MA3201 Algebra II. chap 7: Rings. Date No.

Bao Huan Chen S17-0617 MW in office 10am-4pm.

Defn 1. ring $R=(S,+,\times)$ satisfies:
(i) $(R,+)$ is an Abelian group. (must have a "0")
(ii) $\times$ is associative
(iii) $\times$ distributive over $+$ (both sides) in R.
2. R is commutative if $\times$ is comm.
3. R has a identity if $1\in R$ s.t. $1\times a = a\times 1 = a$ $\forall a\in R$.

Remark + being comm. is forced. Ie, if $\exists 1\in R$, then
$(1+1)(a+b) = 1(a+b)+1(a+b) = a+b+a+b$
$(1+1)(a+b) = a+a+b+b$.
and they must be equal (by defn of $\times$ as a fn).

$(\mathbb{Z},+,\times)$ is a ring (in fact, comm. ring)
$(\mathbb{Z},+)$ is a group.
$(\mathbb{Z},\times)$ is not a group (inverse)

Defn (Division ring / skew field) is $R\neq 1\in R$ (s.t. $1a=a1=a$) if
$\forall a$, $\exists$ inverse a^{-1} s.t. $aa^{-1}=a^{-1}a=1$. ("$(R,\times)$ is also a group")
(Field): comm. division ring. ↗ not true since 0.
(Division ring) $\Leftrightarrow$ $(R\setminus\{0\},\times)$ is a group.

Eg. 1. $(\mathbb{Z},+,\times)$ is a ring, $\mathbb{Q},\mathbb{R},\mathbb{C}$ are rngs. (all are comm.)
2. $\mathbb{Q},\mathbb{R},\mathbb{C}$, are fields.
3. R be the set of cont/diff functions $f:\mathbb{R}\to\mathbb{R}$. define $(f+g)(x) = f(x)+g(x)$, $(f\cdot g)(x) = f(x)\cdot g(x)$. Then R is a ring with 1 as $x\mapsto 0$ is the 0 in R. $x\mapsto 1$.
R is not a field $f(x)=x$ has no mult. inverse ($x\mapsto \frac{1}{x}$ is not continuous at 0).
3.1 Let R' be the set of cont/diff fns $f:\mathbb{R}\setminus\{0\}\to\mathbb{R}$.
Then $x\mapsto \frac{1}{x}\in R'$ is a rng. (check).
3.2 rng of polynomial fns $f:\mathbb{R}\to\mathbb{R}$.

Date No.

4. Let $V/\mathbb{R}$ be a finite dim. vector space over $\mathbb{R}$. Then let
$\mathrm{End}_{\mathbb{R}}(V)$ = the lin. maps from V to V.
then $(\mathrm{End}_{\mathbb{R}}(V), +, \circ = \text{composition})$ is a rng with 1 (id).

5. $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$ is the quotient gp $(\mathbb{Z},+)/(n\mathbb{Z},+)$
we define $\times : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $(\bar{a}, \bar{b}) \mapsto \overline{a \cdot b}$
where $a \in \mathbb{Z}$, $\bar{a}$ is the cong. class of a mod n.
(Ex: check that $\times$ is well-defined and $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ is a rng.
(Ex. show that if n prime, it is a field).

6. The ring of single elem $\{*\}$, $* = 0 = 1$,
$+ : \{*\} \times \{*\} \to \{*\}$, $\times : \{*\} \times \{*\} \to \{*\}$, $+ = \times$.
Ex: why $0 = 1 \Rightarrow R = \{*\}$? (i.e. $|R| = 1$)
ans: $\forall a \in R$, $a = 1 \times a = 0 \times a = 0$.
(qn: show that $\forall a \in R$, $a \times 0 = 0 \times a = 0$)

7. $2\mathbb{Z}$ is a rng without 1.

Prop. Let R be a rng.
1. $0 \times a = a \times 0 = 0$.
$0 \times a = (0+0)a = 0a + 0a \Leftrightarrow 0 = 0a$ v.v. □.
2. $(-a)b = a(-b) = -(ab)$.
$0 = (a-a)b = ab + (-a)b \Rightarrow (-a)b = -(ab)$. v.v. □
3. if $1 \in R$, then 1 is unique and $-a = (-1)a$.
Suppose $1' \cdot a = a \cdot 1' = a$ $\forall a \in R$.
then $1' \cdot 1 = 1 \cdot 1' = 1 = 1'$ □
$0 = a + (-a) = 1a + (-1)a = (1 + (-1))a$.
$\therefore a + (-a) = a + (-1)a$. □
4. $(-a)(-b) = ab$.
$(a-a)(-b) = a(-b) + (-a)(-b) = 0$.
$\therefore -[a(-b)] = (-a)(-b) \Rightarrow -[-(ab)] = (-a)(-b)$

MA3201 Chap 7 (2). Date No.

Defn 1. (zero divisor) An elem $0 \neq a \in R$ is called a zero divisor if $\exists\ 0 \neq b \in R$, s.t. $a \cdot b = 0$ or $b \cdot a = 0$.
Eg. Let $R = \mathbb{Z}/4\mathbb{Z}$. Then $\bar{2} \cdot \bar{2} = \bar{4} = \bar{0}$ $\therefore$ $\bar{2}$ is a zero divisor.

2. (units) Assume $0 \neq 1 \in R$. $u \in R$ is a unit in R if $\exists v \in R$ s.t. $uv = vu = 1$. Denote the units of R, $R^\times = \{x \in R \mid \exists y \in R, xy = yx =$

Lemma Let $0 \neq 1 \in R$. Then $(R^*, \times)$ is a group.
pf: has inverse, identity, and is assoc.
(unit). (given) (given smeary).

Eg. 1. consider $R = \mathbb{Z}/6\mathbb{Z}$. then $\bar{2}, \bar{3}, \bar{4}$ are zero zero divisors, (note: cannot be 0).
$\bar{1}, \bar{5}$ are units. (note: can be 1
$(\mathbb{Z}/6\mathbb{Z})^* = \mathbb{Z}_6^*$ is a group.

Claim: $(\mathbb{Z}/n\mathbb{Z})^* = \{\bar{a} \mid (a,n) = 1, a \in \mathbb{Z}\}$.
Basically Bezout's lemma. $ax + ny \equiv ax \equiv 1 \pmod n$.
of fns from $\mathbb{R}$ to $\mathbb{R}$.
2. R be the ring . then
$f(x) = \begin{cases} 0 & \text{if } x \leq 0 \\ 1 & \text{if } x > 0. \end{cases}$ is a zero divisor.

Ex 1. $(\mathbb{R}^{\mathbb{R}}, +, \circ)$ is not a rng (distributivity)
we claim $h \circ (f+g) \neq h \circ f + h \circ g$. where $h(x) = x^2$, $f(x) = 2x$, $g(x) = 3x$.
$(5x)^2 = 25x^2$ $4x^2 + 9x^2 = 13x^2$.
2. (Polynomial rng) rng of polynomials $R[x]$ of rng-coeffs.
eg. $\mathbb{R}[x]$, $\mathbb{Q}[x]$, $\mathbb{Z}[x]$.
3. Quaternion (Hamilton). with $\mathbb{R}$ coeffs.
4. (Matrix rng, matadd, matmul) with rng entries.
5. Group rng. G finite group, R comm. rng $\neq 0$. The group rng.
$R[G] = \{\sum_{g \in G} a_g \cdot g \mid g \in G, a_g \in R\}$.
Define $+$: comp. wise add.
$\times$: as usual. $(a_1 g_1 + a_2 g_2)(a_1' g_1' + a_2' g_2')$
$= a_1 \cdot a_1' \cdot g_1 \cdot g_1' + \dots$

int.dom: comm. ring with no zero divisor (just like integers)
div.ring: everything (non-0) is invertible ∃

Date No.

4. The group ring $\mathbb{C}[\mathbb{Z}/2\mathbb{Z}]$. $\mathbb{Z}/2\mathbb{Z} = \{e, x\}$ s.t. $x^2 = e$.
then $a \cdot e + b \cdot x$ are elmts. ($0 \cdot e = 0$, $0 \cdot x = 0$)
then $(2 \cdot e + 3 \cdot x)^2 = 4e + 6x + 6x + 9 \cdot x^2 = 13e + 12x$.

claim: $\mathbb{C}[\mathbb{Z}_2]$ is a 2-dim $\mathbb{C}$-vectorspace with a basis $\{e, x\}$.

Defn (subrings) A subring S of $(R, +, \times)$ is a (+ additive subgp) that is closed under $\times$. Eg: 1. $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$
2. $2\mathbb{Z} \subset \mathbb{Z}$ ✱ $2\mathbb{Z}$ has no 1.

Defn (Integral domain) A comm. ring $R \ni 1 \neq 0$ is called an integral domain if R has NO zero divisor.
Eg: ① $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$ (in fact, any $\mathbb{F}$) are integral domains (everything inv)
② $\mathbb{Z}$ is an int. dom.
③ $\mathbb{C}[\mathbb{Z}_2]$ is NOT an int.dom, even though comm.
$(1+x)(1-x) = 1 - x^2 = 1 - 1 = 0$ are 0 divs.
③.1 G finite, $R[G]$ is NOT int dom. (?)
$\neq \{1\}$.

Prop (cancellation for int.dom.) Let R be an int. dom. Let $x, y, z \in R \setminus \{0\}$.
then if $xy = xz$, $y = z$.
Note: not true for non-int.dom: $(1-x)(1+x) = (1-x) \cdot 0 = 0$ but $(1-x) \neq 0$

Pf: $xy = xz \Rightarrow xy - xz = 0 \Rightarrow x(y-z) = 0$.
but $x \neq 0$. Since int.dom, one of $x, y-z$ must be 0. $\therefore y = z$. □

Thm ($\Rightarrow$ comm.) R finite. int.dom. Then R is a field $\Leftrightarrow$ comm. div.ring (everything (non 0) is inv).

Pf: WTS $\forall x \in R - \{0\}$, $\exists y \in R - \{0\}$ s.t. $xy (= yx) = 1$.
We consider the map $\tilde{x}: R \to R$, $a \mapsto x \cdot a$. $\tilde{x}$ is injective by cancellation
i.e. $x \cdot a = x \cdot b \Rightarrow a = b$ (R is int.dom)
Since R is finite, $\tilde{x}$ has to be bijective. Thus the pre-image of 1 is the y desired (since $x \cdot a = 1$). □

MA3201 Chap 7 (3) Date No.

Defn (product Rng) Let S, R be rngs. Define product rng $S \times R$ as follows:
set: $S \times R = \{(s,r) \mid s \in S, r \in R\}$
$+, \times$: component-wise.
Check: assoc & dist.
Identity (if S, R have): $(1_S, 1_R)$.

Fact. – $S' = \{(s,0) \mid s \in S\}$ is a subring of $S \times R$, identity is $(1_S, 0)$ (if $1_S \in S$)
– $S \times R$ is not an integral domain (even if both are integral domains, given $S, R \neq \{0\}$)
since $(s,0) \cdot (0,r) = (0,0)$.

Lem Consider $R[x]$ the polynomial rng of an int. dom R. Then $R[x]$ is an int. dom. (So $(R[x])[y] = R[x,y]$ is also an int. dom.)

Pf: Let $f(x) = a_n x^n + \dots + a_1 x + a_0 \in R[x]$, $a_n \neq 0$.
we then define $\deg(f(x)) = n$.
Let $f(x), g(x) \in R[x]$, s.t. $\deg f(x) = n$, $\deg g(x) = m$.
Claim: $\deg(f(x)g(x)) = m+n$.
Let $g(x) = b_m x^m + \dots + b_0$, $b_m \neq 0$.
then $f(x)g(x) = a_n \cdot b_m x^{m+n} + \dots$
and R being int. dom. guarantees $a_n \cdot b_m \neq 0$. □claim.

Observe that the highest degree does not vanish $\Rightarrow$ never get 0 $\Leftrightarrow$ all coeff $\neq 0$

Cor. We have $(R[x])^* = R^*$

Pf: ($\subseteq$) Let $a \in (R[x])^*$. Deg $a = 0$, otherwise $\forall b \in R[x]$,
$\deg(ab) \geq 1$ but $\deg(1) = 0$.
($\supseteq$) straightforward. □

Ring Homom. & Ideals.

Date No.

Def Let R and S be rings.

1. A ring homom. $\varphi: R \to S$ a map s.t.
   $\varphi(a+b) = \varphi(a)+\varphi(b)$, $\varphi(a\cdot b) = \varphi(a)\varphi(b)$. $\forall a,b \in R$
2. $\ker\varphi = \{a \in R \mid \varphi(a) = 0_S\} = \varphi^{-1}(0_S)$
3. Bijective ring homom. is a ring isom. $R \cong S$. if $\exists\ R \xrightarrow{\text{hom}} S$.

Eg.

1. The id map is a isom.
2. $\varphi: \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ is a homom, $\ker\varphi = 2\mathbb{Z}$. (we only verify $\times$ more + is silently group hom.)
   Since $\varphi(a\cdot b) = \varphi(a)\cdot\varphi(b)$ ($\overline{a\cdot b} = \bar{a}\cdot\bar{b}$.) (zero map, id map)
3. $\varphi: \mathbb{Z} \to \mathbb{Z}$, $a \mapsto n\cdot a$ is NOT a ring homom. if $n \neq 0, 1$
   we check $\varphi(a+b) = n(a+b) = n\cdot a + n\cdot b = \varphi(a)+\varphi(b)$.
   but $\varphi(a\cdot b) = n\cdot a\cdot b \neq n\cdot a\cdot n\cdot b = \varphi(a)\varphi(b)$.
6. R comm. with $1 \neq 0$. we consider $\varphi: R[x] \to R$, $f(x) \mapsto f(a)$ $a \in R$.
   then φ is a ring hom. (R needs to be comm.
   Check: Let $f(x) = rx$, $g(x) = sx$
   $\varphi(f(x)+g(x)) = rx+sx \mid_{x=a} = ra+sa = (r+s)a = (f+g)(a) = \varphi(f(x)) + \varphi(g(x))$
   $\varphi(f(x)\cdot g(x)) = rsx^2 \mid_{x=a} = rsa^2$
   $\varphi(f(x))\varphi(g(x)) = ra\cdot sa$ //☆
7. Let $G = \{e\}$ be the trivial gp. Then $R[G] \cong R$.

Lem Let $\varphi: R \to S$ be a ring hom.

1. $\mathrm{Im}(\varphi)$ is a subring of S.
2. $\ker\varphi$ is a subring of R.
3. φ is an isom. $\iff \exists$ a ring hom. $\psi: S \to R$ $\varphi\circ\psi = \mathrm{id}_R$ ☆ $\psi\circ\varphi = \mathrm{id}_S$.

Pf(2): we check that $\ker\varphi$ is closed in $\times, +$.
$\varphi(a+b) = \varphi(a)+\varphi(b) = 0+0 = 0$ $\therefore a+b \in \ker\varphi$.
$\varphi(a-b) = \varphi(a)\cdot\varphi(b) = 0\cdot 0 = 0$ $\therefore a\cdot b \in \ker\varphi$.
(1): $\forall\ \varphi(a), \varphi(b) \in \mathrm{Im}(\varphi)$,
$\varphi(a)+\varphi(b) = \varphi(a+b)$ $\because a+b \in R$.
— actually a subring is a subgp first and foremost. we use one step subgp test for $(R,+)$ $\Leftarrow$ closure of subtraction & then closure of $\times$

MA3201 Chap 7 (4).

Date

No.

Pf. (3) $\Rightarrow$ given $\varphi: R \to S$ is a bijective hom., WTS $\exists\ \psi: S \to R$ s.t. $\varphi \circ \psi = id_S$, $\psi \circ \varphi = id_R$.

Define φ^{-1} (set theoretic) inverse: $\varphi^{-1}: S \to R$, $s \mapsto \varphi^{-1}(s)$.

Now we check φ^{-1} is a ring hom.

$\varphi^{-1}(\varphi(a) + \varphi(b)) = \varphi^{-1}(x+y)$ where $a, b \in R$, $x, y \in S$.

$= \varphi^{-1}(\varphi(a+b)) = a+b$

$= \varphi^{-1}(\varphi(a)) + \varphi^{-1}(\varphi(b))$.

$\varphi^{-1}(\varphi(a) \cdot \varphi(b)) = \varphi^{-1}(\varphi(a \cdot b)) = a \cdot b$

$= \varphi^{-1}\varphi(a) \cdot \varphi^{-1}\varphi(b)$. □.

Lem Let $\varphi: R \to S$ be a ring hom. Then φ is inj $\iff \ker \varphi = \{0\}$.

Pf: follows by the fact that φ is also a gp hom. (of abelian gp $(R, +)$)

Def. Let R ring, $I \subseteq R$ a subset. $rI = \{ra \mid a \in I\}$ and $Ir = \{ar \mid a \in I\}$.

1. I is a left ideal of R if I is a subring & $r \cdot I \subseteq I$ $\forall r \in R$.
2. " right " $I \cdot r \subseteq I$ $\forall r \in R$.
3. I is a (2-sided) ideal of R if I subring of R, both left & right ideal.

Lem $\varphi: R \to S$ be a ring hom. Then $\ker \varphi$ is an ideal of R.

Pf: Suffices to show $\forall r \in R$, ~~[illegible]~~

$r \cdot \ker \varphi \subseteq \ker \varphi \ \wedge\ \ker \varphi \cdot r \subseteq \ker \varphi$.

$\therefore \varphi(r \cdot x) = \varphi(r) \cdot 0 = 0 \Rightarrow r \cdot x \in \ker \varphi \ \forall x \in \ker \varphi,\ r \in R$

$\varphi(x \cdot r) = 0 \cdot \varphi(r) = 0 \Rightarrow x \cdot r \in \ker \varphi \ \forall$ ——.

Eg. 1. $n\mathbb{Z} \subseteq \mathbb{Z}$ is an ideal.

2. $0 \subseteq R$, $R \subseteq R$ are ideals.

3. $(R, 0) \subseteq R \times S$ is an ideal.

Def. (Quotient rngs) $I \subseteq R$ be an ideal, then R/I is defined as follows:

- As an Abelian gp, R/I is just the quotient group. $(a + I = \bar{a})$.
- Define multiplication: $R/I \times R/I \to R/I$.

$(\bar{a}, \bar{b}) \mapsto \overline{a \cdot b}$.

since we pick representatives, check $\bar{a}' = \bar{a}$, $\bar{b}' = \bar{b}$

then $\overline{a' \cdot b'} = \overline{a \cdot b}$:

Date No.

Pf: (well-def) $(a+I, b+I) \mapsto (a+I)(b+I)$. $\{i \cdot j \mid i, j \in I\}$.

$= a\cdot b + a\cdot I + I\cdot b + I\cdot I$.

Let $a' = a+i_1$, $b' = b+i_2$.

$a'\cdot b' = a\cdot b + a\cdot i_2 + i_1\cdot b + i_1\cdot i_2 \in a\cdot b + I$.

$\therefore \overline{a'\cdot b'} = \overline{a\cdot b}$ □

Claim R/I is a rng, $\bar{a}+\bar{b} = \overline{a+b}$, $\overline{a\cdot b} = \bar{a}\cdot\bar{b}$.

Eg. $\mathbb{Z}/n\mathbb{Z}$, $R/0 \cong R$, $R/R \cong 0$.

Thm. (Isom. Thm) $I \subseteq R$ be an ideal.

1. Natural quotient map $\pi: R \to R/I$, $a \mapsto \bar{a}\ (= a+I)$, is a rng hom.
2. Let $\varphi: R \to S$, be a rng hom. Then $R/\ker\varphi \cong \varphi(R)$.
3. $\|$ such that $I \subseteq \ker\varphi$. Then φ factors thru R/I, that is, $\exists!$ a rng hom $\bar{\varphi}: R/I \to S$ such that the following diagram commutes:

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ \pi \downarrow & \nearrow_{\bar{\varphi}} & \\ R/I & & \end{array}$$

(3 is usually called the universal prop. of quotient).

Pf: (1) Show π is a rng hom:

$\pi(a+b) = (a+b)+I = a+I+b+I$.

$\pi(a\cdot b) = a\cdot b + I = (a+I)(b+I)$

(actually $+$ is given by group hom).

(2). We already have $\cong$ groups. remains to check for mult.

(no need for bijections, since group isom implied it).

$\therefore$ WTS $\varphi': R/\ker\varphi \to \varphi(R)$, and $\varphi'(\overline{a\cdot b}) = \varphi'(\bar{a})\cdot\varphi'(\bar{b})$.

where $a, b \in R$.

$\therefore \varphi'(\overline{a\cdot b}) = \varphi'(a\cdot b + I) = \varphi(a\cdot b) = \varphi(a)\cdot\varphi(b)$

$= \varphi'(\bar{a})\cdot\varphi'(\bar{b})$.

MA3201 Chap 7 (5) Date No.

Pf (3): Let $\bar{\varphi}: R/I \to S$ $\quad a+I \mapsto \varphi(a)$.

This is the intuitive map following the diagram.

Check: well-defined Let $a+I = a'+I$.

then WTS $\bar{\varphi}(a+I) = \bar{\varphi}(a'+I)$.

but clearly LHS: $\varphi(a)$, rhs $= \varphi(a') = \varphi(a+i)$ for some $i \in I$

$= \varphi(a) + 0 = \varphi(a)$.

Ringhom: $\bar{\varphi}(\bar{a}\cdot\bar{b}) \stackrel{?}{=} \bar{\varphi}(\bar{a}) + \bar{\varphi}(\bar{b})$

Eg. 3. G finite group, R comm. rng. with $1 \neq 0$. Then

$\pi: R[G] \to R$, $\sum_{g\in G} a_g \cdot g \mapsto \sum_{g\in G} a_g$. is a rng. hom.

WTS $\pi((ag+bh)(a'g'+b'h')) = \pi(ag+bh)\pi(a'g'+b'h')$

$= \pi(aa'gg' + ab'gh' + ba'hg' + bb'hh')$

$= aa' + ab' + ba' + bb'$

$= (a+b)(a'+b') = \pi(ag+bh)\pi(a'g'+b'h')$.

Lem. $\varphi: G \to H$ be a gp hom. Then φ induces a rng hom $\varphi': R[G] \to R[H]$,

$\sum_{g\in G} a_g \cdot g \mapsto \sum_{g\in G} a_g \cdot \varphi(g)$.

Pf: + is trivial. $\varphi'(a_1 g_1 + a_2 g_2) = a_1\varphi(g_1) + a_2\varphi(g_2)$

$= \varphi'(a_1 g_1) + \varphi'(a_2 g_2)$.

$\times$. $\varphi'((a_1 g_1 + a_2 g_2)(a_3 g_3 + a_4 g_4)) = \varphi(a_1 a_3 g_1 g_3 + a_1 a_4 g_1 g_4 + a_2 a_3 g_2 g_3 + a_2 a_4 g_2 g_4)$

$= a_1 a_3 \varphi(g_1)\varphi(g_3) + a_2 a_4 \varphi(g_2)\varphi(g_4) + \cdots$.

$= (a_1\varphi(g_1) + a_2\varphi(g_2))(a_3\varphi(g_3) + a_4\varphi(g_4)) = \varphi'(a_1 g_1 + a_2 g_2)\varphi'(a_3 g_3 + a_4 g_4)$

Eg Study the Mf. solns to $x^2 + y^2 = 3z^2$. (mod 3).

If $(x, y, z) \in \mathbb{Z}^3$, is a soln, then consider $\pi: \mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$.

$\therefore$ We must have $\pi(x^2+y^2) = \pi(3z^2) = 0$.

$\therefore (\pi(x))^2 + (\pi(y))^2 = 0$.

Brute force checking ($\pi(x) = \bar{0}, \bar{1}, \bar{2} = \pi(y)$) gives us $\pi(x) = \pi(y) = 0$

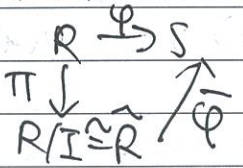
Thus $3 \mid x$ and $3 \mid y$. Let $x = 3x'$, $y = 3y'$, by infinite descent,

we must have $(x, y, z) = (0, 0, 0)$.

Date No.

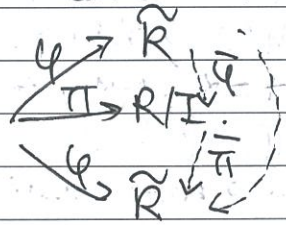
Defn (Quotient Rings using universal prop.). Let $I \subset R$ be an ideal. Then the quot ring of R by I is defined to be any $\tilde{R}$ ($\cong R/I$) together with a ring hom $\pi: R \to \tilde{R}$ s.t.

$\forall \varphi: R \to S$ with $I \subset \ker\varphi$, $\exists!\ \bar{\varphi} \neq \tilde{R} \to S$ making the diag. below comm



Prop. (category theory) The quotient ring $\tilde{R}$ exists and is unique up to isom.

Pf: Existence is shown before. (3). we show uniqueness:



$\Rightarrow \bar{\pi}\cdot\bar{\varphi} = id. \quad \tilde{R} \cong R/I.$ □.

Thm (Isomorphism thms, cont'd). Let R be a ring.

(2nd): $A \subset R$ be a subring, $B \subset R$ an ideal. Define $A+B = \{a+b \mid a\in A, b\in B\}$. Then $A+B/B \cong A/A\cap B$. (check! $A+B$ is a ring).

(3rd): Let $I \subset J \subset R$ be ideals. Then $R/J = R/I \,/\, I/J$.

(4th/Cor): $\pi: R \to R/I$. Then

$\{I \subset \text{subring of } R\} \longleftrightarrow \{\text{subring of } R/I\}$.

$\{\text{ideals in } I\} \overset{\text{bijection}}{\longleftrightarrow} \{\text{ideals of } I\}$ (preserving inclusion).

Pf (3rd). $R \xrightarrow{\pi_J} R/J$ (φ is surjective (why? comm. and surj. of π_J)

$\pi_I \downarrow$ $\quad \overset{\varphi}{\nearrow}$ $a+J$.

R/I

$a+I$

$\overset{1^{st}\text{ isom.}}{\curvearrowleft}$

- By 1st isom $R/I/\ker\varphi \cong \varphi(R/I) \cong R/J$ (surj.).

we just show $\ker\varphi = I/J$.

$\ker\varphi$ ⁂

Def. I, J be ideals of R. Then write:

$I+J = \{i+j \mid i\in I, j\in J\}$.

$I-J = \{\underset{\text{finite sum}}{\sum} i-j \mid i\in I, j\in J.\}$.

$I^n = I I^{n-1}$

Properties of Ideals

Ref. Let $A\subset R$ be a subset.

1. Denote (A) be the ideal generated by A, that is, $(A) = \bigcap_{A\subset I \text{ ideal}} I$.
   $= R\cdot A\cdot R = \{\sum r_1 a r_2 \mid r_1, r_2\in R, a\in A\}$.
   check RAR is an ideal: $R(RAR) = (RAR)R = RAR$.
   or $\forall x\in(A)$, $r\cdot x\in I$ for any $A\subset I$. $\therefore r\cdot x\in(A)$.
2. Denote the left ideal gen. by A, $R\cdot A = \{\sum r\cdot a\} = \bigcap_{A\subset I, I \text{ left ideal}} I$.
3. Similarly right ideal ——— $A\cdot R$.
4. Principle ideals are ideals gen. by a single elem, denoted by (x).
5. Ideal generated by a finite set is called finitely gen.

Eg
1. $(0)\subset R$, $(1) = R\subset R$ are prin. ideals.
2. $n\mathbb{Z} = (n)\subset\mathbb{Z}$ is principle. $= (n, 2n, 3n)$ ← gen. by 3 elem.
3. The ideal $(2, x)\subset\mathbb{Z}[x]$ is not a prin. ideal.
   Pf: Suppose otherwise $(2,x) = (r)$ for some $r\in R[x]$.
   Since we must generate 0 power, $r\in\mathbb{Z}$. $\to\leftarrow$.
4. Let $R = 2\mathbb{Z}[x]$ (without id). Then R is not a fin. gen. ideal.
   "pf": assume the contrary: then $R = (f_1, \dots f_n)$.
   say $\deg f_n = m \geq \deg f_i$ Then we claim $2x^{m+1}\notin (f_1, \dots, f_n)$.
   (coeff need to be atleast (4).

field → comm ring
simple → group (?)

Lem R ring, $1\neq 0$.
1. Let $I\subset R$, then $I = R \Leftrightarrow I$ contains a unit.
2. If R is commutative, then R is a field $\Leftrightarrow$ only ideals of R is R and (0).

Pf (1) ($\Rightarrow$) 1 is a unit.
($\Leftarrow$) If u is unit, $uu^{-1} = 1\in I$. Then $r\cdot(u^{-1}u)\in I\ \forall r\in R \therefore I = R$.

dv. m Date No.

(2) ($\Rightarrow$) $\forall I \neq (0)$, I contains a unit. By (1), $I = R$.

($\Leftarrow$) Let $0 \neq u \in R$. we consider $(u) = I$, since $I = (0)$ or R, $I \supset R$.

$\because (u) = R \cdot u$ u and $1 \in R = R \cdot u \Rightarrow \exists v \in R$, $vu = 1$.

Def. (Maximal Ideal) Let $I \subset R$. be a (left, right-2-sided) ideal. Then I is called (non-trivial) maximal if. $I \neq R$ and any ideal $J \supset I$ is either I or R.

Lem Let R be comm. with $1 \neq 0$. Then

(1) R is a field $\Leftrightarrow$ (0) is a max ideal.

(2) Let $I \subset R$ be an ideal, then I is maximal. $\Leftrightarrow$ R/I is a field.

Pf 1. By lemma, ~~since the only ideals are~~ field $\Leftrightarrow$ $R, (0)$ are the only ideals.

2. Straightforward by 4th Isom. thm, since only ideals in R/I

$\Leftrightarrow$) $\{\text{ideal} \supset I\} \leftrightarrow \{\text{ideal of } R/I\}$ $(\pi : R \to R/I)$.

$\{R, I\} \leftrightarrow \{R/I, I/I\}$.

$\therefore$ R/I is a field by (1).

($\Leftarrow$) similar to above, use the bijection in the quotient map.

Eg. 1. $(p) \subset \mathbb{Z}$ is a max ideal for a prime p in $\mathbb{Z}$ $((p) = p\mathbb{Z})$

$\Leftrightarrow$ $\mathbb{Z}/p\mathbb{Z}$ is a field (by lemma above)

$\Leftrightarrow$ $\mathbb{Z}/p\mathbb{Z}$ is an Int. dom.

Pf: Let $\bar{a}, \bar{b} \in \mathbb{Z}/p\mathbb{Z}$, $\bar{a} \neq 0 \neq \bar{b}$. then $p \nmid a$, $p \nmid b \Rightarrow p \nmid ab$ $\therefore$ $\bar{a}\bar{b} \neq 0$. $\therefore$ $\mathbb{Z}/p\mathbb{Z}$ is an Int. dom $\therefore$ a field.

2. $(x - a) \in \mathbb{C}[x]$ is maximal for any $a \in \mathbb{C}$.

Pf: we consider the map $\varphi : \mathbb{C}[x] \to \mathbb{C}$, $f(x) \mapsto f(a)$.

Date No.

Thm Let R be a ring with $1 \neq 0$ (crucial). Then any (left, right, 2-sided) proper ideal I is contained in a maximal (left, right, 2-sided) ideal of R.

Pf: (Standard pf using Zorn's Lemma).

