3201 Commutative Algebra Notes

Based on the 2011 autumn lectures by Dr J López Peña

Chapter I: Revision on Rings

Examples of Rings

i) $\mathbb{Q}$
ii) $\mathbb{R}$
iii) $\mathbb{C}$
iv) $\mathbb{Z}$
v) $\mathbb{C}[x]$
vi) $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$
vii) $M_n(\mathbb{R})$ - restrict to square matrices to allow for multiplication

$+$
$\cdot$
0
1

Defn 1.1

A ring, R, is a (non-empty) set with two operations:

$+ : R \times R \longrightarrow R$ (addition)
$\cdot : R \times R \longrightarrow R$ (multiplication)

s.t

* $(R, +)$ abelian group
A1: associativity - $(a+b)+c = a+(b+c) \quad \forall a,b,c \in R$
A2: Zero - $\exists\, 0 \in R : a+0 = a = 0+a \quad \forall a \in R$
A3: Additive inverses - $\forall a \in R \ \exists\, b \in R : a+b = 0 = b+a$

We can easily show b is the unique inverse and $b = -a$
Assume b is not unique and c is also an inverse.
Then $a+b=0$ and $a+c=0 \Rightarrow a+b = a+c$
$\Rightarrow b = c$
$\therefore b$ is unique inverse and $a+b=0 \Rightarrow b=-a$

* $(R, \cdot)$ is a monoid
M1 Associativity - $(a\cdot b)\cdot c = a\cdot(b\cdot c) \quad \forall a,b,c \in R$

$M2$: Identity - $\exists\, 1 \in R$ s.t $a \cdot 1 = a = 1 \cdot a \quad \forall a \in R$

Plus

D: Distributive - $(a+b) \cdot c = a \cdot c + b \cdot c$

$a \cdot (b+c) = a \cdot b + a \cdot c$

If a ring, R, ~~then~~ satisfies:

true for all earlier ex. except $M_n(R)$

* $M3$: Commutivity - $ab = ba \quad \forall a, b \in R$

then we say that R is a commutative ring, which is what we will be studying.

* $M4$: Inverses - $\forall a \in R$, $a \neq 0$ $\exists\, b \in R$ s.t $ab = 1 = ba$

then we say that R is a division ring.

If $M3$ and $M4$ are satisfied, we say that R is a field.

Examples

① $R = \{0\}$ trivial ring

$0 + 0 = 0$, $0 = 1$

$0 \cdot 0 = 0$

We will never work with this ring. It is the only ring with $0 = 1$, all the rings we will be interested in will have $0 \neq 1$

② Polynomials in two variables

$\mathbb{R}[x,y] = a_{00} + a_{10}x + a_{01}y + a_{11}xy + \dots + a_{nm}x^n y^n \,/\, a_{ij} \in \mathbb{R}\}$

R ring $\Rightarrow R[x] = \{a_0 + a_1 x + \dots + a_n x^n \,/\, a_i \in R\}$ ring

$(\mathbb{R}[x])[y] = \mathbb{R}[x,y]$ $\quad\quad$ $[\,R[x,y,z] = (R[x,y])[z]\,]$

③ Polynomials in n-variables

$\mathbb{R}[x_1, x_2, \dots, x_n]$

④ <u>Notation</u>: stop using $\mathbb{Z}_n$, we now use:
$\mathbb{Z}/(n)$ or $\mathbb{Z}/n\mathbb{Z}$, integers (mod n)

⑤ p-adic integers, $\mathbb{Z}_p$ where p prime.

$$\mathbb{Z}_p = \left\{ \frac{a}{b} \,\middle|\, a, b \in \mathbb{Z} \;, p \nmid b \right\}$$

<u>e.g</u> $\mathbb{Z}_2 = \left\{ \frac{1}{3}, \frac{1}{5}, \frac{1}{7}, \frac{2}{15}, \dots \right\}$

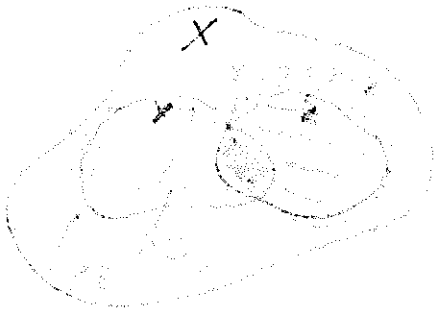
the reason this is nice is because, when multiplying a/b and c/d, where $p \nmid b$, $p \nmid d$, then $p \nmid bd$
and $\frac{a}{b} + \frac{c}{d} = \frac{ab+bc}{bd}$, $p \nmid bd$

⑥ Power set ring

X (non-empty) set

$P(X) = \{ Y \mid Y \subseteq X \}$ $\quad\quad$ set of all subsets

$Y + Z = Y \underset{\substack{\uparrow \\ \text{symmetric} \\ \text{difference}}}{\triangle} Z = (Y \cup Z) \setminus (Y \cap Z)$



$Y \cdot Z = Y \cap Z$

$\Rightarrow (P(X), \Delta, \cap)$ is a ring

valid subset

$0 = \phi$

$1 = X$

N.B: whenever we encounter a new def^n, we should check them with the examples here

⑦ Endomorphisms rings (operator rings)

V vector space $(/k)$

$End(V) = \{f : V \longrightarrow V \mid f \text{ linear map}\}$

$f, g \in End(V)$

$f + g : V \longrightarrow V$

$\quad : v \longmapsto (f+g)(v) = f(v) + g(v)$ Pointwise addition

addition in $End(V)$ — two different additions — addition in v.s V

N.B: add or multiply a linear map and get a linear map

$f \cdot g := f \circ g : V \longrightarrow V$

$v \longmapsto (f \circ g)(v) = f(g(v))$ non-commutative

N.B: Composition of a linear map is a linear map

$(End(V), +, 0)$ ring

⑧ $C(\mathbb{R}) = \{f : \mathbb{R} \longrightarrow \mathbb{R} \mid f \text{ continuous}\}$

$(f+g)(x) = f(x) + g(x)$

add of function — add of real numbers

commutative

$(fg)(x) = f(x)g(x) = g(x)f(x) = (gf)(x)$

$0(x) = 0$
$1(x) = 1$

<u>Question</u> Is $(C(x), +, \circ)$ a ring? Need to check distributivity.

$$(f+g)\circ h \stackrel{?}{=} f\circ h + g\circ h$$

<u>Counter example</u>

$f(x) = 1$
$g(x) = 2$
$h(x) = 3$

$$((f+g)\circ h)(x) = (f+g)(h(x)) = (f+g)(3) = f(3) + g(3) = 1 + 2 = 3$$

Now, $(f\circ h)(x) + (g\circ h)(x) = f(h(x)) + g(h(x)) = f(3) + g(3) = 1 + 2 = 3$

So it works, try another set.

$f(x) = \sin(x)$
$g(x) = x$
$h(x) = 3x$

$$(f+g)(h(x)) = (f+g)(3x) = f(3x) + g(3x) = \sin 3x + 3x$$

$$(f\circ h)(x) + (g\circ h)(x) = f(3x) + g(3x) = \sin 3x + 3x$$

Again, appears to work!

Try $f\circ(g+h)(x) = f(g(x) + h(x)) = f(x + 3x) = f(4x) = \sin(4x)$

$\neq$

$(f\circ g + f\circ h)(x) = f(x) + f(3x) = \sin x + \sin 3x$

different $\Rightarrow$ $(C(x), +, \circ)$ is not a ring, it fails the distributive condition

(9) X (non-empty) set, R any ring

take set $R^X = \{ f : X \longrightarrow R \}$

$(f+g)(x) = f(x) + g(x)$
$(fg)(x) = f(x)g(x)$

why can we do this? Because we have addition in R and can mult as R ring.

Is R^X commutative? Only if R commutative!

(10) Quaternion ring, $\mathbb{H} = \{ a + bi + cj + dk \mid a,b,c,d \in \mathbb{R} \}$

$i \to j \to k \to i$

$i^2 = -1$	$ij = k$	$ji = -k$
$j^2 = -1$	$jk = -i$	$kj = -i$
$k^2 = -1$	$ki = j$	$ik = -j$

$0 = 0 + 0i + 0j + 0k$
$x = a + bi + cj + dk \neq 0$ $\quad x^{-1} = ?$ Use a trick!

