2022.9.14 Lec1-2

Category perspective = (Objects, functions between objects).

A set S is a collection of elements (in some universe), s.t. any x is exactly $\begin{cases} ① \text{ In the set} \\ ② \text{ not in the set} \end{cases}$

A function f between sets A and B $f: A \to B$ is a rule in which every elements a in A is assigned exactly element in B, typically $f(A)$, a^f, $a(f)$, af

Goal: add an operation or 2 to sets.

Q: ① how do we characterize objects?

② What are the functions.

Groups: the nicest object to study with only one operation.

Q: what is the simplest sets to study with only one operation?

Def: A (binary) operation on a set S is of the form:

$\star : S \times S \to S$ (go back to S.)

the operation satisfies the closure axiom (implicitly implied in definition)

Def: A megma is a set M equipped with a (binary) operation

$\star : M \times M \to M$. that satisfying the closure axiom.

Q: what is a good definition for a function between magmas?

$(M, \star)$ is a magma.

$(N, \cdot)$ is another magma

We say a function $f: M \to N$ preserves the binary operation (or, is a function between magmas) iff $f(a \star b) = f(a) \cdot f(b)$ $(a, b \in M)$

Q: Is the empty set a magma? Yes, maybe.

Groups: What are the prototypes / number system that groups were based on?

$\mathbb{Z}$ = integers = $\{0, \pm 1, \pm 2, \cdots\}$

$\mathbb{N}$ = natural numbers = $\{1, 2, 3, \cdots\}$

$\mathbb{R}$: real numbers.

Def: A group is a (nonempty) set G equipped with a binary operation

$+/\cdot : G \times G \to G$, satisfying

0. Closure = if $a, b \in G \Rightarrow a \cdot b \in G$. (Implied Implicitly)
1. Associativity = if $a, b, c \in G \Rightarrow (a \cdot b) \cdot c = a \cdot (b \cdot c)$
2. Identity = $\exists e \in G$, s.t. $\forall a \in G$, $a \cdot e = a = e \cdot a$.
3. Inverses = If $a \in G$, then $\exists b \in G$, s.t. $a \cdot b = b \cdot a = e$.

Def: A group is called commutative (or abelian) if the binary operation is commutative, i.e.

4. $a \cdot b = b \cdot a$, $\forall a, b \in G$.

Q: What are the functions between groups that preserve the group structure?

Def: Let $(G, \star)$ and $(H, \cdot)$ be two groups, we say that a map of sets $f: G \to H$ is a group homomorphism iff $f(a \star b) = f(a) \cdot f(b)$ $\forall a, b$.

Q: Do we need to state $f(e_G) = e_H$? $f(a \star e_G) = f(a) \cdot f(e_G) = f(a) \Rightarrow f(e_G) = e_H$

Q: Is the identity unique in a group G? $e \cdot e' = e = e'$

What questions about groups help us build intuition?

- What is the best way to describe the structure of a particular example of a group?
- How do we classify all groups?

2022.9.15 Lec3

- How do we describe the possible homomorphism between groups?

Last time: we spoke about group homomorphisms as set functions.

$f: G \to H$ on the groups. $f(g_1 g_2) = f(g_1) f(g_2)$

we saw that for any homomorphism, $f(e) = e$. 也证明了 $f^{-1}(a) = f(a^{-1})$

注 $(ba)c = b(ac) \Rightarrow c = b$ 依赖于 associativity, 即 uniqueness of inverse depends on associativity

Examples:

Commutative examples:

$(\mathbb{Z}/\mathbb{R}/\mathbb{Q}/\mathbb{C}, +)$

$(\mathbb{Z}/m\mathbb{Z}, +)$

commutative non-example:

$(\mathbb{Z}, \cdot)$ 没有逆元.

$(\mathbb{Q}, \cdot)$ 0有问题

non-commutative example:

$GL_n(\mathbb{Q})$ ← $\mathbb{R}, \mathbb{Z}/m\mathbb{Z}$

$GL_n(\mathbb{Z})$ ← 可补充要求 $\det = \pm 1$

2022.9.21 Lec4-5

Groups acting on sets:

Permutation groups:

$\mathbb{N}_n = \{1, 2, \cdots, n\}$

Define a permutation as a bijection of $\mathbb{N}_n$, i.e. a 1-1 mapping (function of sets).

$\{1, 2, \cdots, n\} \xrightarrow{\sigma} \{1, \cdots, n\}$, s.t. $\sigma(a) = \sigma(b) \Rightarrow a = b$.

or s.t. $\forall y \in \mathbb{N}_n, \exists x \in \mathbb{N}_n$, s.t. $\sigma(x) = y$.

The set of all permutations of $\mathbb{N}_n$ is denoted S_n "symmetric group"

Need to show it's a group

Operation: composition of functions

$\mathbb{N}_2 = \{1, 2\}$ $1 \to 1$, $2 \to 2$; $1 \to 2$, $2 \to 1$ abelian!

$S_2 = \{\varepsilon, \sigma\}$

$\circ$	ε	σ
ε	ε	σ

"cycle notation" $(1,2)$

In cycle notation, there are many different ways to represent the same notation.

$N_3 = \{1,2,3\}$ $\quad id,\ (23),\ (12),\ (13),\ (123),$

not commuting $\quad (123)\circ(12) = (13)$

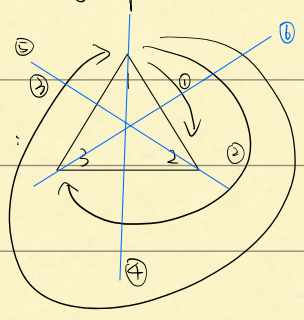
$\tau \quad \sigma$

$\neq$ $\quad \tau\circ\sigma(x) = \tau(\sigma(x))$ 从右往左.

$(12)\circ(23) = (23)$

为有S_3更多换的 n>3时可以直接用这个

Dihedral groups: rotations and reflections of a regular n-gon



① : (123) ④ : (23)

② : (132) ⑤ : (13)

③ : id ⑥ : (12)

$D_3 \cong S_3$.

notation of $D_n = \langle \sigma, \tau \rangle$

σ: rotation of $\frac{360°}{n}$ degree $\quad$ τ: one of the reflections

Example of creating new groups from old group

Direct Product: $(G,\cdot)$, $(H,\star)$

$G \times H = \{(g,h) \mid g \in G,\ h \in H\}$

$(G\times H, *)$ $\quad (g,h)*(g',h') = (g\cdot g', h\star h')$

Exercise: $G\times H$ is a group.

Q: How can we tell that a group G is secretly a direct product?

Def: A subgroup H of $(G,\cdot)$ is a (nonempty) subset of G that forms a group under $\cdot$.

Subgroup criterion: $H \le G \iff$

① non-empty

② $a,b\in H \Rightarrow ab^{-1}\in H$

Proof of "$\Leftarrow$"

H nonempty $\Rightarrow \exists h\in H,$

$\Rightarrow hh^{-1}=e\in H \Rightarrow$ 幺元

Associativity 从 G 中继承.

$a=e,\ b=h \Rightarrow eh^{-1}=h^{-1}\in H \Rightarrow$ 逆元

If $a,b\in H \Rightarrow b^{-1}\in H \Rightarrow a(b^{-1})^{-1}=ab\in H \Rightarrow$ 封闭性.

Def: If $f: G\to H$ is a group homomorphism, define

$\ker(f)=\{g\in G \mid f(g)=e_H\}$ $\quad \mathrm{Im}(f)=\{h\in H \mid \exists g\in G,\ f(g)=h\}$

Prop: $\ker(f)$, $\mathrm{Im}(f)$ are subgroups of G and H.

Def: $\text{Center}(H) = Z(H) = \{a \in H \mid ax = xa, \forall x \in H\}$

exercise: $Z(H)$ is a subgroup of H.

$f: G \to H$

Note: the $\ker(f)$, If $g \in \ker(f)$, then $f(g) \cdot h = h \cdot f(g)$ $\forall h \in H$

$\Rightarrow f(g) = h \cdot f(g) h^{-1}$ $\forall h \in H$

$\forall h \in \text{im}(f)$, we have $f(x) = h$ for some h.

$\Rightarrow f(g) = f(x) f(g) f(x)^{-1}$

$e_H = f(g) = f(xgx^{-1})$

$\Rightarrow \forall x \in G$, $xgx^{-1} \in \ker(f)$ if $g \in \ker(f)$

Def: A subgroup $H \leq G$ is called normal if $\forall g \in G$,

$gHg^{-1} \subseteq H$

Theorem: Every normal subgroup is the kernel of some group homomorphism.

$N \trianglelefteq G$, $G \to H = G/N$.

Def: The order of G is $|G|$, the cardinality of underlying set.

A finite group: $|G| < \infty$. infinite ---

Q: What are all groups of order n?

Groups of order 1: $\{e\}$

Groups of order 2: $\{e, x\}$

	e	x
e	e	x
x	x	e

← $x^2 = x$ 不行

Group of order 3:

Group of order 4: $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ / C_4 or $C_2 \times C_2$.

↳ cyclic group of order n.

Group of order 5: $\mathbb{Z}/5\mathbb{Z}$

Group of order 6: $S_3 = D_3$.

Def: a group G is generated by $S \subseteq G$ if $\forall g \in G$, g can be written as a finite product of elements in S or their inverses (写了g就不需要加上g^{-1}了)

$D_n = \langle \sigma, \tau \mid \sigma^n = 1, \tau^2 = 1, \sigma\tau = \tau\sigma^{-1} \rangle$

S_n is generated by all simple transpositions (i.e., 2-cycles)

Def: the order of $g \in G$ is the smallest element n, s.t. $g^n = e$ (if n exists) or infinite (if n doesn't exist)

Ex. $(\mathbb{Z}, +)$, 1 is a generator, infinite order.

Def: An isomorphism between groups G, H, $f: G \xrightarrow{\sim} H$ or $G \cong H$ is a group homomorphism that is also a set bijection.

Def: A group is finitely generated if it can be generated by a finite set of generators.

Exs: D_n

All finite group.

non-Exs: $(\mathbb{Q},+)$ is not finitely generated

Def: A cyclic group is a group that can be generated by 1 element.

$G = \langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$

Properties of cyclic groups:

- abelian.
- any 2 cyclic groups of the same order (either ∞, nit) are isomorphic.
- every subgroup of a cyclic group is cyclic.

Classification of cyclic groups:

$\{\text{cyclic group}\} \Leftrightarrow \mathbb{N} \cup \{\infty\}$

阶被大小映射

Def: the order of $g \in G$ is the smallest element n, s.t. $g^n = e$ (if n exists) or infinite (if n doesn't exist)

Ex. $(\mathbb{Z},+)$, 1 is a generator, infinite order.

Classify finite generated abelian groups:

"primary decomposition":

Thm: If g is finitely generated abelian group. then

$G \cong \mathbb{Z}^n \times \mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \mathbb{Z}/p_2^{k_2}\mathbb{Z} \cdots \times \mathbb{Z}/p_n^{k_n}\mathbb{Z}$

p_i are all primes (not necessarily distinct) $n \geq 0$,

(Up to rearranging, this is a unique decomposition)

Ex. Order 4:

$(n=0)$ $\begin{cases} \mathbb{Z}/4\mathbb{Z} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \end{cases}$ $\Rightarrow$ Thm tells us we're done.

Another decomposition:

$G \cong \mathbb{Z}^n \times \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z}$ $\quad m_i \mid m_{i+1}$

"free part of G" the decomposition of G.

Group action

S_n = symmetric group on n letters acting on the set

$\mathbb{N}_n = \{1, \ldots, n\}$

Let S be a set, we can define

$\mathrm{Sym}(S)$ = group of bijections on the set (under composition)

Cayley's Thm:

Every group G is isomorphic to a subgroup of the symmetric group acting on G.

Pf: To any element $g \in G$, we associate the function

$f_g : G \to G. \quad x \mapsto gx$

need to show f_g is a bijection for it $\in \mathrm{Sym}(G)$

strategies: either show { f_g is both injective and surjective
$f_{g^{-1}}$ satisfies $f_g \circ f_{g^{-1}} = id = f_e = f_{g^{-1}} \circ f_g$

Assuming $gx = f_g(x)$, $gy = f_g(y)$ for $x, y \in G$.

$gx = gy \Rightarrow x = y$, injective.

$\forall\, y \in G$, $f_g(g^{-1}y) = y \Rightarrow$ surjective. $\Rightarrow$ f_g bijection

Let $K = \{f_g \mid g \in G\} \subseteq Sym(G)$

Remains to check: K is a subgroup

strategies: { subgroup criterion
we can illustrate K as the image subgroup inside of G of a group homomorphism.