Let I be a proper ideal, consider the set

$\Sigma = \{J \subset R \mid J \text{ is an ideal}, J \supset I, J \neq R\}$.

- $\Sigma \neq \emptyset$, since $I \in \Sigma$,

Let $C \subset \Sigma$ be a chain w.r.t. inclusion partial order. (i.e., $\forall J_1, J_2 \in C$, $J_1 \subseteq J_2$ or $J_2 \subseteq J_1$)

Define $K = \bigcup_{J \in C} J \subset R$.

- K is an ideal containing I.

  $\forall a, b \in K$, $a, b \in J \in C$ for some J. Then $a - b \in J \Rightarrow a - b \in K$.

- $K \neq R$. (since $1 \notin K$).

So any chain in Σ has an upper bound. By Zorn's lemma, $\exists$ maximal element in Σ. ~~we claim M is such a maximal ideal~~.

Say M. Then we claim M is a maximal ideal in K containing I. ∎

(given by Zorn; by construction)

Eg. We consider $(pq) \in \mathbb{Z}$ for element primes p, q. Then $(pq) \subset (p)$ and $(pq) \subset (q)$. So the max. ideal containing (pq) is not unique!

Def. (prime ideals) R be comm. with $1 \neq 0$. An ideal $P \subset R$ is called prime if.

- $P \neq R$.
- $\forall a \cdot b \in P$, we have either $a \in P$ or $b \in P$ (or both)

Eg. 1. $(p) \subset \mathbb{Z}$ is a prime ideal. for any prime $p \in \mathbb{Z}$.

Pf: if $a \cdot b \in P$, $ab = cp \Rightarrow p \mid a$ or $p \mid b$ since p prime.

$\therefore$ either $a = a' \cdot p \Rightarrow a \in P$ or $b = b'p \Rightarrow b \in P$. ∎

2. (0) is a prime ideal in any integral domain.

Pf: if $a \cdot b = 0$, then $a = 0$ or $b = 0$ since R is int. dom.

So $a \in (0)$ or $b \in (0)$. □

Date No.

Lem. Let R be comm with $1 \neq 0$. Let $P \subset R$ be an ideal (proper). Then P is prime ideal $\iff R/P$ is an int. dom. (cor: since field $\Rightarrow$ int dom, P is max $\Rightarrow$ prime).

Pf: ($\Rightarrow$) assume P prime, show R/P is an int dom
$\iff \forall \bar{a}, \bar{b} \in R/P$, $\bar{a}\cdot\bar{b} = 0 \Rightarrow \bar{a} = \bar{0}$ or $\bar{b} = \bar{0}$.
$\iff a \in \ker$ or $b \in \ker$ ($\ker = P$)
but $\bar{a}\cdot\bar{b} = \overline{a\cdot b}$ #, and $\bar{a}\cdot\bar{b} = 0 \Rightarrow a \in \ker$ ↑..
($\Leftarrow$)

Defn Let R be comm. with $1 \neq 0$. Define.
$$\mathcal{N}(R) = \{ x \in R \mid x^n = 0 \text{ for some } n > 0 \}.$$

Lem. $\mathcal{N}(R)$ is an ideal.

Pf: recall: if $x \in \mathcal{N}(R)$, $r \cdot x \in \mathcal{N}(R)$ $\forall r \in R$.
Say $x^n = 0$, then $(rx)^n = r^n \cdot x^n = 0$.
- Let $x, y \in \mathcal{N}(R)$, with $x^n = y^n = 0$. We compute
$$(x-y)^{2n} = \sum_{i=0}^{2n} \frac{2n!}{i!\,(2n-i)!}\, x^i y^{2n-i} (-1)^{2n-i} = 0$$
since for each $x^i y^{2n-i}$, we have either $i \geq n$ or $2n-i \geq n$.
$\therefore x^i y^{2n-i} = 0$.

Thm $\mathcal{N}(R) = \bigcap_{P \text{ is a prime ideal of } R} P$.

Pf: (1) We first show $\mathcal{N}(R) \subset \bigcap P$.
Let $x^n = 0$. Then $x \cdot x^{n-1} \in P$ (since $0 \in (0)$ is a prime).
if $x^{n-1} \in P$, we repeat. (Then $x \cdot x^{n-2} \in P$...)
Because base case: $1 \notin P$.

MA3201 Chap 7 (8). Date No.

Pf (cont'd) (2) show $\mathcal{J}(R) \supseteq \bigcap P$.

We show the contrapositive: if $x \notin \mathcal{J}(R)$, $x \notin P$ for some ideal P.

(Zorn's lemma again). Let x be given, $x \notin \mathcal{J}(R)$.

Let $\Sigma = \{J \subset R \mid J \text{ ideal}, J \neq R \text{ and } x^m \notin J \ \forall m \in \mathbb{Z}_{\geq 0}\}$. $\supseteq (0)$

Let $C \subset \Sigma$ be a chain wrt the incl. partial ord.

- $K = \bigcup_{J \in C} J$ is an ideal.
- $K \neq R$ ($1 \notin K$).
- $x^m \notin K \ \forall m > 0$.

$\therefore K$ is an u.b of C. Thus by Zorn's, let the max elem. be $M \in \Sigma$

Claim: M is a prime ideal

We alr have ($M \neq R$, $x^m \notin M \ \forall m > 0$). M is also an ideal.

We show M is prive: suppose otherwise, let $a, b \in R$ s.t.

$a \notin M$, $b \notin M$ but $a \cdot b \in M$.

Then $(a)+M \supsetneq M \subsetneq (b)+M$ either way, ~~contradicting~~

By maximality of M, $(a)+M$, $(b)+M$ must contain some power of x, ~~the~~

Let $x^s \in (a)+M$, $x^t \in (b)+M$ for $s, t > 0$,

$\therefore x^{s+t} \in ((a)+M)((b)+M)$

$\subsetneq (ab)+M = M$ (since $ab \in M$).

$\therefore M$ is a prime ideal and ~~(cont)~~ $x \notin M$. □

Field of fractions and localizations. (only for comm. rings)

3 depths, more & more generalized.

Motivation Recall the construction of $\mathbb{Q}$ from $\mathbb{Z}$.

$\mathbb{Q} = \{\frac{a}{b} \mid a \in \mathbb{Z}, b \in \mathbb{Z} \setminus \{0\}\}$.

$= \{(a,b) \mid a \in \mathbb{Z}, b \in \mathbb{Z} \setminus \{0\}\} / \sim$

$\sim : (a,b) \sim (c,d) \iff ad = bc \quad (\frac{a}{b} = \frac{c}{d})$.

Then $(a,b) + (c,d) \overset{\text{def}}{=} (ad+bc, bd)$. (is well defined but not trivial).

$(a,b) \times (c,d) \overset{\text{def}}{=} (ac, bd)$ (1)

Then $\mathbb{Q}$ is a ring (in add, a field).

Date ↙ or $[(b,a^n)]$ as a conj. class. No. $\forall n \geq 0$.

Eg. 2. Let $0 \neq a \in \mathbb{Z}$. We define $\mathbb{Z}[\frac{1}{a}] = \{\frac{b}{a^n} \mid b \in \mathbb{Z}\} \subset \mathbb{Q}$. (localization)
In $\mathbb{Z}[\frac{1}{a}]$, a is invertible. $a \cdot (\frac{1}{a}) = 1$

Defn/Thm Let R be an int. dom. (with $1 \neq 0$). Let $D = R - \{0\}$. define the field of fraction of R, or the quotient field of R, denoted Q, as follows:

1. define the set $\tilde{Q} = \{(a,b) \in R \times D\}$. Define equiv. relation $\sim$,
$(a,b) \sim (c,d) \iff ad = cb$.
Define $Q = \tilde{Q}/\sim$. Write $\frac{a}{b}$ be the equiv. class (a,b).

Pf: $\sim$ is an equiv. relation.
refl: $ab = ab \iff ab = ba \iff (a,b) \sim (a,b)$
sym: $ad = cb \iff cb = ad \iff (c,d) \sim (a,b)$.
trans: $ad = bc$, $cf = de$ WTS $\frac{a}{b} = \frac{c}{d} = \frac{e}{f}$
$\Rightarrow adf = bcf \Rightarrow acf = bcf \Rightarrow af = be \Rightarrow (a,f) \sim (b,e)$

2. Define $+$: $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$. check well-def.
Pf: Let $\frac{a'}{b'} = \frac{a}{b}$. Then WTS $\frac{a'd+b'c}{b'd} = \frac{ad+bc}{bd}$ given $a'b = b'a$.
we show $(a'd+b'c)bd = (ad+bc)b'd$.
$= a'bd^2 + b'bcd$
$= ab'd^2 + b'bcd$
$= (ad+bc)b'd$.
and similarly with $\frac{c}{d} = \frac{c'}{d'}$.

3. Define $\times$ on Q: $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$. Check well-def.
Pf: let $\frac{a'}{b'} = \frac{a}{b}$. WTS $\frac{a'c}{b'd} = \frac{ac}{bd} \iff a'cbd = acb'd$.
$\Rightarrow a'cbd = (a'b)cd = ab'cd = acb'd$. ∎

Then Q is a (well-def) field containg R via an inj. hom:
$R \to Q$, $r \mapsto \frac{r}{1}$.
Pf: $\ker\varphi = \{r \in R \mid \frac{r}{1} = 0 = \frac{0}{d} \in Q\}$. $rd = 0 \Rightarrow r = 0$ since $d \neq 0$, and R is an int dom.

MA3501 Chap 7 (9). Date No.

Eg 1. $\mathbb{Q}$ is the field of fractions (div. field) of $\mathbb{Z}$.

2. Let $R = \mathbb{R}[x]$. Then the field of fractions of R consists of elems of the form $\frac{f(x)}{g(x)}$.

Def/Thm Let R be a comm. rng with $1 \neq 0$ (not nec. int. dom). Let $D \subseteq R - \{0\}$ be s.t. $D \neq \emptyset$, $1 \in D$, and zero divisors $\notin D$, closed under mult. (imagine $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \leftarrow \neq 0, \in D$.)

we define the localization of R wrt. D denoted by $D^{-1}R$, as follows:

1. As a set, define $D^{-1}R = \{(a,b) \mid a \in R, b \in D\}$,
define eqv. rln $\sim$: $(a,b) \sim (c,d)$ if $ad = bc$,
Then $D^{-1}R = D^{-1}R/\sim$. Write $\frac{a}{b}$ as the eqv. class containg (a,b).

2. Define $+, \times$ on $D^{-1}R$ as before.
$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}, \quad \frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}.$$

Then we claim:

1. $D^{-1}R$ is a (well-defn) rng with embedding.
$i: R \to D^{-1}R$, $r \mapsto \frac{r}{1} = \frac{rd}{d}$.
2. and $d \in D$ is invertible in $D^{-1}R$ via the embedding i, i.e., $\frac{d}{1}$ is invert
3. (Universal property) Let S be any comm. rng with $1 \neq 0$. Let $\varphi: R \to S$ be a hom. s.t. $\varphi(D) \subseteq S^*$. Then there is a unique map $D^{-1}\varphi: D^{-1}R \to S$ making the following diagram $\circlearrowleft$:

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ {\scriptstyle i}\downarrow & \nearrow_{\exists!} & \\ D^{-1}R & & \end{array} \qquad D^{-1}\varphi$$

$\ast$ (defn)

Pf: (1) & (2) are same as before.

Claim 1: $\ker i = \{r \in R \mid i(r) = \frac{r}{1} = 0 = \frac{0}{d}\}$
$\therefore rd = 0$ but $d \in D$ must not be a zero div, $\neq 0 \Rightarrow r = 0$.
$\therefore$ injective. (embedding).

$d \longmapsto \varphi(d)$ Date No.

Pf Claim 3:

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ {\scriptstyle i}\downarrow & \nearrow & \\ D^{-1}R & & \end{array} \qquad \varphi(D) \subset S^{\times}.$$

$\downarrow \frac{\cdot}{d}$

"define" $D^{-1}R \to S$, $\frac{r}{d} \mapsto \varphi(r)\cdot\varphi(d)^{-1}$

Check $D^{-1}\varphi$ is well-defined.

Let $\frac{r}{d} = \frac{r'}{d'} \in D^{-1}R$.

$\therefore D^{-1}\varphi\left(\frac{r}{d}\right) = \varphi(r)\cdot\varphi(d)^{-1}$

$D^{-1}\varphi\left(\frac{r'}{d'}\right) = \varphi(r')\cdot\varphi(d')^{-1}$.

but $rd' = dr' \Rightarrow \varphi(rd') = \varphi(dr')$

$\varphi(r)\varphi(d) = \varphi(d)\varphi(r')$ as desired.

Eg. 1. Let $R = \mathbb{Z}$, $D = \{p^n \mid n \geq 0\}$. Then $D^{-1}R = \mathbb{Z}[\frac{1}{p}]$.

2. Let $R = \mathbb{R}[x]$ as poly. fns on $\mathbb{R}$. Then $D = \{x^n \mid n \geq 0\}$. Then. $D^{-1}R = \{f(x)/x^n \mid f(x) \in \mathbb{R}[x], n \geq 0\}$. as functions $\mathbb{R} - \{0\} \to \mathbb{R}$.

Prop. Let R be an int. dom ($1 \neq 0$), Then the field of fractions Q is the smallest field containing R. Ie. if F is a field containing R, then F must contain a subring $\cong Q$.

Pf: Let $D = R - \{0\}$, $Q = D^{-1}R$. Then

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & F \\ {\scriptstyle i}\downarrow & \nearrow_{D^{-1}\varphi} & \\ D^{-1}R & & \end{array}$$

we claim $D^{-1}R$ is injective, since $\ker(D^{-1}\varphi)$ is an ideal in the field $D^{-1}R$ #, $\ker(D^{-1}\varphi) = (0)$.

MA3201 Chap 7 (10). (~~zero~~ might have zero div)

Def/Thm Let R be a comm. ring with $1 \neq 0$. Let D be closed under $\times$, a subset of R containing 1. Then $\exists$ a ring $D^{-1}R$ together with a ring hom $i: R \to D^{-1}R$ s.t.

(1) $i(D)$ is invertible.

(2) Let S be any comm. ring with $1 \neq 0$. Let $\varphi: R \to S$ s.t. $\varphi(D) \subset S^*$. Then $\exists$ a unique map $D^{-1}\varphi: D^{-1}R \to S$ making the diagram commute:

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ {\scriptstyle i}\downarrow & \nearrow_{D^{-1}\varphi} & \\ D^{-1}R & & \end{array}$$

$D^{-1}R$ is unique upto isom. Recall the univ. prop. of R/I. Uniqueness is proved there.

Pf: we construct $D^{-1}R$ and the ring hom $i: R \to D^{-1}R$.

(1) $D^{-1}R = \{(a,b) \mid a \in R, b \in D\}/\sim$ where

$\sim$: $(a,b) \sim (c,d)$ if $\exists x \in D$ s.t. $x \cdot (ad - bc) = 0$.

[Recall defns 1, 2:
1. R is an int. dom. Thus $x(ad-bc)=0 \Rightarrow (x \neq 0 \Rightarrow ad-bc=0)$.
2. D has no zero-div. Thus $x \in D \not\ni 0 \Rightarrow (ad-bc=0)$.
Thus this defn generalizes both.]

(2) Define $+$ on $D^{-1}R$.

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}.$$

(check)

(3) Define $\times$ on $D^{-1}R$

$$\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}.$$

(check). Let $\frac{a}{b} = \frac{a'}{b'} \Leftrightarrow x(ab' - ba') = 0$

Then wts $\frac{ac}{bd} = \frac{a'c}{b'd}$.

$\Leftrightarrow \exists y,\ y(ac \cdot b'd - a'c \cdot bd) = 0$

$y(ab' - a'b)(cd) = 0$.

done. $= 0$.

Then $D^{-1}R$ is a well-def. ring with $i: R \to D^{-1}R$, $r \mapsto \frac{r}{1} = \frac{rd}{d}$. satisfying (the univ. prop) conditions (1), (2).

Date No.

Eg 1. Let R be any comm rng with $1 \neq 0$. Let $D = \{0, 1\}$, then we claim $D^{-1}R \cong \{*\}$.

Pf: $i : R \to D^{-1}R$, $0 \mapsto 0$ is invertible.

2. Let $R = \mathbb{Z}/6\mathbb{Z}$. Let $D = \{\bar{1}, \bar{4}, \bar{7}\}$. Then, we claim $D^{-1}R \cong \mathbb{Z}/3\mathbb{Z}$ $\quad \bar{3} = \frac{3}{1}$

Pf: in $D^{-1}R$, we have $\frac{3}{1} \cdot \frac{2}{1} \cdot \frac{1}{2} = \frac{3}{1} = \bar{0} = \bar{3}$.

- $\frac{\bar{5}}{\bar{1}} = \frac{\bar{2}}{\bar{1}}$ $\left(\frac{\bar{2}}{\bar{1}} + \frac{\bar{3}}{\bar{1}} = \frac{\bar{5}}{\bar{1}}\right)$
- $\frac{\bar{1}}{\bar{2}} = \frac{\bar{2}}{\bar{1}} \Leftrightarrow x(\bar{1}\cdot\bar{1} - \bar{1}\cdot\bar{2}) = x \cdot (-\bar{3}) = 0$ in $\mathbb{Z}/6\mathbb{Z}$. if $x = \bar{2} \in D$.
- $\frac{\bar{2}}{\bar{1}} \neq 1 = \frac{\bar{1}}{\bar{1}}$
- $\frac{\bar{1}}{\bar{4}} = \frac{\bar{4}}{\bar{1}}$, $\frac{\bar{4}}{\bar{1}} = 1$.

$\mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$ claim $D^{-1}R \not\cong \mathbb{Z}/2\mathbb{Z}$.

$\downarrow$ $\quad D = \{\bar{3}^n \mid n \geq 0\} = \{\bar{3}, \bar{1}\} \subset \mathbb{Z}/6$

$\mathbb{Z}/2\mathbb{Z}$

Lemma 1. $\ker(i) = \{r \in R \mid x \cdot r = 0 \text{ for some } x \in D\}$.

2. $D^{-1}R = 0 \Leftrightarrow 0 \in D$.

Pf (1) $i : R \to D^{-1}R$, $r \mapsto \frac{r}{1}$

Then $\frac{r}{1} = \frac{0}{2} \overset{\text{def}}{=} \frac{0}{1} \Leftrightarrow x \cdot (r \cdot 1 - 1 \cdot 0) = x \cdot r = 0$.

(2) ($\Leftarrow$) If $0 \in D$, then $\frac{a}{b} = \frac{0}{1}$ in $D^{-1}R$ since $0 \cdot (a - b \cdot 0) = 0$.

($\Rightarrow$) If $D^{-1}R = 0$, then $\frac{1}{1} = \frac{0}{1}$, so

$x(1 \cdot 1 - 0 \cdot 1) = x = 0$. $\square$

MA3001 Chap 7.6 Date No.

Thm Chinese Remainder Thm.

Eg. $\exists$ ring isom.

$\mathbb{Z}/2\times3\times5\mathbb{Z} \cong \mathbb{Z}/30\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$

$x \mapsto \bar{1}, \bar{2}, \bar{2} \quad x=17$

there is a unique integer mod 30, s.t.

$x\equiv 1 \pmod 2$, $x\equiv 2 \pmod 3$, $x\equiv 2 \pmod 5$.

Def. R comm, $I\neq 0$. Two ideals A, B of R are coprime if $A+B=R$.

($(2)+(3)=\mathbb{Z}$ so "2", "3" are coprime.)

Recall in HW1, under A, B coprime, we have $A\cap B = A\cdot B$.

Thm (CRT) Let R comm $I\neq 0$, $A_1, \dots, A_k$ pairwise coprime ideals of R. Then we have the isom.

$R/A_1A_2\dots A_k \cong R/A_1 \times R/A_2 \times \dots \times R/A_k$.

$(\cong R/A_1\cap A_2\cap\dots\cap A_k)$

Pf: First we have a ring hom

$\varphi: R \to R/A_1 \times R/A_2 \times \dots \times R/A_k$.

$r \mapsto (r+A_1, r+A_2, \dots, r+A_k)$

Note that $\varphi(r)=0 \Rightarrow r\in A_1, r\in A_2, \dots, r\in A_k$.

$\therefore \ker(\varphi) = A_1\cap A_2\cap\dots\cap A_k$.

Case: $k=2$

Claim: $\varphi: R\to R/A_1\times R/A_2$ is surjective.

Recall $A_1+A_2=R$ by assumption. Let $a_1+a_2=1$ for some a_1, a_2.

Then $\varphi(a_1) = (a_1+A_1, a_1+A_2)$

$= (0+A_1, 1-a_2+A_2)$

$= (0+A_1, 1+A_2) = (\bar{0}, \bar{1}) \in R/A_1\times R/A_2$.

Similarly, $\varphi(a_2) = (\bar{1}, \bar{0}) \in R/A_1\times R/A_2$.

Thus for any $(\bar{a}, \bar{b}) \in R/A_1, R/A_2$,

$\varphi(aa_2+ba_1) = \varphi(aa_2+ba_1+A_1, aa_2+ba_1+A_2)$

$= (\bar{a}, \bar{b})$.

$\therefore$ By 1st isom, $R/A_1A_2 \cong R/A_1\times R/A_2$

Date No.

Case: General. (induction on k.)

WTS $R/A_1 \cdots A_k \cong R/A_1 \times R/A_2 \cdots A_k \cong R/A_1 \times \cdots \times R/A_k$.

claim: if $A_1, A_2 \cdots A_k$ are coprime, then we are done by the $k=2$ case and induction.

Pf of claim: since pairwise coprime, we have

$\forall i = 2, \ldots, k$, $\exists x_i, y_i$, $x_i \in A_1$, $y_i \in A_i$ s.t.

$x_2 + y_2 = 1$

$x_3 + y_3 = 2$

$\therefore (x_2 + y_2)(x_3 + y_3) \cdots (x_k + y_k) = 1$.

expanding, $\sum_{i=2}^{k} (\ ) x_i + y_2 y_3 \cdots y_k = 1$

$\in A_1$ $\quad \in A_2 \cdots A_k$.

$r \in R$ s.t. $rA_1 = A_1$. thus coprime. $\square$

MA3201 Chap 8. PID. (all rings are comm. in this chap.) Date No.

Overview: Integral Domain ⊋ UFD ⊋ PID ⊋ Euclidian Domain ⊋ (fields).

Def. (PID) A principle ideal domain is an int. dom in which every ideal is principle, i.e, (x) (gen by a single elem) $= Rx = \{ax \mid a \in R\}$ (for every subgp of a cyclic gp. is cyclic) (not $R \times R$ since comm).

Eg. $\mathbb{Z}$ is a PID (actually a Euclidian Domain).

pf: Let $(0) \neq I \subset \mathbb{Z}$ be an ideal. Then let $r \in I$ be the elem s.t. $|r|$ is minimal. We claim $I = (r)$.

Clearly $(r) \subset I$.

We show $I \subset (r)$. Let $x \in I$ be given, then do euclid. div.

$x = qr + y$ for some $q, y \in \mathbb{Z}$ s.t. $|y| < |r|$.

Then by the assumption that $|r|$ is minimal ($\neq 0$),

we must have $y = 0$. $\therefore x = qr \Rightarrow x = (r) = R \cdot r$.

$\therefore I = (r)$ and $\mathbb{Z}$ is a PID.

Rem. Generalizing this gives us Euclidian Domains.

Prop ☆ Let R be a PID. Then any prime ideal P is also maximal.

pf: 1. Let $P = (p)$. (R is a PID.)

2. Let $I \supsetneq P$. If $I = R$, we are done. (defn of max).

2.1 Let $I = (a)$, $a \notin P$. (otherwise $I = P$).

2.2 since $P \subset I$, $p \in I = R \cdot a$. then $\exists b \in R$, $p = a \cdot b$. (comm)

2.3 $\therefore p = a \cdot b \in P \Rightarrow a \in P$ (impossible) or $b \in P = Rp$

2.4 $b = pc$ for some c.

$\therefore p = a(pc) \Rightarrow ac = 1 \Rightarrow (a) = R$. □

Date No.

Def. Let R be a comm. rng $1 \neq 0$. (or an int. dom). Let $a, b \in R$ with $b \neq 0$.

1. we say a is a mult. of b, or b divides a, if $a = bc$ for $c \in R$. we write $b \mid a$.
2. GCD of a, b is a non-0 elem $d \in R$, s.t.
   - $d \mid a$, $d \mid b$.
   - $\forall d'$, $d' \mid a$, $d' \mid b \Rightarrow d' \mid d$.

(abuse of) notation: write $d = \gcd(a, b)$. we dunno existence / uniqueness

Lemma. R int. dom, $a, b \in R$, $b \neq 0$. Let d, e be gcd of a, b. Then $d = u \cdot e$ for some unit u.

Pf: since both d, e are gcd, we have

$d \mid e$, $e \mid d$.

$\therefore dx = e$, $ey = d$ for some $x, y \in R$.

$\Rightarrow eyx = e$. Then $yx = 1$, since $e \neq 0$. □

Prop. Let R be PID, $a, b \in R$, with $b \neq 0$. Let $(a, b) = (d)$. Then $d = \gcd(a, b)$. So gcd always exists in a PID and is of the form $ax + by = d$.

Pf: 1. we show $d \mid a$ and $d \mid b$.

1.1 $a \in (d) \Rightarrow a = da'$ for some $a' \in R$

1.2 $b \in (d) \Rightarrow b = db'$ for some $b' \in R$

2. we show $\forall d' \in R$, $d' \mid a \wedge d' \mid b \Rightarrow d' \mid d$

2.1 then $a = d'a''$, $b = d'b''$. $\therefore a \in (d')$, $b \in (d')$.

2.2 $\therefore (a, b) \subset (d') \Rightarrow (d) \subset (d')$.

2.3 Thus $d \in (d) \subset (d') \Rightarrow d' \mid d$. □

Remark 1. We don't need R to be PID, only $(a, b) = (d)$.

2. It's more natural to define GCD using ideals.

   ie, if mult. ple GCD, then $(d) = (d')$ if $d = ud$.

MA3201 Chap 8 (2) Date No.

Defn (Noetherian Rngs) R comm with $1 \neq 0$ is called Noetherian if $\forall$ chain of ideals in R, $I_1 \subset I_2 \subset I_3 \subset \dots$, (asc. chain condition) we can find $m > 0$ such that $I_m = I_k$ for all $k \geq m$.
or equivalently $\bigcup_{i=1}^{\infty} I_i = I_m$.

Rem Asc. chain cond (ACC) is a finiteness assumption.
If R is Noetherian, then we can show any ideal is contained in a maximal ideal without Zorn's lemma. (no ∞ here, we have $\exists m$.)

Thm Let R be a PID. Then R is Noetherian (and thus any ideal is contained in a max. ideal)

Pf: We show the chain of ideals $I_1 \subset I_2 \subset \dots$ stabilizes.
Then $I = \bigcup_{i=1}^{\infty} I_i$ is an ideal. (check if unsure)
$= (r)$ for some $r \in R$.
Then $r \in I \Rightarrow r \in I_m$ for some $m > 0$. Then $(r) = I \subseteq I_m \subseteq I$. $\square$
(r) = I and $r \in I_m$.

~~Def.~~

Defn. Let R be an int. dom. A norm on R is a fn $N: R \to \mathbb{Z}_{\geq 0}$ s.t. $N(0) = 0$.
R is called a Euclidean Domain if we can perform the Euclidean division wrt some norm N:
$\forall a, b \in R$ with $b \neq 0$, we have
$a = qb + r$ with $r = 0$ or $N(r) < N(b)$.
q is called the quotient, r remainder.

Rem we often consider the case $N(r) > 0$ $\forall r \in R \setminus 0$ ($r = 0 \Leftrightarrow N(r) = 0$)
Then we just need $a = qb + r$ with $N(r) < N(b)$.

Eg. 1. Let $R = \mathbb{Z}$, $N(r) = |r|$. R is an Euclidean domain.
2. Any field with any norm. (∵ the choice of norm is not unique.)
3. $\mathbb{R}[x]$ with $N(f(x)) = \deg f(x)$.
Pf by eg: Let $a = x^2 + x + 1$, $b = x + 1$
$\therefore a - xb = x^2 + x + 1 - x^2 - x = 1$ has a lower degree.
q r

Date No.

4. Any discrete valuation ring $R \subset F$ a field, with $N(r) = v(r)$ for $r \neq 0$ and $N(0) = 0$, where $v : K^* \to \mathbb{Z}$ is the discrete valuation. (*) check.

5. Gaussian Integers: $\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$.
with $N(a+bi) = a^2+b^2 = (a+bi)(a-bi)$. is ED.

Pf: Let $\alpha, \beta \in \mathbb{Z}[i] \subset \mathbb{C}$ with $\beta \neq 0$. Then

$$\frac{\alpha}{\beta} = x+yi \in \mathbb{Q}[i] = \{a+bi \mid a \in \mathbb{Q}, b \in \mathbb{Q}\} \subset \mathbb{C}$$

Let m, n be integers s.t. $|x-m| \leq \frac{1}{2}$, $|y-n| \leq \frac{1}{2}$.

$$\begin{aligned} \alpha &= (x+yi)\beta \\ &= (m+ni+(x-m)+(y-n)i)\beta \\ &= (m+ni)\beta + \underbrace{((x-m)+(y-n)i)\beta}_{r}. \end{aligned}$$

Then $N(r) = N((x-m+(y-n)i)\beta)$
$= N((x-m+(y-n)i) \cdot N(\beta)$ (norm of complex num).
$\leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2) \cdot N(\beta) < N(\beta)$.

Prop. Let R be a Euclid. Dom. Then R is a PID.

Pf: Let $I \subset R$ be a non-0 ideal. Then $I = (r)$ where r is the element in I with with minimal norm.
$r \in I \Rightarrow (r) \subset I$. we now $a \in (r)$.
we just show $I \subset (r)$. Choose any $a \in I$. Then since R is ED, $a = qr+b \Rightarrow N(b) < N(r) = \hat{0}$ or $b = 0$.
$\therefore b = 0 \Rightarrow a = qr \Rightarrow a \in (r)$ □

Rem There are eg's of PID that is not a ED, eg.
$\mathbb{Z}[\frac{1+\sqrt{-19}}{2}] = \{a+b(?) \mid a, b \in \mathbb{Z}\}$. (DPF 8.2)

Pf (Discrete valuating Rings are Euclidean Domains).
Recall 1. $v(ab) = v(a)+v(b)$, 2. $v(a+b) \geq \min(v(a), v(b))$, 3. v is surj.
Let $a, b \in R$, $b \neq 0$. Then $v(a) \geq v(b)$ or $v(a) < v(b)$.
Case 1: $v(a) \geq v(b) \Rightarrow v(ab^{-1}) + v(b) = v(a) \Rightarrow ab^{-1} \in R$
Case 2: $v(a) < v(b) \Rightarrow a = 0 \cdot b + a$. □
$\Rightarrow ab^{-1} = q \Rightarrow a = bq$

MA3201 Chap 8 (3). Date No.

Recall in PID (⊃ a ED), the gcd(a,b) always exist. (b≠0).

Thm Let R be a Euclidean domain with norm N. Then we can find the gcd of a, (b≠0) using the Euclidean Algorithm:

Let R=ℤ, N(r)=r, a=1071, b=462. Let d=gcd(1071, 462). we just want the element in (1071, 462) with minimum norm. ie, (d)=(1071, 462).

$$1071 = 2\times 462 + 147$$
$$462 = 3\times 147 + 21$$
$$147 = 7\times 21 + 0.$$

Then we see that (1071, 462) = (462, 147) (147 ∈ ↗, 1071 ∈ ↗)
= (147, 21) = (21, 0) = (21) = (gcd).