We know $\quad z = a + bi$
$\bar{z} = a - bi$
$z\bar{z} = a^2 + b^2 = |z|^2 \in \mathbb{R}$
$$\frac{z\,\bar{z}}{|z|^2} = 1$$
$\frac{\bar{z}}{|z|^2} = z^{-1}$

$\bar{x} = a - bi - cj - dk$
we know $|x|^2 = a^2 + b^2 + c^2 + d^2$
$= x\bar{x}$

So, $x^{-1} = \dfrac{\bar{x}}{|x|^2}$

(11) Quaternion Algebras

$\mathbb{Q}$

$\alpha, \beta \in \mathbb{Q}$

$${}^{\alpha}\mathbb{Q}^{\beta} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{Q}\}$$

$$\left.\begin{array}{ll} i^2 = \alpha & ij = k \\ j^2 = \beta & ji = -k \end{array}\right\} \Rightarrow ji = -ij$$

$$k^2 = (ij)^2 = ij\,ij$$
$$= -\alpha\beta$$

${}^{\alpha}\mathbb{Q}^{\beta}$ is a <u>division ring</u>

(12) Formal Power Series

$$\mathbb{R}[[x]] = \{a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n + \dots \mid a_i \in \mathbb{R}\}$$
$$= \{\sum_{n \geq 0} a_n x^n \mid a_n \in \mathbb{R}\}$$

(13) Group rings

G finite group, $\mathbb{Z}$ integers

$$\mathbb{Z}[G] = \{\sum_{g \in G} a_g \cdot g \mid a_g \in \mathbb{Z}\}$$

e.g $G = C_2 = \{e, \sigma \mid \sigma^2 = e\}$

$$\mathbb{Z}[G] = \{ae + b\sigma \mid a, b \in \mathbb{Z}\}$$

$$(\underset{\in\mathbb{Z}}{a} \cdot \overset{\in G}{g}) \cdot (\underset{\in\mathbb{Z}}{b} \cdot \overset{\in G}{h}) = (ab)(\underset{\in G}{gh})$$

Returning to example

$$(2e+3\sigma)(-e-\sigma) = 2e(-e) + 2e(-\sigma) + 3\sigma(-e) + 3\sigma(-\sigma)$$
$$= -2e - 2\sigma - 3\sigma - 3e$$
$$= -5e - 5\sigma$$

$R[G]$ for any R ring

If $\left.\begin{array}{l} R \text{ commutative} \\ G \text{ abelian} \end{array}\right\}$ $R[G]$ commutative

$R = \mathbb{R}$, $G = C_2 = \{e, \sigma\}$

$\mathbb{R}[G] = \{ae + b\sigma \mid a, b \in \mathbb{R}\}$

$1_{R[G]} = 1 \cdot e$

$\sigma \in \mathbb{R}[G]$ $\quad \sigma \cdot \sigma = e = 1e$

$7 \in \mathbb{R}[G]$ $\quad 7 = 7 \cdot e$, $7^{-1} = \frac{1}{7} e$

$(1+\sigma)^{-1} = ?$ No!

Assume $\exists\, (1+\sigma)^{-1}$

Then $\quad 1 = (1+\sigma)(a+b\sigma) = a + b\sigma + a\sigma + b\sigma^2$

$\Rightarrow (a+b) + (a+b)\sigma = 1$

$\Rightarrow a+b = 1$ and $a+b = 0$

$\Rightarrow 1 = 0$ ✗

$\therefore$ there is no inverse

If $y(1+\sigma) = 1$

$y(1+\sigma)(1-\sigma) = y \cdot 0$

$(1-\sigma) = 0$

G group, R ring

$R[G] = \{\underbrace{\sum_{g \in G} a_g \cdot g}_{x} \mid a_g \in R\}$, $x = \sum_{g \in G} a_g \cdot g$

$= \{f : G \to R\}$

$f_x : G \to R$
$g \to a_g$

$\varphi, \psi : G \to R$

$f : G \to R$
$x_f := \sum_{g \in G} f(g) \cdot g$

$(\varphi + \psi)(g) = \varphi(g) + \psi(g)$
$(\varphi \cdot \psi)(g) = \varphi(g)\psi(g)$? No! Works but has a different ring structure to what we want

$(\varphi * \psi)(g) = \sum_{h \in G} \varphi(h)\psi(h^{-1}g)$ | convolution product

$R[G]$
$x \rightsquigarrow f_x$
$y \rightsquigarrow f_y$
can take $xy \rightsquigarrow f_{xy} = f_x * f_y$

<u>Direct Product of Rings</u>

R, S rings

$R \times S = \{(r,s) \mid r \in R, s \in S\}$

$(r_1, s_1) + (r_2, s_2) := (r_1 + r_2, s_1 + s_2)$
$(r_1, s_1)(r_2, s_2) := (r_1 r_2, s_1 s_2)$

$(R \times S, +, \cdot)$ is a ring

When studying groups we want to know what is going on in the group, subgroups etc. This is analogous.

Subring, Ideals and Quotient Rings

Def^n 1.2

R ring
$S \subseteq R$ is a subring if:

$$\forall s, t \in S \Rightarrow \begin{array}{l} s.t \in S \\ s + t \in S \\ -s \in S \\ 0 \in S \\ 1 \in S \end{array}$$

Or, more formally:

S is a subring if:

i) $(S, +)$ is a subgroup of $(R, +)$
ii) $(S, \cdot)$ is a submonoid of $(R, \cdot)$

$S \leq R$

A subgroup is normal when left and right cosets are equal. We are dealing with additive subgroup, which is commutative, so all subgroups are normal.

Subrings are interesting, but not for quotients.

<u>Examples</u>

$$\begin{array}{ccccccc}
 & & \mathbb{Z}_p & & & & \\
 & \subseteq & \cap & & & & \\
\mathbb{Z} & \subseteq & \mathbb{Q} & \subseteq & \mathbb{R} & \subseteq & \mathbb{C} \\
\cap & & \cap & & \cap & & \cap \\
\mathbb{Z}[x] & \subseteq & \mathbb{Q}[x] & \subseteq & \mathbb{R}[x] & \subseteq & \mathbb{C}[x] \\
\cap & & & & & & \\
\mathbb{Z}[x,y] & \subseteq & \cdots & & & &
\end{array}$$

$R[C_3] \subseteq R[D_6]$ As C_3 is subgroup of D_6. This works

$$\mathbb{R} \qquad M_2(\mathbb{R})$$

$$x \longmapsto \begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix}$$

$$1 \longmapsto \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

So, we need to use diagonal matrices

$$x \longmapsto \begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix}$$

$$\mathbb{R} \longrightarrow \mathrm{Diag}_2(\mathbb{R}) \subseteq M_2(\mathbb{R})$$

set of all upper triangular 2×2 matrix

$$U_2(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \;\middle|\; a, b, c \in \mathbb{R} \right\}$$

$$\begin{array}{c} \cap \\ M_2(\mathbb{R}) \\ \cup \\ L_2(\mathbb{R}) \end{array}$$

↑lower triangle

More examples

If $S_i \subseteq R$ subring $\forall i \in I$

$\Rightarrow \bigcap_{i \in I} S_i \subseteq R$ subring

If $S, T \subseteq R$ subring
$\Rightarrow S \cap T \subseteq R$

If $X \subseteq R$ any subset
we can consider the family

$\emptyset \neq \{S \mid S \subseteq R, X \subseteq S\}$ the ring itself is part of it

$\bigcap_{\substack{S \subseteq R \\ X \subseteq S}} S \subseteq R$

$X \subseteq T = \langle X \rangle$ subring generated by X

$\langle X \rangle$ is the smallest subring of R that contains X

Ideals

R commutative ring
an ideal of R is a subset $I \subseteq R$
s.t
I1: $(I, +)$ is a subgroup of $(R, +)$
I2: Absorbency which says
$\forall x \in I, \forall r \in R \Rightarrow r \cdot x \in I$

Notation: $I \trianglelefteq R \equiv$ Ideal of R

Examples

① If $1 \in I \Rightarrow I = R$
as $\forall r \in R$, $r \cdot 1 \in I$
$R \trianglelefteq R$ and only ideal containing unit

② $0 = \{0\} \trianglelefteq R$ Zero ideal

③ $2\mathbb{Z} = \{0, \pm 2, \pm 4, \pm 6, \dots\} \trianglelefteq \mathbb{Z}$

0 must be there for it to be additive subgroup

$3\mathbb{Z}, \dots, n\mathbb{Z} \trianglelefteq \mathbb{Z}$

④ $\mathbb{R}[x]$
$I = \{a_1 x + a_2 x^2 + \dots + a_n x^n \mid a_i \in \mathbb{R}\}$
$= \{x \cdot g(x) \mid g \in \mathbb{R}[x]\}$

$I \trianglelefteq \mathbb{R}[x]$

If R ring, $a \in R$ $\quad I = (a) = \{ar \mid r \in R\}$
$0 \in I$ as $a \cdot 0 = 0$ $\quad s \in R$
$as + ar = a(s+r)$ so additive subgroup
$s(ar) = sar = asr \in a$
$\Rightarrow (a) \trianglelefteq R$
$(a) \equiv$ principal ideal generated by a

Recap

i) $I \leq (R, +)$ additive subgroup
($0 \in I$, $a, b \in I \Rightarrow a + b \in I$
$a \in I \Rightarrow -a \in I$)

ii) (Absorbancy) $\forall x \in I, \forall r \in R \Rightarrow rx \in I$

$I \trianglelefteq R$ Ideal

More examples

i) $R = (1)$ total ideal

$I \trianglelefteq R$, I is a proper ideal

ii) $a_1, \dots, a_n \in R \Rightarrow (a_1, \dots, a_n) = \{r_1 a_1 + \dots + r_n a_n \mid r_i \in R\} \trianglelefteq R$

$(a_1, \dots, a_n) \equiv$ Ideal generated by $a_1, \dots, a_n$

- **Intersection of Ideals**

$$I, J \trianglelefteq R \Rightarrow I \cap J \trianglelefteq R \text{ Ideal}$$

Biggest Ideal contained in both I and J

$I \cup J$ is not an ideal

e.g. $R = \mathbb{Z}$

$I = (2) = \{2n \mid n \in \mathbb{Z}\}$

$J = (3) = \{3n \mid n \in \mathbb{Z}\}$

$I \cup J = \{0, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 9, \dots\}$

closed for addition? No!