Let $T: G \to Sym(G)$, $g \mapsto f_g$. 欲证 $T(g) \circ T(h) = T(g \cdot h)$

if $x \in G$, $f_g \circ f_h(x) = f_g(hx) = ghx = f_{gh}(x)$

Conclude that T is a group homomorphism.

$im(T) = \{T(g) \mid g \in G\} = \{f_g \mid g \in G\} = K \Rightarrow K$ is a group.

But, is $K \subseteq G$? or equivalently, is T injective?

T is injective, since $f_g = f_{g'} \Leftrightarrow \forall x,\ gx = g'x \Rightarrow g = g'$.

Take away: All groups G act on some set S (worst case, $S = G$)

? 为什么呢.

$G = S_3$ $|G| = 6$ $Sym(G) \leq S_6$

Left group action: If G group S set, a (right) left group action is a function $f: G \times S \to S$ ($f: S \times G \to S$) satisfying 2 properties:

(1) $f(e, s) = s$

(2) $f(g, f(h, s)) = f(gh, s)$

different notation: $\cdot : G \times S \to S$

(1) $e \cdot s = s$

(2) $g \cdot (h \cdot s) = (gh) \cdot s$

所以这里是个 monoid homo?

Another way to think about group actions: $G \to Fun(S)$ $(S \xrightarrow{fun} S)$

satisfying (1) (2).

(这里提到3-嘴, group homo 与 monoid homo 的定义是完全一样的, 因为我们在定义时不需要 inverse 这个条件).

If G does act on a set S, then G is a subgroup of $Sym(S)$

(Q: does (1) and (2) imply that the image of any element $g \in G$ under the map $G \to Fun(S)$ actually send g to a bijection? i.e. $\in Sym(S)$?)

G defines an equivalence relation on S:

$x \sim_G y \iff y = gx$ for some $g \in G$.

recall: equivalence { reflexive, symmetric, transitive } ✓

Def: If G is a group, acting on S, for any element $s \in S$,

let "G-orbit" of x, aka $Gx = \{g \cdot x \mid g \in G\}$

Exercise: The G-orbits form a partition of S.

Special Case: $H \leq G$, H acts on G.

If $x \in G$, then the H-orbits of x is $Hx = \{hx \mid h \in H\}$

$\Rightarrow$ partition.

If G is a finite group, $G = Hx_1 \sqcup Hx_2 \sqcup \cdots \sqcup Hx_n$ (不交的并)

If $x_i = e$, then $He = H$

We can show that $\forall x, y \in G$, $|Hx| = |Hy|$

note: this + partition implies $|H| \mid |G|$ $\forall H$

Define a function $Hx \to Hy$.

$$z \mapsto zx^{-1}y$$
$$hx \quad hy$$

To see its a bijection, Assume $z_1x^{-1}y = z_2x^{-1}y \Rightarrow z_1 = z_2 \Rightarrow$ 单

满也显然. $\Rightarrow |Hx| = |Hy|$

Cor: $x^{|G|} = e$.

If $f: G \to H$ homo

$\ker(f) = \{g \in G \mid f(g) = e\}$

$\text{im}(f) = \{h \in H \mid \cdots\cdots\}$

Every kernel is normal:

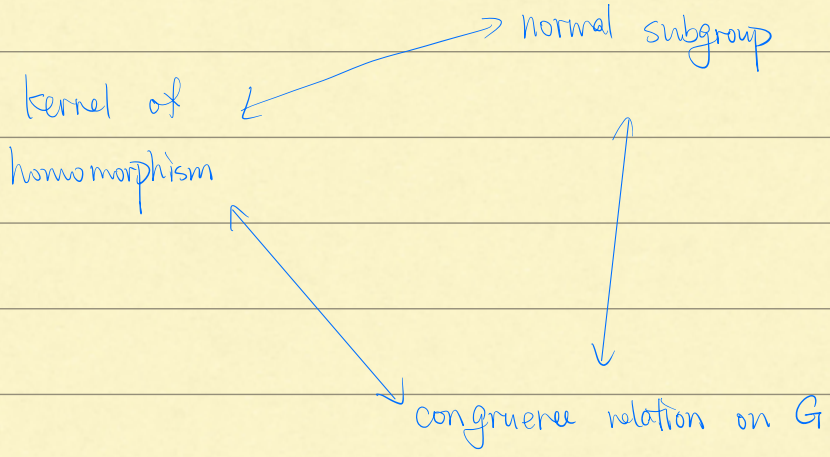
Def: A subgroup K is normal if $\forall g \in G$, $gkg^{-1} = K$.

Theorem: if $K \trianglelefteq G$, then $a \equiv b \pmod{K}$ defines a multiplicative

$\Leftrightarrow a^{-1}b \in K$.

equivalence relation $\quad a \equiv a' \pmod K,\ b \equiv b' \pmod K \Rightarrow ab \equiv a'b' \pmod K$

Conversely, any congruence relation "$\equiv$" on G defines a normal subgroup.



"$\Rightarrow$"

pf: If $a \equiv b \pmod K$, then $a^{-1}b \in K \Rightarrow b \in aK = \{ka \mid k \in K\}$

$\Rightarrow$
- reflective: $a a^{-1} = e \in K$
- symmetric: $a \equiv b \Rightarrow a^{-1}b \in K \Rightarrow b^{-1}a \in K \Rightarrow b \equiv a$
- transitive: $a \equiv b,\ b \equiv c \Rightarrow a^{-1}b,\ b^{-1}c \in K, \Rightarrow a^{-1}c \in K$.

至此证明了 normal 等价

multiplicativity: if $a \equiv a',\ b \equiv b', \Rightarrow a = a'k_1,\ b = b'k_2$.

要证 $ab \equiv a'b'$

$ab = a'k_1 b'k_2$. 即 $b'^{-1}k_1 b' = k_3 \in K \Rightarrow k_1 b' = b'k_3$

$\Rightarrow ab = a'b'k_3 k_2 \Rightarrow ab \equiv a'b'$.

"$\Leftarrow$": Assume we have $a \equiv$ on G,

Let K be the congruence class of 1.

i.e, $K = \{g \in G \mid g \equiv 1\}$ 下证 K normal sbgp.

① $\forall k_1, k_2 \in K,\ k_1 \equiv 1,\ k_2 \equiv 1 \Rightarrow k_1 k_2 \equiv 1 \Rightarrow k_1 k_2 \in K$. (性质) $\Rightarrow$ closed.

反正很好证是 subgroup.

下证 normal

$\forall g \in G,\ k \in K.\quad g^{-1}kg \equiv g^{-1}g \equiv 1 \in K$.

So $\vec{g}Kg = K$.

Def: If $K \trianglelefteq G$, $G/K = \{gK = Kg \mid g \in G\}$. $(gK)\cdot(hK) = gh\cdot K$.

↑ 陪集构成的集合.

Note: $eK = K$. $(gK)^{-1} = \vec{g}K$

Examples of normal subgroups:

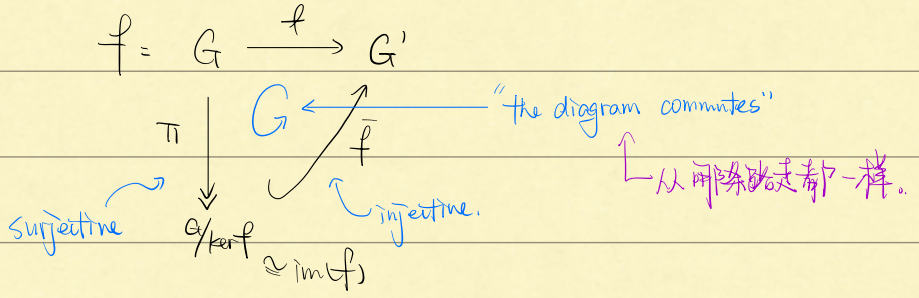
- $\{e\} \trianglelefteq G$
- $G \trianglelefteq G$
- center of the group
- 阿贝尔群的所有子群

Ex: $S_3 = \{e, (13), (23), (12), (123), (132)\}$

$\Rightarrow \{e, (12)\}$, $\{e, (23)\}$, $\{e, (12)\}$, $\{e, (123), (132)\}$, e, S_3 (index 2)

Fundamental Theorem of Group Homomorphisms:

If $f: G \to G'$, it can be "uniquely factored" into $f = \bar{f} \circ \pi$



Corollary: Surjective group homomorphisms are in 1-1 bijection with normal subgroups of G

pf of fund thm

We'll prove this by showing $G/\ker(f) \cong \mathrm{im}(f)$

$G/\ker(f) \xrightarrow{i} \mathrm{im}(f)$ $(K = \ker(f))$

$gK \xmapsto{i} f(g)$ 要先证这是 well-defined 的，不然把同一个陪集送到不同地方去.

Q: Is it well defined?

if $g_1K = g_2K$, $\overset{?}{\Rightarrow} f(g_1) = f(g_2)$?

$g_1K = g_2K \Rightarrow g_2^{-1}g_1K = K \Rightarrow g_2^{-1}g_1 \in K$ ✓

$f(g_2^{-1}g_1) = 1 \Rightarrow f(g_2) = f(g_2g_2^{-1}g_1) = f(g_1)$

Q: Is it a group homomorphism? ✓ 说明是 "i" 而不是 f.

recall that f is group homo, "$i(g_1K)\,i(g_2K) \overset{?}{=} i(g_1Kg_2K)$"

$i(g_1K)\,i(g_2K) = f(g_1)f(g_2) = f(g_1g_2) = g_1g_2K$. $\Leftrightarrow g_1Kg_2 = g_1g_2K \Leftrightarrow K = g_2Kg_2^{-1}$ ✓.

Q: Injective? Surjective?

Inj: if $i(g_1K) = i(g_2K) \Leftrightarrow f(g_1) = f(g_2)$

应该乘左边的. 为何得? $\Leftrightarrow f(g_1g_2^{-1}) = f(g_1g_2^{-1}) = e_G \Leftrightarrow g_1g_2^{-1} \in K$.

$\Rightarrow g_1g_2^{-1}K = K \Leftrightarrow g_1K = g_2K$

Surj: let "$\forall$" $y \in \mathrm{im}(f)$, $\exists x \in G$, s.t. $f(x) = y$

$i(xK) = f(x) = y \Rightarrow$ 对 $\mathrm{im}(f)$ surjective. 稍多于陪集引导词.

So $G/\ker(f) \cong \mathrm{im}(f)$ $\left(\begin{matrix} G \to G/\ker(f) \\ g \mapsto gK \end{matrix}\right)$

然后 $\mathrm{im}(f) \hookrightarrow G'$ injective since $\mathrm{im}(f) \leq G$,

$f(g) \mapsto f(g)$ 实质 inclusion function 罢了.

First Isomorphism Theorem:

Let $K \trianglelefteq G$.

$\{$subgroup of G containing $K\} \overset{1\text{-}1}{\Longleftrightarrow} \{$subgroups of $G/K\}$

"$\longrightarrow$" $H \longmapsto H/K$

"$\longleftarrow$" all elements of $G^{(H)}$ contained in cosets of S $\longleftarrow\!\shortmid$ $S \leq G/K$.

If $H \trianglelefteq G$, iff $H/K \trianglelefteq G/K$. $\iff G/H \cong \frac{G/K}{H/K}$.

Second Isomorphism thm:

Let $H \leq G$, $K \trianglelefteq G$,

Then $HK = \{hk \mid h \in H, k \in K\}$ is a subgroup of G containing K.

$H \cap K$ is a normal subgroup of H.

$HK/K \cong H/H\cap K$.

"choose" z to be in H.

$z \longmapsto z(H \cap K)$

pf of 2:

if zK is a coset of K in HK, if $z = hk$

The implicit claim by writing down the map $zK \mapsto z(H\cap K)$ is that if $z = hk$, then $zK = hK$.

① We will first show $HK \leq G$.

- $1 \in HK$ since $1 \in H$, $1 \in K$.
- if $hk \in HK$, then $(hk)^{-1} = k^{-1}h^{-1} \in Kh = hK$

  Fact: $\forall h$, $hK = Kh$
- Associativity inherited
- $h_1k_1h_2k_2 = h_1h_3k_3k_2 \in HK$.

  ↳ $hK = Kh \iff hkK = khK$.

② Now show $H \cap K \trianglelefteq H$

$\forall x \in H \cap K \subseteq K$, $\forall g \in G$, $gxg^{-1} \in K$.

if $g \in H$, then $gxg^{-1} \in H$ $\Rightarrow$ $gxg^{-1} \in K \cap K$, $\forall g \in H$.

idea: $H/H\cap K \cong HK/K$ "HUK" 最小 (小?) subgp.