Unique Factorization Domains (UFD) (eg 6=2×3).

Def Let R be an int dom.

1. Let r∈R, r≠0, r not a unit. Then r is irreducible in R if whenever r=a·b, either a or b is a unit.
2. A non-zero elem p is a prime in R if (p) ⊊ R is a prime ideal. IOW, if p|ab ⇒ p|a or p|b. (ab∈(p) ⇒ a∈(p) or b∈(p).

Rem 1, 2 are actually different in general.

Eg. 1. Consider ℤ[√-5], then 3 is irreducible but not a prime.

Not prime: $3^2 = (2+\sqrt{-5})(2-\sqrt{-5})$.
so $[(2+\sqrt{-5})\cdot(2-\sqrt{-5})] \in (3)$, but $2\pm\sqrt{-5} \notin (3)$ (?)

Irreducible: Let $3=\alpha\cdot\beta$, we show α or β is a unit.

$\alpha = x_\alpha + y_\alpha\sqrt{-5}$
$\beta = x_\beta + y_\beta\sqrt{-5}$

complex norm: $N(3)=9=N(\alpha\cdot\beta)=N(\alpha)\cdot N(\beta)$ (↙ complex.) (1≤9, 3×3)

But $N(\alpha)\neq\pm 3$ $\forall\alpha\in R$ because $= x_\alpha^2 + y_\alpha^2$ if x_α, y_α are $\in\mathbb{Z}$. ⇒ $N(\alpha)=\pm 1$ wLOG

⇒ α=1 (↙ complex norm)

claim: f a unit, $(u)=R$.

Date No.

Lemma Let R be an int. dom. If p is prime, then p is irreducible.

Pf: Let $p=ab$ and WTS a or b is a unit.
p is prime $\Rightarrow p \mid a$ or $p \mid b$. ($a \in (p)$ or $b \in (p)$)
WLOG If $p \mid a$, then $a=rp$ for some $r \in R$.
$\therefore p=ab=prb$.
$\therefore p(1-rb)=0 \Rightarrow 1-rb=0$ since int dom, $p \neq 0$.
$\Rightarrow b$ is a unit.

Prop Let R be a PID. Then p is prime $\iff p$ is irreducible.

Pf: ($\Rightarrow$) True as above, for all int dom.
($\Leftarrow$) Let p be irreducible (non-zero, non-unit).
We want to prove (p) is a (nontrivial) prime ideal.
But in PID, prime ideals = maximal ideals.

Let $M=(m) \supseteq (p)$ be a maximal ideal (existence given by Noetherian Ring, or Zorn's Lemma).
$\therefore p \in (m) \Rightarrow p=mr$ for some $r \in R$.
If m is unit, $M=R$ which we do not want.
$\therefore m$ not unit, p irreducible $\Rightarrow r$ is a unit.
So $pr^{-1}=m \Rightarrow M \subset (p)$ (why?)
$\Rightarrow M=(p) \Rightarrow p$ is maximal ($\iff$ prime).

Cor. $\mathbb{Z}[\sqrt{-5}] \subset \mathbb{C}$ is an int. dom (since $\mathbb{C}$ is a field) but not a PID (since 3 is irreducible but not prime)

Def. (Unique Factorization Domain) UFD is an int. dom. R such that every non-zero, non-unit $r \in R$ satisfies
1. $r=p_1 \cdots p_n$ can be written as a (finite) pdt of irreducible elems p_i (not necessarily distinct).
2. The factorization $r=p_1 \cdots p_n$ is unique, upto mult by units. That is, if $r=q_1, \ldots q_n$, then $q_i=u_i p_i$ for some unit u_i.

MA3201 Chap 8 (4). Date No.

Eg. In $\mathbb{Z}$, $6 = 2\times 3 = (-3)\times(-2)$. (up to perm & unit mult.)

Prop. Let R be a UFD. Then a non-zero, non-unit $p \in R$ is prime $\iff$ p is irreducible.

Pf: ($\Rightarrow$) Is true again under integral domains.

($\Leftarrow$) Let p be irreducible. We show p is a prime.

We then consider the unique fac of:

$p \neq 0$, p not unit, p irreducible. Let $ab \in (p) \iff p \mid ab$

(WTS $p \mid a$ or $p \mid b$) $\iff p r = ab$

$\therefore pr = ab$ for some $r \in R$. We use UFD and factorize, similar to this eg:

Eg Let $a = p_1$, $b = p_2$, $r = p_3$.

$\therefore p p_3 = p_1 p_2$.

$\Rightarrow p = u_1 p_1$ or $p = u_2 p_2$ for some units $u_1, u_2 \in R$.

$\Rightarrow u_1^{-1} p = p_1$ or $u_2^{-1} p = p_2 \Rightarrow p \mid p_1$ or $p \mid p_2$.

$\Rightarrow a \in (p)$ or $b \in (p)$

Recall UFD is a int dom R in which every non-0, non-unit element r satisfies 2 things:

1. $r = q_1 \dots q_n$ into a finite pdt of reducibles.
2. The factorization in (1) is unique upto perm and unit. mult. ie, if $r = p_1 \dots p_n$, then $p_i = u_i q_{\sigma(i)}$ for some unit u_i. after rearrangement. ($\sigma \in S_n$)

Prop R UFD. $a, b \in R$, non zero. Suppose

$a = u p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$, $b = v p_1^{b_1} p_2^{b_2} \dots p_n^{b_n}$

for irreducibles $p_1, \dots, p_n$ and $a_i, b_i \geq 0$

Then $\gcd(a,b) = c = p_1^{c_1} \dots p_n^{c_n}$ where $c_i = \min(a_i, b_i)$ $\forall i$.

(and exists).

Date No.

Pf: (gcd is lowest power of all irreducible factors)
Let $d|a$. we claim then we can write
$d = w \cdot p_1^{d_1} \cdots p_n^{d_n}$ with $d_i \le a_i$ (and w is a unit)
then we also have, if $d|b$,
$d = w p_1^{d_1} \cdots p_n^{d_n}$ with $d_i \le b_i$.
$\Rightarrow d_i \le \min(a_i, b_i)$
for any common divisor.
(left as exercise)

Thm PID $\Rightarrow$ UFD.

Pf In any PID, "prime" $\Leftrightarrow$ "irreducible" $=$ "maximal".
Let $r \in R$ be non-0, non-unit in a PID R.
Claim: r has a irreducible factor.
Pf If r is irreducible, we are done.
Otherwise, $r = a \cdot b$ where a, b not units. (def'n)
If a or b is irreducible, we are done.
Otherwise, say $a = a_1 b_1$ where a_1, b_1 not units.
Continuing all these
$r = a \cdot b \Rightarrow a | r \Rightarrow (r) \subset (a) \subset (a_1) \subset \cdots$
But PIDs are Noetherian. So the chain stabilizes and r has a reducible factor, am.
Cor. of pf: $\forall r \in R$ PID, r has only finitely many irreducible factors.
Claim: The factorization $r = p_1 \cdots p_n$ is unique up to unit. by units and perm.
Pf: Idea! use the fact that prime $\Leftrightarrow$ irreducible.
Let $q_1 \cdots q_m = r = p_1 \cdots p_n$, then $q_1 | p_1 \cdots p_n$
$\Leftrightarrow p_1 \cdots p_n \in (q_1)$. since (q_1) is a prime (irreducible) ideal, we must have $p_i \in (q_1) \Leftrightarrow q_1 | p_i$. but this division WLOG. $\Leftrightarrow q_1 u = p_1$, must see u as a unit since p_1 is irreducible.

repeating, we have QED.

MA320 | W5L1 Date No.

Gaussian Integers $\mathbb{Z}[i] = \{a+bi \mid a,b \in \mathbb{Z}\}$. Euclidean Dom.

Thm 1. $p \in \mathbb{Z}^+$ be a prime. Then $p = a^2+b^2$ for some $a,b \in \mathbb{Z}$ iff $p \equiv 2, 1 \pmod 4$.
The expr is unique up to -1 and perm.

2. The irreducible elems in $\mathbb{Z}[i]$ are of the form (up to units)
(i) $1+i$ (norm 2, $1+1=2$)
(ii) a prime $p \in \mathbb{Z}$ with $p \equiv 3 \bmod 4$ (norm p^2)
(iii) $a+bi$ where $a^2+b^2 = (a+bi)(a-bi) = p$ for some $p \in \mathbb{Z}$.

we prove (2), and show (2) $\Rightarrow$ (1).

Lem The units in $\mathbb{Z}[i]$ are $\pm 1, \pm i$.

Pf. Let u be a unit. Then $u \cdot u^{-1} = 1$, so
$N(u \cdot u^{-1}) = N(u) \cdot N(u^{-1}) = N(1) = 1 = a^2+b^2$.
$\therefore a = 0$ and $b = \pm 1$, or $a = \pm 1, b = 1$. □

Lem 1. Let $\alpha \in \mathbb{Z}[i]$ be irreducible. Then $N(\alpha) = p^2$ or $N(\alpha) = p$ for some prime $p \in \mathbb{Z}$.

2. Let $\beta \in \mathbb{Z}[i]$ be such that $N(\beta) = p$ for some prime $p \in \mathbb{Z}$, then β is irreducible.

Pf (1): Since irreducible $\Leftrightarrow$ prime ($\overset{\text{UFD}}{\underset{\text{CED}}{\text{PID}}}$ $\subset$ Field), Then (α) is a prime ideal. Consider the embedding $\mathbb{Z} \hookrightarrow \mathbb{Z}[i]$, then $(\alpha)^c = (\varphi^{-1}((\alpha))) \cap \mathbb{Z}$ is a prime ideal in $\mathbb{Z}$. (HW2)
(we are clear here the pre-image, $\varphi^{-1}((\alpha)) \neq \mathbb{Z}$ since otherwise $\pm 1 \in (\alpha)$ not prime).
Since (α) is prime, $\exists$ prime $p \in \mathbb{Z}$, $p \in (\alpha)$.
$\Rightarrow p = \alpha \cdot \alpha' \Rightarrow N(p) = N(\alpha \cdot \alpha') = p^2+0^2$
$= N(\alpha) \cdot N(\alpha')$
$N(\alpha) = 1, p, p^2$. But $N(\alpha) \neq 1$, $\therefore N(\alpha) = p, p^2$.

Date No.

Pf(2): WTS if $N(\beta)=p$, for some p prime, then β is irreducible.
Clearly then, if $\beta=\beta_1\beta_2$,
$N(\beta)=N(\beta_1\beta_2)$
$=N(\beta_1)N(\beta_2) = 1 \times p$ or $p \times 1$
$\Rightarrow$ either β_1, β_2 is unit. $\Rightarrow \beta$ is irreducible.

Rem
1. If we can decompose a prime $p \in \mathbb{Z}$ in $\mathbb{Z}[i]$, then case (1) applies: $N(p)=p^2$ and we have at most 2 irreducible factors:
$N(\alpha)=N(\alpha')=p$. where $p=\alpha\cdot\alpha'$.
or $N(\alpha)=p^2$.
2. If α is irreducible and $N(\alpha)=p^2$, then $\alpha=up$ for some unit u.
3. We shall study irreducibles of the form $N(\alpha)=p$ (a/w. irreducibles)

Lem Let $p \in \mathbb{Z}$ be a prime integer.
1. If $p=2$ (or $2 \bmod 4$) then $p=(1+i)(1-i)$.
2. If $p=3$ (or $3 \bmod 4$) Then p is irreducible in $\mathbb{Z}[i]$

Pf: (2) $N(p)=p^2$. If we show $\forall \alpha \in \mathbb{Z}[i]$, $N(\alpha) \neq p$, then $p \in \mathbb{Z}$ can only be expressed as a $p=\alpha\cdot\alpha'$ with either being unit (which is, by definition, irreducible).
WTS: $\forall \alpha \in \mathbb{Z}[i]$, $N(\alpha) \neq p$
Let $\alpha=x+yi$, $x, y \in \mathbb{Z}$. Then $N(\alpha)=x^2+y^2 \in \mathbb{Z}$.
Consider $\overline{N(\alpha)} \in \mathbb{Z}/4\mathbb{Z}$.
$\overline{x^2+y^2} = \overline{x^2}+\overline{y^2} = \underset{0,1}{\overline{x}^2} + \underset{0,1}{\overline{y}^2} \neq 3$. □

Cor. Let p be a prime. If $p \equiv 3 \bmod 4$, then $p \neq a^2+b^2$ $\forall a, b \in \mathbb{Z}$.

(1)

MA3201 WSL1 (2) Date No.

lem. If $p \equiv 1 \pmod 4$, then $p \mid n^2+1$ for some $n \in \mathbb{Z}$.

"Pf": consider $n^2+1=0$ in $\mathbb{Z}/p\mathbb{Z}$.
Then lemma $\Leftrightarrow$ $n^2+1 \equiv_4 0$ has a soln.

Note that $\mathbb{Z}/p\mathbb{Z}^* \cong \mathbb{Z}/(p-1)\mathbb{Z}$ is a cyclic gp of order $p-1$.
(classification of finite abelian groups.)

Since $p \equiv 1 \pmod 4 \Rightarrow 4 \mid p-1$ Then we can find an elem. $r \in (\mathbb{Z}/p\mathbb{Z})^*$ of order 4 (since cyclic group of order $(p-1)$ has one and only one subgroup for each divisor of its order). ~~:~~
then $r^4=1$. ....

Cor. Let $p \in \mathbb{Z}$ be a prime s.t. $p \equiv 1 \bmod 4$. Then p is reducible in $\mathbb{Z}[i]$.
(we know $p = \alpha \cdot \alpha'$ for irreducible α and α') ← both of ↑ unique (due to UFD)
$\Leftrightarrow$

Pf: Assume p is reducible. Lemma above gives us $p \mid n^2+1$ for some $n \in \mathbb{Z}$. $\therefore p \mid (n+i)(n-i)$
Since prime $\Leftrightarrow$ irreducible ( ),
we must have $p \mid (n+i)$ or $p \mid n-i$.
WLOG if $p \mid n+i$, $pr = n+i$ for some $r \in \mathbb{Z}[i]$.
taking complex conjugate,
$\overline{pr} = \bar{p}\bar{r} = n-i$ but since $p \in \mathbb{Z}$, $\bar{p}=p$
$\therefore p\bar{r} = n-i$ for some $\bar{r} \in \mathbb{Z}[i]$
$\therefore p \mid n+i$ AND $p \mid n-i$
$\Rightarrow p \mid (n+i)-(n-i) = 2i$
but $p \nmid 2$ (odd), $p \nmid i$ (since $p \in \mathbb{Z}$) $\lightning$ □

Cor $p \equiv 1 \bmod 4 \Rightarrow \exists \alpha \in \mathbb{Z}[i]$, $N(\alpha) = p$

MA3201 WS(2)(2). Date No.

Cor If I is prime in $R \to (I) \subset R[x]$ is also prime.
(R is int dom → polynomial rngs over int dom is Int dom.)

Pf: $R[I][x] \cong R[x]/(I)$ is an int. dom, thus (I) is prime. (↖ implies $[I]$ is prime.)

Polynomial rngs over Fields

Let F be a (non-trivial) field. Then $F[x]$ is a Euclidean Domain with the norm $N(f(x)) = \deg(f(x))$

Eg: in $\mathbb{Q}[x]$: $5x^3+x-1$, $x-1$

$5x^3+x-1 = 5x^2(x-1)+(5x^2+x+1)$

$5x^2+x+1 = 5x(x-1)+6x+1$

$6x+1 = 6(x-1)+11$.

Summary
1. $F(x)$ where F is a field is a ED (PID, UFD).
2. Let $f(x) \in F[x]$. Then $f(a)=0$ for some $a \in F \iff x-a \mid f(x)$.

Pf: Consider $f(x)$ divided by $(x-a)$.
Since ED, $f(x) = q(x)(x-a)+c$ for some $c \in F$ since $N(x-a)=1$
$\therefore f(a) = q(x)(a-a)+c = 0 \Rightarrow c=0$
$= c$ □

3. Let $f(x) \in F[x]$ with deg n. Then $f(x)$ has at most n roots in F. (counting multiplicity).

Pf: Induction on degree n. $n=0$ is clear.
Let deg k be given. If there are NO roots, we are done.
Otherwise, $f(x) = q(x)(x-a)$ by the previous lemma, with root a.
By defn of Euclidean Dive, $\deg(q) = n-1$, which means $q(x)$ has at most $n-1$ roots.

Date (PID) No. (PID)

4. $F[x]/(f(x))$ is a field $\Leftrightarrow$ $f(x)$ is irreducible (or prime or maximal)

5. Let $p(x), q(x)$ be irreducible in $F[x]$.
If $(p(x)) \neq (q(x))$ or $p(x) \neq u \cdot q(x)$ for some unit $u \in F[x]$
then $(p^a(x))$ and $(q^b(x))$ are coprime. ($(p^a(x)) + (q^b(x)) = F[x]$)

6. Let $f(x) = p_1^{a_1}(x) p_2^{a_2}(x) \cdots p_n^{a_n}(x)$ be the irreducible factorization.
Then $F[x]/(f(x)) \cong F[x]/(p_1^{a_1}(x)) \times \cdots F[x]/(p_n^{a_n}(x))$
(Recall $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$).

Prop F be a field, $G \subset F^\times$ be a finite subgp. Then G is cyclic.
In particular $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic for prime p.

Pf: G must be Abelian and finite (since G is abelian).
By the classification of finite Abelian groups,
$G \cong \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_n\mathbb{Z}$.
where $d_n | d_{n-1} | \cdots | d_1$ (divisibility chain)

Consider the polynomial $x^{d_1} - 1$ in $F[x]$. Then it can have
at most d_1 roots in F, hence in G as well.
But $\forall r \in \mathbb{Z}/d_1\mathbb{Z}$, it is a root for $x^{d_1} - 1$.
and $d_2 | d_1$, $\forall r \in \mathbb{Z}/d_2\mathbb{Z}$, ——
$\therefore$ we must have $n = 1$ (to have at most d_1 roots).

Polynomial ring vs functions
F field, P the ring of polynomial fns on F.
$P = \{ f(x) : F \to F \mid f(x) = \sum_{i=0}^{a} a_i x^i \ \forall\, a_i, x_i \in F \}$.

Eg: $F = \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$
Then the fn $f(x) = x+1 : F \to F$
$0 \mapsto 1$
$1 \mapsto 0$.
$g(x) = x^2 + 1$ $F \to F$
$0 \mapsto 1$
$1 \to 0$.
$\therefore f = g$ on P.

MA3201 W5L2 (3). Date No.

We have a ring hom: $F[x] \to P$

"expr" $\leftarrow f(x) \longmapsto f(x)$ "f_x"

Clearly from the eg., P_2, this is not always isom.

Prop $\varphi: F[x] \to P$ is an isom $\iff$ F is infinite.

Pf: φ is surjective by defn of P.

φ is isom $\iff$ φ is inj $\iff \ker\varphi = 0$.

We see that $\ker\varphi = \{f \in F[x] \mid f(a) = a \ \forall a \in F\}$.

If F is finite $= \{a_1, \dots, a_n\}$, then.

$(x-a_1)\dots(x-a_n) \in \ker\varphi \neq \{0\}$.

F is infinite, then $\forall f(x) \in F[x]$, it has only finitely many (at most $= n = \deg(f)$) roots. Thus $\forall f \in F[x]$, $f \notin \ker\varphi$ unless is the zero map.

Thm (D&F 9.3) Let R be comm with $1 \neq 0$. Then R is a UFD $\iff R[x]$ is a UFD. ($\iff R[x_1, x_2]$ is a UFD $\iff \dots$)

Cor $\mathbb{Z}[x]$ is a UFD (but not a PID)

Irreducible Polynomials in $F[x]$ (?) ← field.

Let F be a field. Recall $(F[x])^\times = F^\times = F - \{0\}$.

Lem. Let $f(x) \in F[x]$ with deg 2 or 3. Then $f(x)$ is irreducible if $f(x)$ has no root in F. Then $F[x]/(f(x))$ is a field.

Pf: If $\deg(f) = 2$ or 3, and $f(x)$ is reducible, then $a(x) \cdot b(x) = f(x)$ where $\deg(a) < \deg(f)$ and $\deg(b) < \deg(f)$.

(ie. a, b has deg > 0 (& F). Otherwise, a, b is a unit in $F[x]$ $\to\leftarrow$ reducible).

one of them must give rise to a root. We have shown the contrapositive of the lemma. □

Date No.

Eg. (1) Consider the field $\mathbb{F}_{11} \cong \mathbb{Z}/11\mathbb{Z}$. Then
(x^2+3x+4) in $\mathbb{F}_{11}[x]$ since
$f(3) = 3^2+3^2+4 = 22 \equiv 0$ in $\mathbb{F}_{11}$.
$\therefore f(x) = (x-3)(x-5)$
$= x(x-3)+6x+4$
$= x(x-3)-5(x-3)$.

(2) x^2+x+1 is irreducible in $\mathbb{F}_2[x] = \mathbb{Z}_2[x]$ by the lemma.
$\therefore \mathbb{F}_2[x]/(f(x))$ is a field.
We claim $\mathbb{F}_2[x]/(f(x))$ is a $\mathbb{F}_2$-vector space of 2-dim.
Pf: We claim that $\{\bar{1}, \bar{x}\}$ is the basis of the vector space.
$\Leftrightarrow a\bar{x}+b\bar{1}$ spans $\mathbb{F}_2[x]/(f(x))$. □

Eg. $\overline{x^3} = \bar{x}\cdot\bar{x}^2 = \bar{x}(-\bar{x}-\bar{1})$ $\quad (\overline{x^2+x+1} = \bar{1})$
$= -\bar{x}^2 - \bar{x}$
$= \bar{x}+\bar{1}-\bar{x} = \bar{1}$

Eg. $(\bar{1}+\bar{x})\cdot\bar{x} = \bar{x}+\bar{x}^2$
$= \bar{x}-\bar{x}-\bar{1} = -\bar{1}$
$= \bar{1}$ $(\mathbb{F}_2)$

(2') If we want to construct a field of 256 elems (recall QR code).
we just want to find the "correct" polynomials.

MA3201 W6L1 Irreducible Polynomials, Modules. Date No.

Recap: - $F[x]$, field $F \Rightarrow$ is a Euclidian Dom. ($\Rightarrow$ PID $\Rightarrow$ UFD)
- $\deg f(x) \in F[x]$ is of deg 2 or 3, then $f(x)$ is irreducible $\Leftrightarrow$ $f(x)$ has no roots in F.

Irreducible Polynomials in $\mathbb{Z}[x]$. (as prep for NT/Galois)

Lemma: Let R be an int. dom, with prime ideal $I \subset R$.
Let $p(x) \in R[x]$ be monic (leading coeff $= 1$) and non-constant.
then if $\overline{p(x)}$ is irreducible in $R/I[x] \cong R[x]/I$,
$\Rightarrow p(x)$ is irreducible in $R[x]$

(Monic $\Rightarrow$ no interference from R). ↙ non-unit.
eg $2x+2 = 2(x+1)$ is reducible. with factor $2 \in R[x]$.

Pf: Assume the contrary that $p(x) = a(x)b(x)$.
Monic $p(x) \Rightarrow \deg a(x) \geq 1$, $\deg b(x) \geq 1$.
(otherwise $a(x) = 1$ is a unit. $\to \in$)
Then consider the image of $p(x)$ in $R/I[x] \cong R[x]/I$.
$\therefore \overline{p(x)} = \overline{a(x)} \cdot \overline{b(x)}$.
we claim $\deg \overline{a(x)} \geq 1$ and $\deg \overline{b(x)} \geq 1$, contradicting assumption

we have $a(x) = a_k x^k + \dots$, $b(x) = b_l x^l + \dots$
where $a_k b_l = 1$. since $p(x) = a(x)b(x)$.
$\Rightarrow \overline{a_k}, \overline{b_l} \in R/I^\times$ are not 0. (?)
$\Rightarrow \deg \overline{a(x)}, \deg \overline{b(x)} \geq 1 \Rightarrow \overline{p(x)} = \overline{a(x)} \cdot \overline{b(x)}$
$\Rightarrow$ reducible in $R/I[x]$. $\to \in$.
(recall units in $R/I[x] = (R/I)^\times$). (?)

Eg. 1. x^2+x+1 is irred. in $\mathbb{Z}[x]$, since it is irreducible in $\mathbb{Z}_2[x]$.
(both $0, 1$ are not roots)
2. x^2+1 is irreducible in $\mathbb{Z}[x]$ since it is irred. in $\mathbb{Z}_3[x]$.
$0+1 \equiv 1$, $1+1 \equiv 2$, $4+1 \equiv 2$.
($\overline{x^2+1} = (\overline{x}+\overline{1})(\overline{x}-\overline{1})$)

Date No.

Prop (Eisenstein's criterion for divisibility) Let R be an int. dom (usually $\mathbb{Z}$) with a prime ideal $I \subset R$. Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in R[x]$ be a monic polynomial, non-constant.

Then $a_{n-1}, a_{n-2}, \ldots, a_0 \in I$ but $a_0 \notin I^2 \Rightarrow f(x)$ is irred. in $R[x]$.

Eg: Let $f(x) = x^2 + 10x + 5 \in \mathbb{Z}[x]$. Let $I = (5)$
since $I^2 = (25)$, $5 \notin (25)$, $f(x)$ is irred.

Pf: By contrad. Suppose the contrary,
(Reg) Let $f(x) = (x-a)(x-b)$ for $a, b \in \mathbb{Z}$
$= x - (a+b)x + ab$.
$= x + 10x + 5$
then $5 \mid ab \Rightarrow 5 \mid a$ or $5 \mid b$.
If $5 \mid a$, then since $5 \mid (a+b)$, $5 \mid b$. $\Rightarrow 5^2 \mid ab$.

Pf: Assume $f(x) = a(x) \cdot b(x)$, with $\deg a(x)$, $\deg b(x) \geq 1$.
we want to show contradiction that $a_0 \in I^2$.
Let $a(x) = a_r x^r + \ldots + a_0$
$b(x) = b_s x^s + \ldots + b_0$.
$\therefore a_r b_s = 1 \longleftrightarrow I$ since int. dom.
Consider the image of $f(x)$ in $R/I[x]$, which is an int dom since I is prime.
we have $\overline{f(x)} = \overline{a(x)} \cdot \overline{b(x)}$.
since $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$
$\in I$, sent to 0.
$\therefore \overline{f(x)} = \bar{x}^n$.
$\therefore \overline{a(x)} \cdot \overline{b(x)} = \bar{x}^{r+s} + \ldots + (\bar{b}_0\bar{a}_2 + \bar{b}_1\bar{a}_1 + \bar{b}_2\bar{a}_0)\bar{x}^2$
$+ (\bar{b}_0\bar{a}_1 + \bar{b}_1\bar{a}_0)x + \bar{b}_0\bar{a}_0$.

Comparing coeff, $\bar{a}_0\bar{b}_0 = \bar{0} \Rightarrow a_0 \in I$ or $b_0 \in I$.
suppose $a_0 \in I$, $\bar{a}_1\bar{b}_0 + \bar{a}_0\bar{b}_1 = \bar{0} \Rightarrow \bar{a}_1\bar{b}_0 = \bar{0}$ (by x)
if $b_0 \in I$, we are done. Else $\bar{a}_1 = 0$, $\Rightarrow \bar{b}_0\bar{a}_2 = \bar{0}$ (by x^2)
Similarly, ..., we assume at the end, $r \leq s$,
$\bar{a}_r \cdot \bar{b}_0 + \sum_{i+j=r} a_i b_j = \bar{b}_0 = \bar{0}$. $\Rightarrow \in$ $\square$

$\frac{1}{1}$ (why?)

MA3201 W6L1 (2) Date No.

Eg 2. $R[x,y]$ for int dom R, then $y^n - x$ is irreducible.
$x \in (x) \subset R[x]$ but $x \notin (x)^2 = (x^2)$
↑ prime since $R[x]/(x) \cong R$ is int dom.

Modules (simple group? simple ring?)

right.

Defn. Let R ring, A left R-module is an Abelian gp M, together with an action map $R \times M \to M$, $(r,m) \mapsto r \cdot m = rm$.
s.t. $\forall m,n \in M$, $r,s \in R$, (action. $m\cdot(r+s) = m\cdot r + m\cdot s$)
1. $(r+s)\cdot m = r\cdot m + s\cdot m$ 1. $m\cdot(rs) = (m\cdot r)\cdot s$
2. $(rs)\cdot m = r\cdot(s\cdot m)$. 2. (illegible)
(act on ↑ action)
3. $r\cdot(m+n) = r\cdot m + r\cdot n$. 3. $(m+n)\cdot r = m\cdot r + n\cdot r$
4. $1\cdot m = m$ if $1 \in R$. 4. $m\cdot 1 = m$ if $1 \in R$.

Rem. 1. M admits a R-mod structure $\Leftrightarrow$ A ring hom. from R to $\mathrm{Hom}_{Ab}(M,M)$ such that $1_R \mapsto \mathrm{id}$. (conditions: $r: M \to M$ is a gp hom)
2. we focus on left actions/modules.
3. R comm $\Rightarrow$ left = right.

Eg. 1. We have the $M = 0$ module for any ring R. (the only elem. in M is 0.)
Then we can define $r\cdot 0 = 0$. $(R \times M \to M,\ (r,0) \mapsto 0)$
(trivial action?)

2. Let R be a ring, then R is a left-mod via left multiplication.
define the action $R \times M \to M$ as the multiplication, where $M = R$.
check that 1. dist 2. assoc. 3. dist 4. id all are fulfilled.
R is also a right-mod.
If R is commutative, these are the same. $m\cdot r = r\cdot m$.

3. If F is a field, then F-modules are F-vector spaces.

4. Let M be an Abelian gp. Then M is a $\mathbb{Z}$-mod via the action.
$a\cdot m = \underbrace{m+m+\cdots+m}_{a \text{ times}}$ if $a > 0$.

Date No.

5. Let $I \subset R$ be a left ideal. Then I is a left R-mod. via the left multiplication. Note that $R \times I \to I$ is fulfilled, as the range is with I.

Gp action: gp acting on a set
Modules: ring acting on an Abelian group (unit +)
and hence the extra properties

Note $\mathrm{Hom}_{Ab}(M, M)$ is a rng, since $\forall f, g \in \mathrm{Hom}_{Ab}(M, M)$
$(f+g)(m) = f(m) + g(m)$.
$(f \cdot g)(m) = f(g(m))$.

Eg. (cont) 6. (non-eg). Let $R = M = \mathbb{Z}$. We know $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ ($R \times M \to M$, $r \cdot m \mapsto rm$) is an action of R on M. But if we define $(r, m) \mapsto r + m$ is not an action of R on M. (Why?)
(particularly distributive prop fail).

Def. Submod Let R be a rng. Let M be a R-Mod. Let $N \subset M$ be an (Abelian) subgroup. N is called a R-submodule of M if N is closed under the R-action, that is.
$r \cdot n \in N \quad \forall r \in R, n \in N$.

Eg. 1. If we consider $R \curvearrowright R$ via the left mult, then $\forall$ left ideal $I \subset R$ will be a R-submod. of R.

$\emptyset$
2. $\{0\}$ mod is the submod of any R-mod, since $r \cdot 0 = 0$.
2'. M is a submod of M. (trivial).

