*

A good case is finite field, in that case frobenius endomorphism is furthermore a automorphism, so the frobenius map will be in Galois group and it reflects the structure of the finite field.

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, it is very clear after commutative ring:

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 princiapl 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, and it can be written as $K(c)$.*

$$K(c) = \{a_0 + a_1c + ... + a_kc^k | a_1, ..., a_k \in K, k = \deg f - 1\}$$

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 3.2 *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 commute diagram to finish.

$$\begin{tikzcd}
K[X] \arrow[r, "h"] \arrow[d, "h'"'] \arrow[dr, "\pi"'] & K[a] \\
K[a'] & K[X]/I \arrow[l, "\simeq"'] \arrow[u, "\simeq"]
\end{tikzcd}$$

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

■

3.1.1 splitting field

Theorem 3.6 (Kronecker) *If K is a field and $f \in K[X]$, then there exists a field L containing K as a subfield and with $f(X)$ a product of linear polynomial in $K[X]$.*

By Kronecker's theorme, we deduce a larger field where f can be decomposed completlely, so it is meaningful to define the field

Definition 3.3 *Let L/K be a field and $f \in K[X]$.*

- f splits over L/K if there exists $c, a_1, ...a_n \in K$ such that

$$f(x) = c(x - a_1) \cdots (x - a_n)$$

with $n = \deg f$.

- L/K is called a splitting field of f over K if it is the smallest field such that f splits.

The existence of the splitting field is ensured by above theorem, since for any $f \in K[X]$, we can obtain a field extension L/K such that f splits, and then $K(a_1, ..., a_n) \subset L$ as a splittin field.

4 Linear algebra: Bilinear form

In this section E is always a vector space over a field K.

Definition 4.1 *Let E be a vector space over a field K, we define a bilinear form on E as a application $B : E \times E \to K$ which satisfies the linear properties: for any $x \in E$, application $B(x, \cdot)$ and $B(\cdot, x)$ are all linear.*

Remark The matrix representation of a bilinear form can be deduced as following: Suppose that B is a bilinear form over a finite-dimensional space E, and $\{e_1, ..., e_n\}$ is a base for E, then for any $x, y \in E$, we have

$$x = x_1e_1 + ... + x_ne_n$$
$$y = y_1e_1 + ... + y_ne_n$$

then for $B(x, y)$ we can fix x such that

$$\begin{aligned} B(x, y_1e_1 + ... + y_ne_n) &= y_1B(x, e_1) + ... + y_nB(x, e_n) \\ &= (B(x, e_1), ..., B(x, e_n)) \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \end{aligned}$$

Here we decompose x then we can get for any $i = 1, ..., n$

$$\begin{aligned} B(x, e_i) &= B(x_1e_1 + ... + x_ne_n, e_i) \\ &= (x_1, ..., x_n) \begin{pmatrix} B(e_1, e_i) \\ \vdots \\ B(e_n, e_i) \end{pmatrix} \end{aligned}$$

Hence under a base $\mathcal{E} = \{e_1, ..., e_n\}$ a bilinear form can be denoted by

$$B(x, y) = x^tAy$$

here $A = (B(e_i, e_j))_{1 \leq i,j \leq n}$, it is Gram matrix when A satisfies certain condition (symmetric and positive).

We define $\mathrm{BL}(E)$ be the set of all bilinear form on E, by adding the normal opreations of function, we can verify that $\mathrm{BL}(E)$ actually a vector spoace over K, the idea of the definition is to consider a natural decompoistion like that any function can be written as the sum of odd function and even function:

$$B(x, y) = \frac{1}{2}(B(x, y) + B(y, x)) + \frac{1}{2}(B(x, y) - B(y, x))$$

Definition 4.2 *Let B be a bilinear form on E,*

-B is symmetric if for any $x, y \in E$ we have $B(x, y) = B(y, x)$, and we define $\mathrm{BLS}(E)$ as the set of all symmetric bilinear forms.

-B is anti-symmetric if for any $x, y \in E$ we have $B(x, y) = -B(y, x)$, and we define $\mathrm{BLA}(E)$ as the set of all anti-symmetric bilinear forms.

It is easy to verify that $\mathrm{BLS}(E)$ and $\mathrm{BLA}(E)$ are the subspace of $\mathrm{BL}(E)$, which allows us to say more about the bilinear form, we can conclude the following propoerties.

Proposition 4.1 (The structure of the bilinear form)
Let K be a field with $\mathrm{char}(K) \neq 2$ and B is a bilinear form on E, then

-(alternating) B is anti-symmetric if and only if $B(x, x) = 0$ for any $x \in E$.