It remains to show this is an isomorphism

$G \xrightarrow{\pi} G/K$, $g \mapsto gK$. restrict to H $\Rightarrow$ $H \xrightarrow{\pi_H} G/K$, $h \longrightarrow hK$? $\pi(h) = hK$, $= hekK$ $\in eK$ ← "HK"-coset of K.

if hkK is an HK-coset of K. $\Rightarrow$ $hkK = hK$

$\Rightarrow$ $\pi_H(h) = hkK$ So $\pi|_H$ is a surjective group homomorphism on HK/K.

By construction, $\ker(\pi) = K$,

Q: $\ker(\pi|_H)$? ⊆ 既在H中, 又在K中 (均为限制定义域)

↳ $= H \cap K$.

By fun thm of group homomorphism,

$H/H\cap K \cong HK/K$ ← RHS 为原始 image.

pf of ①: skip, (法雷对称的对偶) 2021.9.22.

Group Actions:

G acts on a set S if $\exists$ a map $\circ : G \times S \to S$

$(g, x) \mapsto g \circ x \in S$.

satisfies: ① $(1, x) \mapsto x$

② $(g_1, (g_2, x)) = (g_1 g_2, x) \Leftrightarrow g_1 \circ (g_2 \circ x) = (g_1 g_2) \circ x$.

Example: G acts on G by multiplication. $g \circ x = gx$

G acts on G by conjugation. $g \circ x = gxg^{-1}$

Def: If G acts on S, then the G-orbit of $x \in S$.

$$Gx = \{g \cdot x \mid g \in G\}$$

Ex (cont): ① $Gx = \{gx \mid g \in G\}$

② $Gx = \{gxg^{-1} \mid g \in G\}$

The G-orbit of $x \in G$ (under conjugation) is its conjugacy class.

We say an action of G on S is transitive if there is only one orbit.

$\Leftrightarrow \forall x, y \in S$, $\exists g$, s.t. $gx = y$.

Q: What if all conjugacy classes are singletons?

($S = G$, action = conjugation.)

$g \cdot x = gxg^{-1}$, $\Rightarrow \forall x$, $\forall g$, 有 $gxg^{-1} = x \Rightarrow G$ abelian.

$\Rightarrow$ if x has conjugacy class of size 1,

then x 与所有 g 交换 $\Leftrightarrow x \in Z(G)$

G acts on S, notation: $G \curvearrowright S$,

If $x \in S$, the $\mathrm{Stab}(x) = \{g \in G \mid g \cdot x = x\}$

↳ normal subgroup of G.

Theorem: If G acts transitively on S, and $H = \mathrm{Stab}(x)$ for some $x \in S$, then the action of G on S

is equivalent to action of G on the cosets of G/H.

First, we show that $\mathrm{Stab}(x) \leq G$.

- $\forall x \in S$, $e_G \in \mathrm{Stab}(x)$
- if $g_1, g_2 \in \mathrm{Stab}(x)$, $g_1 \circ x = x$, $g_2 \circ x = x$.

  $\Rightarrow (g_1 g_2) \circ x = x$.
- if $g \in \mathrm{Stab}(x)$, $g \circ x = x$

  $x = e \circ x = (g^{-1} g) \circ x = g^{-1} \circ (g \circ x) = g^{-1} \circ x \Rightarrow g^{-1} \in \mathrm{Stab}(x)$

Exercise: $\mathrm{Stab} \leq G$. → 这个好像不对，往下看

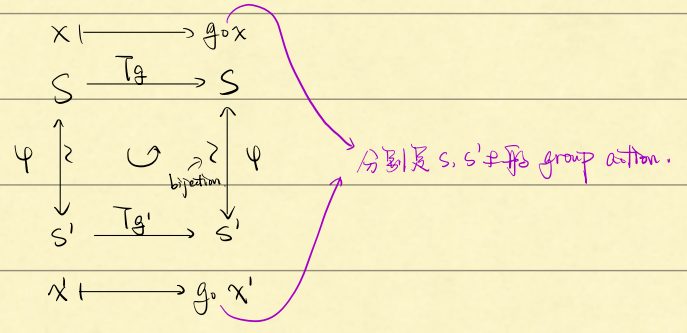
Def: We say that G acts on S, S' are equivalent if

$\exists$ bijection $S \xrightarrow{\varphi} S'$, s.t. $\varphi(g \circ x) = g \circ (\varphi(x))$

($g \circ x$: action on S; $g \circ (\varphi(x))$: action on S')

In the language of commutative diagrams:

If $g \in G$



The diagram commutes. i.e. $T_g = \varphi T'_g \varphi^{-1}$

Orbit-Stabilizer Theorem:

If $|G| < \infty$ acting transitively on S, then

$$|S| = [G : \mathrm{Stab}(x)] \quad , \forall x \in S$$

$[G:H]$ = number of cosets of H in G.

If G acts on S but isn't transitive, and G, S are both finite, then

$$|S| = \sum [G : \mathrm{Stab}(x)]$$

(sum: run over representatives of orbits.)

$g \in G,\ x \in S$

Note: $\mathrm{Stab}(gx) = \{h \in G \mid h \cdot gx = gx\}$

$\Rightarrow \{h \in G \mid g^{-1}hgx = x\}$

$= g\,\mathrm{Stab}(x)\,g^{-1}$

Theorem 1.10: Let $G \curvearrowright S$ transitively (G not necessarily finite). Let $H = \mathrm{Stab}(x)$ for some $x \in S$, then the action of G on S is equivalent to the action of G acts on the set of cosets G/H.

例: (Stab 不 G, 作用 transitively):

$S_3 = G$ $\quad S = \{(12), (23), (13)\}$

Conjugation by $(23) = g$

$(23)(12)(23) = (13)$. $\Rightarrow$ G acts on S transitively.

$\mathrm{Stab}(12) \neq \mathrm{Stab}(13)$

Pf: Fix $x \in S$, Consider the map $f_x : G \to S$

$g \mapsto g \cdot x$

G acts transitively, so f_x is surjective.

Define the set of equivalent classes on G by $\bar{g} = \{a \in G \mid f_x a = f_g\}$ ($ax = gx$)

$\Leftrightarrow \{a \in G \mid g^{-1}a\,x = x\}$

$\Leftrightarrow \{a \in G \mid g^{-1}a \in \mathrm{Stab}(x)\}$

$\Leftrightarrow \{a \in G \mid a \in g\,\mathrm{Stab}(x)\}$

Here, f_x induces a bijection from $\overline{G} = \{\text{cosets of } \mathrm{Stab}(x)\} \to S$

$g\,\mathrm{Stab}(x) \mapsto g \cdot x$

To see that these bijections for $x \in S$ give an equivalence of action by G, we need to see:

If $y \in G$, then $y(g\,\mathrm{Stab}(x)) = yg(\mathrm{Stab}(x)) \longmapsto ygx$

$f_x(ygg\,\mathrm{Stab}(x)) = ygx$

$f_x(y(g\,\mathrm{Stab}(x))) = y(gx)$

Notation: $\mathrm{Orb}(x) = \{gx \mid g \in G\} \in S$ (orbit of x)

$\mathrm{Stab}(x) = \{g \in G \mid gx = x\} \leq G$.

if G acts on G s.t. finite,

$S = \bigsqcup_{i=1}^{n} \mathrm{Orb}(x_i)$ orb 两两不相交.

$|\mathrm{Orb}(x)| = [G : \mathrm{Stab}(x)]$

↳ $|S| = \sum_{i=1}^{n} [G : \mathrm{Stab}(x)]$ Orbit-Stabilizer Thm

Application to conjugation action of G on itself

$G \curvearrowright G$ by conjugation,

For $x \in G$, $\mathrm{Stab}(x) = \{g \in G \mid gxg^{-1} = x\}$

$= \{g \in G \mid gx = xg\}$

$=$ centralizer of x

If $x \in Z(G)$, $\mathrm{Stab}(x) = G$

If G finite, $|G| = \sum_{i=1}^{n} [G : \mathrm{Stab}(x_i)]$

$= |Z(G)| + \sum_{i=1}^{n} [G : \mathrm{Stab}(x_i)]$ ← Class equation

How's such a class formula use? → number / combi

Thm: Any group G of prime power order has to have a non-trivial center

Pf: $|G| = p^k$ p prime.

$p^k = |Z(G)| + \sum [G : Stab(x_i)]$

↳ p-power group ↑ 都被 p 整除

Note: if G abelian, done.

if G not-abelian, $\exists\, y \in G$, $y \notin Z(G)$

↳ $\Rightarrow \exists\, z \in G$, s.t. $yz \neq zy$.

then $[G : Stab(y)] > 1$.

Sylow thm:

Assume G finite (not nec... abelian)

(I) If p is a prime number, and $p^k \mid |G|$, then G contains a subgroup of order p^k

Def: A p-sylow sbgp of G is any maximal p-power subgroup of G.

(II) ① Any p-sylow subgroups are conjugate in G

($\forall\, P_1, P_2$, $\exists\, g$, s.t. $gP_1g^{-1} = P_2$).

② # of p-sylow subgroups of g is

(a) $\equiv 1 \pmod p$

(b) divider $[G : P]$ ↖ 除掉所有 p 之后的那个数.

③ Any p-power subgroup is contained in some p-Sylow sbgp.

Pf: 2021.10.5

Sketch of (I):

Strategy: induct the size of $|G|$

base case: $|G|=1$. → true. $p^0 \mid |G|$ ← only

Strong induction: Assume true for any group G with size $< |G|$.

$$|G| = |Z(G)| + \sum [G : Stab(x_i)]$$

Case 1: $p \nmid |Z(G)|$

Since $p \mid |G| \Rightarrow \exists j$ s.t. $p \nmid [G : Stab(x_j)]$.

Recall, $G = |Stab(x_j)| \cdot [G : Stab(x_j)]$

$\Rightarrow p^k \mid |Stab(x_j)|$

We're assuming $x_j \notin Z(G) \Rightarrow Stab(x_j) \neq G$.

$\Rightarrow |Stab(x_j)| < |G| +$ ⇒ 归纳假设

$\Rightarrow$ 有 p^k subgroup. $\Rightarrow G$ 也有.

Case 2: $p \mid Z(G)$

Lemma: $p \mid Z(G) \Rightarrow Z(G)$ contains an element of order p.

$z \in Z(G)$, s.t. $z^p = 1$

$\langle z \rangle = \{ z^k \mid k \in \mathbb{Z} \} \trianglelefteq G$ 因为在 center 里

$p^k \mid |G| \Rightarrow p^{k-1} \mid G/\langle x \rangle$

$\Rightarrow G/\langle x \rangle$ has subgroup of order p^{k-1}

First isomorphism thm says $\exists H$ in G, is a subgroup s.t. $H/\langle z \rangle$ can be the description of the group of order p^{k-1}

Conclusion: $|H| = [H : \langle z \rangle] |\langle z \rangle| = p^k$

Thm: Suppose G group, $H, K \trianglelefteq G$, s.t. $H \cap K = \{e\}$

then $HK = \{hk \mid h \in H, k \in K\} \cong H \times K$

Recall: 2nd iso thm: $H/1 = HK/K$, $K/1 = HK/H$

Pf: HK is a subgroup of G, (more generally, if H is in the normalizer of K in G, then HK is a subgroup of G).

$HK \to H \times K$

$hk \to (h, k)$

↳ need it to be well-defined. if $h_1k_1 = h_2k_2 \Rightarrow h_2^{-1}h_1k_1 = k_2$.

$\Rightarrow h_2^{-1}h_1 = k_2k_1^{-1}$ ∵ $H \cap K = \{e\}$, so $h_1 = h_2$, $k_1 = k_2$

($h_2^{-1}h_1 \in H$, $k_2k_1^{-1} \in K$)

well-defined.

This argument proves that φ is a bijection of sets.

To see φ is an isomorphism,

$\varphi(h_1k_1h_2k_2)$?

$\varphi(h_1k_1)\varphi(h_2k_2) = (h_1, k_1)(h_2, k_2) = (h_1h_2, k_1k_2) = \varphi(h_1h_2k_1k_2)$

want to show: $h_1k_1h_2k_2 = h_1h_2k_1k_2$.

$\Leftrightarrow k_1h_2 = h_2k_1$

$k_1h_2k_1^{-1} \in H$ $(H \trianglelefteq G)$

$h_2k_1h_2^{-1} \in K$.

$\Rightarrow \underbrace{k_2h_1k_2^{-1}h_1^{-1}}_{\in H} = e \Rightarrow k_2h_1 = h_1k_2$.