$2 + 3 = 5$ and $5 \notin I \cup J$

hence, not an ideal

- **Sum of Ideals**

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

Smallest Ideal ~~contained~~ containing both I and J

$$\begin{tikzcd}
 & I+J \arrow[dl] \arrow[dr] & \\
I & & J \\
 & I \cap J \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

$I + J$ ← tells us any other ideal ~~containing~~ containing I and J must also contain $I + J$

$I \cap J$ ← tells us any other ideal contained in I and J must be contained in $I \cap J$

R (commutative) ring, $I \trianglelefteq R$, ideal
$a \in R$, we define the coset of a wrt I as

$$a + I \ (= \bar{a}) = \{a + x \mid x \in I\}$$

only if $a \in I$ as we need $(-a)$ to exist to give us a 0.

Q: When do we have $a + I \subseteq b + I$?

$$a \in a + I \subseteq b + I \Rightarrow a = b + x \quad \text{for some } x \in I$$
$$a - b = x \in I$$
$$b - a = -x \in I$$
$$b = a + \underbrace{(-x)}_{I} \in a + I$$

$a + I \subseteq b + I \iff a + I = b + I$
and that happens when their difference is an element on the ideal

! $a + I = b + I \iff b - a \in I$!

Define $R/I = \{a + I \mid a \in R\}$

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

$(R/I, +)$ additive group

$+$ well defined?

$a + I = a' + I \iff a - a' \in I$
$b + I = b' + I \iff b - b' \in I$

$$(a+b)+I \overset{?}{=} (a'+b')+I$$

Well, look at

$$(a+b)-(a'+b') \overset{?}{\in} I$$

$$\begin{aligned}(a+b)-(a'+b') &= a+b-a'-b' \\ &= \underbrace{(a-a')}_{\in I} + \underbrace{(b-b')}_{\in I} \in I\end{aligned}$$

$$\therefore (a+b)+I = (a'+b')+I$$

Exercise: $(R/I, +)$ is the quotient subgroup of $(R,+)$ by $(I,+)$

Now define $(a+I)(b+I) := ab+I$

i) Well defined? $ab+I \overset{?}{=} a'b'+I \iff ab-a'b' \overset{?}{\in} I$

$$\begin{aligned}ab-a'b' &= ab-a'b+a'b-a'b' \\ &= \underbrace{\underbrace{(a-a')}_{\in I}b}_{\in I} + \underbrace{a'\underbrace{(b-b')}_{\in I}}_{\in I} \in I\end{aligned}$$

absorbing

$\Rightarrow$ product is well defined.

<u>Claim</u>: R/I is a ~~commutative~~ ring called the quotient of R by I

$1_{R/I} = 1+I$

<u>Examples</u>

i) $I=(0) \Rightarrow R/0 = R$

ii) $I = R \Rightarrow R/R = 0$

$\{a+R \mid a \in R\}$ $\quad a+R = b+R$

$\iff a-b \in R$

$1+R = 0+R$

iii) $R = \mathbb{Z}$, $I = (2) = 2\mathbb{Z}$

$\mathbb{Z}/(2) = \{a + (2) \mid a \in \mathbb{Z}\}$

$0 + (2)$ $\quad\quad 0 + (2) \overset{?}{=} 1 + (2)$ No, as $1 - 0 \notin (2)$

$1 + (2)$

$1 + (2) \neq 2 + (2) = 0 + (2)$

So, $\mathbb{Z}/(2) = (n \bmod 2) + (2)$

$\mathbb{Z}/(2) = \{\bar{0}, \bar{1}\}$

iv) $R = \mathbb{R}[x]$

$I = (x) = \{xg \mid g \in \mathbb{R}[x]\}$

$= \{a_1 x^1 + a_2 x^2 + \ldots + a_n x^n \mid a^i \in \mathbb{R}\}$

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

e.g.

$f(x) = 2 + \frac{1}{3}x + 5x^2 + 13x^4$ $\quad\quad f(x) + (x) \overset{?}{=} 2 + (x)$

$f(x) = a_0 + a_1 x + \ldots + a_1 x^n$

$f(x) + (x) = a_0 + (x)$

$\left.\begin{array}{l} f(x) = a_0 + \ldots + a_n x^n \\ g(x) = b_0 + \ldots + b_m x^m \end{array}\right\} \Rightarrow \begin{array}{l} f + g = (a_0 + b_0) + \ldots \\ fg = a_0 b_0 + \ldots \end{array}$

$\Rightarrow \mathbb{R}[x]/(x) = \mathbb{R}$

—

$R = \mathbb{R}[x]$

$I = (x^2 + 1) = \{(x^2+1) f(x) \mid f \in \mathbb{R}[x]\}$

$f(x) = a_0 + a_1 x + \cdots + a_n x^n \Rightarrow f(x) = (x^2+1) q(x) + r(x)$

$\deg(r(x)) < \deg(x^2+1) = 2 \Rightarrow r(x) = c_0 + c_1 x$ at most

$f(x) + (x^2+1) = r(x) + q(x)(x^2+1) + (x^2+1) = r(x) + (x^2+1)$

$\mathbb{R}[x]/_{x^2+1} = \{\overline{c_0 + c_1 x}\}$

$1 = \bar{1}$ $\qquad \bar{x} \cdot \bar{x} = \overline{x^2}$

$i = \bar{x}$ $\qquad = \overline{x^2+1-1} = \underbrace{\overline{x^2+1}}_{=0} - \bar{1} = -\bar{1}$

$\mathbb{R}[x]/_{x^2+1} = \{\overline{c_0 + c_1 x}\} = \{a + bi \mid a, b \in \mathbb{R}\}$

$\Rightarrow \mathbb{R}[x]/(x^2+1) = \mathbb{C}$

Examples

Is there any polynomial $f(x)$ s.t
$\mathbb{R}[x]/_{(f(x))} = \mathbb{H}$?

$\mathbb{R}[x, y, z]/(f, g, h, \dots) \neq \mathbb{H}$ Why? Our ring is commutative whereas $\mathbb{H}$ is not commutative

R comm $I \trianglelefteq R \Rightarrow R/I$ comm

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

Ring homomorphism

R, S rings (not necessarily commutative).
We say that a map $f : R \to S$ is a ring homomorphism if:

1. $f : (R, +) \longrightarrow (S, +)$ group homomorphism
   - i. $f(0) = 0$
   - ii. $f(a+b) = f(a) + f(b)$, $\forall a, b \in R$
   - iii. $f(-a) = -f(a)$, $\forall a \in R$
2. $f : (R, \cdot) \longrightarrow (S, \cdot)$ is a homomorphism of monoids
   - i. $f(1) = 1$

ii/ $f(ab) = f(a)f(b)$, $\forall a, b \in R$

<u>Examples</u>

1/ $Id : R \to R$ ring homomorphism.

2/ $0 : R \to S$ Not a ring homomorphism. Why?

$R \mapsto 0$ $\quad f(1) \neq 1$ i.e. $1 \not\mapsto 1$

complicated → 3/ $\mathbb{R}[x] \longrightarrow \mathbb{C}$ $\qquad f(x) = q(x)(x^2+1) + r(x)$

$f(x) \longmapsto a+bi$ $\qquad$ where $a + bx = r(x)$

4/ $\mathbb{R}[x] \longrightarrow \mathbb{R}$

$f(x) \longmapsto a_0 + \dots + a_n$

group homomorphism? Yes

product? $\quad (x+1)(x+1) = x^2+2x+1$

$$\begin{array}{ccc} (x+1) & (x+1) & x^2+2x+1 \\ \downarrow & \downarrow & \downarrow \\ 2 & 2 & 4 \end{array}$$

So far, so good

$$\begin{array}{ccc} (x-2) & (x+2) & = x^2-4 \\ \downarrow & \downarrow & \downarrow \\ -1 & 3 & -3 \end{array}$$

Shouldn't work, check it out to see if it does or not.

5/ $\mathbb{R}[x] \longrightarrow \mathbb{R}$ $\qquad$ ring homomorphism

$f(x) \longmapsto f(0)$

6/ $ev_a : \mathbb{R}[x] \longrightarrow \mathbb{R}$

evaluation $\quad f(x) \longmapsto f(a)$

constant polynomial

$ev_a(1) = 1(a) = 1$

$ev_a(0) = 0$

$ev_a(f+g) = (f+g)(a) = f(a) + g(a) = ev_a f + ev_a(g)$

$ev_a(fg) = (fg)(a) = f(a)g(a) = (ev_a f)(ev_a g)$

Def^n 1.5 (Image and kernel)

$f: R \to S$ ring homomorphism.