-(decompoistion) $\mathrm{BL}(E) = \mathrm{BLS}(E) \oplus \mathrm{BLA}(E)$

-(matrix) If E is a n-dimensional space, then we have the following structure

$$\begin{cases} \mathrm{BL}(E) & \cong M_n(K) \\ \mathrm{BLS}(E) & \cong S_n(K) = \{A \in M_n(K) | A^t = A\} \\ \mathrm{BLA}(E) & \cong A_n(K) = \{A \in M_n(K) | A^t = -A\} \end{cases}$$

Proof. ■

Notice that for a field with characteristic 2, the situation will be complicated, that is because $\frac{1}{2}$ makes no sense in this field, hence we can not use the decompoistion. Moreover, in this case we will find that anti-symmetric form is just symmetric form by observing that $-1 = 1$ in this field, so the decompoistion will dependend on alternating form.

Lemma 4.2 *If K is a field with characteristic 2 and B is a bilinear form,*
(1) B is alternating, then B is anti-symmetric.
(2) When $\mathrm{Char}(K) = 2$, B is anti-symmetric if and only if B is symmetric.

Proof. (1) Let $x, y \in E$, suppose B is alternating then we can caculate

$$\begin{aligned} 0 = B(x + y, x + y) &= B(x, x) + B(x, y) + B(y, x) + B(y, y) \\ &= B(x, y) + B(y, x) \end{aligned}$$

so B is anti-symmetric: $B(x, y) = -B(y, x)$.

(2) Notice that in this field $1 + 1 = 0$, which implies $B(x, y) = B(y, x)$ if and only if $B(x, y) = -B(y, x)$. ■

Proposition 4.3 *If K is a field with characteristic 2, then for any bilinear form B onn E, there exists an unique decompoistion such that*

$$B = B_a + B_d$$

where B_a is an alternating form: $B_a(x, x)$ for any $x \in E$; B_d is a diagonal form: $B(x, y) = 0$ for any $x \neq y$ in E.

Proof. We define D be a diagonal form with $D(x, x) = B(x, x)$ and $D(x, y) = 0$ if $x \neq y$. then we can get a bilinear form $A = B - D$, notice that $A(x, x) = B(x, x) - D(x, x) = 0$, which implies that A is alternating. Hence we get our decompoistion $B = A + D$.

To prove the uniqueness, we suppose that A' and D' be another pair bilinear form such that $B = A' + D'$, then we must have $L = A - A' = D' - D$, $A(x, x) = 0$ since $A - A'$ is still alternating, and $L(x, y) = 0$ if $x \neq y$ since $D - D'$ is still diagonal.

■

One of the classic bilinear form is inner product, it will be an important tool to study different space. Here we give it a formal definition.

Definition 4.3 *Let E be a vector space over K - An application $B : E \times E \to K$ is sesquilinear form if it is linear on one argument.*

-If $K = \mathbb{R}$, an real inner product is a symmetric and definite positive sesquilinear form, usually we use $\langle \cdot, \cdot \rangle$ to denote.

*-If $K = \mathbb{C}$, B is a **Hermite form** if $B(x, y) = \overline{B(y, x)}$; an complex inner product is a Hermite and definite positive sesquilinear form.*

*- An inner product space is a vector space equipped by an inner product; espcailly, If the vector space over field $\mathbb{R}$ or $\mathbb{C}$, we call a complet inner product space as **Hilbert space**.*

*- **Euclidean space** is finite-dimensional real inner product space.*

Remark By the representation of the matrix, inner product can be described as following:

-If $K = \mathbb{R}$, $\langle \cdot, \cdot \rangle$ is an inner product if there exists a symmetric ($A^t = A$) and definite positive matrix A such that $\langle x, y \rangle = x^t Ay$.

-If $K = \mathbb{C}$, $\langle \cdot, \cdot \rangle$ is an inner product if there exists a Herimitian ($\overline{A^t} = \overline{A}^t$) and definite positive matrix A such that $\langle x, y \rangle = \bar{x}^t Ay$

Although the definition of the inner product just need sesquilinear form, but we can prove that togther with other condition, inner product can be a bilinear form.

Proposition 4.4 *Let $\langle\cdot,\,\cdot\rangle$ be an inner product on E,*

- If $K=\mathbb{R}$, $\langle\cdot,\,\cdot\rangle$ is a bilinear form.