($k_2h_1k_2^{-1} \in K$, $h_1^{-1} \in H$)

$\Rightarrow \varphi$ iso

Semidirect Product:

What if $H \trianglelefteq G$, but $K \leq G$? $H \cap K = \{e\}$

Thinking about the proof of prev thm, we shall still use

the "set bijection" part $HK \to H\times K$. 但是 $\varphi(h_1k_1h_2k_2) \neq \varphi(h_1k_1)\varphi(h_2k_2)$

$\Rightarrow$ not group homomorphism.

$h_1k_1h_2k_2 = h_3k_3$ for some h_3, k_3. only assuming H normal.

$h_3 = h_1(k_1h_2k_1^{-1})$ $\Rightarrow$ multiplication in HK.

$k_3 = k_1k_2$.

左再积里, 这里又 commute 取

For general semiproduct, we do not assume H, K in some G.

Assume H, K groups.

Q: Can we define a group G, s.t. $H \trianglelefteq G$, $H \cap K = \{e\}$?

$(h_1, k_1)\cdot(h_2, k_2) = (h_1\underbrace{k_1h_2k_1^{-1}}_{\varphi_{k_1}(h_2)}, k_1k_2)$

Theorem: If H, K are groups, and φ is a homomorphism

$$K \xrightarrow{\varphi} \mathrm{Aut}(H)$$

then define G to be the set $H\times K$ with multiplication

$$(h_1, k_1)(h_2, k_2) \longmapsto (h_1\varphi(k_1)(h_2), k_1k_2)$$

then $G = H \rtimes_\varphi K$.

Pf: Identity $= (1, 1)$

Associativity: $(h_1, k_1)(h_2, k_2)(h_3, k_3)$

$= (h_1\varphi(k_1)(h_2), k_1k_2)(h_3, k_3)$

$= (h_1\varphi(k_1)(h_2)\,\varphi(k_1k_2)h_3, k_1k_2k_3)$

$= (h_1\varphi(k_1)(h_2)\,\varphi(k_1)\varphi(k_2)h_3, k_1k_2k_3)$

$= (h_1\varphi(k_1)(h_2\varphi(k_2)h_3), k_1k_2k_3)$

$= (h_1k_1)(h_2\varphi(k_2)(h_3), k_2k_3)$

Inverse : $(h_1, k_1)(h_2, k_2) = (h_1 \varphi(k_1)(h_2), k_1 k_2) = (1, 1)$

$\Rightarrow h_2 = \varphi(k_1^{-1}) h_1^{-1}, \quad k_2 = k_1^{-1}$

$\Rightarrow (h_1, k_1)^{-1} = (\varphi(k_1^{-1}) h_1^{-1}, k_1^{-1})$

Exact Sequence :

A sequence of group homomorphisms

$$H \xrightarrow{\alpha} G \xrightarrow{\beta} K.$$

is called exact at G if $\operatorname{im}\alpha = \ker\beta$.

This means : ① $\beta \circ \alpha(h) = 1$, $\forall h$

② if $\beta(g) = 1$ for some $g \in G$

$\Rightarrow \exists\, h$, s.t. $\alpha(h) = g$

Notation :

$1 \to G \xrightarrow{f} K$ is exact iff f is injective. 要不然, 会有至少两个元素映射到 e_K.

$H \xrightarrow{f} G \to K$ is exact iff f is surjective. 要不然, 变成"="

A short exact sequence (SES) is of the form :

$$1 \to H \xrightarrow{\alpha} G \xrightarrow{\beta} K \to 1$$

which is exact at H, G, K, i.e.

- α inj
- β surj
- $\ker(\beta) = \operatorname{im}(\alpha)$

Example : if $N \trianglelefteq G$, then $\exists$ SES

$$1 \longrightarrow N \xrightarrow[\text{embedding}]{} G \xrightarrow{g \mapsto gN} G/N \to 1$$

if H, K, then $\exists$ SES

$$1 \longrightarrow H \hookrightarrow H \times K \longrightarrow K \longrightarrow 1$$

If H, K are groups and $\varphi : K \to \mathrm{Aut}(H)$ is a group hom,

then $\exists$ SES,

$$1 \longrightarrow H \longrightarrow H \rtimes_\varphi K \longrightarrow K \longrightarrow 1$$

Concrete examples: if $\mathbb{F}$ field,

$$1 \longrightarrow \underbrace{SL_2(\mathbb{F})}_{\det = 1} \longrightarrow GL_2(\mathbb{F}) \longrightarrow \mathbb{F}^\times \longrightarrow 1$$

$(\det)^{-1}$ 有定义

"SES" 有以有限种对于半直积的拆分。

$GL_2(\mathbb{F}) \cong SL_2(\mathbb{F}) \times \mathbb{F}$

$0 \to \mathbb{Z}/2 \to \mathbb{Z}/4 \to \mathbb{Z}/2 \to 0$. 是 SES, 但 $\mathbb{Z}/4$ 无法写成

$\mathbb{Z}/2$ 与 $\mathbb{Z}/2$ 的半直积, 只需考虑 order 4 element 即可。

(abelian case: 半直积 = 直积)

Exercise: D_4 = symmetries of a square.

$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$

$i^2 = j^2 = k^2 = ijk = -1$

$$\begin{cases} 1 \to C_2 \to D_4 \to C_2 \times C_2 \to 1 \\ 1 \to C_2 \to Q_8 \to C_2 \times C_2 \to 1 \end{cases}$$

Q_8 可以被写成半直积吗?

"$H \hookrightarrow G \twoheadrightarrow K$"

Theorem: If $1 \to H \xrightarrow{\alpha} G \xrightarrow{\beta} K \to 1$ is a SES, then

$G \cong H \times K$ if $\exists$ a homomorphism $\gamma : G \to H$, s.t.

$\gamma \circ \alpha(h) = h$, $\forall h \in H$

Theorem: If $H \xrightarrow{\alpha} G \xrightarrow{\beta} K$, then $\exists$ map $\varphi: K \to \mathrm{Aut}(H)$ s.t. $G \cong H \rtimes_\varphi K$ if $\exists$ a group homomorphism $\gamma: K \to G$, s.t. $\beta \circ \gamma(k) = k$

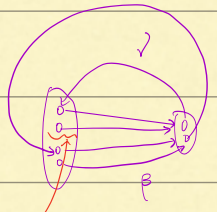
In the case of γ existing, $H \hookrightarrow G \twoheadrightarrow K$ is a split short exact sequence.

What is the criterion for a split SES to actually give a direct product?

$\Leftrightarrow$ K needs to be normal and $\varphi: K \to \mathrm{Aut}(H)$ must be trivial (因为 $h_1 \varphi(k)(h_2)$ 要 $= h_2$ $\forall k, h_2$, 所以 trivial)

Pf of semi thm:

Strategy: $H \xrightarrow{\alpha} G \underset{\gamma}{\overset{\beta}{\rightleftarrows}} K$



$\beta(\gamma(k)) = k$. $\Rightarrow$ 并不一定意味着 $\gamma \circ \beta = id$ (此情景就有问题)

$\varphi: K \to \mathrm{Aut}(H)$

If $k \in K$, $h \in H$, $\gamma(k)\alpha(h)\gamma(k)^{-1} \in \alpha(H)$

$\alpha(H)$ is normal in G

$\gamma(k)\alpha(h)\gamma(k)^{-1} = \alpha(h')$

想证存在性，我们直接把 φ 搭出来.

$\varphi: K \longrightarrow \mathrm{Aut}(H)$

$k \longrightarrow (h \to h')$ $\left(h \mapsto \alpha^{-1}(\gamma(k)\alpha(h)\gamma(k)^{-1})\right)$

α 是 well-defined 推出 φ 也是.

Need to check: φ is an automorphism.

$\varphi(k)(h_1 h_2) = \alpha^{-1}(\gamma(k)\alpha(h_1 h_2)\gamma(k)^{-1})$

$= \alpha^{-1}(\gamma(k)\alpha(h_1)\alpha(h_2)\gamma(k)^{-1}) = \alpha^{-1}(\gamma(k)\alpha(h_1)\gamma(k)^{-1}\gamma(k)\alpha(h_2)\gamma(k)^{-1})$

$$\varphi(k)(h_1)\,\varphi(k)(h_2) = \alpha^{-1}\big(\gamma(k)\alpha(h_1)\gamma(k)^{-1}\big)\,\alpha^{-1}\big(\gamma(k)\alpha(h_2)\gamma(k)^{-1}\big)$$

Since α is a group hom,

$$\alpha(\gamma(k)(h_1h_2)) = \gamma(k)\alpha(h_1)\gamma(k)^{-1}\gamma(k)\alpha(h_2)\gamma(k)^{-1}$$

$$= \alpha\big(\varphi(k)(h_1)\,\varphi(k)(h_2)\big)$$

$\Rightarrow$ $\varphi(k)$ is hom

To show: $\varphi(k)$ is iso.

① injectivity: 设 $x \in H$ s.t. $\varphi(k)(x) = e$, $\forall k \in K$.

$$\Rightarrow \gamma(k)\alpha(x)\gamma(k)^{-1} = \alpha(e) = e.$$

$$\Rightarrow \gamma(k)\alpha(x) = \gamma(k)$$

$$\Rightarrow \alpha(x) = e_G$$

Since x is injective, $x = e_H$

exercise: $\varphi(k)$ surjective.

前面是 $\varphi(k)$, 别混了.

auto 们

Still need to show: φ is a hom i.e. $\varphi(k_1)\circ\varphi(k_2) = \varphi(k_1k_2)$

$\forall h \in H$, $\varphi(k_1k_2)(h)$ satisfies:

$$\alpha(\varphi(k_1k_2)(h)) = \gamma(k_1k_2)\alpha(h)\gamma(k_1k_2)^{-1}$$

$$= \gamma(k_1)\gamma(k_2)\alpha(h)\gamma(k_2)^{-1}\gamma(k_1)^{-1}$$

$$= \gamma(k_1)\,\alpha(\varphi(k_2)(h))\,\gamma(k_1)^{-1}$$

$$= \alpha\Big(\gamma(k_1)\big(\gamma(k_2)(h)\big)\Big)$$

$\Rightarrow$ $\varphi(k_1k_2) = \varphi(k_1)\circ\varphi(k_2)$ (α injective.)

So we can construct the semiproduct $H \rtimes_\varphi K$.

$$H \overset{\alpha}{\hookrightarrow} G \overset{\beta}{\twoheadrightarrow} K, \quad \gamma: K \to G$$

$H \rtimes_\varphi K \xrightarrow{f} G$, and show it is a group iso.

$(h, k) \longmapsto \alpha(h)\gamma(k)$

NTS: ① $f((h_1,k_1)(h_2,k_2)) = f(h_1,k_1)f(h_2,k_2)$

② bijection

①: $f((h_1,k_1)(h_2,k_2))$

$= f(h_1 \varphi(k_1)(h_2), k_1 k_2)$

$= \alpha(h_1 \varphi(k_1)(h_2))\, \gamma(k_1 k_2)$

$= \alpha(h_1)\, \alpha(\varphi(k_1)(h_2))\, \gamma(k_1)\gamma(k_2)$

$= \alpha(h_1)\, \underbrace{\gamma(k_1)\alpha(h_2)\gamma(k_1)^{-1}}_{\| \text{ (conjugation)}}\, \gamma(k_1)\gamma(k_2)$

$= \alpha(h_1)\gamma(k_1)\alpha(h_2)\gamma(k_2)$

$= f(h_1,k_1) f(h_2,k_2)$

$\Rightarrow$ f is homo, now to show iso.

① Injective:

Assume $f(h,k) = e$

$\Rightarrow \alpha(h)\gamma(k) = e$

$\Rightarrow \beta(\alpha(h)\gamma(k)) = \beta(e_G) = e_K$

$\Rightarrow (\beta\circ\alpha)(h)\ \beta(\gamma(k)) = e_K$ ($\beta\circ\gamma = Id$)

$\downarrow$ $\mathrm{im}(\alpha) = \ker(\beta) \Rightarrow \beta\circ\alpha(h) = e$

$\Rightarrow e_K k = e_K \Rightarrow k = e_K$.

$\alpha(h)\, e_H = e_H \Rightarrow h = e_H$

$\Rightarrow (h,k) = (e,e)$

② Surjective:

$\forall g \in G_1$, we need to show $\exists h,k$, s.t. $f(h,k) = g$

$\alpha(h)\gamma(k) = g$.