$Im\, f := \{ f(r) \mid r \in R \} \subseteq S$

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

Lemma 1.1

$Im\, f \leq S$ Subring

$\ker f \trianglelefteq R$ Ideal

Proof

Exercise

Lemma 1.2

$f: R \to S$ is injective $\iff \ker f = 0$

$f: R \to S$ is surjective $\iff Im\, f = S$

Proof

Exercise

Reminder

Def^n 1.6

$f: A \to B$

f is surjective when, for each $b \in B$ $\exists a \in A$ s.t $f(a) = b$

i.e. $\forall b \in B$ $\exists a \in A : f(a) = b$

f is injective when, for each $a \in A$ and $a' \in A$ with $f(a) = f(a')$

$\Rightarrow a = a'$, i.e. $\forall a, a' \in A$ s.t $f(a) = f(a') \Rightarrow a = a'$

f injective := monomorphism

surjective := epimorphism

bijective := isomorphism

Theorem 1.1 (First Isomorphism theorem) If $f: R \to S$ is a ring homomorphism, then there is a ring isomorphism

$$\varphi : R/_{\ker f} \xrightarrow{\sim} \operatorname{Im} f$$

given by $\varphi(r + \ker f) = f(r)$

Proof Need to show:
1/ φ well defined
2/ φ injective
3/ φ surjective
4/ ring homomorphism

1/ $r + \ker f = r' + \ker f \Rightarrow r - r' \in \ker f$

$\Rightarrow f(r-r') = 0 \Rightarrow f(r) - f(r') = 0$
$\Rightarrow f(r) = f(r')$
$\varphi(r + \ker f) = \varphi(r' + \ker f)$

$\therefore$ well defined
QED(1)

2/ assume $\varphi(r + \ker f) = \varphi(s + \ker f)$ $\qquad \varphi : R/_{\ker f} \to \operatorname{Im} f$
i.e. $f(r) = f(s)$

$\Rightarrow f(r) - f(s) = 0$
$\Rightarrow f(r-s) = 0$
$\Rightarrow r - s \in \ker f$
$\Rightarrow r + \ker f = s + \ker f$
$\therefore \varphi$ injective
QED(2)

3/ $y \in \operatorname{Im} f \implies \exists\, r \in R$ s.t. $y = f(r)$
$\implies y = \varphi(r + \ker f)$
$\implies \varphi$ surjective

QED(3)

4/ $\varphi(0 + \ker f) = f(0) = 0$

$$\begin{aligned}\varphi((r+\ker f) + (s + \ker f)) &= \varphi((r+s) + \ker f) \\ &= f(r+s) \\ &= f(r) + f(s) \\ &= \varphi(r + \ker f) + \varphi(s + \ker f)\end{aligned}$$

$$\begin{aligned}\varphi(-(r + \ker f)) = \varphi(-r + \ker f) = f(-r) &= -f(r) \\ &= -\varphi(r + \ker f)\end{aligned}$$

$\therefore \varphi$ is a group homomorphism

$\varphi(1 + \ker f) = f(1) = 1$

$$\begin{aligned}\varphi((r+\ker f)(s+\ker f)) &= \varphi(rs + \ker f) \\ &= f(rs) \\ &= f(r)f(s) \\ &= \varphi(r + \ker f)\varphi(s + \ker f)\end{aligned}$$

$\therefore \varphi$ ring homomorphism

$\implies \varphi$ is an isomorphism

QED

Examples

1. $Id : R \to R$

$x \in \ker Id \implies Id(x) = 0$

$\ker(Id) = \{0\}$ ← can never be empty as homs always takes $0 \to 0$
$= (0)$

Id injective and surjective $\iff$ belongs to ker

$\operatorname{Im} Id = R$

$\therefore R/(0) \cong R$

23

2. <u>Canonical Projection</u>

R ring, $I \trianglelefteq R$ $\quad \pi_I : R \to R/I$

ring homomorphism $\quad r \mapsto \bar{r}$
$= r+I$

$\operatorname{Im} \pi_I = R/I$

$$\begin{aligned}\ker \pi_I &= \{ r \in R \mid \pi_I : \pi_I(r) = 0 \} \\ &= \{ r \in R \mid r + I = 0 \} \\ &= \{ r \in R \mid r \in I \} = I\end{aligned}$$

$R/I \cong R/I$

3. $ev_a : R[x] \longrightarrow R \quad , \quad a \in R$

$p(x) \longmapsto p(a)$

$b_0 + b_1 x + \dots + b_n x^n \longmapsto b_0 + b_1 a + b_2 a^2 + \dots + b_n a^n$

$r \in R \quad p(x) = r \Rightarrow r(a) = r$

$\Rightarrow \operatorname{Im} ev_a = R$

$\ker ev_a = \{ p(x) \in R \mid p(a) = 0 \}$

$= \{ p(x) \mid p(x) = (x-a) q(x) \}$

If $p(a) = 0 \Rightarrow (x-a) \mid p(x) \Rightarrow p(x) = (x-a) q(x)$

$\therefore \ker ev_a = \{ (x-a) q(x) \mid q(x) \in R[x] \}$

$= (x-a)$

$\overset{\text{1 IT}}{\Rightarrow} \quad R[x]/(x-a) \cong R$

<u>Lemma 1.3</u>

If $f : R \to S$
$g : S \to T$ $\quad$ | ring homomorphism

$\Rightarrow g \circ f : R \to T \quad$ ring homomorphism also

Proof

Exercise - essentially the same as proof that composition of linear maps is linear

Lemma 1.4

R ring, $I \trianglelefteq R$, $S \leq R$ subring

then:

1/ $S+I \leq R$ subring

2/ $I \trianglelefteq S+I$ Ideal

3/ $S \cap I \trianglelefteq S$ Ideal

Proof

1/ $S+I = \{s+i \mid s\in S, i \in I\}$

$0\in S,\ 0\in I \implies 0 = 0+0 \in S+I$

$(s+i)+(s'+i') = \underbrace{(s+s')}_{\in S} + \underbrace{(i+i')}_{\in I} \in S+I$

$-(s+i) = \underset{\in S}{-s} - \underset{\in I}{i} = -s+(-i) \in S+I$

$(R,+)$

$1 = \underset{\in S}{1} + \underset{\in I}{0} \in S+I$

$(s+i)(s'+i') = ss' + \underbrace{(\underset{\in I}{si'} + \underset{\in I}{is'} + \underset{\in I}{ii'})}_{\in I} \in S+I$

absorbency

$\implies S+I \leq R$

2/ Only need to check $I \leq S+I$
We know $I \trianglelefteq R$, $r \cdot i \in I \quad \forall r \in R, \forall i \in I$
So, absorbency already taken care of.

3/ $S \cap I \trianglelefteq S$

addition isn't a problem as we are intersecting two additive subgroups.

$x \in S \cap I \qquad \underset{\in S}{s}\underset{\in S}{x} \in S$

$s \in S \qquad \underset{\underset{\in R}{\in S}}{s}\underset{\in I}{x} \in I$

$\Big\} \; sx \in S \cap I \implies S \cap I \trianglelefteq S$

QED

Theorem 1.2 (Second Isomorphism Theorem)

R ring, $I \trianglelefteq R$, $S \leq R$

$$\implies \frac{S+I}{I} \cong \frac{S}{S \cap I}.$$

N.B. The previous lemma tells us this statement makes sense.

Proof
(Right now, the only tool we have to prove these are isomorphic is the 1IT)
So, we're trying to find a map

$$\varphi : S \xrightarrow[\iota]{\text{inclusion}} S+I \xrightarrow{\pi_I} \frac{S+I}{I}$$

$$s \longmapsto s+0=s \longmapsto \bar{s}$$

Ring homomorphism? Yes, composition of ring homomorphism
Need to show map is surjective, i.e. Im is itself

$\text{Im}\,\varphi = \underbrace{\{s+I \mid s \in S\}}_{\text{defn of quotient ring } S/I} = \dfrac{S+I}{I}$

generic coset, $s+i+I$
$\varphi(s) = s+I$
Are they equal? Check diff
$s+i-s \in I$
So, yes!

$\ker\varphi = \{s \in S \mid \varphi(s) = 0\}$
$= \{s \in S \mid s+I = 0\}$
$= \{s \in S \mid s \in I\} = S \cap I$

1^{st} IT
$\Rightarrow \dfrac{S}{\ker\varphi} \cong \dfrac{S+I}{I} = \text{Im}\,\varphi$

$\dfrac{S}{S\cap I} \cong \dfrac{S+I}{I}$

QED

Let us return to what we did with the image in that proof.

Defn of surjective, everything in $\dfrac{S+I}{I}$ is in S

$x \in \dfrac{S+I}{I} \Rightarrow x = y + I$ w/ $y \in S+I$

$\Rightarrow y = s+i$, $x = (\underset{s}{s}+i)+I$

$\varphi(s) = \bar{s} = s+I$

So, we check the difference $s+i-s = i \in I$

$\therefore s+I = x \Rightarrow x \in \text{Im}\,\varphi$ (cosets are equal)

Theorem 1.3 (Third Isomorphism Theorem)

R ring, $I \subseteq J \trianglelefteq R$ ideals
$(I \trianglelefteq R,\ J \trianglelefteq R)$

$\Rightarrow J/I \trianglelefteq R/I$ and moreover

$$\frac{R/I}{J/I} \cong R/J$$

Theorem 1.4 (Correspondence Theorem) (prob won't use this)

R ring, $I \trianglelefteq R$
there is a 1-1 correspondence

$$\{\text{ideals of } R/I\}$$
$$\updownarrow 1:1$$
$$\{J \trianglelefteq R \text{ s.t. } I \subseteq J\}$$

Chapter II : Integral Domains

Euclidean Domains and Unique Factorisation Domains

Domains

Defn 2.1 remember this notation

$a \in R^* = R \setminus \{0\}$ is a unit if $\exists b \in R$ s.t
$ab = 1$ ($a \in U(R)$)

a is a zero divisor if $\exists\ b \in R^*$ s.t $ab = 0$

N.B. In a field, any non-zero element is a unit

Defn 2.2

R is an Integral Domain (ID) if it has no zero divisors,

i.e. $a \neq 0, b \neq 0 \Rightarrow ab \neq 0$

equiv $ab = 0 \Rightarrow$ either $a = 0$ or $b = 0$

Propn 2.1 (Cancellation Law)