3. Let M be a $\mathbb{Z}$-mod. $\Leftrightarrow$ M is an Ab. gp. Then
$N \subset M$ is a $\mathbb{Z}$-submod $\Leftrightarrow$ $N \subset M$ is a (abelian) subgp.
3'. F field $\Rightarrow$ any F-mod, M is a F-vector space.
Then any F-submod (of M) is a F-subspace of M.

4. Let $S \subset R$ be a subrng containing 1. Then R is a S-mod via left-mult $S \times R \to R$. Then $S \subset R$ is a ~~submod~~ S-submod of R.

MA3201 W6L1 (3) Date No.

5. Let F be a field. Consider $F[x]$. Let M be a $F[x]$-mod.
Then by (4) we can consider the actions of only elements in $F \subset F[x]$.
Then M is also a module over F (via restriction).
$F[x] \times M \to M$ restrict to $F \times M \to M$.
So M is a F-vectorspace with an action of x.
$x: M \to M$, $m \mapsto x \cdot m$.

We claim $x: M \to M$ is a linear transf.

Pf: WTS $x \cdot (a\underline{v}) = a(x \cdot \underline{v})$.
RHS: $a, x \in F[x] \Rightarrow a(x \cdot v) = x \cdot (a \cdot v)$ (mod. action)
LHS: $x \cdot (a\underline{v}) = (xa) \cdot \underline{v}$ □

similarly $\forall f(x): M \to M$, $m \mapsto f(x) \cdot m$ is a linear. trans.

5'. (reverse) given a F-vector space M with a linear map $T: M \to M$, we can define a $F[x]$-module structure on M via.
$F[x] \times M \to M$
$(f(x), m) \longmapsto f(T) \cdot m$
$= (a_n T^n + a_{n-1} T^{n-1} + \dots + a_0) \cdot m$

Recap Irreducible Polynomials:
1. Check in quotient gp. irreducible in $R[x]/I \Rightarrow$ irreducible in $R[x]$.
2. Eisenstein's criteria, $a_{n-1}, a_{n-2}, \dots, a_0 \in I$, $a_n = 1$, $a_0 \notin I^2 \Rightarrow$ irreducible

Module defn: R ring with 1, abel. an sp M. left R-action, $R \times M \to M$
$(r, m) \mapsto rm$
s.t. 1. $r(m+n) = rm + rn$
2. $(r+s) \cdot m = r \cdot s + rm$
3. $rs(m) = r \cdot (sm)$
4. $1 \cdot m = m$.
- M is Ab sp $\Leftrightarrow$ M is a $\mathbb{Z}$-mod.
- M is a F-vs. for field $F \Leftrightarrow$ M is a F-mod.
- M Ab. gp, write $\mathrm{Hom}_{Ab}(M, M) = \mathrm{End}_{Ab}(M)$. Then M is a $\mathrm{End}_{Ab}(M)$-Mod, $f \cdot m = f(m)$

MA3201 W6L2 Date No.

Recap (cont'd)

- F field, then F^n is a $\mathrm{Mat}_{n\times n}(F)$-mod.
  (Check: $M(v+u)=Mv+Mu$, $(M+N)v=Mv+Nv$, $(MN)v=M(Nv)$, $Iv=v$.)
- M is a R-mod $\Leftrightarrow$ we have a ring hom $R\to \mathrm{End}_{Ab}(M)$.
  ($R\times M\to M$ induces $R\to \mathrm{End}_{Ab}(M)$.)
- Recall G acts on A induces $G\to \mathrm{Aut}(A)$. (bijective)

Lem. Let $\varphi: S\to R$ be a ring hom. s.t. ($1_S\to 1_R$) (cond3, cond4) Let M be a R-mod. (left) Then M is naturally a S-mod w/ the action.

$s\cdot m \overset{\text{def}}{:=} \varphi(s)\cdot m$ for any $s\in S$, $m\in M$.

action: $S\times M\to M$.

Pf: 1st Pf we check the requirements for S modules:

- $\forall s,t\in S$, $(s+t)m=\varphi(s+t)m=[\varphi(s)+\varphi(t)]m$.
- $\forall s\in S, \forall m\in M$, $s(m+n)=\varphi(s)[m+n]$
- $\varphi(st)m=\varphi(s)[\varphi(t)m]$.
- $1_S\cdot M=\varphi(1_S)\cdot m=1_R\cdot M$.

2nd Pf we know $R\curvearrowright M$. we have, equivalently, a ring hom $\phi: R\to \mathrm{End}_{Ab}(M)$, $r\mapsto \varphi_r$ such that $r\cdot m=\varphi_r(m)$

(Pre-) composing with $\varphi: S\to R$, we have $S\xrightarrow{\varphi} R\xrightarrow{\phi}\mathrm{End}_{Ab}(M)$ and thus S induces a ring hom to $\uparrow$ as well $\Rightarrow S\curvearrowright M$. □

Eg

1. Let $S\subset R$ be a subring where $1_R\in S$. Then any R-mod M is also a S-mod, since we already have $R\curvearrowright M$, we have $S\curvearrowright M$ by the restriction ($R\curvearrowright R\to S\curvearrowright R$ is ok, but why?)

2. $F[x]\curvearrowright M\to F\curvearrowright M$ by restriction for any F-vs M.

3. Let R be a ring with 1. (Eg $\mathbb{Z}_3$), then we have a ring hom. $\mathbb{Z}\to R$, $n\to n\cdot 1=1+1+\cdots+1$ n times. Then any R-mod M is also a $\mathbb{Z}$-mod. (check how.)

MA3201 W6L2 (r). Date No.

Basic Properties of Modules.

Prop. Let $R \ni 1 \neq 0$, M be a R-mod. $(R \to \mathrm{End}_{Ab}(M))$

(1) $0_R \cdot m = 0_M$, $(-1)_R \cdot m = -m$.

(2) Any intersection of submods of M is still a submod.

(3) $\mathrm{Ann}_M(R) \subset R$, $\mathrm{Ann}_M(R) = \{r \in R \mid r \cdot m = 0 \ \forall m \in M\}$. is an ideal of R

(4) Let $z \in R$ be central, i.e. $az = za \ \forall a \in R$. Then
$z \cdot M = \{z \cdot m \mid m \in M\}$. is a R-submod of M.

Pf (1) If we see the $R \to \mathrm{End}_{Ab}(M)$ ring hom, then we must have
$0_R \mapsto 0_{\mathrm{End}(M)}$, $-1_R \mapsto -1_{\mathrm{End}(M)}$.

Alternative Proofs: $0_R \cdot m = (0_R + 0_R) \cdot m$
$= 0_R \cdot m + 0_R \cdot m \Rightarrow 0_R \cdot m = 0_M$ in M

$0 = (1 + (-1)) \cdot m = 1 \cdot m + (-1) \cdot m = m + (-1) \cdot m$
$\Rightarrow (-1) \cdot m = -m$. must be the inverse.

(2) Let I be an index set, let M_i with $i \in I$ be a collection of $(R$-$)$submodules of M.
Then $\bigcap_{i \in I} M_i = N$ is an abelian subgp of M. (all subgps are normal)
we just need to check closedness under $\times$:
$\forall r, n \in N$, if exists in all submodule in $M_i \Rightarrow r \cdot n \in$ all submod
$\Rightarrow r \cdot n \in N$. □.

(3) Recall homework: $\mathrm{Ann}_I(R)$ is an ideal in R.
Recall: any ideal is a module.

(4) Check: Abelian Subgp: $\forall zm, zn \in zM$,
$zm - zn = zm + (-z) \cdot n$.
$= zm + (z(-1)) \cdot n$
$= z(m - n) \in z \cdot M$.
Closed under $*$: $\forall r \in R$, $r \cdot (zm) = r \cdot z \cdot m$
R-action $= z \cdot (rm) \in z \cdot M$.

Date No.

lem Let M be a R-mod ($R \ni 1$). Let $I \subset \mathrm{Ann}_M(R)$ be an ideal. Then M is naturally a R/I-mod via the action.

$$(r+I)\cdot m = r\cdot m \quad \text{for } r \in R,\ m \in M.$$

Pf. 1st Pf: we have $\varphi: R \to \mathrm{End}_{Ab}(M)$. Then $\mathrm{Ann}_M(R) = \ker\varphi$ (why?) Then if $I \subset \ker\varphi$, we have.

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & \mathrm{End}_{Ab}(M). \\ \pi \downarrow & \nearrow \bar{\varphi} & \\ R/I & & \end{array}$$

2nd Pf: First, we check well-def. let $r+I = r'+I \iff r = r'+a$ for $a \in I$
Then $(r+I)\cdot m = rm = (r'+a)\cdot m = r'm + a\cdot m = r'm$. (in R/I)

Check requirements:
$(r+I+s+I)\cdot m = (r+s+I)\cdot m = (r+s)\cdot m$
$= (r+I)\cdot m + (s+I)\cdot m = r\cdot m + s\cdot m = (r+s)\cdot m$

Def/Prop Let $R \ni 1 \neq 0$, 1.1. M be a R-mod. $N \subseteq M$ be a subset. Then define

$$R\cdot N = \{\textstyle\sum_{\text{finite}} a_n n \mid a \in R, n \in N\} \subseteq M.$$

It is a submodule of M. (check)

1.2. call any elem in $R\cdot N$ a R-linear combi.

1.3. call $R\cdot N$ the R-submod of M generated by N.

1.4. M is called finitely generated if $M = R\cdot A$ for a finite set A.

1.5. M is cyclic if it is generated by some single elem.

2. Let $M_1, \dots, M_n$ be R-submods of M, we define

$$\sum_{i=1}^n M_i = \left\{ \sum_{i=1}^n m_i \mid m_i \in M_i \right\}.$$ and it is a R-submod of M.

3. Let M_c R-submods of a R-mod M, for $c \in I$ (potentially infinite),

Date No.

then $\sum_{i\in I} M_c = \{ \sum_{c\in I} m_c e_c \mid m_c \in M_c$ with finitely many non-0 terms$\}$.
Is also a submod of M. (check)

Module Homomorphisms

Defn Let $R \ni 1 \neq 0$. Let M, N be R-modules (fix the ring over the mods M, N)

1. A R-mod homomorphism (morphism, map) $\varphi: M \to N$ is a map such that
   (i) $\varphi(m+m') = \varphi(m) + \varphi(m')$ for $m, m' \in M$ (Ab. gp. hom)
   (ii) $\varphi(r \cdot m) = r \cdot \varphi(m)$ for $m \in M$, $r \in R$.
   $R \curvearrowright M$ $R \curvearrowright N$.

2. A R-mod homom. $\varphi: M \to N$ is an isom (of R-modules) if it is a bijection, or equiv. $\exists$ R-mod map $\psi: N \to M$ s.t. $\varphi \circ \psi = id_N$ and $\psi \circ \varphi = id_M$.

3. Let $\varphi: M \to N$ be a R-mod hom. Define $\ker\varphi$ and $\operatorname{Im}\varphi$ naturally: $\ker\varphi = \{ m \in M \mid \varphi(m) = 0 \}$, $\operatorname{Im}\varphi = \{ \varphi(m) \mid m \in M \}$. and both $\ker\varphi$ and $\operatorname{Im}\varphi$ are R-submodules (of M, N resp.)

4. Define the set of R-mod maps $M \to N$ as $\operatorname{Hom}_R(M, N)$. Also write $\operatorname{Hom}_R(M, M) = \operatorname{End}_R(M)$.

Eg (1) F field, M, N F-mods. Then F-mod map $\varphi: M \to N$ is just a F-linear map. (linear-trans between vs. M, N).
$\varphi(m+m') = \varphi(m) + \varphi(m')$, $\varphi(r \cdot m) = r \cdot \varphi(m)$.
(1') $F = \mathbb{R}$, let $M, N = \mathbb{R}^{(\mathbb{N})}$. Then $\mathbb{R}$-mod hom.
$T: M \to N$, $x \mapsto ax$ (cannot add final terms) non- as a $0 \to 0$.
Then $T(x+y) = Tx + Ty$,
$T(cx) = cT(x)$. just like linear maps.

2. $R = \mathbb{Z} = M = N$. M, N are R-mods. Then a $\mathbb{Z}$-mod map $\varphi: M \to N$ is just an Abelian Gp hom $\varphi(q \cdot m) = q \cdot \varphi(m)$,
$\varphi(m+m') = \varphi(m) + \varphi(m')$
$\varphi(\underbrace{1+\cdots+1}_{m} + \underbrace{1+\cdots+1}_{m'}) = \varphi(\underbrace{m+m+\cdots+m}_{q})$.

Date No.

Eg (cont) 3. Let $R \overset{\varphi}{\to} R$ via left mult. Then
$\varphi_a : R \to R$, $r \mapsto r \cdot a$ is a R-mod hom.
Check $\varphi_a(m+m') = (m+m')\cdot a = m\cdot a + m'a = \varphi_a(m) + \varphi_a(m')$.
$\varphi_a(r \cdot m) = a(r \cdot m) = r \cdot (m \cdot a) = r \cdot \varphi_a(m)$

(3') Let $R \overset{\varphi}{\to} R$ via left mult, and $z \in R$ be central ($zr = rz \ \forall r \in R$).
Then $\varphi_z : R \to R$, $r \mapsto z \cdot r = r \cdot z$ is a R-mod hom.

MA3201 WTL1 Date No.

Recap Module defn: R-mod M. Submodule $N \subset M$.
↳ usually with $1 \neq 0$ unless specified otherwise.

Eg. Let $G = S_2 \cong \mathbb{Z}_2$. Let $R = \mathbb{C}[G] = \{ae + b(12) \mid a, b \in \mathbb{C}\}$.

Any R-mod V is naturally a $\mathbb{C}$-vector space $= \mathbb{C}$-mod since we have an embedding $\mathbb{C} \to R$, $a \mapsto a \cdot e$.

we consider $V = \mathbb{C}e_1 \oplus \mathbb{C}e_2$ ($\cong \mathbb{C}^2$). we define a R-action on V via $(12) \cdot (ae_1 + be_2) = ae_2 + be_1$,
extend this linearly: $m, n \in \mathbb{C}$
$[me + n(12)] \cdot (ae_1 + be_2)$
$= m \cdot (ae_1 + be_2) + n \cdot (ae_2 + be_1)$
we can check this defines a R-mod structure on V.

Claim: any $x = ae + b(12)$ is a lin. trans from V to V. (lin trans $\Rightarrow$ $\mathrm{Hom}_{Ab}(V, V)$) but lack proper restriction of the domain
Pf: recall R-mod $V \Leftrightarrow$ A ring hom $R \to \mathrm{Hom}_{Ab}(V, V)$.
check that $\forall v, w \in V$, $x \in \mathbb{C}[G]$.
$x \cdot (v + w) = x \cdot v + x \cdot w$ (abelian hom).
$x \cdot (k \cdot v) = k \cdot (x \cdot v)$ for $k \in \mathbb{C}$.
$= (xk) \cdot v$
$= (kx) \cdot v$ ($\mathbb{C}$ is comm.) $= k \cdot (xv)$.

we the consider submodules of V:
Let $W = \mathbb{C}(e_1 + e_2) \subset V$ be a 1-dim subspace of V.
Claim: W is a submod of V.
Pf: just check W is closed under R-action, that is, we can restrict $R \times V \to V$ to $R \times W \to W$.
eg. $(12) \cdot (k(e_1 + e_2)) = k(e_2 + e_1) \in W$.

Claim: $U = \mathbb{C}(e_1 - e_2)$ is also a submod of V.
Idea: $(12) \cdot k(e_1 - e_2) = -k(e_1 - e_2)$.

Date No.

we also have $V = W \oplus U$ as $\mathbb{C}$-vector spaces.
it is also a R-mod (will be defined).

Recall R-mod hom $\varphi: M \to N$:
1. $\varphi(rx+y) = r\varphi(x) + \varphi(y)$ 2. $\varphi(r \cdot x) = r \cdot \varphi(x)$.

Lem (Basic Properties of R-mod. homomorphisms):
Let M, N, L be R-mods.
(1) Let $\varphi: M \to N$ be a R-mod map. Then $\ker\varphi$ and $\operatorname{Im}\varphi$ are R-submods.
Pf: $\ker\varphi = \{x \in M \mid \varphi(x) = 0\}$. is an Ab. subgp of M.
Just need to check it is closed under R-action.
$\therefore$ Let $m \in \ker\varphi$. $\forall r \in R$, WTS $r \cdot m \in \ker\varphi$.
$\Rightarrow \varphi(r \cdot m) \neq 0$
$\varphi(r \cdot m) = r \cdot \varphi(m)$. but $R \to \operatorname{Hom}_{Ab}(M, M)$.
$= r \cdot 0$ maps $0 \to 0$.
$= 0$. $\therefore r \cdot m \in \ker\varphi$.
$\operatorname{Im}\varphi = \{\varphi(x) \in N \mid x \in M\}$.
$\forall \varphi(x) \in \operatorname{Im}\varphi$, $r \cdot \varphi(x) \in \operatorname{Im}\varphi$.
$r \cdot \varphi(x) = \varphi(r \cdot x)$ but $r \cdot x \in M$.
$= \varphi(m) = n \in N \Rightarrow r \cdot \varphi(x) \in \operatorname{Im}\varphi$.

(2) Let $\varphi, \phi \in \operatorname{Hom}_{Ab}(M, N)$. Define $\varphi + \phi: M \to N$,
$(\varphi + \phi)(m) = \varphi(m) + \phi(m) = \phi(m) + \varphi(m) = (\phi + \varphi)(m)$.
we claim $\varphi + \phi \in \operatorname{Hom}_R(M, N)$.

Pf: Check $(\varphi + \phi)(m_1 + m_2) = (\phi + \varphi)(m_1 + m_2)$ (easy with M, N abelian)

Check $(\varphi + \phi)(r \cdot m) \neq (\phi + \varphi)(r \cdot m)$
$= r \cdot \varphi(m) + r \cdot \phi(m)$
$= (\phi + \varphi)(rm)$.

MAB301 W7L1 (2)

(Props of R-mod maps, cont'd).

(3) Let $\varphi \in \mathrm{Hom}_R(M,N)$, $\phi \in \mathrm{Hom}_R(N,L)$. Then $\phi\circ\varphi \in \mathrm{Hom}_R(M,L)$.

Pf: check: $\phi\circ\varphi(m_1+m_2) \stackrel{?}{=} \phi\circ\varphi(m_1) + \phi\circ\varphi(m_2)$

check: $\phi\circ\varphi(r\cdot m) \stackrel{?}{=} r\cdot[\phi\circ\varphi(m)]$

(4) $\mathrm{Hom}_R(M,M) = \mathrm{End}_R(M)$ is a rng. And M is naturally a $\mathrm{End}_R(M)$-module.

Pf. Check $(\mathrm{End}_R(M), +, \circ)$ is a rng.

The action $\mathrm{End}_R(M) \curvearrowright M$ is just

$f\cdot m = f(m)$.

Eg End of vector spaces are just matrices.

Quotient Modules

Defn. M is a R-mod with a submod $N \subseteq M$. Define the quotient R-mod M/N as
- $M/N = M/N$ as quotient Abelian gp
- $r(m+N) = r\cdot m + N \quad \forall r\in R, m\in M$. (representative dependent-def)

Moreover the quotient map $\pi: M \to M/N$ is a R-mod homomorphism.

$\Rightarrow m = m' + n$

Pf: (well-defn). Let $m+N = m'+N$, $r(m+N) \stackrel{?}{=} r(m'+N)$.

$r(m+N) = r\cdot m + N \in N$

$= r\cdot m' + (r\cdot n) + N = r\cdot m' + N$. □

(Exercise: this defines a R-mod struc on M/N.)

1. $(r+s)\cdot(m+N) = r\cdot m+N + s\cdot m+N$.

$= r\cdot m + s\cdot m + N$ (ab. sp).

$= (r+s)\cdot m + N$.

(*) 2.

Date No.

Eg. 1. Let F be a field, then M/N is just the quotient vector space.
2. Let $I \subset R$ be a (left ideal $\Leftrightarrow$ I is a R-submod of R.
Then $\pi: R \to R/I$ is a R-mod hom.

Lem. (universal property of quotient) Let R be a ring with $1 \neq 0$. Let M be a R-mod with a submod $N \subset M$. Then $\forall$ R-mod L and R-mod map $\varphi: M \to L$ s.t. $\varphi(N) = 0$ ($\Leftrightarrow$ $N \subseteq \ker\varphi$)

Then we have a unique R-mod map $\bar{\varphi}: M/N \to L$ s.t. the following diagram commutes.

$\varphi(m)$

$m \in M \xrightarrow{\varphi} L = \bar{\varphi}(m+N)$.

$\pi \downarrow \quad \nearrow \bar{\varphi}$

$m+N \in M/N$.

Isomorphism Thm for modules.

Thm Let R be a ring with $1 \neq 0$.
(1) Let M, N be R-modules. $\varphi: M \to N$ is a mod. map. Then
$M/\ker\varphi \cong \varphi(M) = \mathrm{Im}(M)$.

Define: $\mathrm{coker}\,\varphi = N/\mathrm{Im}\,\varphi = N/\varphi(M)$.
this is just $M \setminus N$ but the spoqm. s.t.

(2) Let M, N be submodules of L. Then $M+N/M \cong N/N \cap M$
Here $M+N = \{m+n \in L \mid m \in M, n \in N\}$.

(3) Then we have $L/M \cong L/N \,/\, M/N$ as R-modules.

(4) Suppose M, N are R-mods where $N \subset M$. Then we have a bijection via $\pi: M \to M/N$.
$\{$submodules of M containing $N\} \leftrightarrow \{$submodules of $M/N\}$.

MA3201 WTL4 (3) see Cyclic.

Lem: Let $M = R \cdot m$ for some $m \in M$. Then
$R/I \cong M$ as R-mods for some left ideals $I \subset R$.

Pf: we define $\varphi : R \xrightarrow{\text{surj}} M$, $r \mapsto r \cdot m$ we claim φ is a R-mod hom.
Show $\varphi(s+r) \overset{?}{=} \varphi(s) + \varphi(r)$.
$(s+r)\cdot m = s\cdot m + r \cdot m$
Show $\varphi(r \cdot s) \overset{?}{=} r \cdot \varphi(s)$.
$(r \cdot s) \cdot m = r \cdot (s \cdot m)$
So by the 1i0. thm, $R/\ker\varphi \cong M$. where $\ker\varphi$ is a R-submod (or left ideal) of R.

Simple Modules

use modules to study rings: eg. using vector spaces to study matrices.

Defn: Let R ring with $1 \neq 0$. R-mod M is simple (or reducible), if $M \neq 0$ such that $0, M$ are the only submodules of M.

Eg. ① Let F be a field, then 1-dim F-mods are simple. (No subspaces)
② Let $R = \mathbb{Z}$. Then simple $\mathbb{Z}$-mods are of the form $\mathbb{Z}/p\mathbb{Z}$ for prime p's. (can show all simple $\mathbb{Z}$-mods are of $\mathbb{Z}_p$ form)
③ Let $R = \mathrm{Mat}_{n\times n}(F)$ for a field F. Let $V = F^n$ be a R-Mod. Then F^n is simple.
Idea: Let $0 \neq W \subseteq V$ be a R-submodule. we claim $W = V$.
We take any vector $w \in W$. Then $\forall v \in V$, $\exists A \in M_n(F)$ s.t. $Aw = v \in W$ since W is a submodule (closed under mod action).
eg. Given any $v \in F^n$, $\exists A \in M_n(F)$, $Aw = v$ where $w \in W \subseteq V$.

□

It is hard to know how simple modules look like, given a ring/mod.

Lem: (Schur's lemma) R ring with 1. Let M, N be simple R-mods.
Then $\varphi: M \to N$ is either an isom. or 0.
In particular, $\mathrm{End}_R(M)$ is a division ring. (every non-zero are invertibles $\in$ fields but not necessarily commutative)

Pf: $\ker\varphi$ is a submod of M $= 0$ or M.
$\mathrm{Im}\,\varphi$: $\longrightarrow\!\!\!\!\!\!+\!\!\!\!\!\!\longrightarrow N$ $= M$ or 0.
φ is a — isom or 0

$\varphi: F \to F$ s.t. $\varphi(x \cdot y) = x \cdot \varphi(y)$.

Eg. ① $\mathrm{End}_F(F) \cong F$ (module homs $F \to F \cong F$, scalar mult).
(✡) ② $\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z}$
③ $\mathrm{End}_{M_n(F)}(F^n) \cong F$ ($\varphi: F^n \to F^n$ s.t. $\varphi(A \cdot v) = A \cdot \varphi(v)$) (matrices.)
(the center of the mat. ring is the scalar matrices)

Rem. J rng (without 1). Then a J-mod $M \neq 0$ is simple if
- $0, M$ are the only submods of M.
- $J \cdot M = \{j \cdot m \mid j \in J, m \in M\} = M$

Eg. $J = \mathbb{Z}$ as ab. gp but $x \cdot y = 0$. Then $J^2 = 0$.

MA3701 W7L2

Recall: Basic props of mod. hom: $\varphi: M \to N$
Quotient mods: $N \subset M \to M/N$.
Isom. thms for mods (which are Ab gps + additional props).
Simple mods: only 0 and M as submods. Building blocks

R-algebra

Defn: Let R be a comm. ring with 1_R. A R-algebra A is a ring with 1_A together with a ring hom $f: R \to A$, $1_R \mapsto 1_A$ s.t.
$f(R) \subseteq Z(A)$. (image is contained in the center.)

Eg: ① R[x] is a R-algebra. (Any A-module is a R-mod (vs (if R field) via restriction/composition)
② R[G] is a R-algebra for any finite gp G.
③ Let M be a R-mod. Then $\mathrm{End}_R(M)$ is a R-algebra.
The map $f: R \to \mathrm{End}_R(M)$
$r \mapsto (f_r: M \to M,\ m \mapsto r \cdot m)$.
Recall R is comm $\Rightarrow f_r(s \cdot m) = r s \cdot m = s \cdot r \cdot m = s \cdot f_r(m)$
(R-alg) $\Rightarrow f_r$ is a R-mod hom.
→ R comm.
③' R=F be a field. Then $M \cong F^n$ is a F-vs.
Then $\mathrm{End}_F(F^n) \cong \mathrm{Mat}_{n \times n}(F)$ is a F-algebra.

Rem. ① A ring is just a $\mathbb{Z}$-algebra. with the ring hom:
$\mathbb{Z} \to R$, $1 \mapsto 1$
② A R-alg. A is a ring $A \to I$ that is also a R-mod, where the R-action is compatible with the ring operations. eg:
$R \to A = R \cdot A$ $r \cdot a = f(r)a$ where or $f(r) = r \cdot 1$
③ F be a field, A be a F-alg (eg $A = \mathbb{C}[G]$). Then any A-mod is automatically a F-vector space.

Direct sum & Direct pdt of mods of mods I (finite)

Defn: Let R be a ring with $1 \neq 0$. Let $M_1, \dots, M_n$ be R-mods. We define their direct sum (= direct pdt) $M = M_1 \oplus M_2 \oplus \dots \oplus M_n$ as:

- $M = M_1 \oplus \dots \oplus M_n$ as sets / abelian gps $(= M_1 \times M_2 \times \dots \times M_n)$.
- The R-action on M is defined as $r \cdot (m_1, m_2, \dots, m_n) = (r \cdot m_1, r \cdot m_2, \dots, r \cdot m_n)$.

It is easy to check that M is also an R-mod.

Lem: (1) we have R-mod maps $f_i : M_i \to M$, $m_i \mapsto (0, \dots, m_i, \dots, 0)$
$g_i : M \to M_i$, $(m_1, m_2, \dots, m_i, \dots, m_n) \mapsto m_i$.

(2) we have $M_1 \oplus M_2 \cong M_2 \oplus M_1$.
so we write $M_1 \oplus \dots \oplus M_n = \bigoplus_{i=1}^{n} M_i$.

Eg: (1) $R^n = \overbrace{R \oplus \dots \oplus R}^{n} = \bigoplus_{i=1}^{n} R = R^{\oplus n}$.
(ambiguity: $R^n = \{\sum_{i=1}^{n} r_i e_i \mid r_1, \dots, r_n \in R\}$) we call this a free R-mod of rank n. with.
we often write $e_i = (0, \dots, 0, 1, 0, \dots, 0) \in R^{\oplus n}$. They form a R-basis of $R^{\oplus n}$, that is, any $m \in R^{\oplus n}$ can be written uniquely as $m = m_1 e_1 + m_2 e_2 + \dots + m_n e_n$.

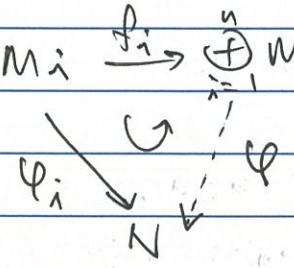
(2) we have (by CRT) $\mathbb{Z}_6 \cong \mathbb{Z}_3 \oplus \mathbb{Z}_2$ as $\mathbb{Z}$-modules. (ideals).
($\mathbb{Z}_3$, $\mathbb{Z}_2$: simple $\mathbb{Z}$-modules (simple gps))

Lem: Let M be a R-mod, $m_1, m_2, \dots, m_n \in M$. Then $\exists$ unique R-mod hom $\varphi : R^{\oplus n} \to M$ such that $e_i \mapsto m_i$.
If $M = R \cdot \{m_1, \dots, m_n\}$ (act.) is finitely generated, then φ is surjective.

Pf: The uniqueness is forced by the R-mod hom, that is,
$\varphi(a_1 e_1 + a_2 e_2 + \dots + a_n e_n) = a_1 \cdot m_1 + \dots + a_n m_n$.
This can be used to define φ. It remains to check that φ is indeed a R-mod map. Eg:
$\varphi(r \cdot (a_1 e_1 + \dots + a_n e_n)) = \varphi(ra_1 e_1 + \dots + ra_n e_n)$
$= ra_1 m_1 + \dots + ra_n e_n = r \cdot \varphi(\dots)$

MA3210 | W7L2 (2).

Prop. (univ. prop of $\oplus$) Let R be a ring with 1. Let $M_1, \dots, M_n$ be R-mod. Then for any collection of R-mod hom $\varphi_i : M_i \to N$ there is a unique R-mod hom $\varphi : \bigoplus_{i=1}^n M_i \to N$ s.t. the diagram commutes:



Pf: we define $\varphi : \bigoplus_{i=1}^n M_i \to N$ (forced by the commuting diag.)
by $(m_1, \dots, m_n) \longmapsto \varphi_1(m_1) + \varphi_2(m_2) + \dots + \varphi_n(m_n)$
$= (m_1, 0, \dots) + (0, m_2, \dots)$
This also shows the uniqueness (by Ab. gp only, no need mod str

It remains to check φ is a R-mod hom (i.e. R-action).
$\varphi(r \cdot (m_1, m_2, \dots, m_n)) = \varphi(rm_1, \dots, rm_n)$
$\overset{?}{=}$ $= \varphi_1(rm_1) + \dots$
$r \cdot \varphi(m_1, \dots, m_n)$ $= r \cdot \varphi_1(m_1) + \dots$ □

Prop: Let R be a ring with id 1. Let $N_1, N_2, \dots, N_k$ be submods of M.
Then the following are equivalent: (characterization of "basis")
(1) The natural map $\bigoplus_{i=1}^k N_i \to \sum_{i=1}^k N_i \left(= \left\{ \sum_{i=1}^k n_i \mid n_i \in N_i \right\} \subseteq M \right)$
is an isomorphism of R-mods.
(2) Any $x \in \sum_{i=1}^k N_i \subset M$ can be written uniquely as $x = a_1 + a_2 + \dots + a_k$ with $a_i \in N_i$.
(3) The intersection $N_j \cap \sum_{i \neq j} N_i = 0$ (i.e. trivial) for any j.