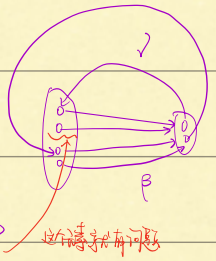
Working backward: β both side

$\beta(\gamma(h))\ \beta(\gamma(k)) = \beta(g)$

$\Rightarrow \quad e_K k = \beta(g)$

$\Rightarrow \quad k = \beta(g)$

$\Rightarrow \quad \alpha(h)\gamma(\beta(g)) = g$



这个确实是有问题

回忆这个例子，虽然我们没有 $\gamma(\beta(g)) = g$ 这么强的条件，但我们 Ab 是

那是 g 与 $\gamma(\beta(g))$ 都在 $\gamma(g)$ 的 preimage 的集合里。可以理解为

"被平移后的 kernel"，而 $\alpha(h) \in \ker(\beta)$，$\alpha(h)$ 就是在把 $\ker(\beta)$ 中元素

挪来挪去的 action，所以很好感觉

$\Leftarrow$ $\alpha(h) = g\,\gamma(\beta(g))^{-1}$ 这里想说明存在 h，所以这里只需证属于 $\ker(\beta)$ 即可

$\alpha(h) \in \ker(\beta) \Rightarrow g\,\gamma(\beta(g))^{-1} \in \ker(\beta)$

实际都应该是"只需证"

$\Leftarrow$ $\beta(g\cdot\gamma(\beta(g)^{-1})) = e_k = \beta(g)\beta(\gamma(\beta(g)^{-1}))$ ($\beta(\gamma) = id$)

$= \beta(g)\beta(g)^{-1}$

即得证。令 $h = \alpha^{-1}(g\,\gamma(\beta(g))^{-1})$

$\Rightarrow$ Surjective.

Rings: 2 operations. $+$ $\cdot$

$(\mathbb{R}, +)$ is an abelian group

$(\mathbb{R}, \cdot)$ is a commutative monoid. ← no inverse.

Def: A ring R is a set equipped with 2 operations $+, \cdot$ and 2 identities $0, 1$, s.t.

① $(R, +)$ with identity 0 is an abelian group

② $(R, \cdot)$ with identity 1 is a monoid ← 封闭，结合率，么元

③ Distributivity: for all $a, b, c \in R$,

$$\begin{cases} a\cdot(b+c) = ab + ac \\ (b+c)\cdot a = ba + ca. \end{cases}$$

Subring: subset of a ring with a properties hold.

Ex: In any ring, we have the subring $\langle 0,1 \rangle$

and R itself

Example: If S_1, S_2 are subrings of $R \Rightarrow S_1 \cap S_2$ is also a subring of R.

pf: $0, 1 \in S_1 \cap S_2$.

if $a, b \in S_1 \cap S_2 \Rightarrow a, b \in S_1$

$\Rightarrow a+b,\ ab,\ ba \in S_1$ (S_2 similar)

$\Rightarrow a+b,\ ab,\ ba \in S_1 \cap S_2$

So closure satisfied.

Example: $(\mathbb{Z}, +, \cdot)$ has no subrings

$\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ as rings

Constructions of rings with other rings:

$\mathbb{Z}[x]$ $(R[x])$

Through addition, there is an action of $\mathbb{Z}$ defined on a ring R.

(Compute $\sum_{}^{\mathbb{Z}} nr^{\in R}$)

Properties: if $a, b \in R$, then

$\begin{cases} (-a)(b) = -ab \\ a(-b) = -ab \\ (-a)(-b) = ab. \end{cases}$

Proposition (Subring Criterion):

$\forall$ R ring, $S \subseteq R$. S is a subring if

① $S \neq \emptyset$

② $s_1, s_2 \in S \Rightarrow s_1 s_2,\ s_2 s_1 \in S$ (unnecessary.)

③ $s_1, s_2 \in S \Rightarrow s_1 - s_2 \in S$.

Lemma: In any ring R, for $a, b, c \in R$,

① $a \cdot 0 = 0 \cdot a = 0$

② $(-a)b = -(ab) = a(-b)$

pf of 2:

$0 = 0 \cdot b \Rightarrow 0 = (a + (-a))b \Rightarrow -(ab) = (-a)b$

others are the same.

A ring is commutative if $\forall a, b \in R$, $ab = ba$,

A communitive ring R is an **integral domain** or **order**

if $\forall a, b \in R$, $ab = 0 \Rightarrow a = 0$ or $b = 0$

"no zero divisor" "has cancellation"

A **division ring** is a ring R in which every non-zero element has a multiplicative inverse.

A commutative division ring is a **field** **skew field**: non-communitive division ring.

Def: In a ring R, an element x is called **unit** if $\exists x^{-1} \in R$,

s.t. $x \cdot x^{-1} = x^{-1} \cdot x = 1$.

Example: $\mathbb{Z}$ is an integ

Prop: R ring $\Rightarrow R[x]$ ring.

Pf: 0, 1 identitires in $R[x]$

懒得写了…把 f,g 写出起啊.

(Objects, Functions)

(Vector Space, linear transformations)

(Groups, group homo)

(Rings, ring homo)

If R, S rings, $f: R \to S$ is a ring homomorphism iff

① $f(a)+f(b) = f(a+b)$

② $f(ab) = f(a)f(b)$

Q: What kind of structure does kernel of ring homomorphism have?

$\ker(f) = \{r \in R \mid f(r) = 0\}$

note: It's generally not the case that $1 \in \ker(f)$

We do not require $1 \neq 0$ for our ring

Example: $\{0\}$

Our definition of subring (should) require that the 0 stay the same.

Q: What about 1?

一个很神奇的结论：对于环同态 φ 而言，虽然我们有 $\varphi(0)=0$，但 $\varphi(1)=1$ 却不一定

考虑 $\varphi: R \to R \times R$，$\varphi(r) = (r, 0)$

易知 R 中的 1 是 1，$R \times R$ 中的 1 是 $(1,1)$，但 $\varphi(1) \neq (1,1)$

所以子环中不一定有原来的 1.

同时理想甚至不一定是子环！只是子群而已！

$\ker(f)$ for a ring homomorphism is a normal subgroup of the abelian group

— multiplicative structure?

$f: R \to R'$

$\ker(f) = \{r \in R \mid f(r) = 0\}$ ($1 \notin \ker f$)

(if $f(1) = 0 \Rightarrow f(x) = f(1)f(x) = 0 \Rightarrow f(x) = 0$ trivial)

Q: What properties do kernels satisfy?

- $\ker(f)$ satisfies all ring properties except $1 \in \ker(f)$
- If $x \in \ker(f)$ and $r \in R$, then $f(xr) = f(x)f(r) = 0$

  $\Rightarrow xr \in \ker(f)$

Def: A (2-sided) ideal of a ring R is a subset of R that is a subgroup (implies normal) under addition and satisfies if $a \in R$, $b \in I \Rightarrow ab, ba \in I$.

Examples. $\{0\}$ ("generated by 0"), R ("generated by 1") is always ideals.

Q: Which rings only have 2 ideals?

Eg. if R communitive, $\forall x \in R$, we can create the principle (generated by 1 element.) ideal generated by x. $(x) = xR = \{xr \mid r \in R\}$

Exercise: (x) is an ideal.

Thm: Every ideal in $\mathbb{Z}$ is principle (generated by 1 element.)

Propersition: kernel $\Leftrightarrow$ Ideal.

Pf: 後補.

To any ideal $I \subseteq R$, we can construct the quotient ring R/I. Elements are of the form $a+I$.

$(a+I)+(b+I) = a+b+I$

$(a+I)\cdot(b+I) = ab + \underbrace{aI+bI+II}_{\in I}$.

Identities are $(0+I)$ $(1+I)$ ← 因为单位1不在I里，要不然 $I=R$ 了.

Note: $x, y \in R$ are in the same coset if $x-y \in R$.

Then we can define $a \equiv b \pmod I$ iff $a-b \in I$. 这里和 normal group 那时候应该类似

Example: $n\mathbb{Z} \subseteq \mathbb{Z}$ is a (principle) ideal, with quotient ring $\mathbb{Z}/n\mathbb{Z}$. We can define $a \equiv b \pmod{n\mathbb{Z}}$

Note: There is a projection ring homomorphism $f: R \to R/I$

$r \to r+I$

$\ker(f) = I$

Properties of ideals.

Lemma: If $I_1, I_2 \subseteq R$ ideals, then $I_1 \cap I_2$ is an ideal.

证明比较简单.

If R is a ring and $S \subseteq R$, we can take intersection of all ideals containing S, namely, (S)

Example: $R = \mathbb{Z}[\sqrt{-5}] = \{a+b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$

$S = \{2, 1+\sqrt{-5}\}$

↳ { Intersection exists because R contains S.

It's an ideal by the previous lemma.

Any ideal containing S will have to contain the ideal generated by S.

Q: $(S)=?$

Assume S is finite. $S=\{a_1,\cdots,a_n\}$

For any $y_i, z_i \in R$, $\sum_{i=1}^{n} y_i a_i z_i \in (S)$

$(S)=\sum_{i=1}^{n} y_i a_i z_i$

For commutative ring: $(S)=\sum_{i=1}^{n} x_i a_i$.

Thm: If R is a commutative ring, then R is a field iff R has only ideals (0) ($=\{0\}$) and (1) ($=R$).

For non-commutative ring, R division ring $\Leftrightarrow$ only have (0), (1).

Pf: "$\Rightarrow$"

R field, I ideal $\Rightarrow I=\{0\}$ or $\exists x\in I,\ x\neq 0$.

R field $\Rightarrow x^{-1}\in R \Rightarrow x^{-1}x\in I \Rightarrow 1\in I \Rightarrow I=R$.

"$\Leftarrow$"

$\forall a\in R$ non-zero, $a\notin(0) \Rightarrow (a)=(1) \Rightarrow 1\in(a)$

$\Rightarrow \exists x\in R,\ ax=xa=1$.

$\Rightarrow R$ field.

Def: A ring homomorphism is $f: R\to R'$ satisfying

$\begin{cases} f(a+b)=f(a)+f(b) \end{cases}$

$f(ab) = f(a)f(b)$

$f(1) = 1'$

related issue: Does the defn of the subring need to to require that the identity to be the same with the full ring?

- Is the map $R \to R'$ $r \mapsto 0$ a ring homo?
- Is the zero-ring an allowed ring?

Overall issue: The ring axioms don't have to require that there's a "1"

Summary Discussion: Do we want to preserve the structure (to have a "1")?

$f: R \to R'$ a ring homomorphism.

$\text{im}(f) = f(R) = \{r' \in R \mid \exists r \in R, \text{ s.t. } f(r) = r'\}$.

Lemma: $\text{im}(f)$ is a subring of R'

Pf: $\text{im}(f)$ is an additive subgroup of R'.

Since $f(1) = 1$, $\Rightarrow f(1 \cdot a) = f(1)f(a) \Rightarrow f(1)f(a) = f(a)$

for all $f(a) \in \text{im}(f) \longrightarrow \Rightarrow f(a)f(1) = f(a)$

$f(1) = 1$ version: $f(1) = 1$ is the identity.

Here, we'd be assuming that subrings need to have the same "1"

If $f(a), f(b) \in \text{im}(f) \Rightarrow f(ab) = f(a)f(b) \in \text{im}(f)$

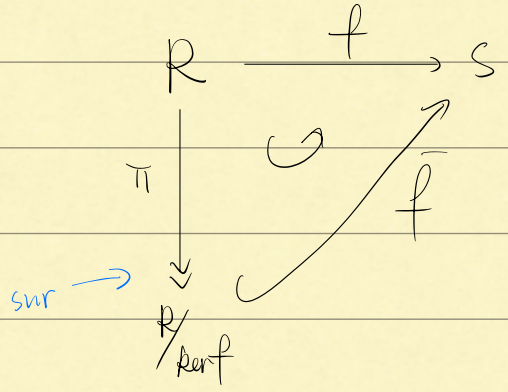
Distributivity is inherited from R'.

R ring, $R \times R$ $\quad (1,1) = 1_{R\times R}$, $\quad (0,0) = 0_{R\times R}$.

Consider $\underbrace{(R,0)}_{(1,0) \text{ is the "1"}} \leq R \times R$

Thm: If $f: R \to S$ a ring homomorphism, then $\ker(f)$ is an ideal, $\text{im}(f)$ is a subring of S, and $R/\ker(f) \cong \text{im}(f)$

Equivalently, there is a unique decomposition of f into a projection $R \to R/\ker f$ composed with an injection $R/\ker f \hookrightarrow R'$, s.t. the following diagram commutes



Theorem:

Let $f: R \to R'$ a surjective ring homomorphism, There is a 1-1 correspondence of the set of additive subgroups of R containing $\ker(f)$ with the set of subgroups of R'

- $\ker(f) \leq H \leq R \iff f(H)$ is a subgroup of R'
- $H \geq \ker(f)$ ideal iff $f(H)$ ideal

If H is such an ideal, then the map $x+H \mapsto f(x)+f(H)$ gives an isomorphism of $R/H \cong R'/f(H)$

Pf: 后面就 skip 了 ??!