R ID $a, b, c \in R$ s.t

$$\left.\begin{array}{l} ab = ac \\ a \neq 0 \end{array}\right\} \Rightarrow b = c$$

We can always do this providing R has no zero divisors

Proof

$ab = ac \Rightarrow ab - ac = 0$
$a(b-c) = 0$

R ID $\Rightarrow$ if $ab = 0 \Rightarrow$ either $a = 0$ or $b = 0$

So, as $a \neq 0$ $b - c = 0$
$\Rightarrow b = c$ $\square$

2

Def^n 2.3

We say R is simple if the only ideals are 0 and R.

ex $\mathbb{F}$ field

Prop^n 2.2

R commutative ring, then R simple $\iff$ R field

Proof

$\Leftarrow$

If $I \trianglelefteq R$, $I \neq 0 \Rightarrow \exists\, a \in I$ s.t $a \neq 0$

$\Rightarrow 1 = a \cdot a^{-1} \in I \Rightarrow I = R$

as R field

$\Rightarrow$ R simple

$a \in R$ s.t $a \neq 0$

take $I = (a) \neq 0 \Rightarrow I = R \ni 1$

$\Rightarrow 1 \in (a)$

$\Rightarrow 1 = ab$ for some $b \in R$

$\Rightarrow a$ invertible $\Rightarrow R$ is a field $\square$

Def^n 2.4

An ideal $I \trianglelefteq R$ is a maximal ideal if $I \neq R$ and $\forall J \trianglelefteq R$ s.t $I \subseteq J \Rightarrow$ either $I = J$ or $J = R$

We could see some examples of maximal ideals but proving they are maximal is quite tricky. So, we will use the following:

Prop^n 2.3

$I \trianglelefteq R$ ideal, then I maximal $\iff$ R/I is a field

3.

Proof (Abstract version)

R/I field $\Leftrightarrow$ R/I simple

$\Leftrightarrow$ The only ideals of R/I are R/I or $0 = I/I$

$\overset{\text{correspondence Thm}}{\Leftrightarrow}$ The only ideals $J \trianglelefteq R$ s.t $I \subseteq J$ are $J = R$, $J = I$

$\Leftrightarrow$ I maximal $\square$

The key here is the correspondence theorem.

$$\{\text{ideals of } R/I\} \xleftrightarrow{1:1} \{\text{Ideals of } J \trianglelefteq R \text{ s.t } I \subseteq J\}$$

equiv. class

$\{\bar{r} \mid r \in R\}$
$=$
$K \trianglelefteq R/I$

$\left.\begin{matrix} J \trianglelefteq R \\ I \subseteq J \end{matrix}\right\} \Rightarrow J/I \overset{3IT}{\trianglelefteq} R/I$

can construct an ideal J s.t $K \subseteq J$

$$K = \{\bar{x}\} \longrightarrow J := \{x \in R \mid \bar{x} \in K\}$$

J ideal?

$x, y \in J$
$\bar{x}, \bar{y} \in K$ $\quad \left.\begin{matrix} \bar{x} + \bar{y} \in K \\ \parallel \\ \overline{x+y} \in K \end{matrix}\right\} \Rightarrow x + y \in J$

J closed for addition

$\left.\begin{matrix} x \in J \\ r \in R \end{matrix}\right\} \quad \left.\begin{matrix} \bar{x} \in K \\ \bar{r} \in R/I \end{matrix}\right\} \Rightarrow \begin{matrix} \bar{r} \cdot \bar{x} \in K \\ \parallel \\ \overline{rx} \end{matrix} \Rightarrow rx \in J$

$\Rightarrow J$ ideal

$I \subseteq J$?

$i \in I \Rightarrow \bar{i} = \bar{0} \in K \Rightarrow i \in J \Rightarrow I \subseteq J$

This is how the correspondence works

$\bar{i}$ means

$$\begin{array}{lcl} R \ni r & & R/I \\ \trianglerighteq & & \\ I & & \bar{r} = r + I \\ \ni i & \longrightarrow & \bar{i} = i + I \end{array}$$

$\underset{(\bar{0})}{0} \trianglelefteq R/I \rightsquigarrow \{x \in R \mid \underset{x+I}{\bar{x}} \in 0\} = I$

$R/I \trianglelefteq R/I \rightsquigarrow \{x \in R \mid \bar{x} \in R/I\} = R$

def^n of I being <u>maximal</u>

<u>Proof</u> (direct version)

$I \trianglelefteq R$

<u>$\Rightarrow$</u>

find an inverse for every non-zero element

Take $\bar{a} \in R/I$ s.t. $\bar{a} \neq 0$

$a \notin I$, take $J = I + (a) \trianglelefteq R$

$I \subseteq J \trianglelefteq R \Rightarrow \begin{cases} J = R & \text{as } I \text{ maximal} \\ \text{or } J = I & \end{cases}$

<u>but</u> $J \neq I$ as $a \in J$, $a \notin I$

so $J = R$

$\Rightarrow 1 = i + ra$ for some $r \in R$, $i \in I$

5

$\bar{1} = \overline{i + ra} = \underbrace{\bar{i}}_{0} + \bar{r}\bar{a} = \bar{r}\bar{a} \Rightarrow \bar{a}$ has an inverse

$\Rightarrow R/I$ is a field
QED($\Rightarrow$)

<u>$\Leftarrow$</u>

R/I field, take $J \trianglelefteq R$ s.t $I \subseteq J$
$I \subsetneq J$
↑ included but not the same

assume $J \neq I$

$\Rightarrow$ take $a \in J$ s.t $a \notin I$

$\Rightarrow \bar{a} \neq \bar{0} \Rightarrow \exists \bar{b} \in R/I$ s.t $\bar{a}\bar{b} = \bar{1}$

$\overline{ab} = \bar{1}$

$\Rightarrow ab - 1 = i \in I$

$\Leftrightarrow 1 = \underbrace{\underbrace{a}_{\in J} b}_{\in J \text{ absorbency}} - \underbrace{i}_{\in I \subseteq J \text{ as } I \subseteq J} \in J \Rightarrow J = R$

$\Rightarrow I$ maximal

<u>N.B.</u> Maximal ideals do not need to be unique, do not confuse maximal with maximum.

<u>Examples</u>

$R = \mathbb{Z}$ $\quad (2)$ maximal $\quad \mathbb{Z}/(2)$ field
$\quad (3)$ maximal $\quad \mathbb{Z}/(3)$ field

Next, we encounter prime ideals which are analogous to prime numbers.

Remember, $n \in \mathbb{Z}$ is prime if $\begin{cases} a \mid n \Rightarrow a = \pm 1 \text{ or } a = \pm n \\ a \mid bc \Rightarrow a \mid b \text{ or } a \mid c \end{cases}$

6

Defn 2.5

$I \trianglelefteq R$ and $I \neq R$, we say that I is a prime ideal if

$$ab \in I \Rightarrow a \in I \text{ or } b \in I$$

equiv $a, b \notin I \Rightarrow ab \notin I$

The converse is not true, if $a \in I$ and $ab \in I$, that is the absorbing property.

Propn 2.4

$I \trianglelefteq R$ ideal, then R/I is an ID $\Leftrightarrow$ I is prime

Proof

$\Rightarrow$

Let $a, b \in R$ s.t. $ab \in I$

$\Rightarrow \overline{ab} = \bar{0}$

$\Rightarrow \bar{a}\bar{b} = \bar{0}$

$\Rightarrow$ either $\bar{a} = 0$ or $\bar{b} = 0$

$\Rightarrow a \in I$ $\qquad$ $\Rightarrow b \in I$

$\Rightarrow I$ is prime

$\Leftarrow$

$\bar{a}\bar{b} = \bar{0}$

$\overline{ab} = \bar{0} \Rightarrow ab \in I \Rightarrow \begin{cases} a \in I \Rightarrow \bar{a} = \bar{0} \\ \text{or } b \in I \Rightarrow \bar{b} = \bar{0} \end{cases}$

$\Rightarrow R/I$ is an ID

$\square$

Corollary 2.1

$I \trianglelefteq R$ maximal $\Rightarrow I$ is prime $\quad (I \neq R)$

Proof

$I \trianglelefteq R$ maximal $\iff R/I$ field

$\Rightarrow R/I$ ID

$\Rightarrow I$ is prime $\square$

We can prove the previous prop^n directly, good exercise

Ideals and Divisibility

Def^n 2.6

R ring $a, b \in R$, we say that a divides b $(a|b)$

(i.e. b is a multiple of a)

i.e. b is divisible by a

if $\exists c \in R$ s.t $b = ac$

$a|b \iff b = ac \iff b \in (a) \iff (b) \subseteq (a)$

Def^n 2.7

We say that a and b are associates if $\exists u \in U(R)$ s.t $b = u \cdot a$ $(a \sim b)$

Example

$R = \mathbb{Z}$

$x \in \mathbb{Z}$ s.t $y \in \mathbb{Z}$ $xy = 1$

$\therefore U(\mathbb{Z}) = \{\pm 1\}$

$a = 5 \Rightarrow b \sim a \iff b \in \{\pm 5\}$

Prop^n 2.5

R ID, $a, b \in R$, then

1. $a \sim b \iff a | b$ and $b | a \iff (a) = (b)$
2. $a \sim 1 \iff a \in U(R) \iff (a) = R$
3. $a \sim 0 \iff a = 0 \iff (a) = 0$
4. $\sim$ is an equivalence relation

Proof

1.