(Recall $\mathbb{Z}_6 = \mathbb{Z}_2 + \mathbb{Z}_3$, "$\mathbb{Z}_2$" $= \{\bar{0}_6, \bar{3}_6\}$, "$\mathbb{Z}_3$" $= \{\bar{0}_6, \bar{2}_6, \bar{4}_6\}$, image in $\mathbb{Z}_6$.)
$\mathbb{Z}_2 \cap \mathbb{Z}_3 = \{\bar{0}\}$.

This generalizes direct sum of vector subspaces to R-mods.

Pf: Note that φ is iso $\iff \ker\varphi = \{0\}$.

$$\ker\varphi = \{(n_1,\dots,n_k) \in \bigoplus_{i=1}^{k} N_i \mid \sum_{i=1}^{k} n_i = 0\}.$$

(1) $\Rightarrow$ (2): Note that for $\ker\varphi = 0 \Rightarrow 0 \in M$ has a unique expression.

WTS unique expr. $\forall x \in \sum N_i$

$0 = 0 + 0 + \dots + 0$

Given any $x \in \sum N_i$, assume (for $\to\in$)

$$x = a_1 + \dots + a_k = b_1 + \dots + b_k$$

$$\Rightarrow x - x = 0 = (a_1 - b_1) + \dots + (a_k - b_k)$$

Since 0 is written uniquely, $a_i - b_i = 0 \ \forall i = 1,\dots,k$.

$\Rightarrow a_i = b_i$. □

(2) $\Rightarrow$ (3) WTS written uniquely $\Rightarrow N_i \cap \bigoplus_{i\neq j} N_j = 0$.

Assume the contrary that $x \neq 0$, $x \in N_j \cap \sum_{i\neq j} N_i$ for some j.

$$\Rightarrow x = 0 + \dots + \underbrace{x}_{\in N_j} + \dots + 0$$

distinct exprs. ($\to\in$)

$$= a_1 + \dots + a_{j-1} + 0 + a_{j+1} + \dots + a_n$$

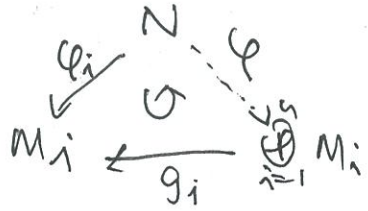
(3) $\Rightarrow$ (1) WTS $N_i \cap \bigoplus_{i\neq j} N_j = 0 \Rightarrow$ iso $\bigoplus \to \sum$ (trivial ker).

Let $(n_1,\dots,n_n) \in \ker\varphi$. Then $\sum_{i=1}^{n} n_i = 0$.

$\Rightarrow -n_j = \sum_{i\neq j} n_i \in N_j \cap \sum_{i\neq j} N_i = 0$.

$\Rightarrow n_j = 0$ for any j.

Prop ("direct pdt"): Let R be a ring with 1. Let $M_1,\dots,M_n$ be R-mods. Then for any R-mod map $\varphi_i : N \to M_i$ then there is a unique R-mod map $\varphi_{\oplus} : N \to \bigoplus_{i=1}^{n} M_i$ $(= \prod_{i=1}^{n} M_i)$ s.t. the following diag. commutes:



(Uniqueness is usually easy. R-mod etc are the real things we need to check.)

MA3201 W7L2 (3).

Pf: Define $\varphi: N \to \bigoplus_{i=1}^{n} M_i$

$s \longmapsto (\varphi_1(s), \varphi_2(s), \dots, \varphi_n(s))$ (forced & defn)

this already forced the uniqueness. We show it's a R-mod hom.

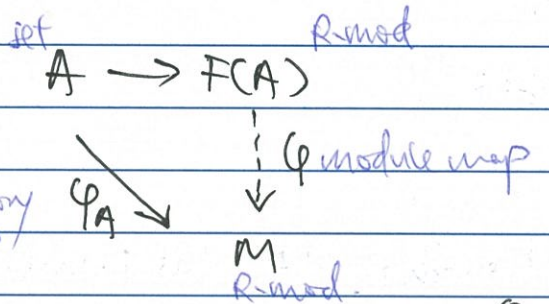
$\varphi(r \cdot s) = (\varphi_1(rs), \varphi_2(rs), \dots, \varphi_n(rs))$

$\overset{?}{=} (r\cdot\varphi_1(s), r\cdot\varphi_2(s), \dots, r\cdot\varphi_n(s))$

$r \cdot \varphi(s)$ ✓ □.

Free Modules

Defn: $R \ni 1$. Let $A = \{a_1, \dots, a_n\}$ be a finite set. Then the **free R-mod over A** (generated by A) is a R-mod $F(A)$ tgt with a set-theoretical map $A \to F(A)$ s.t. for any set-theoretical map $\varphi_A: A \to M$ for a R-mod M, $\exists$ a R-mod hom $\varphi: F(A) \to M$ s.t. diag comm:



we claim such $F(A)$ exists and $F(A) \cong R^{\oplus n}$.

Pf: Consider $F(A) = R^{\oplus n}$, and thus the $A \to F(A)$ map as

$A \to R^{\oplus n}$, $a_i \longmapsto e_i$.

Then given any $\varphi_A: A \to M$, $a_i \longmapsto m_i$, the induced map is nat.

$\varphi: (F(A) \cong) R^{\oplus n} \to M$, $e_i \longmapsto m_i$.

This gives uniqueness, we now check φ is a R-mod map:

(given by univ. prop of $\oplus$).

Preview: We will show if R comm, $R \ni 1$, $R^{\oplus n} \cong R^{\oplus m} \Rightarrow n = m$.

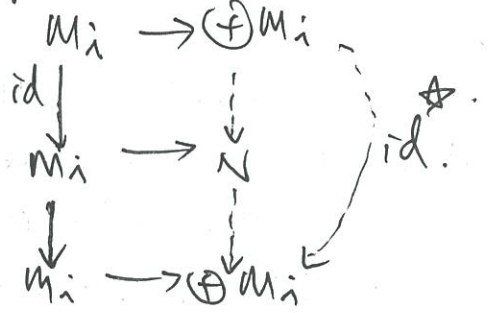
We will talk about $\bigoplus_{i \in I} M_i$ vs $\prod_{i \in I} M_i$.

MA3201 W8L1

Recall: $M_1, \dots, M_n$ R-mods. Define $\bigoplus_{i=1}^n M_i (= M_1 \times \dots \times M_n)$.

- Free modules over a finite set A, $F(A) \cong R^n$ if $\#F(A) = n$.

- $M_i \xrightarrow{\text{embedding}} \bigoplus M_i$ Pf: (uniqueness)



- $\varphi_i : N \to \bigoplus M_i$ $\quad \varphi : n \longmapsto (\varphi_1(n), \varphi_2(n), \dots, \varphi_n(n))$

- Recall $F(A) \cong R^n$.

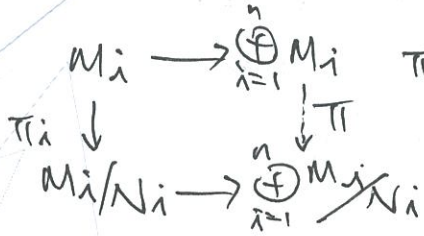
Free Modules

Thm. (11.1 ~~ex~~) F field, then ~~the~~ $F^n \cong F^m$ (as F-modules) $\iff n = m$.

Thm. Let $R \ni 1$ be comm. Then $R^n \cong R^m \iff n = m$.

Lem. Let $R \ni 1$, $M_1, \dots, M_n$ be R-modules with submodules $N_i \subseteq M_i \ \forall i$. Then $\bigoplus_{i=1}^n M_i / \bigoplus_{i=1}^n N_i \cong \bigoplus_{i=1}^n M_i / N_i$.

Pf. Recall $\bigoplus_{i=1}^n M_i = M_1 \times \dots \times M_n$. Then consider the following diag.



We can see Π is surjective with $\ker \Pi = \bigoplus_{i=1}^n N_i$. The Lemma follows from the Isomorphism thm. □

MA3201 W8C1 (2).

Cor: Let $I \subset R$ be a left ideal (thus right module). Then

$$R^n/I\cdot R^n \cong R/IR \oplus \dots \oplus R/IR \cong \bigoplus_{i=1}^{n} R/IR$$

Recall $I\cdot M = \{\sum_{\text{finite}} r\cdot m \mid r\in I, m\in M\} \subseteq M$.

Pf: From the lemma, it suffices to know that $I\cdot R^n \cong \bigoplus_{i=1}^{n} IR$.

"constant" vector. □.

Thm. Pf: $R^n \cong R^m \iff n=m$ (given $R\ni 1$ comm).

Let I be a maximal 2-sided ideal of R. Then if we have $R^n \cong R^m$, we must have $I\cdot R^n \cong I\cdot R^m$.

$\varphi: R^n \to R^m$ $\quad \varphi(I\cdot R^n) = I\cdot\varphi(R^n) = I\cdot R^m$.

By taking quotients, we have.

$M_1 \cong M_2 \Rightarrow M_1/N_1 \cong M_2/N_2$.
$N_1 \cong N_2$

$$\underbrace{R^n/I\cdot R^n}_{\bigoplus_{i=1}^{n} R/I} \cong \underbrace{R^m/I\cdot R^m}_{\bigoplus_{i=1}^{m} R/I}.$$

or

$\swarrow$ I is maximal.

Since I acts trivially (?) R/I = F-modules. So we have a F-mod isom

$$\bigoplus_{i=1}^{n} F \cong \bigoplus_{i=1}^{m} F \Rightarrow n=m \text{ by linear algebra.}$$

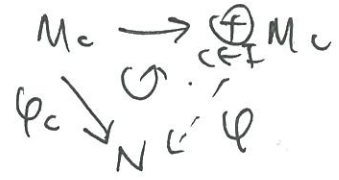
Note: If we have isom: $M_1 \xrightarrow{\cong} M_2$., N_2 sub mod of M_2.

Then $M_1 \xrightarrow{\varphi} M_2 \xrightarrow{\Pi} M_2/N_2$.

1st isom: $M_1/\ker(\varphi\cdot\Pi) \cong M_2/N_2$.

$\Rightarrow M_1/N_1 \cong M_2/N_2$.

Defn/Prop M_c, $c\in I$ R-mods, then direct sum $\bigoplus_{c\in I} M_c$ with R-mod hom $\varphi_c: M_c \to \bigoplus_{c\in I} M_c$. Then for any $\varphi_c: M_c \to N$, there exists a unique $\varphi: \bigoplus_{c\in I} M_c \to N$ such that:



Pf Claim: The direct sum exists and is unique up to isom.

Define $\bigoplus_{c\in I} M_c$ as follows. As sets,

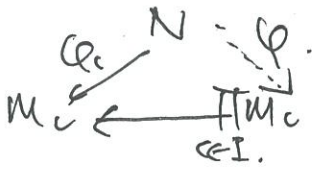
- $= \{(m_c) \in \prod_{c\in I} M_c \mid m_c = 0$ except for finitely many $c.\}$.
- Define $+$ on $\bigoplus_{c\in I} M_c$ as $(m_c)+(n_c) = (m_c+n_c)$.
- Define R-action componentwise. $r\cdot(m_c) = (r\cdot m_c)$.

Then for any R-mod hom $\varphi_c : M_c \to N$, we define.

$\varphi : \bigoplus_{c\in I} M_c \to N$, $(m_c) \longmapsto \sum_{c\in I} \varphi_c(m_c)$ (finite sum due to assump).

Then we can check that the map φ is unique, up to isom. ∎

Defn/Prop (Arbitrary direct product) Let M_c $c\in I$ be R-mods. The direct pdt is a R-mod $\prod_{c\in I} M_c$ together with a R-mod hom $f_c : \prod_{c\in I} M_c \to M_c$ s.t. $\forall$ $\varphi_c : N \to M_c$, the follow holds:



Pf: We define $\prod M_c$ as follows:

- As sets, $\prod_{c\in I} M_c = \prod_{c\in I} M_c$,
- Define $+$ on $\prod_{c\in I} M_c$ component-wise,
- Define R-action on $\prod_{c\in I} M_c$ component-wise,
- $\prod_{c\in I} M_c \to M_c$ be the projection to the c-th component

Then $\forall$ $\varphi_c : N \to M_c$, define

$\varphi : N \to \prod_{c\in I} M_c$, $n \longmapsto (\varphi_c(n))$.

Then we can check uniqueness. □

MA3201 W8L1 (3).

Rem: $\bigoplus_{i\in\mathbb{Z}_{\geq 0}} \mathbb{Z} \ncong \prod_{i\in\mathbb{Z}_{\geq 0}} \mathbb{Z}$ as $\mathbb{Z}$-modules.
(DAF 10.3 Ex 24).

Direct sum & product of modules III

Let $M_1,\dots,M_s, N_1,\dots,N_t$ be R-modules. we want to study
$\mathrm{Hom}_R(\bigoplus_{i=1}^{s} M_i, \bigoplus_{j=1}^{t} N_j)$, $\mathrm{End}_R(\bigoplus_{i=1}^{s} M_i)$, $\mathrm{End}_R(R^n (=\bigoplus_{i=1}^{n} R))$

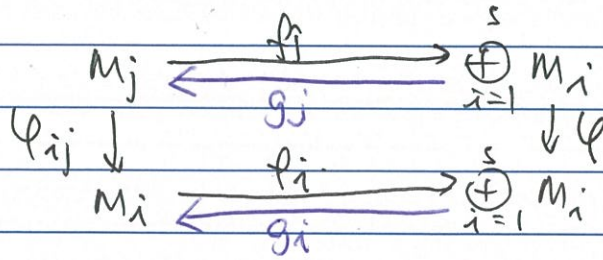
Eg. Let $R=F$ be a field. Then $\mathrm{End}_F(F^n) \cong \mathrm{Mat}_{n\times n}(F)$.

Defn ("temporary") Let $M_1,\dots,M_s$ be R-modules, we define the following "matrix" ring $\mathrm{End}_R(\bigoplus_{i=1}^{s} M_i)$.

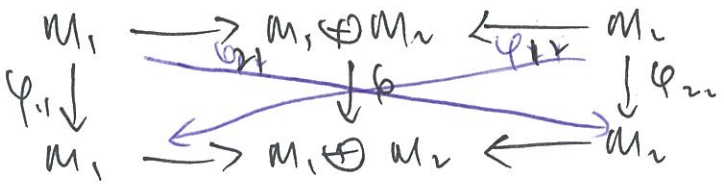
- As a set, $\mathrm{End}_R(\bigoplus_{i=1}^{s} M_i) = \{(a_{ij})_{s\times s} \mid a_{ij} \in \mathrm{Hom}(M_j, M_i)\}$
- Define $+$ in ~~Hom~~ component-wise:
  $(a_{ij}) + (b_{ij}) = (a_{ij}+b_{ij}) \quad \forall i,j.$
- Define $*$ in ~~Hom~~ component-wise:
  $(a_{ij}) * (b_{ij}) = (c_{ij})$ where $\forall i,j$
  $(c_{ij}) = \sum_{k=1}^{s} a_{ik} \circ b_{kj}$ where $a_{ik} \in \mathrm{Hom}(M_k, M_i)$,
  $b_{kj} \in \mathrm{Hom}(M_j, M_k)$

Thm: we have $\mathrm{End}_R(\bigoplus_{i=1}^{s} M_i) \cong \mathrm{End}_R(\bigoplus_{i=1}^{s} M_i)$.
In particular, we have $\mathrm{End}_R(R^n) \cong \mathrm{Mat}_{n\times n}(R)$.

Pf: we define the map as follows:



$\mathrm{End}_R(\bigoplus_{i=1}^{s} M_i) \to \mathrm{End}_R(\bigoplus_{i=1}^{s} M_i)$ by
$\varphi \longmapsto (\varphi_{ij})_{s\times s}$.



Let $M_1 \oplus M_2 \ni a = a_1 + a_2$ with $a_1 \in M_1$, $a_2 \in M_2$. Then

$$\varphi(a) = \begin{bmatrix} \varphi_{11} & \varphi_{12} \\ \varphi_{21} & \varphi_{22} \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \end{bmatrix} = \begin{bmatrix} \varphi_{11}(a_1) + \varphi_{12}(a_2) \\ \varphi_{21}(a_1) + \varphi_{22}(a_2) \end{bmatrix}.$$

The ring hom is the same as linear algebra. ($\mathrm{End}_F(F^n) \cong M_{n\times n}(F)$)

Cor. The following composition can be computed using matrices:

$$\mathrm{Hom}_R(R^s, R^t) \times \mathrm{Hom}_R(R^t, R^s) \longrightarrow \mathrm{Hom}_R(R^t, R^t)$$

$$\text{SS}$$

$$\mathrm{Mat}_{t\times s}(R) \times \mathrm{Mat}_{s\times t}(R) \longrightarrow \mathrm{Mat}_{t\times t}(R).$$

MA3201 W8L2

Recall: $\mathrm{End}_R(R^n) \cong \mathrm{Mat}_{n\times n}(R)$. (we consider the comm. case, usually).

(A: $\mathrm{End}_F(F^n) \cong \mathrm{Mat}_{n\times n}(F)$.

Noetherian Modules

Defn: Let R be a ring with $R \ni 1$. A R-mod M is Noetherian, if any ascending chain of submods of M stabilize. That is,

$A_1 \subseteq A_2 \subseteq A_3 \subseteq \dots$ $\forall A_i$ are submod of M.

Then $\exists k$, $A_k = A_{k+1} = \dots$ or equivalently,

$\bigcup A_i = A_k$ for some $k \in \mathbb{N}$. This is the 'nice' property.

Prop. Let M be a R-mod. Then M is Noetherian $\iff$ any submod of M is finitely generated. That is, $N = R\{n_1, \dots, n_k\} = \{ \sum_{i=1}^{k} r_i n_i \mid r_i \in R \}$.

Pf: ($\Rightarrow$) Assume M is Noetherian. Let $N \subset M$ be a submod.

Assume the contrary, N is not finitely gen, then we can find a seq. of elements in N, denoted $\{n_i\}_{i=1}^{\infty}$. Then any finite subset of that will not generate N, That is,

$n_i \notin R\{n_1, \dots, n_{i-1}\}$ $\forall i \in \mathbb{N}$ by assumption.

Then we have an ascending chain of modules:

$R\{n_1\} \subsetneq R\{n_1, n_2\} \subsetneq \dots$ ∎.

($\Leftarrow$) Suppose all submods of M, N, are fin. gen. Then for any asc. chain:

$N_1 \subset N_2 \subset \dots$, Let $N = \bigcup_{i=1}^{\infty} N_i$.

This is a submod of M hence finitely generated by assumption.

Then $N = R\{n_1, \dots, n_k\}$ for some $n_i \in N$. we find the submod in the chain that contains $\{n_1, \dots, n_k\}$ properly, say N_λ, then

$N_\lambda = N_{\lambda+1} = \dots = N$ ∎

Eg. There are finitely generated M with non-fingen submods N.

$R = F[x_1, x_2, \dots]$, Let $M = R = R \cdot \{1\}$. The polynomials w/out constant term, N is a submod of M and is not fin. gen. (Why?)

Prop. (Noetherian if submod and quotient are Noetherian) M is an R-mod, then M is Noetherian $\Leftrightarrow \forall N$ submod M, N and M/N are Noetherian.

Pf: ($\Rightarrow$) M is Noetherian, therefore any submod N is fingen.
We show further that M/N is Noetherian.
Let $L/N \subset M/N$ be a submod, then
$L \subset M \Rightarrow L = R\{l_1, \dots, l_n\}$, then
$L/N = R\{l_1+N, \dots, l_n+N\}$.

($\Leftarrow$) N, M/N are Noetherian, then any submod of N, M/N are finitely generated. WTS $L \subset M$ is fingen $\forall$ L submod M.

Consider $q(L) \subset M/N$, the image of L in M/N. $= \bar{L}$.
$\therefore \bar{L}$ is fingen, say $\bar{L} = R\{a_1+N, \dots, a_s+N\}$.
$L \cap N \subset N$ is also fingen, $L \cap N = R\{b_1, \dots, b_t\}$.
we claim L is generated as R-submod by
$\{a_1, \dots, a_s, b_1, \dots, b_t\}$. $\forall x \in L$, then
$x+N = r_1 a_1 + r_2 a_2 + \dots + r_s a_s + N$., $(r_i \in R)$.
$\therefore x - (r_1 a_1 + \dots + r_s a_s) \subset N \cap L$.
$\therefore x = r_1 a_1 + \dots + r_s a_s + r_1' b_1 + \dots + r_t' b_t$. (any $x \in L$ is gen. by the set) □.

Defn: Let R be with 1. we say R is left (or right) Noetherian if R is a Noetherian module as a left (or right) R-mod via left (or right) multiplication. (Noetherian is a mod-property)
we say R is Noetherian if it is both left and right Noetherian.

Recall: R is a PID $\Rightarrow R$ is Noetherian.

MA3201 W8L2 (2)

Lemma: Let R be left Noetherian. Then any finitely generated R-mod is Noetherian.

Pf: we first show that R^n is Noetherian. (by induction)
$R \times R = R \oplus R = R^2$, and $R \times \{0\} \subset R^2$, is a submod.
then $\{0\} \times R = R^2/R \times \{0\}$. is also Noetherian.
Continue with this, we have the results desired.

Let $M = R\{m_1, \dots, m_n\}$. be fingen R-mod.
we have a surjective map $R^n \to M$, And thus M is a quotient
R-mod. $e_i \longmapsto m_i$
of a Noetherian module R^n, hence Noetherian.

Cor: Any subgp of a finitely generated Ab. gp (Noetherian $\mathbb{Z}$-module) is finitely generated.

$\operatorname{coker}(\varphi: M \to N) = N/\operatorname{Im}(\varphi)$.

Lem/Defn: Let R be a PID, then any fingen. R-mod M is also finitely presented. That is, $M \cong \operatorname{coker}(\varphi: R^m \to R^n)$ ($\cong \mathrm{Mat}_{m \times n}(R)$)
OR $\forall f: R^n \twoheadrightarrow M$, the kernel is fingen.
so we can find $g: R^m \twoheadrightarrow \ker f \xrightarrow{\text{emb}} R^n \xrightarrow{\varphi}$

Pf: we know $M = R\{m_1, \dots, m_n\}$. Then we can find R-mod map.
$f: R^n \twoheadrightarrow M$, $e_i \mapsto m_i$. Then $M \cong R^n/\ker f$ (BT, 3.3.m).
Since R^n is Noetherian, the submod $\ker f$ is fingen, say
$\ker f = R\{s_1, \dots, s_m\}$. Then we can find R-mod map
$R^m \twoheadrightarrow \ker f$, $e_i \mapsto s_i$.

Then we define $\phi: R^m \to \ker f \subset R^n$ and $\operatorname{Im}\phi = \ker f$.
Then $\operatorname{coker}(\phi: R^m \to R^n) = R^n/\operatorname{Im}\phi = R^n/\ker f \cong M$. □.

Eg. Assume $M \cong \operatorname{coker}(\phi: R^3 \to R^3)$ for a PID R.
Assume $\phi: R^3 \to R^{\prime\prime}$ is the matrix $\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & a \end{bmatrix}$

Then $M \cong R^2 \oplus R/(a)$

Prop: Let R be a ring with 1. Let M be a Noetherian Module.
Then M has a simple quotient, that is $\exists$ submod $N \subset M$ such that M/N is a simple R-mod. (A module need not have a simple submod/quot.)

this happens when N is max. Existence of N is given by Zorn or Noetherian.

Pf: (Recall M/N is simple if $M/N \neq 0$, 0, M/N are submods.)
~~Then~~ If M is simple $\Rightarrow$ we are done.
Otherwise, we can find $N_1 \subsetneq M$, if M/N_1 is simple we are done.
Otherwise, $\exists 0 \neq N_2/N_1 \subset M/N_1$, then $N_1 \subsetneq N_2 \subsetneq M$.
then we continue with M/N_2, etc.
Since M is Noetherian, we have an ascending chain N_i that stabilizes.
$\therefore M/N_k$ must be simple for some k. $\square$

((Cor: Any finitely gen $\mathbb{Z}$-module/Ab sp has a simple quotient)(?))

Example: 1. Let $R = F[x]$ for a field F. But $R^2 R$ has no simple ~~submod~~ quotients.
(any module $M \subset R$, $x \cdot M$ is a submod of M).
2. Let $R = F[x]$, then $M = \operatorname{Hom}_F(F[x], F)$ has no simple ~~submod~~ quotients.
$(g(x) \cdot f)(h(x)) = f(g(x) \cdot h(x))$
$\in R \quad \in M \quad \in F[x]$. $\quad \in F[x] \to \in F$.

(Fact if F a field $\Rightarrow F[x]$ is PID)

Thm: (Hilbert basis theorem) Let R be a comm. Noetherian Ring. Then $R[x]$ is Noe.
Pf: Suppose otherwise, then there is an ideal (submod) I that is not finitely generated (as an $R[x]$-mod). Construct a sequence $\{f_i\}_{i=1}^{\infty}$ in I as follows:
$f_i \notin R[x]\{f_1, \dots, f_{i-1}\}$, $f_i \in I \setminus R[x]\{f_1, \dots, f_{i-1}\}$. Let of minimal deg.
(deg is not preserved in non-int doms)

MA3201 (aka WFLT(3)).

Pf (Hilbert basis thm, cf §2).

Let a_i be the leading coeff of f_i ($= a_i x^{\mu_i} + \dots$).

Consider the chain of ideals in R:

$(a_1) \subset (a_1, a_2) \subset \dots$

R is noetherian.

It stabilizes (why). Say $(a_1, \dots, a_m) = (a_1, \dots, a_m, a_{m+1}) = \dots$

$\therefore a_{m+1} = \sum_{i=1}^{m} r_i a_i$

save deg. ↓ ↓ so the deg is μ_{m+1}.

Then consider $g = \sum_{i=1}^{m} r_i f_i \cdot (x^{\mu_{m+1} - \mu_i})$ where $\deg f_i = \mu_i$.

Since $f_{m+1} \notin R[x]\{f_1, \dots, f_m\}$ so

$f_{m+1} - g \notin R[x]\{f_1, \dots, f_m\}$ with degree $< \deg f_{m+1}$.

$\therefore$ ~~con~~ $\to\leftarrow$ choice of f_{m+1}. □

Recall (conclusion. Ascending chain stabilizes (of submod)

$\Rightarrow$ Noetherian

$\Leftrightarrow$ Any subgp is finitely generated.

$\Leftrightarrow$ Any submod N, M/N are is Noetherian.

Eg :- V finite vector spaces of fields F are Noetherian. (by (A)).

- R PID, then any fngen R-mod M is Noe.

we have surj. map $R^n \xrightarrow{\varphi} M$.

Since R^n is Noe, $\ker \varphi \subset R^n$ is also fngen.

(☆) $\therefore R^n \subset$

MA3201 W9 L1

Eg. Let $f=\begin{bmatrix}1 & 1\\ 2 & 1\end{bmatrix}\in M_2(\mathbb{Z})$. Consider $M\cong \operatorname{coker}(f:\mathbb{Z}^2\to\mathbb{Z}^2)$.

Smith Normal Form (D&F Ex 15-20)

Motivational Lem: Let R be a ring, $\varphi: R^n\to R^m$ be a R-mod hom. Let $S:R^n\to R^n$ and $T:R^m\to R^m$ be isom. of R-mods. Then $\operatorname{coker}(\varphi:R^m\to R^n)\cong \operatorname{coker}(T\circ\varphi\circ S: R^m\to R^n)$

$$\begin{array}{ccc} R^m & & R^n \\ {\scriptstyle S}\updownarrow & \xrightarrow{\varphi} & \updownarrow{\scriptstyle T} \\ R^m & \xrightarrow{\varphi} & R^n \end{array}$$

$=\operatorname{coker}\varphi$. $\pi\circ\varphi: R^m\to M=\operatorname{coker}\varphi=R^n/\varphi(R^m)$. $\pi\circ\varphi(m)=\pi(\varphi(m))=0$. $(\pi\circ\varphi=0)$

$$R^m\xrightarrow{\varphi}R^n\left(\xrightarrow{\pi}M\right)\quad =R^n/\varphi(R^m)$$

$$R^m\xrightarrow{S}R^m\xrightarrow{\varphi}R^n\xleftarrow{T}R^n$$

Pf: consider

we want to show $M\cong\operatorname{coker}(T\circ\varphi\circ S)$

$=\operatorname{coker}(\varphi)$

we consider the map $f: R^n\xrightarrow{T^{-1}}R^n\xrightarrow{\pi}M$.

- f is surjective.
- $R^n/\ker f\cong M$
- $\ker f=T(\ker\pi)$ $\quad\{m\in R^n \mid \pi(T^{-1}(m))=0\}$.

we claim $\operatorname{Im}(T\circ\varphi\circ S)=\ker f$. Then

$$\operatorname{coker}(T\circ\varphi\circ S)\cong\frac{R^n}{\operatorname{Im}(T\circ\varphi\circ S)}\cong R^n/\ker f\cong M.$$

~~Proof claim:~~

① $\operatorname{Im}(T\circ\varphi\circ S)\subset\ker f \iff f(\operatorname{Im}(T\circ\varphi\circ S))=0$.

Then $f(T\circ\varphi\circ S(R^m))=\pi\circ T^{-1}\circ T\circ\varphi\circ S(R^m)$

$=\underbrace{\pi\circ\varphi\circ S}_{=0}(R^m)$

$=0$.

② $\ker f\subseteq\operatorname{Im}(T\circ\varphi\circ S)$ T 13.30

$\ker f=\ker(\pi\circ T)=T(\ker\pi)=T(\operatorname{Im}\varphi)$

$\operatorname{Im}(T\circ\varphi\circ S)=T(\operatorname{Im}(\varphi\circ S))=T(\operatorname{Im}\varphi)$.

(since S is surjective, $S(R^m)=R^m$).

MA3201 Wk11 (2).

Eg. ① Let $R=F$ be a field. Let $M=\operatorname{coker}(\varphi: M^2\to M^2)$ with $\varphi=\begin{bmatrix}1&1\\2&2\end{bmatrix}$.

Then $\varphi\begin{pmatrix}a\\b\end{pmatrix}=\begin{pmatrix}a+b\\2a+2b\end{pmatrix}$.

Then taking $T=\begin{bmatrix}1&0\\-2&1\end{bmatrix}$, $(T^{-1}=\begin{bmatrix}1&0\\2&1\end{bmatrix})$,

$$S=\begin{bmatrix}1&-1\\0&1\end{bmatrix}\ (S^{-1}=\begin{bmatrix}1&1\\0&1\end{bmatrix}),$$

$$\therefore T\varphi S=\begin{bmatrix}1&1\\0&0\end{bmatrix}\begin{bmatrix}1&-1\\0&1\end{bmatrix}=\begin{bmatrix}1&0\\0&0\end{bmatrix}.$$

so $\operatorname{coker}\varphi\cong\operatorname{coker}(T\circ\varphi\circ S)\cong R.\mathbb{Z}$.

since $T\circ\varphi\circ S: R^2\to R^2$, $\begin{pmatrix}a\\b\end{pmatrix}\to\begin{pmatrix}a\\0\end{pmatrix}$.