Thm: Let R be a ring, S a subring, I an ideal of R.

Then $S+I = \{s+i \mid s\in S, i\in I\} \le R$ is a subring of R containg I as an ideal.

Furthermore, $S\cap I$ is an ideal in S.

and $(S+I)/I \cong S/S\cap I$.

$\underset{s+I}{\overset{s+i+I}{\shortparallel}} \mapsto s+(S\cap I)$

Pf: $S+I$ is a subring of R containing I as an ideal:

if $x,y\in S+I$, $x=s_1+i_1$, $y=s_2+i_2$.

$\Rightarrow x+y = s_1+s_2+i_1+i_2 \in S+I$

$xy = (s_1+i_1)(s_2+i_2)$ ($\in I$) } 1,0 都行,

$= s_1s_2 + i_1s_2 + s_1i_2 + i_1i_2 \in S+I$.

if $s+i\in S+I$, then $-s-i\in S+I$

$\Rightarrow S+I$ subring.

To see I is an ideal,

$I\subseteq S+I$, $\forall s+i\in S+I$, $(s+i)I = sI+iI = I$.

Now we show $S\cap I$ is an ideal of S:

S, I are additive sbgp of R. $\Rightarrow S\cap I$ is an additive sbgp.

Since $S\cap I\subset S$, $S\cap I\le S$.

NTS: If $s\in S$, $x\in S\cap I \Rightarrow sx\in S\cap I$.

$s\in S$, $x\in S \Rightarrow sx\in S$. $s\in S$, $x\in I\Rightarrow sx\in I$

$\Rightarrow sx\in S\cap I$.

NTS: isomorphism.

We can apply the previous thm: $R/I \cong R'/f(I)$ if we can find

a good surjection ring homomorphism. ← Typically, projection map.

$R \xrightarrow{\pi} R/I$. restrict the domain to S: $\pi|_S$.

$S \xrightarrow{\pi|_S} R/I$. $\ker(\pi|_S) = S \cap I$. ← 对在kernel中对应S中的元素.

$s \longrightarrow s+I$

$\text{im}(\pi|_S) = {}^{S+I}/_{I}$

Then the map $S \xrightarrow{\pi|_S} {}^{S+I}/_{I}$

$s \longmapsto s+I$ is a surjective ring homs.

$f: R \to R'$

$X+H \mapsto f(x)+f(H)$

$R/H \cong R'/f(H)$

So previous thm says: ${}^{S}/_{S\cap I} \cong {}^{S+I}/_{I}$

$S+(S\cap I) \mapsto S+I$.

If D is a division ring, R a subring of D, then R cannot have zero divisors.

Pf: Assume $a, b \in R$, s.t. $ab=0$, and $a, b \neq 0$.

Since $a, b \neq 0$, and $a, b \in D$, $\exists\, a^{-1}, b^{-1}$ in D. (multiplicative inverses)

$b = 1\cdot b = a^{-1}ab = a^{-1}\cdot 0 = 0$, contradiction.

Q: If R is a ring with no 0-divisors, can it be embedded into some division ring?

A: Not always. Conterexample: Pg 119, # 7-8

Q': If R is a commutative ring with no 0-divisors, can it be embedded into some division ring?

A: Yes! In fact a field.

F: Field

R: Subring of F.

related question: what is the smallest subfield of F containing R?

Equivalently, the field generated by R.

Claim: $F(R) = \{ab^{-1} \mid a, b \in R,\ b \neq 0\}$ (要記得 R commutative.) is a subfield of F.

Pf: ① $ab^{-1} + cd^{-1}$ ($\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ 類似通分)

$= ab^{-1}dd^{-1} + cd^{-1}bb^{-1}$

commutative. $= ad(b^{-1}d^{-1}) + cb(b^{-1}d^{-1})$

$= (ad+cb)(bd)^{-1}$

($ad, cb \in R$; $bd \in R$)

$\Rightarrow$ addition closed.

② $ab^{-1}cd^{-1} = (ac)(bd)^{-1}$

③ $\begin{cases} a=0, & ab^{-1}=0 \\ a\neq 0, & (ab^{-1})^{-1} = (ba)^{-1} \end{cases}$

④ $-(ab^{-1}) = (-a)b^{-1}$

We can conclude that $F(R)$ is a field. We know that $R \leq F(R)$

Is there any proper subfield of $F(R)$ that contains R? No.

Pf of No: Assume $R \leq F' \subsetneq F(R)$

$\Rightarrow \exists\ ab^{-1} \in F(R),\ ab^{-1} \notin F'$

($a, b \in R$, $b \neq 0$) $\Rightarrow$ ($a, b \in F'$, $b \neq 0$) $\Rightarrow b^{-1} \in F'$ (field.)

$a, b^{-1} \in F' \Rightarrow ab^{-1} \in F'$, contradiction

$F(R)$: the field generated by R, the smallest subfield containing R.

Q: What if R (commutative w/out zero-divisors) isn't a priori a subring of a field?

Let R be an integral domain ($ac = bc \Rightarrow a = b$ if $c \neq 0$)

Let $R \times R - \{0\}$ be the product set, (a, b) where $a \in R$, $b \in R - \{0\}$.

($\frac{a}{b}$) $(a, b) \sim (c, d)$ ($\frac{c}{d}$) iff $ad = bc$. This defines a equivalence relation

Let $F(R) = (R \times R - \{0\}) / \sim$

$$= \left\{ \frac{a}{b} \mid a \in R,\ b \in R - \{0\} \right\}.$$

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \iff (a,b) + (c,d) = (ad+bc, bd)$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \iff (a,b)(c,d) = (ac, bd)$$

$F(R)$ is a commutative ring.

Theorem: Any integral domain can be embedded inside a field.

(embedded: injective homomorphism)

Prop: If there is an injective ring homomorphism of $R \hookrightarrow F$, where F is a field, then $f = \bar{f} \circ i$

where $i : R \hookrightarrow F(R)$

$\bar{f} : F(R) \hookrightarrow R$

Idea: If an integral domain embeds inside a field F, so does its fraction field.

Prop: If R is an integral domain, $F(R)$ is its fraction field. Any injective ring homomorphism of R into a field F extends uniquely to an injective homomorphism $F(R) \to F$

Pf: Let $f : R \to F$ injective ring homomorphism

$r \to f(r)$

Define $\underline{f} : F(R) \to F$

$(a,b) \to f(a) f(b)^{-1}$

well-defined: if $(a,b) \sim (c,d) \iff ad = bc$.

$f(a)f(b)^{-1} = f(c)f(d)^{-1}$? ✓ 说明是环同态.

$\Leftrightarrow f(a)f(d) = f(c)f(b)$?

Q: If R is a ring, what is the smallest subring of R?

① If we do not require $1 \in R$, then the smallest ring is $\{0\}$.

② What if we do require $1 \in R$?

Candidate: The ring generated by 1?

若只考虑 R 中包含的最小的 ring 而非 subring 的话答案是 $\mathbb{F}_2$.

Consider the map $\mathbb{Z} \xrightarrow{\varphi} R$.

$n \mapsto \underbrace{1_R + 1_R + \cdots + 1_R}_{n\text{个}}$

$n \mapsto n \cdot 1_R$.

这里不说是整个 R, 比如 $R \times R$, $1_{R\times R} = (1_R, 1_R)$, 只会包含对角线元素.

Claim: image of φ is the smallest subring of R.

Pf: if S is a subring, then since $1_R \in S$, any finite sum of 1_R will be contained in S by closure axiom. So $\mathrm{im}(\varphi) \subseteq S$.

Consider the surjective map $\mathbb{Z} \twoheadrightarrow \mathrm{im}(\varphi)$

So either $\begin{cases} \mathbb{Z} \cong \mathrm{im}(\varphi) & (\ker(\varphi) = 0) \\ \mathbb{Z}/n\mathbb{Z} \cong \mathrm{im}(\varphi) & \end{cases}$

$\mathbb{Z}$ 是 principle ideal domain.

Q: What are the ideals of $\mathbb{Z}$?

A: $(a,b) = (\gcd(a,b))$

Thm: In any ring R, the smallest subring of R is either $\cong \mathbb{Z}$ or $\cong \mathbb{Z}/n\mathbb{Z}$ for some n.

→ any 前面的性质都对这块内容适用.

Def: For a ring R, m is called the characteristic of R. ($\mathbb{Z} \cong \mathbb{Z}/0\mathbb{Z}$)

Note: The subring of an integral domain is also an integral domain.

So for a integral domain, its character is either 0 or a prime number (因为不prime的 $\mathbb{Z}/m\mathbb{Z}$ 不是 integral domain).

Continue from F(R)那里.

Prop: If R is an integral domain, $F(R)$ is its fraction field.

Any injective ring homomorphism of R into a field F extends uniquely to an injective homomorphism $F(R) \to F$

Pf: Let $f: R \to F$ injective ring homomorphism

$r \to f(r)$

Define $\underline{f}: F(R) \to F$

$(a,b) \to f(a)f(b)^{-1}$

这里和上面一样的

well-defined: if $(a,b) \sim (c,d) \Leftrightarrow ad=bc$.

$f(a)f(b)^{-1} = f(c)f(d)^{-1}$? $\surd$ 这个是对的.

$\Leftrightarrow f(a)f(d) = f(c)f(b)$?

$\Rightarrow$ well-defined.

ring-homomorphism:

$$\underline{f}\left(\frac{a}{b}+\frac{c}{d}\right) = \underline{f}\left(\frac{ad+bc}{bd}\right)$$

$$= f(ad+bc)f(bd)^{-1}$$

$$= f(ad)f(bd)^{-1} + f(bc)f(bd)^{-1}$$

这里对应的点在于不能有错

$f(b)^{-1} = f(b^{-1})$

$$= f(a)f(d)f(b)^{-1}f(d)^{-1} + f(b)f(c)f(b)^{-1}f(d)^{-1}$$

对加法成立. $\Rightarrow$ $= f(a)f(b)^{-1} + f(c)f(d)^{-1}$

$$f\left(\frac{a}{b}\cdot\frac{c}{d}\right)=f(ac)f(bd)^{-1}$$

$$=f(a)f(b)^{-1}f(c)f(d)^{-1}$$

对称法则立 $\Rightarrow$ $=f\left(\frac{a}{b}\right)f\left(\frac{c}{d}\right)$

$$f\left(\frac{a}{b}\right)=0 \Rightarrow f(a)f(b)^{-1}=0 \Rightarrow f(a)=0 \Rightarrow a=0.$$

Polynomial Rings:

Assume R is a commutative ring,

$$R[x]=\{a_nx^n+\cdots+a_1x+a_0 \mid a_i\in R\}$$

$R[x]$ is a commutative ring.

Another construction:

Let $R\subset S$ be 2 rings, R subring of S. Let $s\in S$ and define

$$R[s]=\{a_ns^n+\cdots+a_1s+a_0 \mid a_i\in R\}.$$

误区槽，这里真不真知代数数/超越数有关系？若s真R中的代数数，$R[s]$中的收敛数列真有上限的，反之没有。

Then $R[s]$ is a ring, but expression of element in $R[s]$ may not be unique.

Example: $R=\mathbb{R}$, $S=\mathbb{C}$

$$R[i]=\{a+bi\}=\{a-bi\}$$

For polynomial rings, we have that if

$$a_nx^n+\cdots+a_0=b_mx^m+\cdots+b_0,$$

then $a_i=b_i$ $\forall i$.

We can use $R[x]$ to study $R[s]$ for any $s\in S$, $R\subset S$.

$$\begin{cases} R[x] \to S \\ x \mapsto s \\ r \mapsto r. \end{cases}$$

Rename: $\forall s \in S, \exists \varphi_s$.

$$\begin{cases} R[x] \xrightarrow{\varphi_s} S. \\ r \longmapsto r \\ x \longmapsto s \end{cases}$$

$\operatorname{im}(\varphi_s) = R[s]$.

$R[x] \xrightarrow{\varphi_s} R[s]$ surjective.

Hence, $\exists$ ideal I in $R[x]$, s.t. $R[x]/I \cong R[s]$.

这里的所谓的 ideal 就是 s 的最小多项式的 ideal 吧.