$\Rightarrow$

$a \sim b \Rightarrow b = u \cdot a$ for $u \in U(R)$

$\hookrightarrow \exists v \in R$ s.t $uv = 1$, $v \in U(R)$

$\Rightarrow vb = vua = a$

$b = u \cdot a \Rightarrow a | b$

$a = vb \Rightarrow b | a$

$\Leftarrow$

$a | b \Rightarrow \exists c \in R$ s.t $b = ac$

$b | a \Rightarrow \exists d \in R$ s.t $a = bd$

$\Rightarrow a = acd$

$\Rightarrow 1 = cd$ — R ID $\Rightarrow$ cancellation property

if $a \neq 0$

$\therefore c, d \in U(R)$

$\therefore b = u \cdot a \Rightarrow a \sim b$

If $a = 0$

then $b = 0 \cdot u \Rightarrow b = 0$

and $0 = 1 \cdot 0 \Rightarrow a \sim b$

QED(1)

2. $a \sim 1 \iff a \in U(R)$

$\overset{\text{def}^n}{\Updownarrow}$

$1 = a \cdot u$ for $u \in U(R)$

$\Rightarrow a \in U(R)$

QED(2)

3. $a \sim 0 \iff a = 0$

$\Updownarrow$ $0 = a \cdot u$, $u \in U(R)$

$\Rightarrow a = 0$

as $u \neq 0$

QED(3)

4. $a \sim a \iff (a) = (a)$ which is true ✓

$a \sim b \Rightarrow b \sim a$?

$$\left.\begin{array}{l} a \sim b \Rightarrow (a) = (b) \\ b \sim a \Rightarrow (b) = (a) \end{array}\right\} \Rightarrow (a) = (b) = (b) = (a)$$

$\Rightarrow b \sim a$ ✓

$$\left.\begin{array}{l} a \sim b \\ b \sim c \end{array}\right\} \Rightarrow a \sim c? \qquad \left.\begin{array}{l} (b) = (c) \\ (a) = (b) \end{array}\right\} \Rightarrow (a) = (c) \Rightarrow a \sim c$$ ✓

QED

Examples

① $R = \mathbb{Z}$, $U(R) = \{\pm 1\}$

$n \sim m \iff n = \pm m$

② $R = \mathbb{Q}$, $U(\mathbb{Q}) = \mathbb{Q}^*$

$\{0\}$, $\{1\}$

$\overset{\shortparallel}{0}$ $\quad \underset{u \sim 1}{\uparrow} := T$

③ $R = \mathbb{Z}/n\mathbb{Z} \Rightarrow U(R) = \{a \in \mathbb{Z}/n\mathbb{Z}$ s.t $\gcd(a,n) = 1\}$

Q/ What are the equivalence classes of associates?
i.e. how many PIDs

Def^n 2.8

R ID, an element $a \in R^* \setminus U(R)$ is prime if whenever $a | bc \Rightarrow a | b$ or $a | c$

In terms of ideals,

$$bc \in (a)$$
$$\Rightarrow b \in (a) \quad \text{or} \quad c \in (a)$$

i.e. a is prime $\Leftrightarrow (a)$ is a prime ideal

we can also say. $(bc) \subseteq (a)$

Def^n 2.9

R ID, an element $a \in R^* \setminus U(R)$ is irreducible if it has no proper divisors, i.e. if $b | a \Rightarrow$ either $b \in U(R)$ or $b \sim a$

In terms of ideals,

a irreducible if whenever

$$(a) \subseteq (b) \Rightarrow \begin{cases} b \in U(R) \Rightarrow (b) = R \\ \text{or} \\ b \sim a \Rightarrow (a) = (b) \end{cases}$$

i.e. (a) is maximal among principal ideals

Examples

$\mathbb{Z}[x]$

$(2) \subseteq (f(x))$ $\qquad f | 2 \Rightarrow \deg(f) = 0 = f = a \in \mathbb{Z}$

$$\Rightarrow f = \pm 1, \pm 2, \Rightarrow (f) = \begin{cases} \mathbb{Z}[x] \\ (2) \end{cases}$$

$$\Rightarrow 2 \text{ irred}$$

$$\underset{\text{proper inclusion}}{(2) \subsetneq} (2, x) = \{2 \cdot f(x) + x \cdot g(x) \mid f, g \in \mathbb{Z}[x]\}$$

$$= \{2a_0 + a_1 x + \dots + a_n x^n\}$$

only even constant

$$2f(x) = 2b_0 + 2b_1 x + \dots + 2b_n x^n$$

every coefficient even

Prop^n 2.6

R ID, a prime $\Rightarrow$ a irreducible
$\not\Leftarrow$

Proof

Let $b|a \Rightarrow a = bc$ for some $c \in R$
$\Rightarrow a|bc \Rightarrow a|b \Rightarrow a \sim b$

not equal, only up to mult by a unit, could mult by ± 1 etc

or

$a|c \Rightarrow c = da$

$a = bc = bda$
$\Rightarrow 1 = bd$ ← working in ID
$\Rightarrow b \in U(R)$

$\Rightarrow$ a irreducible $\square$

We now try to prove converse for $\mathbb{Z}$ and see what we would need for rings for this to be true.

a irred $\quad a|bc \quad$ $a = p_1 \dots p_r$
$b = q_1 \dots q_s$
$c = q'_1 \dots q'_t$

Let p prime $p|a|bc$
$\Rightarrow p|b$ or $p|c$

this is what we cannot do for an arbitrary ring

as a irred, p must be a unit or associate to a,
but p prime $\Rightarrow p \sim a \Rightarrow a|b$ or $a|c$

This makes things quite difficult for us and so, we shall try to find conditions that allow us to consider the converse.

Defn 2.10

An ID R is a principal ideal domain (PID) if $\forall\ I \trianglelefteq R$ ideal $\exists a \in R$ s.t $I = (a)$

Examples

1. $\mathbb{Z} \trianglerighteq I$ $(\mathbb{Z}, +)$ infinite cyclic group $\Rightarrow I = (n)$ cyclic subgroup

2. $\mathbb{F} \trianglerighteq I \Rightarrow \begin{cases} I = \mathbb{F} = (1) \\ \text{or} \\ I = (0) \end{cases}$

When considering PIDs, think of the integers, they will be 'something' that behaves like the integers

Propn 2.7

R PID, $a \in R$ irred $\Rightarrow a$ is prime

Proof

a irred $\Rightarrow (a)$ maximal among principal ideals.

all ideals are principal

$\Rightarrow (a)$ maximal $\Rightarrow (a)$ prime

$\Rightarrow a$ prime $\square$

Corollary 2.2

In a PID prime $\Leftrightarrow$ irreducible

Corollary 2.3

$$\left.\begin{array}{l}\text{If } a \in R \text{ prime} \\ R \text{ PID}\end{array}\right\} \Rightarrow \underset{\substack{\uparrow \\ (a) \text{ maximal}}}{R/(a)} \text{ is a field}$$

N.B. $R/(a)$ where R ring and (a) maximal is always a field
alt: R PID, $I \trianglelefteq R$ prime ideal $\Rightarrow I$ is maximal

N.B. every PID is an ID (not the converse!)

$I \leqslant (\mathbb{Z}, +)$ ← cyclic
$m, n \in I$

$$\left.\begin{array}{l}(m) \subseteq \mathbb{Z} \\ (n) \subseteq \mathbb{Z}\end{array}\right\}$$

$$\underbrace{(m) + (n) = (\gcd(m,n))}_{d = mh + nk}$$

bezout's

we get this through Euclidean division. So, we are going to try and find a parallel with rings

$m = qn + r$ with integers
we know how to do this with polys with coefficients in a field also.
So,

$\underline{\mathbb{F}[x]}$

$$f(x) = g(x)n(x) + r(x) \qquad \deg(r) < \deg(n) \text{ or } r = 0$$

We know $\deg(f) \in \mathbb{N}$
$\deg(fg) = \deg(f) + \deg(g)$

on field, not 0

$$\deg(f) = 0 \iff f \in \mathbb{F}^* = U(\mathbb{F})$$

Euclidean Domains

Defⁿ 2.11

An ID R is a Euclidean Domain (ED) if it is endowed with a map

$$N : R^* \longrightarrow \mathbb{N} \qquad \text{(Euclidean norm)}$$

s.t

1. If $a \mid b \Rightarrow N(a) \leq N(b)$
2. $\forall a, b \in R$, $b \neq 0$, $\exists q, r \in R$ s.t $a = bq + r$ and either $r = 0$ or $N(r) < N(b)$

Examples

1. $\mathbb{F}[x]$ $\qquad N(f) = \deg f$
2. $\mathbb{Z}$ $\qquad N(a) = |a|$ ← In this case, N defined at 0 but this does not matter
3. $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ $\qquad$ Gaussian Integers

$$N(z) = z\bar{z} \quad , \; z = a + bi$$
$$= a^2 + b^2 \quad , \; \bar{z} = a - bi$$

do not use $\sqrt{\ }$ as we want N to map to $\mathbb{Z}$

Why is this a ED?
$(\mathbb{Z}[i], N)$ is a ED. Check!