② Let $\varphi:\mathbb{Z}^2\to\mathbb{Z}^2$ be $(a,b)\mapsto(a+b,\ 2b)$. Then we claim $\operatorname{coker}\varphi\cong\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$. We have $\varphi=\begin{pmatrix}1&1\\0&2\end{pmatrix}\in M_2(\mathbb{Z})\cong\operatorname{End}_{\mathbb{Z}}(\mathbb{Z}^2)$

Let $S=\begin{bmatrix}1&-1\\0&1\end{bmatrix}$. Then $\varphi S=\begin{bmatrix}1&0\\0&2\end{bmatrix}$

so $\operatorname{coker}\varphi\cong\operatorname{coker}\varphi S$. Then $\varphi\cdot S:\mathbb{Z}^2\to\mathbb{Z}^2$, $\begin{pmatrix}a\\b\end{pmatrix}\mapsto\begin{pmatrix}a\\2b\end{pmatrix}$

$\therefore \operatorname{Im}\varphi S=\mathbb{Z}\oplus 2\mathbb{Z}$. Then $\dfrac{\mathbb{Z}\oplus\mathbb{Z}}{\mathbb{Z}\oplus 2\mathbb{Z}}\cong\mathbb{Z}/\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}\cong\mathbb{Z}/2\mathbb{Z}$.

④ ☆ Let $\varphi:\mathbb{Z}^2\to\mathbb{Z}^2$, $(a,b)\mapsto(2a+3b,\ 5a+7b)$. Then

$\varphi=\begin{bmatrix}2&3\\5&7\end{bmatrix}:\mathbb{Z}^2\to\mathbb{Z}^2$.

$=S_1$, not invertible in $M_n(\mathbb{Z})$.

We try $\begin{bmatrix}2&3\\5&7\end{bmatrix}\begin{bmatrix}2&0\\-1&1\end{bmatrix}=\begin{bmatrix}1&3\\3&7\end{bmatrix}$,

then $\begin{bmatrix}1&0\\-3&1\end{bmatrix}\begin{bmatrix}1&3\\3&7\end{bmatrix}=\begin{bmatrix}1&3\\0&7\end{bmatrix}$.

and $\begin{bmatrix}1&3\\0&7\end{bmatrix}\begin{bmatrix}1&-3\\0&1\end{bmatrix}=\begin{bmatrix}1&0\\0&-2\end{bmatrix}$

Pf: $S_1=\begin{bmatrix}2&-3\\-1&2\end{bmatrix}$ with inverse $\begin{bmatrix}2&3\\1&2\end{bmatrix}$

Easy check $\begin{bmatrix}2&3\\5&7\end{bmatrix}\begin{bmatrix}2&-3\\-1&2\end{bmatrix}=\begin{bmatrix}1&0\\3&-1\end{bmatrix}$.

$\begin{bmatrix}1&0\\-3&1\end{bmatrix}\begin{bmatrix}1&0\\3&-1\end{bmatrix}=\begin{bmatrix}1&0\\0&-1\end{bmatrix}$.

$\therefore$ we have $S=\begin{bmatrix}2&-3\\-1&2\end{bmatrix}$, $T=\begin{bmatrix}1&0\\-3&1\end{bmatrix}$ s.t. $T\varphi S=\begin{bmatrix}1&0\\0&-1\end{bmatrix}$.

Then $\operatorname{coker}(\varphi)\cong\operatorname{coker}(T\varphi S)=0$. (i.e. φ is surjective).

Recall: in PID, $\forall a,b \in R$, $(a,b)=(\alpha)$ for some α and $\alpha = \gcd(a,b)$.
$\exists c,d \in R$, $ac+bd=\alpha$.

Lem: R PID. $a,b \in R$ coprime ($\gcd(a,b)=1 \Leftrightarrow (a,b)=(1)$.) $\exists c,d$, $ac+bd=1$. Then

$\begin{bmatrix} a & b \\ -d & c \end{bmatrix}, \begin{bmatrix} c & -b \\ d & a \end{bmatrix}, \begin{bmatrix} a & -d \\ b & c \end{bmatrix}, \begin{bmatrix} c & d \\ -b & a \end{bmatrix}$ are all invertible in $Mat_2(R)$. (note that if not ED, c,d cannot be found easily using Euclidean algorithm)
(conveniently they are inverses of eo.)

Cor: with the above assumptions, we can embed it into bigger matrices: $\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & a & b & 0 & 0 \\ 0 & -d & c & 0 & 0 \\ 0 & 0 & 0 & 1 & \\ 0 & 0 & 0 & & 1 \end{pmatrix}$ is invertible.

Lem. Let $a,b \in R$, $\alpha = \gcd(a,b)$. Then $\exists$ invertible matrices $S,T \in M_2(R)$, such that.

$\begin{bmatrix} a & b \\ ? & ? \end{bmatrix} \cdot S = \begin{bmatrix} \alpha & 0 \\ ? & ? \end{bmatrix}$ and $T \cdot \begin{bmatrix} a & ? \\ b & ? \end{bmatrix} = \begin{bmatrix} \alpha & ? \\ 0 & ? \end{bmatrix}$

Similarly we have $\begin{bmatrix} a & b & c \\ ? & ? & ? \end{bmatrix} \cdot S = \begin{bmatrix} \alpha & 0 & c \\ ? & ? & ? \end{bmatrix}$.

Pf: Let $a=\alpha a'$, $b=\alpha b'$ and $ac+bd=\alpha$ for some $c,d \in R$.
Then $a'c+b'd=1$, $T=\begin{bmatrix} c & d \\ -b' & a' \end{bmatrix}$.

$\therefore T \cdot \begin{bmatrix} a & ? \\ b & ? \end{bmatrix} = \begin{bmatrix} ac+bd & ? \\ -b'a+a'b & ? \end{bmatrix} = \begin{bmatrix} \alpha & ? \\ 0 & ? \end{bmatrix}$
$-a'b'\alpha + a'b'\alpha$

(S can be shown similarly.) □

Lemma: Let $a,b \in R$, Then $\exists$ invertible $S,T \in Mat_{n\times n}(R)$, s.t.

$T \cdot \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \cdot S = \begin{bmatrix} \alpha & 0 \\ 0 & \beta \end{bmatrix}$ with $\alpha \mid \beta$.

Actually $\alpha = \gcd(a,b)$, $\alpha\beta = ab = \det \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$.

MA3201 W9L1

Pf (Lemma): Let $a=da'$, $b=db'$, $d=\gcd(a,b)$. Then $ac+bd=d$ and $a'c+b'd=1$. Then $T=\begin{bmatrix} c & d \\ -b' & a' \end{bmatrix}$ is invertible.

Consider the following process:

$$\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \to \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} a & 0 \\ b & b \end{bmatrix} \to \begin{bmatrix} c & d \\ -b' & a' \end{bmatrix}\begin{bmatrix} a & 0 \\ b & b \end{bmatrix} \quad //0.$$

$$= \begin{bmatrix} d & db \\ 0 & a'b \end{bmatrix} \to \begin{bmatrix} d & db \\ 0 & a'b \end{bmatrix}\cdot\begin{bmatrix} 1 & -db' \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} d & -db'd+db \\ 0 & a'b \end{bmatrix}$$

$$= \begin{bmatrix} d & 0 \\ 0 & a'b \end{bmatrix}. \text{ Then } a|b \Rightarrow d|a'b.$$

$$\therefore T=\begin{bmatrix} c & d \\ -b' & a' \end{bmatrix},\ S=\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}\cdot\begin{bmatrix} 1 & -db' \\ 0 & 1 \end{bmatrix} \text{ and}$$

$$T\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}\cdot S = \begin{bmatrix} d & 0 \\ 0 & a'b \end{bmatrix}$$

Summary of invertible oprns:

$\varphi: \mathbb{R}^3 \to \mathbb{R}^2$

- $\begin{bmatrix} a & b & c \\ \star & \star & \star \end{bmatrix} \to \begin{bmatrix} \gcd(a,b) & 0 & c \\ \star & \star & \star \end{bmatrix}$
- $\begin{bmatrix} a & b & c \\ \star & \star & \star \end{bmatrix} \to \begin{bmatrix} a & (b+ka) & c \\ ? & ? & ? \end{bmatrix}$
- $\begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix} \xrightarrow{\text{swap row}} \begin{bmatrix} d & e & f \\ a & b & c \end{bmatrix}$

  swap col: $\begin{bmatrix} b & a & c \\ e & d & f \end{bmatrix} = [\ ]\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$.
- $\begin{bmatrix} a & 0 & 0 \\ 0 & b & 0 \end{bmatrix} \to \begin{bmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \end{bmatrix}$ with $\alpha|\beta$.

MA3201 WQLY

Lem: Let $T: M \to M$ iso. $\pi: M \to N$. Then, $\ker(\pi \circ T^{-1}) = T\ker(\pi)$

Pf: $\ker(\pi \circ T^{-1}) = (\pi \circ T^{-1})^{-1}(0) = T \circ \pi^{-1}(0) = T\ker(\pi)$.

Structure Theory of Finitely generated Modules for PID (Noetherian Rings)

Setup: M fingen R-mod, R is a PID. Then $R^n \xrightarrow{f} M$.

Then $\ker f \subset R^n$ is also finitely generated (Noetherian)

Then $R^m \twoheadrightarrow \ker f \hookrightarrow R^n \xrightarrow{f} M$

($R^m \twoheadrightarrow \ker f \hookrightarrow R^n$: φ)

Then $\operatorname{Im}\varphi = \ker f$. So $\operatorname{coker}\varphi = R^n/\operatorname{Im}\varphi = R^n/\ker f \cong M$.

Key Lemma: (R need not be PID) $\varphi: R^m \to R^n$ a R-mod map.

$S: R^m \to R^m$, $T: R^n \to R^n$ are isom of R-mod.

$\therefore$ Then $\operatorname{coker}(\varphi: R^m \to R^n) = \operatorname{coker}(T \circ \varphi \circ S: R^m \to R^n)$.

Summary of matrix operations:

combine row/col to gcd and 0:

$$\begin{bmatrix} a & b & c \\ ? & ? & ? \end{bmatrix} \to \begin{bmatrix} \gcd(a,b) & 0 & c \\ ? & ? & ? \end{bmatrix},$$

$$\begin{bmatrix} a & ? & ? \\ d & ? & ? \end{bmatrix} \to \begin{bmatrix} \gcd(a,d) & ? & ? \\ 0 & ? & ? \end{bmatrix}$$

add multiples: $\begin{bmatrix} a & b & c \\ ? & ? & ? \end{bmatrix} \to \begin{bmatrix} a & b+ka & c \\ ? & ? & ? \end{bmatrix}, \begin{bmatrix} a & ? & ? \\ d & ? & ? \end{bmatrix} \to \begin{bmatrix} a & ? & ? \\ d-ka & ? & ? \end{bmatrix}$.

swap row/col: $\begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix} \to \begin{bmatrix} d & e & f \\ a & b & c \end{bmatrix} \begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix} \to \begin{bmatrix} b & a & c \\ e & d & f \end{bmatrix}$

diagonal mat multiply: $\begin{bmatrix} a & 0 & 0 \\ 0 & b & 0 \end{bmatrix} \to \begin{bmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \end{bmatrix}$ $\alpha \mid \beta$. ($\alpha = \gcd(a,b)$, $\alpha\beta = ab$.

MA3201 WQL2(2).

Thm (Smith normal form) Let R be a PID. Let $\varphi: R^m \to R^n$ be a R-mod hom. We consider φ: $\in Mat_{n\times m}(R) \cong Hom_R(R^m, R^n)$.
Then there exists invertible

$S \in Mat_{m\times m}(R)$, $T \in Mat_{n\times n}(R)$ s.t.

$S \cdot \varphi \cdot T = diag(\alpha_1, \alpha_2, \dots, \alpha_k, 0, 0, \dots, 0)$.

with $\alpha_1 | \alpha_2 | \dots$, $\alpha_i \neq 0 \ \forall i$.

The entries $\{\alpha_i\}$ are called the invariant factors of φ.
The RHS (diag mat) is called the SNF of φ.

Pf: Explain construction by example: a 2x3 matrix.

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{bmatrix} \xrightarrow{\text{invertible operations}} \begin{bmatrix} a_{11}' = \gcd(a_{11}, a_{12}) & 0 & a_{13} \\ ? & ? & ? \end{bmatrix}$$

$$\to \begin{bmatrix} a_{11}' & a_{13} & 0 \\ ? & ? & ? \end{bmatrix}$$

$$\to \begin{bmatrix} a_{11}'' = \gcd(a_{11}', a_{13}) & 0 & 0 \\ a_{21}' \text{ (say)} & ? & ? \end{bmatrix}$$

- if $a_{11}'' | a_{21}$, eliminate 2nd row $\to \begin{bmatrix} 1 & 0 \\ -a_{21}/a_{11}'' & 1 \end{bmatrix} \begin{bmatrix} \ast & \ast & \ast \\ \ast & \ast & \ast \end{bmatrix} = \begin{bmatrix} a_{11}'' & 0 & 0 \\ 0 & ? & ? \end{bmatrix}$
- if $a_{11}'' \nmid a_{21}$, $\to \begin{bmatrix} a_{11}''' (= \gcd(a_{11}'', a_{21})) & ? & ? \\ 0 & ? & ? \end{bmatrix}$

Seems like we are having trouble, but good thing is gcd is getting "smaller".
But if $a_{11}'' \nmid a_{21}$, then # of irred. factors in a_{11}'''
$<$ # of irred. factors in a_{11}'' (PID $\Rightarrow$ UFD, then taking GCD is equal to taking common power. will $\downarrow$.
$\therefore$ After finitely many steps, we will have case 1: $\begin{bmatrix} b_{11} & 0 & 0 \\ 0 & ? & ? \end{bmatrix}$.

Thm (Fundamental Theorem for finitely generated modules over PID, existence, invariant factors).

Let M be a fg R-mod for a PID R. Then, as R-mods,

$M \cong R^k \oplus R/(\alpha_1) \oplus R/(\alpha_2) \oplus \dots \oplus R/(\alpha_r)$ with $\alpha_i \neq 0$, $\alpha_1 \mid \alpha_2 \mid \dots$, $\alpha_i \notin R^*$ (otherwise $R/(\alpha_i) = 0$) (otherwise $M \cong R^{k+r}$)

The $\{\alpha_i \mid k \mid 1 \le i \le r\}$ are called the <u>invariant factors</u> of M.

k is called the <u>free rank</u> of M.

(the decomposition is not proved to be unique, so we say the names are not well defined yet).

Pf: Let $M \cong \operatorname{coker}(\varphi: R^m \to R^n) \cong \operatorname{coker}(S \cdot \varphi \cdot T : R^m \to R^n)$ for some invertible S & T, such that $S\varphi T = \operatorname{diag}(\alpha_1, \dots, \alpha_r, u_1, \dots, u_s, 0, \dots)$ where u_i are units.

$(u_1 \mid u_2 \mid \dots) \mid \alpha_1 \mid \alpha_2 \mid \dots$ ($\alpha_i \neq 0$, $\alpha_i \notin R^*$).

Then we have $\operatorname{Im}(S\varphi T) = (\alpha_1) \oplus (\alpha_2) \oplus \dots \oplus (\alpha_r) \oplus R \oplus \dots \oplus R \oplus 0 \dots$

Then we have

$$\operatorname{coker}(S \circ \varphi \circ T) \cong M \cong R^k \oplus R/(\alpha_1) \oplus \dots \oplus R/(\alpha_r)$$ □

Eg. ① Let $M \cong \operatorname{coker}(\varphi: R^m \to R)$. Then we have

$\operatorname{Im}\varphi = (\varphi(e_1), \varphi(e_2), \dots, \varphi(e_m)) = (\alpha_1)$ since R is a PID. (ideal generated by all of them; is an ideal!)

Then $M \cong R/(\alpha_1)$ where α_1 could be a unit or 0.

② Any fg. F-module for a field F is isom to F^k for some k. (why?) (no ideals except trivial, OR every elem is a unit). In other words every F-vector space has a basis.

③ Any fg Abelian gp. is isom. to $\mathbb{Z}^k \oplus \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \dots \oplus \mathbb{Z}_{n_r}$.

where $n_1 \mid n_2 \mid \dots \mid n_r$, $n_i \notin R \mathbb{Z}^* = \{\pm 1\}$, $n_i \neq 0$.

MA3201 W9 LX(3).

Eg. (4) Let F be a field. Then any finite $G \subset F^*$ subgps G is cyclic.

Pf: Recall $F[x]$ is an Euclidean Domain. Then any $f(x)$ of $\deg(n)$ must have n roots. Then let (since G is Abel. gp).

$G \cong \mathbb{Z}^r \oplus \mathbb{Z}_{n_1} \oplus \dots \oplus \mathbb{Z}_{n_r}$ ✗ since G is finite.

Then we can consider the polynomial $x^{n_r} - 1$ in $F[x]$.

Since $n_1 | n_2 | \dots | n_r$, then $x^{n_r} - 1$ must have at most n_r roots in $G \subset F^*$. $\therefore G \cong \mathbb{Z}/n_r\mathbb{Z}$ or $\cong \mathbb{Z}/n\mathbb{Z}$ for some n. why?

(5) Any finite dimensional $F[x]$-mod. (finite dim. v.s. V and $T : V \to V$, $T \in \mathrm{End}_F(V)$) is isomorphic to $F[x]/(f_1(x)) \oplus \dots \oplus F[x]/(f_r(x))$ with $f_1(x) | f_2(x) | \dots | f_r(x)$, $f_i(x) \neq 0$, $f_i(x) \notin F$.

Recall: CRT for PID:

$R/(a_i) = R/(p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}) = R/(p_1^{a_1}) \oplus \dots \oplus R/(p_r^{a_r})$.

Thm (existence, elementary factors) Let M be a fg R-mod for a PID R.

Then $M \cong R^r \oplus R/(p_1^{a_1}) \oplus \dots \oplus R/(p_s^{a_s})$ for NOT necessarily distinct primes p_i and $a_i > 0$.

Then $\{p_i^{a_i}\}$ (multiset) are called the elementary factors of M.

Pf: The difference now is possible repetition. We can "distribute" factors to $\alpha_1, \alpha_2, \dots$ s.t. $\alpha_1 \alpha_2 \dots$ each one is $\sim$ to $p_1^{a_i}$ that might repeat. $\cong R/(p_1^{b_1}) \oplus \dots$

$M \cong R^r \oplus R/(\alpha_1) \oplus R/(\alpha_2) \oplus \dots$

$\cong R^r \oplus R/(p_1^{a_1}) \oplus \dots$ (IOW, we can combine/split into factors.) ∎

Defn: Let M be a R-mod for any ring R. Define impt

$\mathrm{Tor}(M) = \{m \in M \mid r \cdot m = 0 \text{ for some } 0 \neq r \in R\}$.

M is called torsion free if $\mathrm{Tor}(M) = 0$.

Hwk: If R is a PID, then $\mathrm{Tor}(M) \subset M$ is a submod.

Lemma: (General R) Let $\phi: M \to N$ be a R-mod hom. Then $\phi(\mathrm{Tor}(M)) \subset \mathrm{Tor}(N)$. ($\phi$ is inj then $\mathrm{Tor}(M) = \mathrm{Tor}(N)$.)

Pf: Let $m \in \mathrm{Tor}(M)$ s.t. $rm = 0$ with $r \neq 0$.
Then $\phi(r \cdot m) = r \cdot \phi(m) = 0 \Rightarrow \phi(m) \in \mathrm{Tor}(N)$. □

Prop. Let R be a PID. Let M be a f.g. module over R. Then M is torsion free $\Leftrightarrow M$ is free ($\Leftrightarrow M \cong R^k$ f.g. or infinite).
(characterizes free with torsion free when R is PID and M f.g.)

Pf: Let $M \cong R^k \oplus R/(\alpha_1) \oplus \dots \oplus R/(\alpha_r)$ $\alpha_1 | \alpha_2 | \dots$, $\alpha_i \neq 0$, $\alpha_i \notin R^*$.
Since inj, $\mathrm{Tor}(M) = R/(\alpha_1) \oplus \dots \oplus R/(\alpha_r)$. ($\forall r$, $r \cdot R^k \neq 0$.)
So. $\mathrm{Tor}(M) = 0 \Leftrightarrow M \cong R^k$.

Eg. ① Let $R = \mathbb{Z}[x]$ (NOT a PID). Then $(2, x) = M \subset R$ is torsion free but not free. (cannot be sent to 0)
Pf: (not free) suppose otherwise, $(2, x) \cong R = \mathbb{Z}[x] = (\alpha)$ for some α.
$\Rightarrow (2, \alpha)$ is a principal ideal. ($\leftrightarrow \in$, shown before).

② $\mathbb{Q}$ (as abelian sp) is torsion free but not free. (as a $\mathbb{Z}$-mod).
Pf: (Torsion free): $\forall n \in \mathbb{Z}$, $\frac{p}{q} \in \mathbb{Q}$, $n \cdot \frac{p}{q} \neq 0$ if $n \neq 0$.
(not free): Suppose A s.t. $F(A) \cong \mathbb{Q}$.
Case 1: $A = \{x\}$ single elem.
Then $x \longmapsto p/q$ with $\gcd(p, q) = 1$.
$\varphi: F(A) \xrightarrow{\cong} \mathbb{Q}$
Then $\varphi(F(A)) = \mathbb{Z}\{\frac{p}{q}\} \neq \mathbb{Q}$ (ie, $\frac{p}{q} = \frac{1}{2}$ then $\frac{1}{3} \notin \varphi(F(A))$).
Case 2: $|A| \geq 2$. ($\mathbb{Z} \subset \bigoplus_{x \in A} \mathbb{Z}$)
Let $\mathbb{Z}^2 \hookrightarrow F(A)$, $(1,0) \mapsto x$, $(0,1) \mapsto y$.
Then the composition $\mathbb{Z}^2 \hookrightarrow F(A) \xrightarrow{\cong} \mathbb{Q}$.
($\mathbb{Z}^2$ projects of $|A|$ just map the first 2 coordinates)
$(1,0) \mapsto x \longmapsto p_1/q_1$
$(0,1) \mapsto y \longmapsto p_2/q_2$.
is an injective map with kernel $= 0$.
However, $(q_1 p_2, -p_1 q_2) \mapsto q_1 p_2 \frac{p_1}{q_1} - p_1 q_2 \frac{p_2}{q_2} = p_2 p_1 - p_1 p_2 = 0$.
kernel $\neq 0$. ($\leftrightarrow \in$) □

MA3201 W10 L1

Recall: Let M be a f.g. R-mod for a pid R. Then

$M \cong R^k \oplus R/(a_1) \oplus R/(a_2) \oplus \dots \oplus R/(a_r)$, $a_1 | a_2 | \dots$, $a_i \neq 0, a_i \notin R^\times$

$\cong R^k \oplus R/(p_1^{q_1}) \oplus \dots \oplus R/(p_s^{q_s})$ (by CRT).

where p_i are NOT necessarily distinct primes of R, with $a_i > 0$.

Recall by eg: Let M be an Ab. gp, generated by x, y subject to the relations $2x+5y=0$, $3x+7y=0$. Show that $M \cong 0$.

Pf: we consider the map $\mathbb{Z}^2 \xrightarrow{\Pi} M$, $(1,0) \to x$, $(0,1) \to y$

more precisely, $(a,b) \mapsto ax+by$.

we know $\ker \Pi = ((2,5),(3,7))$. (ideal gen.)

Then we consider a map

$\varphi: \mathbb{Z}^2 \to \mathbb{Z}^2 (\xrightarrow{\Pi} M)$,

$(1,0) \mapsto (2,5)$, $(0,1) \mapsto (3,7)$.

Then $\operatorname{Im}\varphi = \ker \Pi$, $\operatorname{coker}\varphi = \mathbb{Z}^2/\operatorname{Im}\varphi = \mathbb{Z}^2/\ker\Pi \cong M$.

we have $\varphi = \begin{bmatrix} 2 & 3 \\ 5 & 7 \end{bmatrix}$. we then consider $T = \begin{bmatrix} 1 & 0 \\ -3 & 1 \end{bmatrix}$, $S = \begin{bmatrix} 2 & -3 \\ -1 & 2 \end{bmatrix}$

Then $T\varphi S = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ $\left(S^{-1} = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}\right)$

$M \cong \operatorname{coker}\varphi \cong \operatorname{coker}(T\varphi S)$ (as long as T, S are isom$\in T, S$ invertible

$= 0$ (is trivial).

Structure theory II

Let R be a PID. Let M be a f.g. R-mod. we know

$M \cong R^k \oplus R/(p_1^{q_1}) \oplus \dots \oplus R/(p_s^{a^s})$ → these forms come from splitting into χs.

$\cong R^{k'} \oplus R/(q_1^{b_1}) \oplus \dots \oplus R/(q_t^{b_t})$

Here p_i, q_i are not necessarily distinct primes and $a_i, b_1 > 0$.

Thm: we have $k = k'$ and $p_i^{a_i} = u_i q_i^{b_i}$ for some units u_i, upto perm.

Lemma: $\operatorname{Tor}(M) \cong R/(p_1^{q_1}) \oplus \dots \oplus R/(p_s^{q_s})$

$\cong R/(q_1^{b_1}) \oplus \dots \oplus R/(q_r^{b_r})$.

Lemma: we have $k=k'$, and this is the free rank of M.

Pf: $M/\mathrm{Tor}(M) \cong R^k \cong R^{k'}$.

Thus $k=k'$, since R is commutative. (why?).

Recall $(R/I)^k \cong (R/I)^{k'}$ for maximal ideal I. #

$F^k \cong F^{k'}$ (why then $k=k'$?) max ideals are prime

(why?) comm. rngs, fields are int doms

(if PID actually int. dom, but R fin gen $\Rightarrow R$ field.

Assume R is PID,

Lemma. Let $p \in R$ be prime. Then $F = R/(p)$ is a field. Then M/pM is a fin-dim. F-vector space. Similarly, pM/p^2M is also a f.d. vs of F.

Recall $pM = \mathrm{Im}(p: M \to M,\ m \mapsto pm)$ is a R-submod of M.

Pf: we define the $R/(p)$-action on M/pM as

$(a+(p)) \cdot (m+pM) = am + pM$.

Then we can check directly that this is a well-defined $R/(p)$-action

Or we can let $R \curvearrowright M/pM$ where (p) acts trivially, ie the action factors through the quotient.

Then to show M/pM is f.d $\Leftrightarrow$ show M/pM is finitely gen.

we show the F-linear combination of $\bar{m}_1, \dots, \bar{m}_n$ span the space, where $m_1, \dots, m_n \in M$ are the generators of M as a R-mod. $\therefore M = \sum r_i m_i$, $r_i \in R$ existence: M is fingen

$\Rightarrow \bar{m} = \sum r_i \bar{m}_i$. $\forall \bar{m} \in M/pM$.

$= \sum \bar{r}_i \cdot \bar{m}_i$ where $\bar{r}_i = r_i + (p)$. #

Lemma. Let p, q be diff. primes in R. Let $F = R/(p)$ be a field.

(1) Let $M = R/(q^a)$ for $a \geq 1$. Then as F-modules, we have

$p^k M / p^{k+1} M \cong 0$, $k \geq 0$.

(2) Let $M = R/(p^a)$ for $a \geq 1$. Then as F-modules, we have

$$p^k M / p^{k+1} M \cong \begin{cases} F & \text{if } k < a \\ 0 & \text{if } k \geq a. \end{cases}$$

(3) Let $M = R/(p^a) \oplus R/(p^b)$ for $a \geq 1$, $b \geq 1$, then as F-mods, we have $p^k M / p^{k+1} M \cong \begin{cases} F & \text{if } k < a \\ 0 & \text{if } k \geq a. \end{cases}$

MA3201 W10 L1 (2).

Pf (1) we have $p^t.M = p^t.(R/(q^a)) = (p^t)+(q^a)/(q^a)$.

$(p^t)+(q^a) \subset R+(q^a)$ $\quad (\sim (p^t)/(q^a))$

$= (p^t, q^a)/(q^a) = (\gcd(p^t, q^a))/(q^a) = R/(q^a)$. for any $t \geq 0$.

Then $p^t M / p^{t+1} M = 0$.

(2) we compute $p^t M = p^t.(R/(p^a)) = \frac{(p^t)+(p^a)}{(p^a)}$

$= \frac{(\gcd(p^t, p^a))}{(p^a)} = \frac{(p^{\min(t,a)})}{(p^a)}$

If $t \geq a$, then $\min(t,a) = a \Rightarrow p^t M = \frac{(p^a)}{(p^a)} = 0 \Rightarrow p^t M / p^{t+1} M = 0$.

else $\min(t,a) = t$

$\Rightarrow p^t M / p^{t+1} M = \frac{(p^t)/(p^a)}{(p^{t+1})/(p^a)} \cong (p^t)/(p^{t+1}) \cong F \cong R/(p)$.

isom.

define $R \to (p^t)/(p^{t+1})$, $1 \mapsto p^t + (p^{t+1})$.

(3) = (1)+(2).

$$\frac{p^t M}{p^{t+1} M} = \frac{p^t(R/(p^a)) \oplus p^t(R/(q^b))}{p^{t+1}(R/(p^a)) \oplus p^{t+1}(R/(q^b))} \overset{\text{(why?)}}{\underset{\text{(why?)}}{\cong}} p^t.(R/(p^a)) \oplus \frac{p^t(R/(q^b))}{p^{t+1}(R/(q^b))}$$

Thm: $M \cong \mathrm{Tor}(M) \cong R/(p_1^{a_1}) \oplus \cdots \oplus R/(p_s^{a_s})$ then

$\cong R/(q_1^{b_1}) \oplus \cdots \oplus R/(q_r^{b_r})$.

we have $p_i^{a_i} = u_i q_i^{b_i}$ for some units u_i and $s = r$ upto perm.

The elementary factors of M are unique upto perm & unit mult.

Pf: (By eg, for simplicity). Let where $p_1 \neq p_2$, q_i not necessarily distinct.

$M \cong R/(p_1) \oplus R/(p_1^2) \oplus R/(p_2^2) \cong R/(q_1^{b_1}) \oplus \cdots \oplus R/(q_r^{b_r})$

- Let $F_1 = R/(p_1)$ be a field, let $\pi_p(M) = M/pM$. we have the F-vs.

isom: $M/p_1 M \cong \pi(R/(p_1) \oplus R/(p_1^2) \oplus R/(p_2^2))$

$(p_1 \cdot 1 = 0)$ $\quad \cong \pi_{p_1}(R/(p_1)) \oplus \pi_{p_1}(R/(p_1^2)) \oplus \pi_{p_1}(R/(p_2^2))$ $\quad (p_1^t)$ $\quad (p_1^t)$ $\quad //0$.

$\cong F \oplus F \oplus 0$.

RHS $= \Pi_{p_1}(R/(q_1^{b_1})) \oplus \dots \oplus \Pi_{p_1}(R/(q_r^{b_r}))$ ($\cong F \oplus F$)

$\therefore$ RHS has exactly two elem. factors of the form $p_1^?$.

Let us assume $q_1^{b_1} = p_1^{b_1}$, $q_2^{b_2} = p_1^{b_2}$.

Similarly by considering Π_{p_2}, we have.

$q_3^{b_3} = p_2^{b_3}$.

By considering Π_q, or $F_q = R/(q)$ for any other prime $q \in R$, the LHS $= 0$, there are thus no other elem. factors.