- If $K=\mathbb{C}$, $\langle x,\,ay+bz\rangle=\bar{a}\,\langle x,\,y\rangle+\bar{b}\,\langle x,\,z\rangle$ for any $x,y,z\in E$ and $a,b\in\mathbb{C}$.

Proof. ■

4.1 Orthogonal opreator

Let $(E,\langle\cdot,\,\cdot\rangle)$ be a Euclid Space

Definition 4.4 *A linear opreator $f\in\mathcal{L}(E)$ is orthognal if for any $x\in E$*

$$\|f(x)\|=\|x\|$$

sometimes we call the map ”isometry”, it is a important map for a solid motion since it preserves the distance.

Proposition 4.5 *The following statement is equiavlent:*
(1) f is a orthognal opreator.
(2) f changes an orthonormal base to be another orthonormal base.
(3) f changes any orthonormal base to be an orthonormal base.
(4) If $A=[f]_{\mathcal{B}}$ under some base, the column (or the row) of the matrix is composed by an orthonormal base.
() If $A=[f]_{\mathcal{B}}$ under some base, then $A\in\mathrm{GL}_n(\mathbb{R})$ and $A^t=A^{-1}$.

Proof. Suppose that ■

The determinate of the orthognal matrix must be ±1 since

$$|A|=|A^t|=|A^{-1}|=|A|^{-1}$$

Motivated from this we can define different matrix groups:

-Orthogonal group: $O_n(\mathbb{R}):=\{A\in\mathrm{GL}_n(\mathbb{R})|A^t=A^{-1}\}$

-Special Orthogonal group: $SO_n(\mathbb{R}):=\{A\in O_n(\mathbb{R})|detA=1\}$

The two groups satisfying $SO_n(\mathbb{R})\lhd O_n(\mathbb{R})$, and naturally we can define

$$O_n^-(\mathbb{R})=O_n(\mathbb{R})-SO_n(\mathbb{R})=\{A\in O_n(\mathbb{R})|detA=-1\}$$

The real eigenvalue of an orthognal opreator is ± 1, it is clear by

$$\|\lambda x\| = \|f(x)\| = \|x\|$$

However, an orthognal matrix is not necessary to be diagonalized, a typical example is

$$R_\theta = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

The eigenvalue of the matrix can be formulated by $e^{\pm i\theta}$, it gives the geometric sense of the complex number: rotation.

Example 4.1 (Orthogonal symmetry) *Suppose that F is a subspace of E, then there exists a orthognal decompoistion $E = F \oplus F^\perp$, an orthognal symmetry of F is a linear map defined by*

$$S_F : E \to E, \quad x + y \mapsto x - y$$

where $x \in F$ and $y \in F^\perp$ as the unique decompoistion. In particular, when $\dim F = 1$ the maps is actually a reflection with respect to a line. Orthognal symmetry is an orthognal opreator since

$$\|S_F(x+y)\|^2 = \|x-y\|^2 = \|x\|^2 + \|y\|^2 = \|x+y\|^2$$

under certain orthonormal base, orthognal symmetry can be reduced to the form

$$S_F \sim \begin{pmatrix} I_F & 0 \\ 0 & -I_{F^\perp} \end{pmatrix}$$

5 group 6/15

$(G, \cdot)$ IS A GROUP

Definition 5.1 (conjuation) *Let x, y be two elements of a group G, we say that this two elements are conjugated ($x \sim_c y$) iff there exists $a \in G$ such that $axa^{-1} = y$.*

It is easy to prove that conjugation actually is a relation of equivalence.

We can define a opreation, we can naturally define a operation like that

$$aS = a \cdot S = \{a \cdot s | s \in S\}$$

where a is an element of the group, and S is a subset of group. we call the set like this as "coset". Now we study what happens when S is a subgroup of G.

Question: aS is a subgroup if $S < G$?

Consider $G = (\mathbb{Z}, +)$, and subgroup $S = 3\mathbb{Z}$, we take $a = 1$, then

$$aS = 1 + 3\mathbb{Z}$$

It is not a subgroup, since any subgroup of $\mathbb{Z}$ is of the form $n\mathbb{Z}$.

Question: when aS is a subgroup? IFF $a \in S$. $aS = S$
If $as \in aS$, then clearly since $a \in S$ and $s \in S$, so $as \in S$.
If $s \in S$, $s = a \cdot a^{-1}s$, so we want $a^{-1}s \in S$ and it is clear.

Question: when $aS = bS$? IFF $b^{-1}a \in S$ or $a^{-1}b \in S$.