(I) $(\mathbb{Z}[i], N)$ is an ID as we can suppose

$$\underset{\hat{a}}{(a+bi)}\underset{\hat{b}}{(c+di)} = 0 \qquad \text{for two elements } \hat{a}, \hat{b}$$

$\Rightarrow (ac - bd) + (ad + bc)i = 0$

$ac - bd = 0 \quad , \quad ad + bc = 0$

$a = \dfrac{bd}{c}$

$$\Rightarrow \left(\frac{bd}{c}\right)d + bc = 0$$

$$bd^2 + bc^2 = 0$$

$$b(d^2+c^2) = 0$$

$$b = 0 \quad \text{or} \quad d^2+c^2=0 \Rightarrow d, c = 0$$

$\therefore$ an ID.

Now,

(II) $z, w \in \mathbb{Z}[i]$, $z \mid w \Rightarrow w = z\epsilon$

$$\Rightarrow N(w) = N(z\epsilon) = z\epsilon(\overline{z\epsilon}) = z\epsilon\bar{z}\bar{\epsilon}$$

$$= z\bar{z}\epsilon\bar{\epsilon}$$

$$= \underbrace{N(z) N(\epsilon)}_{\mathbb{N}}$$

$$\therefore N(z) \mid N(w) \quad \Rightarrow \quad N(z) \le N(w)$$

N.B. In general, when we have a ring that is a subring of a field, it will be an ID

(III) $z, w \in \mathbb{Z}[i]$, $w \ne 0$

We can also see $\mathbb{Z}[i] \subseteq \mathbb{Q}[i]$
$\mathbb{Q}(i)$ is a field
$0 \ne a+bi \in \mathbb{Q}(i)$
$z \in \mathbb{Q}(i)$

$$z^{-1} = \frac{\bar{z}}{N(z)}$$

$N(z)$ — $\mathbb{N}$, $z\bar{z}$

$\mathbb{Q}(i)$ field , $w \in \mathbb{Q}[i]$
$\Rightarrow w^{-1} \in \mathbb{Q}(i)$

$$zw^{-1} = \underbrace{a + b}_{\text{rational}} i \in \mathbb{Q}(i)$$

Pick $u, v \in \mathbb{Z}$ s.t $|a-u| \le \frac{1}{2}$
$|b-v| \le \frac{1}{2}$

rational number and it is nearer to 3 or 4. So, distance is, at most, a half (which is when it lands directly in the middle)

$q = u + vi \in \mathbb{Z}[i]$

$s = zw^{-1} - q = (a-u) + (b-v)i \in \mathbb{Q}(i)$

$r = sw = (zw^{-1} - q)w$

$$= zw^{-1}w - qw$$

$$= \underbrace{z}_{\in\mathbb{Z}[i]} - \underbrace{q}_{\in\mathbb{Z}[i]}\underbrace{w}_{\in\mathbb{Z}[i]} \in \mathbb{Z}[i]$$

$$\Rightarrow \quad z = qw + r$$

Now,

$$N(r) = N(sw) = N(s)N(w)$$

and

$$N(s) = (a-u)^2 + (b-v)^2$$
$$\leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2} < 1$$

$$\Rightarrow N(r) \leq \frac{1}{2} N(w) < N(w)$$

and we are done

N.B. whereas, when dividing polys, q, r unique we have no uniqueness here.
e.g. take $a + bi = \frac{1}{2} + \frac{3}{4}i$ then $|\tfrac{1}{2} - u| \leq \tfrac{1}{2}$
$\Rightarrow u = 0$ or $u = 1$
$|\tfrac{3}{4} - v| \leq \tfrac{1}{2}$ $\quad v = 1$

N.B. Strictly speaking, we do not have uniqueness in $\mathbb{Z}$
as $a = 4$, $b = 7$ $\Rightarrow$ $7 = 4 \cdot 1 + 3$
or $7 = 4 \cdot 2 - 1$
but we can restrict ourselves to having $r > 0$. Same with polys. However, we cannot do this with rings, this is why there is no uniqueness

Propn 2.8
If R ID, $N: R^* \longrightarrow \mathbb{N}$ satisfying ED2
$\Rightarrow R$ is PID

<u>Proof</u> $I \trianglelefteq R$ ideal, $I \neq 0 \Rightarrow \exists a \in I$ s.t $a \neq 0$

Consider $\emptyset \neq \{N(a) \mid \underset{\neq 0}{a} \in I\} \subseteq \mathbb{N}$

pick $a \in I$, $a \neq 0$ s.t $N(a)$ minimal
For any $b \in I$, $b \neq 0$
$b = aq + r$ where $r = 0$
or $N(r) < N(a)$

$r = \underset{\in I}{b} - \underset{\in I}{\underbrace{aq}} \in I$

any other element in I is generated by a

but $N(a)$ is minimal, $\therefore r = 0 \Rightarrow b = aq$
$\Rightarrow I = (a)$ □

<u>Corollary 2.4</u>
$ED \Rightarrow PID$

(R, N) ED $\forall a \in R^*$, $a = 1 \cdot a$ so $1 \mid a$

$\overset{ED1}{\Rightarrow} N(1) \leq N(a) \Rightarrow 1$ is an element of R with minimal norm.

<u>Propn 2.9</u>
(R, N) ED, $u \in U(R) \Leftrightarrow N(u) = N(1)$

<u>Proof</u>
<u>$\Rightarrow$</u> $u \in U(R) \Rightarrow \exists v$ s.t $uv = 1 \Rightarrow u \mid 1$
$\Rightarrow \left. \begin{matrix} N(u) \leq N(1) \\ N(1) \leq N(u) \end{matrix} \right\} \Rightarrow N(u) = N(1)$

$\underline{\Leftarrow}$ assume $N(u) = N(1)$

by ED2

$1 = q \cdot u + r$ where $r = 0$

or $N(r) < N(u) = N(1)$

BUT $N(1)$ is minimal $\Rightarrow N(r) \not< N(u)$

$\Rightarrow r = 0$

$\Rightarrow 1 = q \cdot u$

$\Rightarrow u \in U(R)$

$\square$

<u>Examples</u>

1. $\mathbb{Z}$, $N(1) = 1$

$U(\mathbb{Z}) = \{ n \in \mathbb{Z} \mid N(n) = 1 \}$

$= \{ n \in \mathbb{Z} \mid |n| = 1 \} = \{ \pm 1 \}$

2. $\mathbb{F}[x]$, $N(1) = \deg(1) = 0$

$U(\mathbb{F}[x]) = \{ f \in \mathbb{F}[x] \mid \deg f = 0 \}$

$= \{$ constant polys $\}$

3. $\mathbb{Z}[i]$ $N(1) = 1$

$U(\mathbb{Z}[i]) = \{ a + bi \mid a^2 + b^2 = 1 \}$

$= \{ \pm 1, \pm i \}$

($a = \pm 1$ and $b = 0$ or $a = 0$ and $b = \pm 1$)

Unique Factorisation Domains

Defn 2.12

An ID R is a Unique Factorisation Domain (UFD) if $\forall a \in R^* \setminus U(R)$, a can be written as a product $a = p_1 \cdots p_s$ of irreducible elements in a unique way (up to reordering and up to associates)

Propn 2.10

R ID, then the following are equivalent:

1. R is a UFD
2. Every $a \in R^* \setminus U(R)$ can be written as a product of primes
3. Every irreducible in R is prime and $\forall a \in R^* \setminus U(R)$, a is a product of irreducibles

Proof

$1. \Rightarrow 3.$

$\forall a \in R^* \setminus U(R)$, a is a product of irreducibles is given as R is a UFD - defn.

So, all we have to show is every irreducible is prime.

$a \in R^* \setminus U(R)$ irred

Suppose $a | bc \Rightarrow ad = bc$

$b = \prod^r b_i$ with b_i irred

$c = \prod^s d_j$ with c_i irred

$d = \prod^t d_k$ with d_k irred

then

$a d_1 \dots d_t = b_1 \dots b_r c_1 \dots c_s$

$\Rightarrow$ $\exists i$ s.t $c_i \sim a \Rightarrow a | c_i \Rightarrow a | c$
or $\exists i$ s.t $b_i \sim a \Rightarrow a | b_i \Rightarrow a | b$

$\Rightarrow a$ is prime

3. $\Rightarrow$ 2. Trivial

2. $\Rightarrow$ 1.

Pick $a \in R^* \setminus \mathcal{U}(R)$
by (2) $a = p_1 \cdots p_r$ with p_i prime

assume $a = q_1 \cdots q_s$ with q_i irred
and we want $r = s$ and $p_i \sim q_i$ (after reordering)

Induction on r

$r = 1$, $a = p_1$ prime $p_1 = q_1 \cdots q_s$, $s = 1$
$p_1 = q_1$

Assume result for $r-1$ $(r > 1)$
and show $p_1 \cdots p_r = q_1 \cdots q_s$

$$\left.\begin{array}{l} p_r \mid q_1 \cdots q_s \\ p_r \text{ prime} \end{array}\right\} \Rightarrow p_r \mid q_s \quad \text{(after relabeling)}$$

$$\Rightarrow p_r \sim q_s$$

$$\Rightarrow q_s = u p_r \quad , \quad u \in \mathcal{U}(R)$$

$$p_1 \cdots p_r = q_1 \cdots q_{s-1} u p_r \quad , \quad p_r \neq 0$$

$$\Rightarrow \quad p_1 \cdots p_{r-1} = q_1 \cdots q_{s-1} \cdot u$$

$\underset{\text{hypothesis}}{\overset{\text{inductive}}{\Rightarrow}}$ $r - 1 = s - 1$

$\therefore p_i \sim q_i \quad \forall i = 1, \dots, s-1$ $\square$

Chain Conditions

Defn 2.13

A ring R satisfies the ascending chain condition (ACC) for principal ideals if, whenever we have a chain of principal ideals

$$(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \dots \subseteq (a_n) \subseteq \dots$$

$$\Rightarrow \exists\, N \in \mathbb{N} \text{ s.t } (a_n) = (a_N) \quad \forall n \geq N$$

Propn 2.11

always on principal ideals

If R is a ring satisfying ACC (on principal ideals), S is a non-empty family of principal ideals.

crucial

$\Rightarrow$ S has a maximal element, i.e. $I \in S$ s.t $\forall J \in S$, if $I \subseteq J \Rightarrow I = J$

[$\mathbb{Z}$ (2) (132) family of ideals]

(3) (6) (19)

We are claiming $\exists$ 'one' which won't have any other ~~[illegible]~~ it - maximal in this set, doesn't have to be a maximal ideal!