Check pt 1: $M \cong R/(p_1) \oplus R/(p_1^2) \oplus R/(p_2^2) \cong R/(p_1^{b_1}) \oplus R/(p_1^{b_2}) \oplus R/(p_2^{b_3})$

Let $F = R/(p_1)$, write $\Pi_{p_1}(M) = p_1M/p_1^2M$. Then

$p_1M/p_1^2M \cong \Pi_{p_1^2}(R/(p_1) \oplus R/(p_1^2) \oplus R/(p_2^2))$

$\cong 0 \oplus F \oplus 0$.

RHS $\cong \Pi_{p_1^2}(R/(p_1^{b_1})) \oplus \Pi_{p_1^2}(R/(p_1^{b_2})) \oplus \Pi_{p_1^2}(R/(p_2^{b_3}))$

we must then have $b_1 = 1$, $b_2 > 1$.

we can continue with p_1^2M/p_1^3M etc. and deduce b_2, b_3 accordingly. □

Cor. Let M be a f.g. R-mod for a PID R. Then the invariant factors of M is unique upto mult. by units.

$M \cong R/(\alpha_1) \oplus R/(\alpha_2) \oplus \dots \oplus R/(\alpha_r)$ with $\alpha_1 | \alpha_2 | \dots$, $\alpha_i \neq 0, \alpha_i \notin R^*$

combine hyperbolic pairs

repeat

Pf: By eg. This is the Reverse Chinese Remainder Theorem.

If $M \cong R/(p_1) \oplus R/(p_1) \oplus R/(p_1^2) \oplus R/(p_2) \oplus R/(p_2^2)$.

Then $\cong R/(p_1) \oplus R/(p_1) \oplus R/(p_2) \oplus R/(p_1^2p_2^2)$.

$\cong R/(p_1) \oplus R/(p_1p_2) \oplus R/(p_1^2p_2^2)$ $\cong R/(p_1) \oplus R/(p_1^2p_2^2)$ by CRT □

Eg. classify all abelian gp of order $180 = 2^2 \times 3^2 \times 5$. ($\mathbb{Z}/k$ impossible since infinite.)

We know $M \cong \mathbb{Z}/(p_1^{a_1}) \oplus \dots \oplus \mathbb{Z}/(p_r^{a_r})$ for not necessarily distinct p_i, order of $M = p_1^{a_1}p_2^{a_2}\dots p_r^{a_r}$. So we have the following possibilities:

$(2,2,3,3,5) \rightsquigarrow \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$. ($\cong \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/30\mathbb{Z}$)

$(2^2, 3^2, 5)$, $(2,2,3^2,5)$, $(2^2, 3, 3, 5)$.

$\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$.

MA3201 W10L2

Review: M is a f.g mod for a PID R. Then $M \overset{(\text{unique})}{\cong} R^k \oplus R/(\alpha_1) \oplus \dots \oplus R/(\alpha_s)$, $\alpha_i \neq R^*$, $\alpha_1 | \alpha_2 | \dots$ $\overset{(\text{unique})}{\cong} R^k \oplus R/(p_1^{a_1}) \oplus \dots \oplus R/(p_s^{a_s})$

Eg. $M \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/p_1\mathbb{Z} \oplus \mathbb{Z}/p_2\mathbb{Z}$.

$\therefore$ we must have $p_1 = 2$, $p_2 = 3$ (upto perm/unit mult)

This allows us to classify (upto iso) finite abelian gp of a given order.

Rational Canonical Form

↗ rare are PID but not ED.

Let F be a field. We consider the PID (Euclidian Dom) $R = F[x]$.

Any $F[x]$-mod V is automatically a F-vs.

We consider $F[x]$-mod V that is f.dim. over F.

✡ we consider V as both $F[x]$-mod and F-mod.

Let us fix a ~~base~~ F-basis of V. Consider $V \cong F^n$ as F-modules, where $\dim_F V = n$.

Then let $F[x]$ act on V where x acts as a lin.trans, or as a matrix $T \in \mathrm{Mat}_{n\times n}(F)$.

☆ If we choose a diff. basis for V, then the matrix representation for x is given by $g \cdot T \cdot g^{-1} \in \mathrm{Mat}_{n\times n}(F)$ where g is the transition matrix.

Since V is fin.dim., it is fin. gen as a $F[x]$-mod (over its basis).

Structure theory gives us

$$V \cong \frac{F[x]}{(f_1(x))} \oplus \dots \oplus \frac{F[x]}{(f_r(x))} \oplus \cancel{F[x]}^{\text{fin.dim.}}$$

with $f_1(x) | f_2(x) | \dots | f_r(x)$, $f_i(x) \neq 0$, $f_i(x) \notin (F[x])^* = F^*$ (why?)

Def. 1. A scalar $\lambda \in F$ is called an eigenvalue of T if there exists a $0 \neq v \in V$ such that $Tv = \lambda v$. The vector v is called the eigenvector of T with eigenvalue λ.

2. $\ker(\lambda I - T)$ is called the eigenspace of T, where $\lambda I - T : V \to V$. with eigenvalue λ.

We see that $\lambda \in F$ is an eigenvalue $\iff \ker(\lambda I - T) \neq 0$.

Lem. Let $T \in \mathrm{Mat}_{n\times n}(F)$. Then $\ker(xI-T) \neq 0 \Leftrightarrow \det(xI-T) = 0$.

Pf: Recall for the F-linear map $xI-T: V \to V$, we have (because we can have isom. since $\dim V < \infty$)
isomorphism $\Leftrightarrow$ injectivity $\Leftrightarrow$ surjectivity ($\Leftrightarrow \det \neq 0$).

Defn. Let x be a formal variable. Then $\det(xI-T) \in F[x]$ is called the characteristic polynomial of T. $= c_T(x)$.

Lem. The polynomial $c_T(x)$ is indep. of the choice of the F-basis of V.
I.e., we have $c_T(x) = c_{gTg^{-1}}(x)$ for invertible $g \in \mathrm{Mat}_{n\times n}(F)$.
Pf: $c_{gTg^{-1}}(x) = \det(xI - gTg^{-1}) = \det(g(xI-T)g^{-1})$
$= \det g \cdot c_T(x) \cdot \det g^{-1} = c_T(x)$.

Thm. Let $xI-T \in \mathrm{Mat}_{n\times n}(F[x])$. Then recall V is the $F[x]$-mod where x acts as the matrix T wrt a chosen basis $\{e_i\}_{i=1}^n$. Then,
$V \cong \mathrm{coker}(xI-T: F[x]^n \to F[x]^n)$ as $F[x]$-modules.

Pf. Let $\{\tilde{e}_i\}_{i=1}^n$ be the $F[x]$-basis of $F[x]^n$. ($\tilde{e}_1 = (1,0,\dots,0)$.)
We define $\pi: F[x]^n \to V, (\tilde{e}_i \mapsto e_i)$. Recall since $F[x]^n$ is a free $F[x]$-mod of rank n, this defines a unique $F[x]$-mod hom.

We have $x\tilde{e}_i \mapsto x \cdot e_i = T \cdot e_i$.
We claim $\mathrm{Im}(xI-T) = \ker\pi$. Then $\mathrm{coker}(\pi I - T)$
$\cong F[x]^n / \mathrm{Im}(\pi I - T)$.
$\cong F[x]^n / \ker\pi \cong V$

Claim 1: $\mathrm{Im}(xI-T) \subset \ker\pi \Leftrightarrow \pi \circ (xI-T) = 0$
It suffices to show that the bases are killed. (clearly) ×
$\pi \circ (xI-T)(\tilde{e}_i) = 0 \ \forall \tilde{e}_i$. (Then $\pi\circ(xI-T)\sum f(x)\tilde{e}_i = \sum \pi\circ(xI-T)$)
We compute $\pi((xI-T)(\tilde{e}_j))$
$= \pi(x\tilde{e}_j - \sum_{i=1}^n a_{ij}\tilde{e}_i)$ where $T = [a_{ij}]$.

MA320 | W10 L2. (2)

$= \sum_{i=1}^{n} x \cdot e_j + \sum_{i=1}^{n} a_{ij} e_i \cdot$

$= T \cdot e_j - \sum_{i=1}^{n} a_{ij} e_i = 0$

↑ the same.

this is hard to show

(the other inclusion $\mathrm{Im}(xI-T) \supseteq \ker T$).

Claim 2: The F-dimension of $\mathrm{coker}(xI-T) \le n$.

Then we have $\mathrm{coker}(xI-T) \twoheadrightarrow V$ as a map from $\le n$ F-dim to F-dim, and the surjectivity ($\ker T$) gives us isomorphism.

$$F[x]^n \xrightarrow{xI-T} F[x]^n \twoheadrightarrow V \cong$$

$$\searrow F[x]^n / \mathrm{Im}(xI-T)$$

we claim the image of $\{\tilde{e}_i\}_{i=1}^n$ in $\mathrm{coker}(xI-T) = F[x]/\mathrm{Im}(xI-T)$.

F-span the space. (thus dim $\le n$.)

Let $f_j(x) = x - \sum_{i=1}^{n} a_{ij}$ $\quad (T = (a_{ij}))$

Let $m = \sum_{j=1}^{n} m_j(x) \tilde{e}_j \in F[x]^n$ be given.

Then $m_j(x)\tilde{e}_j = b_j \tilde{e}_j + f_j(x) b_j(x) \tilde{e}_j$. since $F[x]$-vs. are ED?

considering / entry. remainder, degree / quotient.

$(m_j(x) = b_j + f_j(x) b_j(x)$, $\deg b_j = 0)$

$\therefore m = \sum_{j=1}^{n} b_j \tilde{e}_j + \mathrm{Im}(xI-T)$. (why?).

can be mapped to. multiple of $f_j(x)$.

thus $\tilde{e}_j$ spans V.

Concrete: Let $T = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$. Then $xI-T = \begin{bmatrix} x-1 & -2 \\ -3 & x-4 \end{bmatrix}$

Then $\mathrm{Im}(xI-T) = \left(\begin{bmatrix} x-1 & -2 \\ -3 & x-4 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \begin{bmatrix} x-1 & -2 \\ -3 & x-4 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right)$.

$= \left(\begin{bmatrix} x-1 \\ -3 \end{bmatrix}, \begin{bmatrix} -2 \\ x-4 \end{bmatrix} \right)$

Eg. Let $F = \mathbb{Q}$. consider $\mathbb{Q}[x]$-mod $V \cong \mathbb{Q}^3$, where x acts as $T = \begin{bmatrix} 2 & -3 & 14 \\ 0 & 3 & -7 \\ 0 & 0 & 2 \end{bmatrix}$. Then

$V \cong \mathrm{coker}(xI-T) = \mathrm{coker}\left(\begin{bmatrix} x-2 & 2 & -14 \\ 0 & x-3 & 7 \\ 0 & 0 & x-2 \end{bmatrix} : F[x]^3 \to F[x]^3 \right)$.

Then we can perform the following operations to change $xI-T$ to the Smith normal form:

$$\begin{bmatrix} x-2 & 2 & -14 \\ 0 & x-3 & 7 \\ 0 & 0 & x-2 \end{bmatrix} \xrightarrow{R_1 \leftrightarrow R_2} \begin{bmatrix} 2 & x-2 & -14 \\ x-3 & 0 & 7 \\ 0 & 0 & x-2 \end{bmatrix} \xrightarrow{C_2 - \frac{1}{2}(x-2)C_1} \begin{bmatrix} 2 & 0 & 0 \\ x-3 & -\frac{1}{2}(x-2)(x-3) & 7x-14 \\ 0 & 0 & x-2 \end{bmatrix}$$

$$\rightarrow \begin{bmatrix} 2 & 0 & 0 \\ 0 & -\frac{1}{2}(x-3)(x-2) & 7x-14 \\ 0 & 0 & x-2 \end{bmatrix} \rightarrow \begin{bmatrix} 2 & 0 & 0 \\ 0 & -\frac{1}{2}(x-3)(x-2) & 0 \\ 0 & 0 & x-2 \end{bmatrix}.$$

$$\rightarrow \begin{bmatrix} 2 & & \\ & x-2 & \\ & & -\frac{1}{2}(x-1)(x-2) \end{bmatrix}$$

$\therefore V \cong F[x]/(1) \oplus F[x]/(x-2) \oplus F[x]/((x-3)(x-2))$

Then we want to choose a nice basis of V s.t. T is of some simpler form.

Eg. Let $V \cong F[x]/(f(x))$ where $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$.
Then we can choose the F-basis for V via the isomorphism as.
$1, x, x^2, \dots, x^{n-1}$. eg. $\bar{x}^n = -a_{n-1}\bar{x}^{n-1} - a_{n-2}\bar{x}^{n-2} - \dots - a_0$.
x acts as the matrix $= \begin{bmatrix} -a_0 \\ \vdots \\ -a_{n-1} \end{bmatrix}$ wrt to the basis.

$$\begin{bmatrix} 0 & & & -a_0 \\ 1 & \ddots & & \vdots \\ & \ddots & 0 & -a_{n-2} \\ & & 1 & -a_{n-1} \end{bmatrix}$$

A bonus computation $\det(xI-T) = f(x)$. (check)

Def. (Rational canonical form) Let V be a finite dimensional $F[x]$-mod, where x acts as $T \in \mathrm{Mat}_{n\times n}(F)$, with a given basis of V.
Then by structure theory, $V \cong F[x]/(f_1(x)) \oplus \dots \oplus F[x]/(f_r(x))$.
with $f_1(x) | f_2(x) | \dots$, $f_i(x) \neq 0$, $f_i(x) \notin F[x]^* = F^*$.

Then the RCF of T is of the form $\begin{bmatrix} T_1 & & \\ & T_2 & \\ & & \ddots T_r \end{bmatrix}$ where the blocks T_i is of the form in the example above.
if $f_i(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$.

Eg. RCF of $\begin{bmatrix} 2 & -2 & 14 \\ 0 & 3 & -7 \\ 0 & 0 & 2 \end{bmatrix}$ is $\begin{bmatrix} \textcircled{2} & 0 & 0 \\ 0 & 0 & -6 \\ 0 & 1 & 5 \end{bmatrix}$ since $V \cong F[x]/(x-2) \oplus F[x]/(x^2-5x+6)$
T_1 T_2.

MA3201 WILL

Preview: we can classify conj. classes of $GL_3(\mathbb{F}_3)$.

- we can classify nilpotent matrices $A^k = 0$ in $Mat_{n\times n}(\mathbb{C})$.

Review: Let F be a field, $T \in Mat_{n\times n}(F)$. Let $V = F^n$ be a $F[x]$-mod where x acts as T. Then we know

$$V \cong Coker(xI - T : F[x]^n \to F[x]^n) \cong F[x]/(f_1(x)) \oplus \dots \oplus F[x]/(f_r(x))$$

where $f_1(x) | f_2(x) | \dots$, $f_r \neq 0$, $f_i(x) \notin F(x)^* = F^\times$.

(often assume f_i is monic).

Then we can choose/change the basis.

$$F[x]/(f_1(x)) \oplus \dots \oplus F[x]/(f_1(x))$$

$$\{1, \bar{x}, \bar{x}^2, \dots, \bar{x}^{n_1-1}\}.$$

where $f_1(x) = x^{n_1} + a_{n_1-1}x^{n_1-1} + \dots + a_0$.

Then the matrix/lin.trans. x (or T) has the form.

$$\begin{bmatrix} T_1 & & & \\ & T_2 & & \\ & & \ddots & \\ & & & T_r \end{bmatrix} \quad \text{where } T_1 = \begin{bmatrix} 0 & & & -a_0 \\ 1 & 0 & & \vdots \\ & \ddots & & \\ & & 1 & -a_{n_1-1} \end{bmatrix} \text{ etc.}$$

We have, by direct computation,

$$Mat_{n\times n}(F[x]) \ni \det(xI - T) = \det(xI - T_1)\det(xI - T_2)\dots\det(xI - T_r).$$

$$\det(xI - T) = f_1(x) f_2(x) \dots f_r(x).$$

Thm (Cor proof). Retain the setting, we have ($F^n \cong V$) $V \cong coker(xI - T : F[x]^n \to F[x]^n)$.

Pf: Define $\pi : F[x]^n \to V$; $\tilde{e}_i \to e_i$.

eg. $\begin{bmatrix} 2 \\ 0 \end{bmatrix} \to \begin{bmatrix} 2 \\ 0 \end{bmatrix}$, $\begin{bmatrix} x \\ 0 \end{bmatrix} \to x \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} = T \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix}$.

Claim: $\ker \pi = Im(xI - T)$ $(= I_n)$.

Claim 1: $\pi \circ (xI - T) = 0 \iff Im \subset \ker \pi$

We compute $\pi \circ (xI - T)(\tilde{e}_j) = \pi(x \cdot \tilde{e}_j - T \cdot \tilde{e}_j)$

$$= x \cdot \pi(\tilde{e}_j) - T \cdot \pi(\tilde{e}_j) *$$

$$= T \cdot e_j - T e_j = 0 \quad \forall j.$$

Claim 2:

Pf (cont'd) $\dim_F \operatorname{coker}(xI-T) \le n$.

We show $\sum_{j=1}^{n} b_j \tilde{e}_j + \operatorname{Im}(xI-T) = \operatorname{coker}(xI-T)$ for $b_j \in F$.

coset. $\operatorname{coker}(xI-T) = F[x]/\operatorname{Im}(xI-T)$.

I.e., any elem in $F[x]/\operatorname{Im}(xI-T)$ will be spanned by $\tilde{e}_j$'s in F.

Take any $\sum_{j=1}^{n} m_j(x)\tilde{e}_j + \operatorname{Im}(xI-T) \in F[x]/\operatorname{Im}(xI-T)$.

$m_j(x)$ is a polynomial $\in F[x]$. Suffices to show that x-terms are spanned by F with basis $\tilde{e}_j$.

$$x\tilde{e}_j + \operatorname{Im}(xI-T) = x\tilde{e}_j + (xI-T)\tilde{e}_j + \operatorname{Im}(xI-T)$$
$$= T\tilde{e}_j + \operatorname{Im}(xI-T)$$

Similarly, $x(x\tilde{e}_j + \operatorname{Im}(xI-T)) = x^2\tilde{e}_j + \operatorname{Im}(xI-T) = T^2\tilde{e}_j + \operatorname{Im}(xI-T)$

Therefore $\sum_{j=1}^{n} m_j(x)\tilde{e}_j + \operatorname{Im} = \sum_{j=1}^{n} m_j(T)\tilde{e}_j + \operatorname{Im}$ (all terms with x are sent to the image. (?))

$$= \sum_{j=1}^{n} b_j \tilde{e}_j + \operatorname{Im}, \quad b_j \in F.$$

Since $\operatorname{coker}(xI-T)$ is spanned by n elements, over F,

$\dim_F \operatorname{coker}(xI-T) \le n$.

$\therefore$ $F[x]^n \twoheadrightarrow V$ $\dim_F = n$. (due to the map $\tilde{e}_j \to e_j$).

$F[x]^n / \operatorname{Im}$ $\dim_F \le n$ (as shown).

□

Lemma: Let $T, S \in \mathrm{Mat}_{n\times n}(F)$.

(1) The Rational Canonical Form (RCF) of T is unique. (choice of bases $\gamma_1, \gamma_2, \dots, \gamma^{n_i-1}$ are unique) ✓ $\alpha_1 | \alpha_2 | \dots$

(follows by the uniqueness of invariant factors).

(2) T is similar to its RCF. Recall A similar to B if $A = gBg^{-1}$ for $g \in GL_n(F) = (\mathrm{End}_F(F^n))^*$. This means RCF is obtained by a Δ of basis.

(3) T is similar to $S \iff$ They have the same RCF.

MA3201 WILL (2)

Characteristic & Minimal polynomials

Defn. Let $T \in \mathrm{Mat}_{n\times n}(F)$. We consider the $F[x]$-mod $V = F^n$ where x acts as T. Then let $\mathrm{Ann}_{F[x]}(V) = \{r \in F[x] \mid r.v = 0 \ \forall v \in V\} = (p_T(x))$. (PID). We define the minimal polynomial of T as $u p_T(x)$ for some $u \in F^\times$ s.t. $u p_T(x)$ is monic. So we often assume $p_T(x)$ is monic.

Lem: Let $f(x) \in F[x]$ s.t. $f(T) = 0$ in $\mathrm{Mat}_{n\times n}(F)$. Then $p_T(x) \mid f(x)$.

Pf: Let $V = F^n$ where x acts as T. Then $f(T) = 0 \Rightarrow f(x) \in \mathrm{Ann}_{F[x]}(V) = (p_T(x))$. Then $p_T(x) \mid f(x)$. (Explains the "maximal" uniqueness due to PID.) PID. □

Lem: (1) Let $V \cong F[x]/(f_1(x)) \oplus \cdots \oplus F[x](f_r(x))$, $f_r \neq 0$, $f_1 \mid \cdots \mid f_r$, then $p_T(x) = f_r(x)$ — min poly divides char poly $\Rightarrow$ same ideal $= \mathrm{Ann}(V)$.

(2) We have $p_T(x) \mid c_T(x) = \det(xI - T)$. Now, $c_T(T) = 0$. ← (This is the Hamilton–Cayley Thm.)

Pf: (1): $\mathrm{Ann}_{F[x]}(F[x]/(f_1(x)) \oplus \cdots \oplus F[x]/(f_r(x))) = (f_r(x)) = (p_T(x))$ ← defn of $p_T(x)$ = generator of Ann.

$\therefore f_r(x) = p_T(x)$ if both monic.

(2): Recall $\det(xI - T) = c_T(x) = f_1(x) \cdots f_r(x)$. (we can compute using $K(F)$). Then $p_T(x) = f_r(x) \mid c_T(x)$. Then $c_T(T) = 0$.

Jordan Canonical Form

Invariant Factors Form ⇝ Rational Canonical Form.

Elementary ⇝ Jordan.

Defn: Let F be a field. We say F is algebraically closed if any non-constant, $f(x) \in F[x]$ has a root in F.

Eg. ① $\mathbb{R}$ is not algebraically closed, since $x^2 + 1$ has no root in $\mathbb{R}$.

② $\mathbb{C}$ is algebraically closed by the Fundamental Thm of Algebra.

Fact. ③ Any field is contained in some algebraically closed field. eg $\mathbb{R} \subsetneq \mathbb{C}$.

Lemma: Let F be algebraically closed.

(1) F is infinite.

(2) Let $f(x) \in F[x]$ be irreducible (not a unit, additionally). Then $f(x) = (x-\lambda)\cdot b$ for some $\lambda \in F$, and some $b \in F^{\times}$ (non zero).

Pf (1): By $\neg\exists$. Assume $F = \{a_1, \dots, a_n\}$. Then $(x-a_1)(x-a_2)\cdots(x-a_n)+1$ has no root. ($\Rightarrow\Leftarrow$).

(2) Let $f(x)$ be given. Since Alg. closed, let λ be a root. Then $(x-\lambda) \mid f(x) \Leftrightarrow f(x) = p(x)\cdot(x-\lambda)$ for some $p(x) \in F[x]$. Since $f(x)$ irreducible, $p(x)$ is a unit. $\therefore f(x) = (x-\lambda)\cdot b$ for $b \in F^{\times}$, $\lambda \in F$. $\square$

Cor. Let F be alg. closed. Then any non-const $f(x) \in F[x]$ is a pdt of linear factors, or $f(x) = b(x-\lambda_1)(x-\lambda_2)\cdots(x-\lambda_n)$ for $b \in F^{\times}$, $\lambda_i \in F$. (Fundamental Thm)

Lem. If F is alg. closed, then any $T \in \mathrm{Mat}_{n\times n}(F)$ has an eigenvalue.

Pf: Let $c_T(x) = \det(xI - T)$ be the char. poly. Let λ be a root of $c_T(x)$ (guaranteed by alg. closure). Then,

$\det(\lambda I - T) = 0 \Leftrightarrow \lambda I - T$ is not invertible.

$\Leftrightarrow \lambda I - T : F^n \to F^n$ is NOT injective

$\Leftrightarrow \ker(\lambda I - T) \neq 0$

$\Leftrightarrow \exists$ eigenvector $v \in \ker(\lambda I - T)$ with ev. λ.

Eg. Let $T = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \in \mathrm{Mat}_{2\times 2}(\mathbb{R})$. Then $c_T(x) = x^2 + 1$ has no root in $\mathbb{R}$,

$= (x-i)(x+i)$ — eigenvalues.

so T has no ev. in $\mathbb{R}$.

MA3201 W1C1(3).

Eg. of Jordan CF: Let F be alg. closed. $V \cong F[x]/(p(x))^n$ for some irreducible $p(x) = x-a$. then we can choose a (F basis):

1. $(x-a), (x-a)^2, \ldots, (x-a)^{n-1} \in F[x]/(p(x))^n \cong V$.

Then x acts as the matrix.

$$T = \begin{bmatrix} a & 1 & 0 & \\ 0 & a & 1 & 0 \\ & \ddots & \ddots & 1 \\ 0 & & & a \end{bmatrix}$$

eg. $x \cdot 1 = 1\cdot(x-a) + a\cdot 1$.

$$\begin{bmatrix} 0 \\ \vdots \\ 1 \\ 0 \end{bmatrix} \quad \begin{bmatrix} a \\ 1 \\ \vdots \\ 0 \end{bmatrix}$$

Then $\det(xI - T) = (x-a)^n$.

Pf. General case: Let F be alg. closed. Let $T \in \mathrm{Mat}_{n\times n}(F)$. Let $V = F^n$ be a $F[x]$-mod where x acts as T. then.

$$V \overset{\text{v}}{=} \mathrm{coker}(xI - T) \cong F[x]/(p_1^{a_{11}}) \oplus \cdots \oplus F[x]/(p_r^{a_{1r}})$$
$$\cong F[x]/((x-a_1)^{n_1}) \oplus \cdots \oplus F[x]/((x-a_r)^{n_r}).$$

(alg. closed $\Rightarrow$ pmid $\Rightarrow$ has this form)

with not necessarily distinct $a_i \in F$.

Jordan Canonical form of T as $\begin{bmatrix} T_1 & & \\ & \ddots & \\ & & T_r \end{bmatrix}$ where T_i are in the eg.

$$\sim \begin{bmatrix} a_1 & 1 & & & & \\ & a_1 & 1 & & & \\ & & a_1 & & & \\ & & & a_2 & 1 & \\ & & & & a_2 & \\ & & & & & \ddots \end{bmatrix}$$

only well-defined up to permutation of blocks. (another $\leq$ of bases)

Lem. F alg-closed. Let $T, S \in \mathrm{Mat}_{n\times n}(F)$.

(1) T is similar to its JCF.

(2) T is similar to $S \Leftrightarrow T, S$ have the JCF up to permutation of blocks.

Eg. (1) Let $T = \begin{bmatrix} 2 & -2 & 14 \\ 0 & 3 & -7 \\ 0 & 0 & 2 \end{bmatrix} \in \mathrm{Mat}_{3\times 3}(\mathbb{C})$ $\therefore xI - T = \begin{bmatrix} x-2 & 2 & -14 \\ 0 & x-3 & 7 \\ 0 & 0 & x-2 \end{bmatrix}$.

(need sdc ie PID)

Smith NF $\begin{bmatrix} 1 & 0 & 0 \\ 0 & x-2 & 0 \\ 0 & 0 & (x-2)(x-3) \end{bmatrix}$ $\therefore V (= \mathbb{C}^3) \cong \mathbb{C}[x]/(x-2) \oplus \mathbb{C}[x]/(x-2)(x-3)$

$\cong \mathbb{C}[x]/(x-2) \oplus \mathbb{C}[x]/(x-2) \oplus \mathbb{C}[x]/(x-3)$

$\therefore$ JCF of T is $\begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{bmatrix} = A$.

$\mathbb{Z}[x]$ is not pid, consider $I(2, x)$.

we have $A = gTg^{-1}$ for $g \in GL_3(\mathbb{C})$.
we also have $A = h \cdot T \cdot h^{-1}$ for $h \in GL_3(\mathbb{Q})$ (did not use assumption of $\mathbb{C}$)
★ Note that $T \in Mat_{3\times 3}(\mathbb{C})$ is also diagonalizable in $\mathbb{C}$. (or in $\mathbb{R}$).

② Let $T = \begin{bmatrix} 0 & 1 & 0 \\ -1 & 0 & \\ & & \end{bmatrix} \in Mat_{2\times 2}(\mathbb{C})$.
$xI - T = \begin{bmatrix} x & -1 \\ 1 & x \end{bmatrix}$ smith normal form $\begin{bmatrix} 1 & 0 \\ 0 & x^2+1 \end{bmatrix}$.
Then we have $V \cong \mathbb{C}[x]/(x^2+1) \cong \mathbb{C}[x]/(x-i) \oplus \mathbb{C}[x]/(x+i)$.

$\therefore$ JCF of T in $\mathbb{C}$: $\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$ is diagonalizable in $\mathbb{C}$,
but not diagonalizable in $\mathbb{R}$. (otherwise the diagonal entries are eigenvalues in $\mathbb{R}$.).

Review: (Structure theorem of PID) M is a f.g. R-mod, R is PID, $M = R\{m_1, \dots, m_n\}$.
Then we consider $R^n \xrightarrow{\Pi} M$. consider $\ker \Pi \subset R^n$.
Free mod $e_i \longmapsto m_i$.
★ R is PID $\Rightarrow$ Noetherian $\Rightarrow$ Any submod of R^n is f.g. $\Rightarrow \ker \Pi$ is f.g.
$\therefore \ker \Pi = R\{q_1, \dots, q_n\}$ for some $q_i \in R^n$.

$R^n \xrightarrow{\varphi} \ker \Pi \hookrightarrow R^n \xrightarrow{\Pi} M$.
$e_i \longmapsto a_i$.
Then $\varphi(R^n) = \ker(\Pi)$

MA3201 Wk12

Recall: Jordan canonical form. Let F be alg. closed. Let $V = F^n$ be a $F[x]$-mod where x acts as $T \in Mat_{n\times n} F$. Then we know $V \cong F[x]/(p_1^{n_1}) \oplus \cdots \oplus F[x]/(p_r^{n_r})$ for not nec. distinct pmes p_i,
$\cong F[x]/(x-a_1)^{n_1} \oplus \cdots \oplus F[x]/(x-a_r)^{n_r}$.

Eg.: $V \cong F[x]/(x-1)^2 \oplus F[x]/(x-2)^2$ for $F = \mathbb{C}$.
Then JCF for T $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{bmatrix}$.

Eg. ① Let $T = \begin{bmatrix} 0 & -1 \\ 1 & 2 \end{bmatrix} \in Mat_{2\times 2}(\mathbb{C})$. Then we can compute JCF:

$xI - T = \begin{bmatrix} x & 1 \\ -1 & x-2 \end{bmatrix} \xrightarrow{\text{Smith Normal Form}} \begin{bmatrix} 1 & 0 \\ 0 & (x-1)^2 \end{bmatrix}$.

This means $V \cong \mathbb{C}[x]/(x-1)^2$, Then the JCF of T is. $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ is not diagonalizable.

② (char poly is not enough to get JCF). We know $T = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ and $S = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ are not similar, however $C_T(x) = x^2$, $C_S(x) = x^2$.

Cor: Let F be alg. closed. Let T be a matrix, $n\times n$ with a JCF $J \in Mat_{n\times n}(F)$.
Then T is diag $\Leftrightarrow$ J is diagonal.
$\Leftrightarrow$ The min. poly $m_T(x)$ has no (repeated) multiple roots &
$\Leftrightarrow m_T(x) = (x-a_1)\cdots(x-a_r)$. with $a_i \neq a_j$ if $i \neq j$.

eg. $T = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$, $\mathbb{C}[x]$ $V \cong \mathbb{C}[x]/(x-2)^2$, then $m_T(x) = (x-2)$.