Example: $\mathbb{R}$, $\mathbb{C}$

$\mathbb{C} = \mathbb{R}[i]$

$\mathbb{R}[x] \longrightarrow \mathbb{R}[i]$

$x \longmapsto i$

$\Rightarrow \exists$ an ideal in $\mathbb{R}[x]$, $\mathbb{R}[x]/(x^2+1) = \mathbb{R}[i]$

$\mathbb{R}[x] \xrightarrow{\varphi_i} \mathbb{R}[i]$

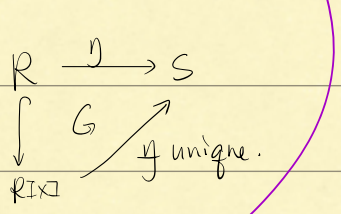
$f(x) \longmapsto f(i)$

$f \in \ker \Leftrightarrow f(i) = 0 \Leftrightarrow x^2+1 \mid f(x)$

If $a_n s^n + \cdots + a_0 = b_m s^m + \cdots + b_0 \quad (a_i, b_i \in R)$

$\Rightarrow a_n s^n + \cdots + (a_m - b_m) s^m + \cdots + (a_0 - b_0) \in I$

Theorem: if R, S commmnitive rings, $\exists$ a ring homomorphism $\eta: R \to S$, if $s \in S$, then there is a unique extension $\eta: R[x] \to S$, s.t. $\begin{cases} \eta(r) = \eta(r) \\ \eta(x) = s. \end{cases}$



Pf 再证两个方向即可

Cor: If η injective, then $R[x]/I \cong R[s]$ for some ideal I.

where $I \cap R = \{0\}$

Assume I is an ideal of $R[x]$, s.t. $R \cap I = \{0\}$.

Q: Is there a converse to the Cor?

$R[x] \xrightarrow{\pi} R[x]/I$ projection map.

$f(x) \longmapsto f(x)+I$.

$\pi|_R$, $\ker(\pi) = I$ $\ker(\pi|_R) = I \cap R = \{0\}$.

$\pi|_R$ is injective, this gives a subring relationship to $R \subset R[x]/I$.

$a \mapsto a+I$.

Let $s = x+I \in R[x]/I$.

$\text{im}(\pi|_R)[s] \xrightarrow{\psi} R[x]/I$

ψ is surjective since R (inside of $R[x]/I$, looks like $R+I$) and $x+I$ generate $R[x]/I$.

ψ: $r \longmapsto r+I$

$s \longmapsto x+I$.

Since ψ sends elements of LHS to all the generators, it's surjective.

It is injective if $\text{im}(\pi|_R)[s] \ni \alpha = a_n s^n + \cdots + a_1 s + a_0$

satisfies $\psi(\alpha) = 0$, then $\psi(\alpha) = (a_n x^n + \cdots + a_1 x + a_0) \in I$

Then $\alpha = 0$ since the difference between $a_n x^n + \cdots + a_1 x + a_0$ and 0 are in I

If R is a subring of a commutative ring S and $s \in S$, then we have

evaluation map @ s

$$R[x] \xrightarrow{ev_s} S$$

$$r \longmapsto r$$

$$x \longmapsto s$$

$$f(x) \longmapsto f(s)$$

Q: When is ev_s injective homomorphism?

ev_s is injective $\Leftrightarrow f(s)=0 \Rightarrow f(x)=0$

Such s (for which ev_s is injective) is called transcendental over R

If s is not transcendental, i.e. ev_s is not injective, then

$$\exists f(x) \in R[x],\ f(x) \neq 0,\ f(s)=0.$$

Then s is algebraic over R

$R \longmapsto R[x]$ is a ring homo whenever R is commutative ring.

Let $R' = R[x]$, commutative ring, we can use the same construction:

$R'[y]$ = polynomial in y with coef in $R' = R[x]$

= polynomials in x, y with coef in R

$= R[x,y]$.

Thm: For any commutative ring R and positive integer n,

$\exists$ a ring $R[x_1, \cdots x_n]$ with the following (universal)

property: If S is a ring, s.t. $\eta: R \to S$, is a homomorphism,

and we have a set function $\{1,2,\cdots,n\} \longrightarrow S$

$$i \overset{\varphi}{\longmapsto} s_i$$

Then there exist a unique extension of η to a ring homo

$$R[x_1,\cdots,x_n] \xrightarrow{\eta_\varphi} S \qquad r_0 x_1^2 x_3 \longmapsto \eta(r_0) s_1^2 s_3.$$

这些东西都没左乞事的.

$$x_i \longmapsto s_i$$

$$r \longmapsto \eta(r)$$

左事确定 $x_1,\cdots,x_n$ 去的位置即可.

If η is injective $\Rightarrow R \subset S$, and so the image of $R[x_1,\cdots,x_n] \subset S$.

η_φ is injective iff $s_1, s_2, \cdots s_n$ are algebraically independent over R.

algebraically independent: $\sum_{\text{finite}} a s_1^{k_1} \cdots s_2^{k_2} = 0$ iff all coefficients are 0. ($a \in R$)

$$\deg : R[x] \longrightarrow \mathbb{Z}_{\geq 0} \cup \{-\infty\}$$

$$f(x) \longmapsto \deg(f)$$

$$0 \longmapsto -\infty$$

$$\deg(f+g) \leq \max(f,g)$$

$$\deg(f(x)g(x)) \leq \deg f(x) + \deg g(x)$$

If R has no zero divisors, then $\deg(fg) = \deg(f) + \deg(g)$

Thm: If R is an integral domain, then so is $R[x]$.

and the units of $R[x]$ are simply the units in R.

① $fg = 0 \Rightarrow \deg(fg) = -\infty$

$\Rightarrow \deg f + \deg g = -\infty$

$\Rightarrow f = 0$ or $g = 0$

② $fg = 1 \Rightarrow \deg f + \deg g = 0$

$\Rightarrow \deg f = 0,\ \deg g = 0$

$\Rightarrow f, g$ constants, units.

Cor: If R an integral domain, then $R[x_1, \cdots, x_n]$ is an integral domain, its units are units of R

Pf: $R \to R[x_1] \to R[x_1, x_2] \to \cdots \to R[x_1, \cdots, x_n]$.

Division algorithm in $R[x]$:

Thm: Let $f(x), g(x) \in R[x]$ be nonzero polynomials, where R a commutative ring. Assume $g(x)$ has degree m with coefficient $b_m \in R$. Then there exist $k > 0$ and polynomials $q(x), r(x) \in R[x]$, s.t.

$\deg(r) < \deg(g)$ and

$(b_m)^k f(x) = q(x)g(x) + r(x)$

Cor: If $f(x) \in R[x]$ is nonzero and $a \in R$, then $\exists$ a unique $q(x) \in R[x]$, s.t. $f(x) = (x-a)q(x) + f(a)$ ← just plug in a.

Cor: $(x-a) \mid f(x) \iff f(a) = 0$.

Pf: Case 1: $\deg f(x) < \deg g(x)$

$f(x) = 0 \cdot g(x) + f(x)$ $\begin{cases} q(x) = 0 \\ r(x) = f(x) \end{cases}$

Case 2: $\deg f(x) \geq \deg g(x)$ (n, m)

$\begin{cases} f(x) = a_n x^n + \cdots + a_1 x + a_0 \\ g(x) = b_m x^m + \cdots + b_1 x + a_0 \end{cases}$

Let $f_1(x) = b_m f(x) - a_m x^{n-m} g(x)$ 消掉最高次项.

$\deg f_1(x) < \deg f(x)$

之后归纳即可, 我有点懒得写了.

$$b_m f(x) = a_m x^{n-m} g(x) + f_1(x)$$

（对 f_1 的 degree 归纳，设 $b_m^k f_1(x) = q(x)g(x) + r(x)$ $\quad \deg(r) < \deg(g)$

$$b_m^{k+1} f(x) = b_m^k a_m x^{n-m} g(x) + b_m^k f_1(x)$$

$$= b_m^k a_m x^{n-m} g(x) + q(x)g(x) + r(x)$$

$$= \left(b_m^k a_m x^{n-m} + q(x)\right) g(x) + r(x)$$

新的 $q(x)$

最开始的 b_m 应该是 $f_1(x) = b_m f(x) - a_m x^{n-m} g(x)$ 这里出来的，之后就套娃套上了。主要是因为不能作除法。

我们现在证之前 $f(x) = (x-a)q(x) + f(a)$ 的 uniqueness.

$$(x-a)q_1(x) + f(a) = (x-a)q_2(x) + f(a)$$

$$\Rightarrow \quad (x-a)\left(q_1(x) - q_2(x)\right) = 0 \quad \Rightarrow \quad q_1(x) = q_2(x)$$

$\{\text{fields}\} \subseteq \{\text{PID}\} \subseteq \{\text{integral domain}\} \subseteq \{\text{commutative ring}\}$

Def: An integral domain is a P.I.D if every ideal is principle, i.e., every ideal can be generated by a single element

Ex: F field has (0), (1) ideals.

$\mathbb{Z}$ (Bezout), $\mathbb{Z}[i]$.

Thm: If F a field, then $F[x]$ is a PID.

Pf: We can assume that $\exists f(x) \in I$, s.t. $\deg(f(x)) \geq 0$

This allows us to find $g(x) \in I$ has the smallest degree.

$\forall f \in I$, $f(x) = q(x)g(x) + r(x)$ 只能是 0.

$$\Rightarrow f = qg \quad \Rightarrow \quad I \supseteq (g) \quad \Rightarrow \quad I = (g)$$

Remark: If F field, $F[x_1, x_2]$ is not a PID.

(x_1, x_2) X

If F a field, we can consider F[u]

$$F[x] \xrightarrow{ev_u} F[u]$$

$$x \longmapsto u$$

$$F \longmapsto F$$

$\ker(ev_u) = I$, s.t. $I \cap F = \{0\}$

Thm: Let u be an algebric number in F with minimal polynomial g

Then $F[u] \cong F[x]/(g(x))$

① F[u] is a field if $g(x)$ is irreducible. 要不然基本不是 integral domain.

if $g(x) = h_1(x)h_2(x)$, then either h_1 or h_2 a unit.

② F[u] has zero divisor if $g(x)$ is reducible.

Pf: ① Ideals in $F[u] \cong F[x]/(g(x))$ are of the form $I/(g(x))$ where I is an ideal of F[x] containing $(g(x))$. Since F[x] PID, we can write $I = (f(x))$

$(f(x)) \supseteq (g(x)) \Rightarrow f(x) \mid g(x)$, since g irreducible.

1) f = constant (unit) $\Rightarrow (f) = F \Rightarrow (f)/(g) = (1)$.

2) $f = g \Rightarrow (f) = (g) \Rightarrow (f)/(g) = (0)$

② 反証法

Thm: Let F be a field, $f(x)$ be a degree n polynomial in F[x],

Then $f(x)$ has at most n distinct roots in F.

($f(a) = 0 \iff (x-a) \mid f(a)$)

設 $\{r_i\}$ roots, 再归纳证 $\prod (x-r_i) \mid f$, 那么最少有 # i degree.

Thm: Any finite subgroup of the non-zero element of a field F is cyclic.

Lemma: $\exp(G)$ = G中最大的 order, G cyclic $\Leftrightarrow \exp(G) = |G|$

Pf: Let G be a finite subgroup of $F\setminus\{0\}$

Let $f(x) = x^{\exp(G)} - 1$

$f(x)$ has at most $\exp(G)$ roots in $F \Rightarrow$ has most $\exp(G)$ roots in G.

However, $\forall x \in G$, $f(x) = 0$ (definition of exp) $\Rightarrow |G| \le \exp(G)$

$\Rightarrow |G|$ cyclic.

Remark: The analogous statement does not hold for division rings

$\{\pm 1, \pm i, \pm j, \pm k\} \le$ Quaterion ring.

Communitive setting:

Fields $\subseteq$ Enclidean domains $\subseteq$ PID $\subseteq$ UFD $\subseteq$ Integral domain.

Def: An integral domain R is called a **unique factorization domain** if every nonzero nonunit element has a "unique" factorization into irreducible elements.

Def: x is **irreducible** if $x = ab \Rightarrow a$ or b unit.

"unique" factorization means unique up to units.

Example: $\mathbb{Z}$ is a UFD. $25 = 5\times 5 = -5 \times -5$

Non-Example: $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$

$6 = 2\times 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ 易证 factor up to a unit

irreducible.

Consider a norm $\mathbb{Z}[\sqrt{-5}] \xrightarrow{N} \mathbb{Z}$

$a+b\sqrt{-5} \longmapsto a^2+5b^2$.

$N(a)=1 \Leftrightarrow a$ a unit

$N(2)=4$, $N(3)=9$, $N(1+\sqrt{-5})=6$.

Thm Any PID is a UFD.