Question: We can define $a \sim b \iff a^{-1}b \in S$, then it is a relation of equiavlence?
If we take $s \in S$, then $[s] = \{x \in G | x \sim s\} = sS = S$.
If we take $a \notin S$, then $[a] = aS$.
So we can conlude that $aS \cap S = \emptyset$. We can generalize the result:
If $a \nsim b$, then $aS \cap bS = \emptyset$. otherwise $aS = bS$.
A immediate result is **theorem of lagrange**: If G is a group with S as a subgroup, if G is finite, then $|S|$ divides $|G|$. Hint: $|aS| = |bS|$ if $aS \neq bS$.

$$G = S \cup aS \cup bS \cup ....$$

Example 5.1 *Let $G = (\mathbb{Z}, +)$, take $S = 4\mathbb{Z}$, then we can find that*

$$G = 4\mathbb{Z} \cup (1 + 4\mathbb{Z}) \cup (2 + 4\mathbb{Z}) \cup (3 + 4\mathbb{Z})$$

6/4 —2 ; 10/4—-2

Question: $a \cdot S = S \cdot a$**? or any group is a normal group ?**

Ans: If ur group is abelian, then we always have this property. In other words, for two elements in an abelain group, they are not conjugated. for examples, $x \in G$, then we take $a \in G$

$$axa^{-1} = aa^{-1}x = x$$

the unique element conjougated with x is x itself, so that means,

$$G/\sim_c = G$$

Another case is that G **is not abelian.** In this case whether left coset equals to right coset depends on S. for example, $G = S_3$, and we consider two subgroup A_3 and $H = \{(1), (12)\}$.

$aA_3a^{-1} = A_3$? Yes! By sign.

$a = (13)$, $aH = \{(13), (13)(12) = (123)\}$ and $Ha = \{(13), (12)(13) = (132)\}$, so $aH \neq Ha$!

Proposition 5.1 *There are some equiavlent definition for normal group* $N \lhd G$

- $aN = Na$ for any $a \in G$.
- $aga^{-1} \in N$ for any $a \in G$ and $g \in N$.
- If we can find a group morphism $\phi : G \to H$ such that $\ker \phi = N$.

Definition 5.2 *Let* $(G, \cdot)$ *be a group and* X *be a set, a group action means that a group* G *acts on a set* X*, and we denote it by* $G \circlearrowleft X$*, it relates to a binary operation*

$$(\cdot * \cdot) : G \times X \to X, \quad (g, x) \mapsto g * x$$

which satisfies:

(identity) $e * x = x$ *for any* $x \in X$.

(associative law) $(g \cdot h) * x = g * (h * x)$.

Example 5.2 $X = G$ *a simple case.* $g * x = g \cdot x$ *in this case. Let us look at map*

$$\sigma_g : G \to G, \quad x \mapsto g \cdot x$$

we call this map " translate action by g". So we can consider $\phi(g) = \sigma_g$

$$\phi : G \to ?$$

$? = S_G = \{$*all bijection from G to G*$\}$*!* ***(Here u should verify*** σ_g ***is bijective)*** *If G is finite with* $|G| = n$*, then clearly* $S_G \cong S_n$*.*

We can veirfy that ϕ *is a group morphism:*

$$\begin{aligned} \phi(a \cdot b) &= \sigma_{a \cdot b} \\ &= \sigma_a \circ \sigma_b \\ &= \phi(a) \circ \phi(b) \end{aligned}$$

WE need to prove that $\sigma_{a\cdot b} = \sigma_a \circ \sigma_b$. So we get a beautiful group morphism:

$$\phi : G \to S_G, \quad g \mapsto \sigma_g$$

You can prove that this morphism is injective, so by The first isomorphism theorem, we can conclude ***Calay theorem***

$$G \cong \phi(G) < S_G$$

We jump out of the example, we can define the **permutation representation** of a group action $G \circlearrowleft X$ as a group morphism as following

$$\phi : G \to S_X, \quad g \to \sigma_g$$

where $\sigma_g : X \to X$ by $\sigma_g(x) = g * x$. **(Here you should prove that σ_g is a bijection on X, and u can verify that ϕ is a group morphism)**

SOME DEFINITION DERIVED FROM representation

$$Stab(x) = \{g \in G | g * x = x\} = \{g \in G | \sigma_g(x) = x\}$$

We can describe stabiliser of x by the set of transalation action which contains x as a fixed point.

$$\{\sigma_g \in S_X | \sigma_g(x) = x\}$$

correspondence between g and σ_g.

$$Orb(x) = \{g * x | g \in G\} = \{\sigma_g(x) | g \in G\}$$

Hence orbite of an element x means the image of different translation actions on x.