Lem: Let F be any field. Then
1. If $T = \begin{bmatrix} 0 & 0 & -a_0 \\ 1 & 0 & -a_1 \\ 0 & 1 & -a_2 \end{bmatrix}$, then the RCF of T is just T. (generalizable to blockwise).
2. If $S = \begin{bmatrix} a & 1 & 0 \\ 0 & a & 1 \\ 0 & 0 & a \end{bmatrix}$, then the JCF of S is just S. (++).

Pf (1): Let $V=F^3$ be the $F[x]$-mod where x acts as T. Then $V\cong \operatorname{coker}(xI-T)$.

$xI-T=\begin{bmatrix} x & 0 & a_0 \\ -1 & x & a_1 \\ 0 & -1 & x+a_2 \end{bmatrix}$. we apply invertible operations,

$$\begin{bmatrix} x & 0 & a_0 \\ -1 & x & a_1 \\ 0 & -1 & x+a_2 \end{bmatrix} \xrightarrow{R_1\leftrightarrow R_2} \begin{bmatrix} -1 & x & a_1 \\ x & 0 & a_0 \\ 0 & -1 & x+a_2 \end{bmatrix} \to \begin{bmatrix} -1 & 0 & 0 \\ x & x^2 & a_0+a_1x \\ 0 & -1 & x+a_2 \end{bmatrix}$$

$$\to \begin{bmatrix} -1 & 0 & 0 \\ 0 & x^2 & a_0+a_1x \\ 0 & -1 & x+a_2 \end{bmatrix} \to \begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & x+a_2 \\ 0 & x^2 & a_0+a_1x \end{bmatrix} \to \begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & x+a_2 \\ 0 & 0 & a_0+a_1x+a_2x+x^3 \end{bmatrix}$$

$$\to \begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & x^3+a_2x^2+a_1x+a_0 \end{bmatrix} \sim .$$

$\therefore V\cong \operatorname{coker}\left(\begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & x^3+a_2x^2+a_1x+a_0 \end{bmatrix} : F[x]^3 \to F[x]^3\right)$.

$\cong F[x]/(x^3+a_2x^2+a_1x+a_0)$.

So the RCF of T is $C(T)=\begin{bmatrix} 0 & 0 & -a_0 \\ 1 & 0 & -a_1 \\ 0 & 1 & -a_2 \end{bmatrix}$. □

(2) Let $V=F^3$ be the $F[x]$-module where x acts as S. Then

$V\cong \operatorname{coker}(xI-S)$. $xI-S=\begin{bmatrix} x-a & -1 & 0 \\ 0 & x-a & -1 \\ 0 & 0 & x-a \end{bmatrix}$ Apply invertible ops,

$$\begin{bmatrix} x-a & -1 & 0 \\ 0 & x-a & -1 \\ 0 & 0 & x-a \end{bmatrix} \to \begin{bmatrix} -1 & x-a & 0 \\ x-a & 0 & -1 \\ 0 & 0 & x-a \end{bmatrix} \to \begin{bmatrix} -1 & 0 & 0 \\ x-a & (x-a)^2 & -1 \\ 0 & 0 & x-a \end{bmatrix}$$

$$\to \begin{bmatrix} -1 & 0 & 0 \\ 0 & (x-a)^2 & -1 \\ 0 & 0 & x-a \end{bmatrix} \to \begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & (x-a)^2 \\ 0 & x-a & 0 \end{bmatrix} \to \begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & (x-a)^2 \\ 0 & 0 & (x-a)^3 \end{bmatrix} \to \begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & (x-a)^3 \end{bmatrix}$$

$\therefore V\cong \operatorname{coker}\left(\begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & (x-a)^3 \end{bmatrix} : F[x]^3 \to F[x]^3\right) \cong F[x]/(x-a)^3$.

So the JCF of S is S. □

Applications of modules over PID / RCF/JCF.

Let F be a field, $A\in \operatorname{Mat}_{n\times n}(F)$ be such that $A^k=0$ for some $k>0$. Such A is nilpotent. Consider $GL_n(F)\curvearrowright \operatorname{Mat}_{n\times n}(F)$, $g\cdot A=gAg^{-1}$.

($GL_n(F)$: invertible matrices)

we want to classify the orbits of nilpotent matrices.

MA3201 WILL 2 (2).

Lem: Let $A \in \mathrm{Mat}_{n\times n}(F)$ be nilpotent. Then $C_A(x) = x^n$ and $m_A(x) = x^r$ for some $r > 0$.

Pf: A is nilpotent, say $A^k = 0$. Then let $f(x) = x^k$. We have $f(A) = 0$. Thus $m_A(x) \mid f(x)$ by minimality. Then $m_A(x) = x^r$ for some $r \le k$. Then recall we have

$F[x], x=T_A$ gives $F[x]^n \cong F[x]/(f_1(x)) \oplus \cdots \oplus F[x]/(f_r(x) = m_A(x))$, $f_1 \mid f_2 \mid \cdots$

we know $C_A(x) = f_1(x) f_2(x) \cdots f_r(x)$ and $m_A(x) \mid C_A(x)$.

since $f_1 \mid f_2 \mid \cdots$, they must be powers of x, so must $C_A(x)$. □.

Prop: The orbits of nilpotents in $\mathrm{Mat}_{n\times n}(F)$ is in bijection with the set of (combinatorics) partitions of n. where $\{(\lambda_1, \lambda_2, \cdots, \lambda_r) \mid \sum \lambda_i = n,\ \lambda_1 \ge \lambda_2 \ge \cdots\}$. (why?)

Pf: The $GL_n(F)$-orbits of $\mathrm{Mat}_{n\times n}(F)$ is determined by the rational canonical form (since similar matrices have the same RCF).

If $C_A(x) = x^{a_1} x^{a_2} \cdots x^{a_r}$, where $\sum a_i = n$. □.

(Gilenky phrasing)

Eg. There are 3 orbits of nilpotent matrices in $\mathrm{Mat}_{3\times 3}(F)$, they are orbits of

$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$, $\begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$, $\begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$ (why are they?)

Conjugacy classes in $GL_2(F_2)$ ~~$F_2 \cong \mathbb{Z}/2\mathbb{Z}$~~

~~Prop: There are 6 conjugacy classes in $GL_2(F_2)$~~ orbits of conjugation. $GL_2(F_2) \curvearrowright \mathrm{Mat}_{2\times 2}(F_2)$.

Pf: We consider the conjugation of $GL_2(F_2) \curvearrowright GL_2(F_2)$. We want to classify the orbits. It suffices to consider the "invariant factors":

$\forall A \in \mathrm{Mat}_{2\times 2}(F)$, we consider the RCF of A similar to $\begin{bmatrix} T_1 & \\ & T_2 \end{bmatrix}$.

$F_2[x]^2 \overset{x=A}{\curvearrowright} F^2 \cong F[x]/(f_1(x)) + F[x]/(f_2[x])$.

To find all possible f_1, f_2, we need to find all irreducible polynomials of degree ≤ 2. x, $x-1$ ($x+1$), x^2+x+1.

Pf (cont'd) we have the following possibilities for $f_1 | f_2$:

f_1 x $x-1$

f_2 x $x-1$

or $F[x]/m_T(x) \cong F^2$, $m_T(x) = x^2, (x-1)^2, x(x-1), x^2+x+1$

6 possibilities. □.

Cor. we have 2. conjugacy classes of $GL_2(F_2)$.

$f_1 = f_2 = x \Rightarrow \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$. (not in $GL_2(F_2)$ since not invertible) ✗

$f_1 = f_2 = (x-1) \Rightarrow \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ ✓

$m_T(x) = x^2 \Rightarrow \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ ✗

$(x-1)^2 \Rightarrow \begin{bmatrix} 0 & -1 \\ 1 & 2 \end{bmatrix}$ but $2=0, 1=1 \Rightarrow \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ ✓

$x(x-1) \Rightarrow \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}$ ✗.

$x^2+x+1 \Rightarrow \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$ ✓.

orbits of $GL_3(\mathbb{Q})$ on the set $A = \{g \in GL_3(\mathbb{Q}) \mid g^6 = id\}$.

(Note that the conj. action is well defined, since $g^6 = id \Rightarrow (hgh^{-1})^6 = id$.

we want to find the corresponding RCFs.

Let $f(x) = x^6 - 1$. Then $\forall B \in A$, $f(B) = B^6 - 1 = 0$.

$\therefore m_B(x) \mid f(x) = (x^2+1)(x^2-1) = (x+1)(x-1)(x^2+x+1)(x^2-x+1)$.

On the other hand, we know $\deg m_B(x) \leq 3$. (why?) (GL_3)

Possible $m_B(x)$ and invariant factors:

(1) $(x+1)$ $(x-1), (x-1), (x-1)$ ①

(2) $(x-1)$ $(x+1), (x+1), (x+1)$. ②

(3) (x^2+x+1) impossible since $\deg c_A(x) = 3$.

(4) (x^2-x+1)

(5) $(x-1)(x+1)$ $(x-1)$, ③ self or $(x+1)$, ④ self

(6) $(x-1)(x^2+x+1)$ self ⑤

(7) $(x-1)(x^2-x+1)$ ⑥

(8) $(x+1)(x^2+x+1)$ ⑦

(9) $(x+1)(x^2-x+1)$. ⑧

Conclusion: there are 8 orbits of the $GL_3(\mathbb{Q})$-conj. action on $A = \{g \in GL_3(\mathbb{Q}) \mid g^6 = id\}$.

MA3201 WEEK 2 (3).

Tensor product of modules

We start with a motivating example.

Let $V=\mathbb{R}^3$, $W=\mathbb{R}^3$ be $\mathbb{R}$-vector spaces. We write the elements as row vectors.

$\{(a,b,c)\}$ $\{(d,e,f)\}$.

Then we know $V\oplus W=\mathbb{R}^6$. of $\dim_{\mathbb{R}}=6=3+3$.

$\{(a,b,c,d,e,f) \mid (a,b,c)\in V,\ (d,e,f)\in W\}$.

We define a new $\mathbb{R}$-vector space:

$$V\otimes_{\mathbb{R}} W=\left\{\sum_{\text{finite}} \begin{pmatrix}a\\b\\c\end{pmatrix}\cdot(d,e,f)=\sum_{\text{finite}} \begin{pmatrix}ad & ae & af\\ bd & be & bf\\ cd & ce & cf\end{pmatrix} \mid (a,b,c)\in V,\ (d,e,f)\in W\right\}$$

with the (obvious) $\mathbb{R}$-vector space structure. Then $\dim_{\mathbb{R}} V\otimes_{\mathbb{R}} W=9=3\times 3$

We can write element $\begin{pmatrix}a\\b\\c\end{pmatrix}\cdot(d,e,f)$ as $\begin{pmatrix}a\\b\\c\end{pmatrix}\otimes_{\mathbb{R}}(d,e,f)=v\otimes_{\mathbb{R}} w$

for $v\in V$, $w\in W$.

We have the following "identities":

① $(v_1+v_2)\otimes_{\mathbb{R}} w=v_1\otimes_{\mathbb{R}} w+v_2\otimes_{\mathbb{R}} w$.

② $v\otimes_{\mathbb{R}}(w_1+w_2)=v\otimes_{\mathbb{R}} w_1+v\otimes_{\mathbb{R}} w_2$.

③ $=$ ① + ②: $(v_1+v_2)\otimes_{\mathbb{R}}(w_1+w_2)=v_1\otimes_{\mathbb{R}} w_1+v_1\otimes_{\mathbb{R}} w_2+v_2\otimes_{\mathbb{R}} w_1+v_2\otimes_{\mathbb{R}} w_2$.

④ $(kv)\otimes_{\mathbb{R}} w=k(v\otimes_{\mathbb{R}} w)=v\otimes_{\mathbb{R}}(kw)$.

Next we will use the 3 "identities" to define a more general tensor product. ($\mathbb{R}$ is comm

MA3201 W12 L1

Recall: we finished JCF, RCF and applications: eg. conjugacy classes on $GL_2(\mathbb{F}_2)$.

Prop: $A, B \in Mat_{n\times n}(F)$. Let V, W be two $F[x]$-mods, where x acts as A, B resp. The the following are equivalent:

(1) A and B are similar.
$\Uparrow$ $A = gBg^{-1}$, $\therefore g(xI-A)g^{-1} = xI-B$ $\quad \therefore \mathrm{coker}(g(xI-A)g^{-1}) \cong \mathrm{coker}(xI-A) \cong V \cong \mathrm{coker}(xI-B)$
(2) A and B have the same RCF.
$\Updownarrow$ same inv. factors.
(3) $V \cong W$ as $F[x]$-mods.
$\Downarrow$
(4) V & W have the same invariant factors.
$\Updownarrow$
(5) V and W have the same elem. factors.
$\Updownarrow$
(6) F is alg-closed, then A, B have the same JCF.

Prop: Let $F(V\times W)$ be the free Ab. gp of infinite rank. over the set $V\times W$. Let A be the subgp of $F(V\times W)$ generated by:
$$(v_1+v_2, w) - (v_1, w) - (v_2, w),$$
$$(v, w_1+w_2) - (v, w_1) - (v, w_2),$$
$$(kv, w) - (v, kw) \quad \text{for } k\in\mathbb{R},\ v_v\in V,\ w_w\in W.$$

Then the natural map $F(V\times W)/A \to V\otimes_{\mathbb{R}} W$
$$(v, w) \longmapsto v\otimes_{\mathbb{R}} w \ (= v^{tr}\cdot w).$$
is an isom. of abelian groups (also as $\mathbb{R}$-vector spaces).

Pf we consider the map $F(V\times W) \to V\otimes_{\mathbb{R}} W$
$$(v, w) \longmapsto v\otimes_{\mathbb{R}} w.$$
This is well-defined, since $F(V\times W)$ is free with basis $(v, w) \in V\times W$.
Surjection is free (LHS is "large"), we just check kernel is A.

MA3201 W12 (3).

Eg. ① Let $\mathbb{Z} \subset \mathbb{Q}$, $N = \mathbb{Z}/2\mathbb{Z}$ be the $\mathbb{Z}$-mod.

– Then for any $\mathbb{Q}$-mod V, and $\mathbb{Z}$-mod hom

$$\mathbb{Z}/2\mathbb{Z} = N \longrightarrow \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} = 0$$

$N \to V$, $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \dashrightarrow V$

$0 =$ (since cannot map to a $\mathbb{Q}$-vs).

St $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} = 0$ as $\mathbb{Q}$-mods.

– We also consider $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$ concretely using the construction.

Then $\forall\, r \otimes_{\mathbb{Z}} n$, $= \frac{1}{2} r \cdot 2 \otimes_{\mathbb{Z}} n$

$= \frac{1}{2} r \otimes_{\mathbb{Z}} 2n$. since $N = \mathbb{Z}_2$.

$= \frac{1}{2} r \otimes_{\mathbb{Z}} 0 . = \frac{1}{2} r \otimes_{\mathbb{Z}} 0 \cdot 0$

$= (\frac{1}{2} r)\, 0 \otimes_{\mathbb{Z}} 0$

$= 0 \otimes_{\mathbb{Z}} 0 = 0$.

② For any R-mod N, $R \otimes_R N \cong N$.

Or concretely, $N \to R \otimes_R N$

$n \mapsto 1 \otimes_R n$.

$N \xrightarrow{id} N$, $\varphi: N \to M$, $\varphi: N \dashrightarrow M$.

③ For any $\mathbb{R}$-vs. $V \cong \mathbb{R}^n$, then $\mathbb{C} \otimes_{\mathbb{R}} V \cong \mathbb{C}^n$.

④ Let $H \subset G$ be a subgp of a finite gp G. Then $\mathbb{C}[H] \subset \mathbb{C}[G]$. Let V be a $\mathbb{C}[H]$-mod, then

$\mathrm{Ind}_H^G V = \mathbb{C}[G] \otimes_{\mathbb{C}[H]} V$ on $\mathbb{C}[G]$-mod.

$(g \otimes v)$ $(gh \otimes v = g \otimes hv)$

Tensor product of modules I.

Let M be a (right) R-mod and N be a (left) R-mod. We can then define $M \otimes_R N$ (as an Ab. gp) using the universal property:
(just with these info we can only have Ab gp.)

Defn/Thm (existence): The tensor product $M \otimes_R N$ is defined as an Ab. gp together w/ a map $i: M \times N \to M \otimes_R N$ such that

$$i(m, r, n) = i(m, rn)$$

$i(mr, n) = m \otimes_R rn = mr \otimes_R n$. satisfying the following prop:

for any maps from $M \times N$ to an Ab gp L,

$$\phi: M \times N \to L \text{ s.t. } \phi(m \cdot r, n) = \phi(m, r \cdot n).$$

then there exists a unique map $\bar{\phi}: M \otimes_R N \to L$ making the diagram commutes:

$$\begin{array}{ccc} M \times N & \xrightarrow{i} & M \otimes_R N \\ & \searrow^{\phi} & \downarrow \bar{\phi} \\ & & L \end{array}$$

ϕ is called R-balanced. $M \otimes_R N$ exists and is unique upto isom.

Pf: we define $M \otimes_R N$ as the free Ab. gp $F(M \times N)$ modulo the relations:

(1) $(m_1 + m_2, n) - (m_1, n) - (m_2, n)$

(2) $(m, n_1 + n_2) - (m, n_1) - (m, n_2)$.

(3) $(m \cdot r, n) - (m, r \cdot n)$. for $r \in R$.

Then we define $i: M \times N \to M \otimes_R N$.
$(m, n) \mapsto m \otimes_R n \in F(M \times N)/\sim$. (Q: is this a relation?)

We check this is R-balanced, that is, ...

$\forall$ R-balanced map $\phi: M \times N \to L$, we can define $M \otimes_R N \to L$
$m \otimes_R n \mapsto \phi(m, n)$

Then it remains to check (check) everything is well-defined, and we have a comm. diagram. $\square$

MA3201 W12L2 Date No.

Recap Two examples:- as matrices, $(\ )\times(\ )$.
- "reverse restriction", from module over a subring to module over the larger ring.

Let M_R and ${}_R N$.

Defn. Let L be any Ab gp. A map of sets $\varphi: M\times N \to L$ is R-balanced (additional prop.) if
- $\varphi(m_1+m_2, n) = \varphi(m_1, n) + \varphi(m_2, n)$.
- $\varphi(m, n_1+n_2) = \varphi(m, n_1) + \varphi(m, n_2)$.
- $\varphi(m_1+m_2, n_1+n_2) = \varphi(m_1,n_1) + \varphi(m_1,n_2) + \varphi(m_2,n_1) + \varphi(m_2,n_2)$
  $\neq \varphi(m_1,n_1) + \varphi(m_2,n_2)$.
- $\varphi(mr, n) = \varphi(m, rn)$ ("balanced")

Defn/Thm Reform setting. The tensor product $M\otimes_R N$ is an abelian gp with a R-balanced map (not Ab. hom) $i: M\times N \to M\otimes_R N$ s.t. $\forall$ R-balance map (universal) $\phi: M\times N \to L$, we have

$$\begin{array}{ccc} M\times N & \xrightarrow{i} & M\otimes_R N \\ & \searrow^{\phi} \quad \swarrow_{\bar{\phi}} & \\ & L & \end{array}$$

fixing n, we have a $\mathrm{Hom}_{\mathbb{Z}}$.

Pf: $M\otimes_R N = F(M\times N)/\sim$ where
$\sim$: (1) $(m_1+m_2, n) - (m_1, n) - (m_2, n)$.
(2) $(m, n_1+n_2) - (m, n_1) - (m, n_2)$. (fixing m is the same)
(3) $(mr, n) - (m, rn)$.

And $i: M\times N \hookrightarrow M\otimes_R N$
$(m, n) \mapsto m\otimes_R n = (m, n) + \sim$. □

Lem. Let M_R, ${}_R N$, Let ${}_R L$ be an R-mod. Then we have a bijection of sets:

$$\mathrm{Hom}_{\mathbb{Z}}(M, \mathrm{Hom}_R(N, L)) \overset{\text{Abgps.}}{\longleftrightarrow} \{R\text{-balanced maps } M\times N \to L\} \overset{\text{left } R\text{-mods}}{\longleftrightarrow} \{\mathrm{Hom}_{\mathbb{Z}}(M\otimes_R N, L)\}.$$

Date No.

Pf: we construct the maps:

(1) Let $\phi \in \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, L))$. Then we define.

$\tilde{\phi} : M \times N \to L, \quad (m,n) \mapsto \phi(m)(n)$.

(2) Let $\psi : M \times N \to L$ be R-balanced. Then we define, $\forall n \in N$,

$\psi(-, n) : M \to L$. □

Tensor Product of Modules II

Let R be commutative with 1.

Defn Let M, N, L be R-modules (both left & right). A map of sets $\phi : M \times N \to L$ is called R-bilinear if

① $\phi(r_1 m_1 + r_2 m_2, n) = r_1 \phi(m_1, n) + r_2 \phi(m_2, n)$.

② $\phi(m, r_1 n_1 + r_2 n_2) = r_1 \phi(m_1, n_1) + r_2 \phi(m, n_2)$. $(m_i \in M, n_i \in N, r_i \in R)$

Automatically balanced: $\phi(rm, n) \overset{①}{=} r\phi(m,n) \overset{②}{=} \phi(m, rn)$.

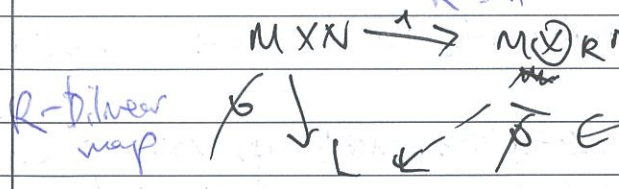
Eg ★★ Let $M = N = \mathbb{R}^3$, $L = \mathbb{R}$. Then the standard bilinear form:

$$(\ ) : \underset{M}{\mathbb{R}^3} \times \underset{N}{\mathbb{R}^3} \to \underset{L}{\mathbb{R}}.$$

$$(v_1, v_2, v_3), (w_1, w_2, w_3) \mapsto v \cdot w^T = v_1 w_1 + v_2 w_2 + v_3 w_3$$

is $\mathbb{R}$-bilinear (in the new definition).

Def/Thm Let R be comm. with 1. Let M, N be R-mods, then their tensor prdt $M \otimes_R N$ (over R) is a R-mod together with R-bilinear maps $i : M \times N \to M \otimes_R N$ s.t. any bilinear map $\phi : M \times N \to L$, (L R-mod) there exists a unique R-mod map $\tilde{\phi} : M \otimes_R N \to L$ s.t. the diag. comm:



MA3201 W12L2 (2). Date No.

Pf: We mod out the bilinear relation / abel. subgp.

$M \otimes_R N = F(M \times N)/\sim$ where

$\sim$: ① $(m_1+m_2, n) - (m_1, n) - (m_2, n)$.

② $(m, n_1+n_2) - (m, n_1) - (m, n_2)$

③ $(rm, n) (= (mr, n)) = (m, rn)$.

Then we give (equip) $M \otimes_R N$ with a R-mod structure as

$r \cdot (m \otimes_R n) = (rm) \otimes_R n = m \otimes_R (rn)$.

$= (m, n) + \sim$, ☆ check well-defined.

we then need to check that this is a well-defined R-mod structure.

$\forall \phi : M \times N \to L$, we define $\overline{\phi} : M \otimes_R N \to L$

$m \otimes_R n \mapsto \phi(m, n)$

☆

and check this is a R-mod.

Eg (cont'd)

$\mathbb{R}^3 \times \mathbb{R}^3 \xrightarrow{i} \mathbb{R}^3 \otimes_{\mathbb{R}} \mathbb{R}^3 \cong Mat_{3\times 3}(\mathbb{R})$.

$(v, w) \mapsto v \otimes_{\mathbb{R}} w = v^{tr} \cdot w$

ϕ ↓ ↘ trace.

$\mathbb{R}$

Eg. $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \cong 0$ since both are not free over $\mathbb{Z}$.

torsion, not torsion — flatness of modules.

Tensor product of Modules III

Let S and R be rngs with 1. (Previously $S = R$ or $S = \mathbb{Z}$).

Defn Let S-R-bimodule M be an Ab. gp that is a left S-mod and right R-mod simultaneously, such that.

$(sm)r = s(mr) = smr$.

Eg. ① R is a R-R-bimodule via the left & right multiplications.

② If M is a right R-mod, then M is a $\mathbb{Z}$-R-bimodule.

$(2m)r = (m+m)r = mr + mr = 2(mr)$.

Date No.

Eg. (3) Let R be commutative. Then any R-mod M is a R-R-bimodule.
ie. $(r_1 r_2)m = r_1 m r_2 = (r_1 m) r_2 = r_1 (m r_2)$.
(left action = right action = mult. commutative)

Defn/Thm Let R, S be rngs with 1. Let M be a S-R-bimodule, and N be a left R-mod. Then the tensor product (depends on situation, can be Ab gp or a module) $M \otimes_R N$ is a S-mod together with a R-balance map $i: M \times N \to M \otimes_R N$ such that $i(sm, n) = s(i(m,n))$ satisfying the following properties:

For any R-balance map, $\phi: M \times N \to L$ (L is S-mod) such that we have a unique S-mod map $\bar{\phi}: M \otimes_R N \to L$ s.t.

$$\begin{array}{ccc} M \times N & \xrightarrow{i} & M \otimes_R N \\ & \searrow^{\phi} \quad \swarrow_{\bar{\phi}} & \\ & L & \end{array}$$

$\bar{\phi}$ ← S-mod map.

pf Similar to previous examples, define the Ab gp
$M \otimes_R N = F(M \times N)/\sim$.
Add S-mod structure to it (via the S-mod structure on M):
$s \cdot (m \otimes_R n) = (sm) \otimes_R n$.
(could be $sm = ms$ for some r, and
recall we have $= (mr) \otimes_R n = m \otimes_R (rn)$ as expected.)
We check: - everything is well-defined.

Define $\bar{\phi}: M \otimes_R n \to L$, $m \otimes_R n \mapsto \phi(m,n)$ and we check this is a S-mod hom. (similar to previous, just check more props of S-mod.)

□

MA3701 W12L2(37). Date No.

Eg. ① we consider $\mathbb{Z}$-mods: $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$. (or as a $\mathbb{Z}$-$\mathbb{Z}$-bimod).
Then we claim $\mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathbb{Z}_3 \cong 0$. is trivial.
Pf: note that 4 acts as 1 in $\mathbb{Z}_3$, $\therefore \forall m \in \mathbb{Z}_2, n \in \mathbb{Z}_3$,
we have $m \otimes n = m \otimes 4 \cdot n$ (identity)
$= 4 \cdot m \otimes n$ (bilinear/bilinear).
$= 0 \otimes n$ ($= 0 \cdot 0 \otimes n = 0 \otimes 0 \cdot n$).
$= (0,0) + \sim \in F(\mathbb{Z}_2, \mathbb{Z}_3)/\sim$.
$\therefore$ since m, n are arbitrary, $\mathbb{Z}_2 \otimes \mathbb{Z}_3$ is trivial.

② we consider $\mathbb{Z}$-mods $\mathbb{Z}_2$ and $\mathbb{Z}_2$. Then we claim $\mathbb{Z}_2 \otimes \mathbb{Z}_2 = \mathbb{Z}_2$.
The $\mathbb{Z}$-bilinear map $\mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_2$
$m \times n \to L$.
$(a, b) \mapsto ab$.
Then $(a, b_1 + b_2) \mapsto a(b_1 + b_2) = ab_1 + ab_2 =$
Then by defn, we have a $\mathbb{Z}$-mod hom.
$\mathbb{Z}_2 \otimes \mathbb{Z}_2 \to \mathbb{Z}_2$.
$a \otimes b \mapsto a \cdot b$. that is surjective.

$|\mathbb{Z}_2 \otimes \mathbb{Z}_2|$ is at most 2, since $1 \otimes 0 = 0 \otimes 1 = 0 \otimes 0$.
Then surjectivity forces an isomorphism: $\mathbb{Z}_2 \otimes \mathbb{Z}_2 \cong \mathbb{Z}_2$.

Thm **Properties of Tensor Products**
Thm Let M_R and $_R N_S$, and $_S L$. Then we have an isom. of Ab. gps, $(M \otimes_R N) \otimes_S L \cong M \otimes_R (N \otimes_S L)$

Pf: In textbook.

Thm: Let M_1, M_2 $_R$, $_R N_1$, $_R N_2$. Then we have the following isomorphism of Ab. gps:
① $(M_1 \oplus M_2) \otimes_R N_1 \cong (M_1 \otimes_R N_1) \oplus (M_2 \otimes_R N_1)$.
② $M_1 \otimes_R (N_1 \oplus N_2) \cong (M_1 \otimes_R N_1) \oplus (M_1 \otimes_R N_2)$

Pf sketch: of ①: to map to a direct sum, we just need to define the map component wise. This is done by having a R-balanced map to the first comp. (verify).

Date No.

Eg ① Let $R=\mathbb{R}$. Let $M_1=\mathbb{R}^3=\mathbb{R}\oplus\mathbb{R}\oplus\mathbb{R}$.
$N_1=\mathbb{R}^3=$ ″

Then $M_1\otimes_{\mathbb{R}}N_1=(\mathbb{R}\oplus\mathbb{R}\oplus\mathbb{R})\otimes_{\mathbb{R}}(\mathbb{R}\oplus\mathbb{R}\oplus\mathbb{R})$
$=\bigoplus_{n=1}^{9}\mathbb{R}\otimes_{\mathbb{R}}\mathbb{R}\cong\bigoplus_{n=1}^{9}\mathbb{R}\cong\mathbb{R}^9$.

② Recall $\mathbb{C}$ is a 2-dim $\mathbb{R}$-vectorspace. Then.
$\mathbb{C}\otimes_{\mathbb{R}}\mathbb{C}=\mathbb{R}^2\otimes_{\mathbb{R}}\mathbb{R}^2\cong\mathbb{R}^{2\times2}=\mathbb{R}^4$.
But $\mathbb{C}\otimes_{\mathbb{C}}\mathbb{C}=\mathbb{C}$.

Pf: we consider the $\mathbb{C}$ bilinear map,
- $\mathbb{C}\times\mathbb{C}\to\mathbb{C}$
$(a,b)\mapsto a\cdot b$ then this induces
- $\mathbb{C}\otimes_{\mathbb{C}}\mathbb{C}\to\mathbb{C}$
$a\otimes_{\mathbb{C}}b\mapsto a\cdot b$.

$\mathbb{C}$-
we claim $\mathbb{C}\otimes_{\mathbb{C}}\mathbb{C}$ is spanned by $1\otimes1$.
$a\otimes b=1\otimes ab\cdot1=ab(1\otimes1)$. □

Free gp!

Defn ① Free group of $\{a,b\}$, $F(a,b)$, is the words formed by a,b, that is, words by the alphabets $\{a,b,a^{-1},b^{-1}\}$.

② $\{a,b\}\to F_2$
$\searrow G\swarrow$
$R\subseteq M$, $R^n\to M$.
$e_i\mapsto m_i$.

③ every group is a quotient of some free group (?).

$S=\{\text{generators}\}\to F_S$
generates ↘ ↙ quotient out relations that define G
G

④ $\mathbb{Z}\cap C F_2$. (?).