Def: An integral domain R is called a **Euclidean Domain** if

$\exists S: R \to \mathbb{Z}_{\geq 0}$, $\forall a, b \neq 0 \in R$, $\exists q, r \in R$, s.t.

$a = bq + r$, where $S(r) < S(b)$

Thm: If R is an UFD, then $R[x]$ an UFD

Def: An element is **prime** if $x \mid ab \Rightarrow x \mid a$ or $x \mid b$.

Claim: Every prime element is irreducible.

$p = ab$ 不妨设 $\wedge$ $p \mid a$ 证 b unit $\Rightarrow a = pk$.

$p = pkb \Rightarrow kb = 1 \Rightarrow b$ unit.

If $a, b \in R$, $\gcd(a,b)$ exists if $\forall d$, $d \mid a \wedge d \mid b \Rightarrow d \mid ab$.

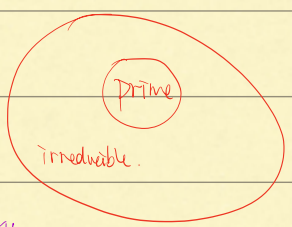
Thm: An integral domain R is an UFD iff

① R contains no infinite properly ascending chain of principle ideals. i.e. if $(a_1) \subseteq (a_2) \subseteq \cdots \subseteq (a_n) \subseteq \cdots$

then for large enough n, $(a_n) = (a_{n+1})$

② Every irreducible element is a prime.

irreducible 不能拆出 unit ⟵ ⟶ $p \mid ab \Rightarrow p \mid a \vee p \mid b$



但在 UFD 上证明，因为可以拆成"一" time 的乘积。

Pf: "UFD ⇒ ① ② / (②)"

Assume $(a_1) \subsetneq (a_2) \subsetneq \cdots \subsetneq (a_n) \subsetneq \cdots$

($(3) \supsetneq (9) \supsetneq (27) \supsetneq \cdots$ 反被允许的)

$\forall\, i,\ (a_i) \supsetneq (a_1) \Rightarrow a_i \mid a_1$

Since R UFD, factor a_1 into $a_1 = \prod_1^r p_i^{k_i}$, 矛盾

Let x be an irreducible element in R, s.t. $x \mid ab$.

if a/b unit ⇒ ✓

if $a = q_1 q_2 \cdots q_n$

$b = q_1' q_2' \cdots q_m'$

$\Rightarrow ab = q_1 q_2 \cdots q_n q_1' q_2' \cdots q_m'$

x must be one of them (UFD)

① ② ⇒ UFD.

Let $x \in R$.

1) x irreducible ⇒ x has unique ~~factorization~~.

2) x not irreducible: $x = a_1 b_1$, where a_1, b_1 not units.

$x = a_1 b_1 \rightarrow a_1 = a_2 b_2 \rightarrow a_2 = a_3 b_3 \cdots$ $a_i b_i$ are all reducible.

$\Rightarrow (x) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \cdots$

By ①, $\exists\, a_i$, a_i irreducible. Let $p_1 = a_i$

$\Rightarrow x = p_1 x_1$

$\Rightarrow x = p_1 p_2 \cdots p_n x_n$, where x_n irreducible.

if $x = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$

对 n 归纳.

Base case: $n = 1$, then $x = p_1 = q_1 \cdots q_m \Rightarrow m = 1$

$\Rightarrow p_1 = q_1 \Rightarrow$ factorization is unique.

Inductive Step: Assume any element that factors into $n-1$ irreducible elements has a unique factorization.

Since p_1 is irreducible, it is prime by 2.

$p_1 \mid q_1 \cdots q_m \Rightarrow p_1 \mid q_i$ for some i. WLOG, $i=1$

$\Rightarrow q_1 = p_1 k$

$x = p_1 \cdots p_n = q_1 \cdots q_m \Rightarrow y = \underbrace{p_2 \cdots p_n}_{\text{unique.}} = k q_2 \cdots q_m$

■

Thm: Any PID is a UFD.

Pf: WTS: PID satisfies ① & ②.

For ①, if $(a_1) \subsetneq (a_2) \subsetneq \cdots \subsetneq (a_n) \subsetneq \cdots$

$I = \bigcup_{i=1}^{\infty} (a_i)$ is a ideal. Let $I = (b)$

$\Rightarrow b \in (a_j)$ for some j. $\Rightarrow (b) \subseteq (a_j)$

$\Rightarrow (b) \subseteq (a_j) \subseteq (a_{j+1}) \subseteq I = (b) \Rightarrow (a_j) = (a_{j+1})$

So ① holds.

For ②: Let x be an irreducible element in R

$x \mid ab$. Consider (x) to contain is to divide.

x irreducible $\Rightarrow \exists I$, s.t. $(x) \subsetneq I \subsetneq R$.

Assume $x \nmid a \Rightarrow a \notin (x) \Rightarrow (x) \subsetneq (x, a) \Rightarrow (x, a) = (1) = R$.

$\Rightarrow c, d \in R$, s.t. $ac + dx = 1$

$\Rightarrow abc + dbx = b$

$\Rightarrow xkc + dbx = b$

$\Rightarrow x \mid b$

Def: An integral domain R is called a Euclidean Domain if

$\exists\, \delta : R \to \mathbb{Z}_{\geq 0}$, $\forall\, a, b \neq 0 \in R$, $\exists\, q, r \in R$, s.t.

$$a = bq + r \quad , \text{ where } \delta(r) < \delta(b)$$

Example: ① $\mathbb{Z}$ with $\delta(z) = |z|$

② F field, $F[x]$ with $\delta(f(x)) = 2^{\deg(f)}$

③ $\mathbb{Z}[i]$ with $\delta(a+bi) = a^2 + b^2$

$\delta(z_1)\,\delta(z_2) = \delta(z_1 z_2)$

if $z_1, z_2 \in \mathbb{Z}[i] \Rightarrow \frac{z_1}{z_2} = \alpha + \beta i \in \mathbb{Q}[i]$

$\Rightarrow \exists\, u, v \in \mathbb{Z}$, s.t. $|u-\alpha|, |v-\beta| < \frac{1}{2}$

Let $q = u + vi$, $z_1 = z_2 q + r$.

$r = z_1 - z_2 q$

$= z_2\left((u-\alpha) + (v-\beta)i\right)$

$\delta(r) = \delta(z_2)\left(\underbrace{(u-\alpha)^2}_{\leq \frac{1}{4}} + \underbrace{(v-\beta)^2}_{\leq \frac{1}{4}}\right)$

$\leq \frac{1}{2}\delta(z_2)$

$< \delta(z_2)$

So $\mathbb{Z}[i]$ is an Euclidean Domain.

Q: For which (squarefree, negative) d, does the analogous proof holds for $\mathbb{Z}[\sqrt{d}]$?

$$\delta(a+b\sqrt{d}) = x^2 - dy^2$$

Thm: Every Euclidean domain is a PID.

Pf: Let R be an Euclidean domain with δ, I be an ideal of R.

If $I = (0)$, then I is principal

Assume I is nonzero:

Let $b \in I$, where $S(b)$ smallest.

If $a \in I$, then $\exists q, r \in R$, s.t. $a = bq + r$, where $S(r) < S(b)$

Since $a \in I$, $bq \in I$, $\Rightarrow r \in I \Rightarrow r = 0$

$\Rightarrow \forall a \in I$, $a = bq \Rightarrow I = (b)$

Thm: R UFD $\Rightarrow R[x]$ UFD

Pf: Let R be an UFD. 我们在 UFD 里可以算 gcd.

Modules over ~~Rings~~ PIDs. (Vector Spaces over fields)

Modules, like Vector Spaces, are abelian groups.

Let M be an (additive) abelian group.

Def: The set of endomorphisms on M

$\mathrm{End}(M)$ consists of group homomorphism $M \to M$

和以前像 antomorphism 一样，只不过这里是 homomorphism.

If $f \in \mathrm{End}(M)$, then $f: M \to M$ and $f(x+y) = f(x) + f(y)$

Prop: $\mathrm{End}(M)$ is a ring.

Pf: 封闭性显然，只需证是 homomorphism.

Recall: All group $G \leq S_{|G|}$. Every group can be thought of an action on a set.

Q: Is every ring a subring of $\mathrm{end}M$ of some abelian group M?

Theorem: Yes.

Pf: If R is a ring, then let M = additive group R (forget multiplicative structure)

If $r \in R$, let $f_r : M \to M$, $f_r(x) = r \cdot x$

Then $f_r(x+y) = r(x+y) = rx + ry = f_r(x) + f_r(y)$

$\Rightarrow f_r \in \mathrm{End}(M)$, but in particular, f_r allow us to use $r \in \mathrm{End}(M)$

Define a map : $R \longrightarrow \mathrm{End}(M)$

$r \longmapsto f_r$

这里是要把 R 集中地射到 End(M) 里，有点像 Cayley's thm.

To show that this map is a ring homomorphism

$\forall\, r_1, r_2 \in R$, $f_{r_1+r_2} = f_{r_1} + f_{r_2}$.

$f_{r_1 r_2} = f_{r_1} \circ f_{r_2}$.

And this map is injective: suppose $f_s = f_r$,

then $f_{s(1)} = s = r = f_{r(1)}$. So $s = r$.

So there is an injective ring homomorphism

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

Def: If R is a ring, a (left) R-module is an abelian group M together with a map $R \times M \to M$, (scalar product.)

satisfying
① $r(x+y) = rx + ry$
② $(r+s)y = ry + sy$ } 两个分别分配率
③ $rs(x) = r(sx)$ 结合率
④ $1 \cdot x = x$ 标量乘法的麻…

If there is a homomorphism φ of $R \to \mathrm{End}(M)$ for some abelian group M, then we can define the map

$R \times M \to M$

$r(m) \longmapsto \varphi(r)(m)$

will satisfy ①②③④, hence M gets equipped with a left R-module structure.

Conversly, if M has a R-module structure, then we can define a map $f_r : M \to M$, $x \mapsto rx$, and define that

$$R \longrightarrow \mathrm{End}(M)$$
$$r \longrightarrow f_r \quad \text{is a ring hom.}$$

Def: right R-module.

From now on, all modules are left module.

Def: A submodule N of a module M is:

$N \leq M$ (as groups) and N is closed under the action of R, i.e.

$$\begin{cases} x \in N,\ r \in R \Rightarrow rx \in N \\ x, y \in N \Rightarrow x+y \in N. \end{cases}$$

Submodule criterion: (Subspace criterion)

$\forall r \in R,\ x, y \in N, \Rightarrow rx+y \in N$

Lemma: Let M be an R-module:

① $r \cdot 0_M = 0_M$, $\forall r$. $f_r : M \xrightarrow{f_r} M$ homomorphism.
$f_r(m+(-m)) \Rightarrow rm + r(-m) = 0 \Rightarrow r(-m) = -(rm)$

② $r \cdot (-m) = (-r) \cdot m = -(r \cdot m)$, $\forall m, r$. $f_{-r} = -f_r$.

③ $0_R \cdot m = 0_M$, $\forall m$ $f_0 = 0$

Example: Linear transformations of vector space over a field.

Let $R = F$ field

Let $M = V$ be a vector field over F

Let $T: V \to V$ be a linear transformation:

Then $\begin{cases} T(v_1) + T(v_2) = T(v_1 + v_2) & ① \\ T(cv) = cT(v) & ② \end{cases}$

① $\Rightarrow T \in \mathrm{End}(M)$

② $\Rightarrow T \circ f_c = f_c \circ T$, $\forall c \in F$.

"在左边乘上 c"

Then $F \xrightarrow{\varphi} \mathrm{End}\, V$ $\qquad V \xrightarrow{f_c} V$

这里我们已经有 V 这个 vector space 了，所以我们定义 $f_c(x) = cx$.

$c \longmapsto f_c$ is a ring homomorphism

- $\varphi(F) = \mathrm{im}(\varphi) = \{ f_c \text{ "c"} \mid c \in F \}$ is a subring of $\mathrm{End}\, V$.
- $\varphi(F)[T] = \{ f_{c_0} + f_{c_1} T + f_{c_2} T^2 + \cdots \mid c_i \in F \}$ 这里就相当于 $\mathbb{R}[x] = \{ a_0 + a_1 x + a_2 x^2 + \cdots \}$

By ②, $\varphi(F)[T]$ is communitive.

$F[x] \longrightarrow \varphi(F)[T] \hookrightarrow \mathrm{End}\, V$

$\sum a_i x^i \longmapsto \sum f_{a_i} T^i$

Altogether: we get the map $F[x] \to \mathrm{End}\, V$

So V is a $F[x]$ module.

$(a_n x^n + \cdots + a_0)(v) = f_{a_n} \circ T^n(v) + \cdots + f_{a_0} v$.