Take the example of (6) in this family. (6) is a maximal as nothing else contains it, we would need (2) and (3) in this family for (6) not to be maximal whereas they are not.

(19) is maximal but is also a maximal ideal as 19 is prime

Proof

By contradiction, assume S has no maximal element.

Take $I_1 \in S$ exists as S non-empty

$\therefore \exists I_2 \in S$ s.t $I_1 \subsetneq I_2$ as no maximal

$\exists I_3 \in S$ s.t $I_2 \subsetneq I_3$

$\vdots$

$\exists I_n \in S$ s.t $I_{n-1} \subsetneq I_n$

$\Rightarrow$ we get a chain

$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \dots \subsetneq I_n \subsetneq \dots$$

an infinite chain of principal ideals.

However, ACC tells us $I_n = I_N \quad \forall n \geq N$

Contradiction as $I_n \neq I_N \quad \forall n \geq N$ $\square$

Exercise - Show converse is true.

Example

R UFD, take $a \in R^* \setminus U(R)$

$I_1 = (a)$

If $(a) = I_1 \subseteq (a_2) \subseteq (a_3) \subseteq \dots \subseteq (a_n) \subseteq \dots$

$(a) \subseteq (a_i) \Rightarrow a_i / a$

$a = p_1 \cdots p_r$ product of primes

If $b/a \Rightarrow b = q_1 \dots q_s$ product of primes

$\Rightarrow q_j = p_{i_j} \quad \forall j$

$\Rightarrow a$ has a finite no° divisors

Assume $\ldots \subsetneq (a_i) \subsetneq (a_{i+1}) \subsetneq \ldots$

chain with all different elements that do not stabilise

$a_n \nsim a_m$ if $n \neq m \Rightarrow a_n \neq a_m$

and $a_n / a \Rightarrow$ we get an infinite no° divisors of a ✗.

$\Rightarrow$ UFD satisfies ACC

$\boxed{\text{UFD} \Rightarrow \text{ACC}}$

Prop^n 2.12

R ID satisfying ACC

$\Rightarrow$ every non-zero non-unit is a product of irreducibles

Proof

Suppose $\exists\, a \in R^* \setminus U(R)$ which is not a product of irreducibles

Then $S = \{(a) \mid a$ is not a product of irreducibles$\} \neq \emptyset$

$\Rightarrow \exists\, (b) \in S$ maximal in S

b is not irreducible

$\Rightarrow b = cd$, c, d proper divisors of b.

c is a product of irreds

$(b) \subsetneq (c) \Rightarrow (c) \notin S \Rightarrow c = p_1 \ldots p_r$

d is a product of irreducibles

$(b) \subsetneq (d) \Rightarrow (d) \notin S \Rightarrow d = q_1 \ldots q_s$

$\therefore b = p_1 \ldots p_r q_1 \ldots q_s$ product of irreds ✗

$\therefore$ we cannot find $a \in R^* / U(R)$ which is not a product of irreducibles

$\square$

So, R ACC $\Rightarrow$ R has factorisation into irreducibles
R UFD $\Rightarrow$ R has factorisation into irreducibles and every irreducible is prime
R PID $\Rightarrow$ every irreducible is prime

Prop^n 2.13
R PID $\Rightarrow$ R satisfies ACC

Proof
Take $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots \subseteq I_n \subseteq \dots$ chain of ideals in R and consider
$$I = \bigcup_{n \in \mathbb{N}} I_n \subseteq R$$

Claim $I \trianglelefteq R$

1. $0 \in I_1 \subseteq I$
2. $x, y \in I \Rightarrow x \in I_n,\ y \in I_m \Rightarrow x, y \in I_N$, $N = \max\{n, m\}$
$\Rightarrow x + y \in I_N \subseteq I$
3. $\left.\begin{array}{l} x \in I,\ r \in R \\ \Downarrow\ x \in I_n, \text{ for some } n \end{array}\right\} \Rightarrow rx \in I_n \subseteq I \Rightarrow I \trianglelefteq R$

$\Rightarrow I = (a)$ for some $a \in R$
$a \in I = \bigcup_{n \in \mathbb{N}} I_n \Rightarrow \exists n$ s.t. $a \in I_n$

$\left.\begin{array}{l} I = (a) \subseteq I_n \\ I_n \subseteq I \end{array}\right\} \Rightarrow I = I_n$ $\quad \forall m \geq n$ $\quad I = I_n \subseteq I_m \subseteq I = I_n$
$\Rightarrow I_m = I = I_n$

So, the chain stabilises $\Rightarrow$ R has ACC $\square$

ED $\Rightarrow$ PID $\Rightarrow$ UFD

Corollary 2.5

Every PID is a UFD

Proof

PID $\Rightarrow$ ACC $\Rightarrow$ $\exists$ a factorisation into irred $\Big\}$ $\Leftrightarrow$ R UFD
PID $\Rightarrow$ every irred is prime

$\square$

Corollary 2.6

ED $\Rightarrow$ PID $\Rightarrow$ UFD

In $\mathbb{Z}[i]$, $\quad 2 = (1+i)(1-i)$

The rings $\mathbb{Z}[\sqrt{m}]$

$m \in \mathbb{Z}$ s.t m is NOT a square, $m \notin \{0, 1, 4, 9, 16, \ldots\}$

$\mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$

$$\left.\begin{aligned}(a+b\sqrt{m}) + (a'+b'\sqrt{m}) &= (a+a') + (b+b')\sqrt{m} \\ (a+b\sqrt{m})(a'+b'\sqrt{m}) &= (aa'+mbb') + (ab'+ba')\sqrt{m}\end{aligned}\right\} \in \mathbb{Z}[\sqrt{m}]$$

$\mathbb{Z}[\sqrt{m}] \subseteq \mathbb{C} \Rightarrow \mathbb{Z}[\sqrt{m}]$ is an ID

$\overline{z\omega} = \bar{z} \cdot \bar{\omega}$, $\quad z = a + b\sqrt{m} \in \mathbb{Z}[\sqrt{m}] \Rightarrow \bar{z} := a - b\sqrt{m}$
$\bar{1} = 1$ $\qquad\qquad\qquad \bar{z} = z \Leftrightarrow z \in \mathbb{Z}$

$N(z) = |z\bar{z}| = |(a+b\sqrt{m})(a-b\sqrt{m})| = |a^2 - mb^2|$

take mod so we def get a +ve (what if $m > 0$?)

Properties

1/ $N(z\cdot\omega) = |z\omega\,\overline{z\omega}| = |z\omega\,\bar{z}\,\bar{\omega}| = |z\bar{z}||\omega\bar{\omega}| = N(z)N(\omega)$

$\Rightarrow$ if $\alpha|\beta \Rightarrow \beta = \alpha\gamma \Rightarrow N(\beta) = N(\alpha)N(\gamma)$

$\Rightarrow N(\alpha) \,|\, N(\beta) \quad (N(\alpha) \leq N(\beta))$

11/ $\alpha \in \mathcal{U}(\mathbb{Z}[\sqrt{m}]) \iff N(\alpha) = 1$

$\Rightarrow$) $\alpha \in \mathcal{U}(\mathbb{Z}[\sqrt{m}]) \Rightarrow \exists\beta$ s.t $\alpha\beta = 1$

$1 = N(1) = N(\alpha)N(\beta) \Rightarrow N(\alpha) = 1$

$\Leftarrow$)

$1 = N(\alpha) = |\alpha\bar{\alpha}| = |a^2 - mb^2|$, $\alpha = a + b\sqrt{m}$

If $a^2 - mb^2 = 1$

$(a + b\sqrt{m})(a - b\sqrt{m}) = 1 \quad \Rightarrow \bar{\alpha} = \alpha^{-1}$

If $a^2 - mb^2 = -1$

$(a + b\sqrt{m})(a - b\sqrt{m}) = -1 \Rightarrow (a + b\sqrt{m})(-(a - b\sqrt{m})) = 1$

$\Rightarrow -\bar{\alpha} = \alpha^{-1}$

$\Rightarrow \alpha \in \mathcal{U}(\mathbb{Z}[\sqrt{m}])$

111/ $\alpha \sim \beta \iff \alpha|\beta$ and $N(\alpha) = N(\beta)$

$\Rightarrow$) $\alpha \sim \beta \Rightarrow \beta = u\alpha$ for $u \in \mathcal{U}(\mathbb{Z}[\sqrt{m}])$

$\Rightarrow \alpha|\beta$

and $N(\beta) = N(u\alpha) = \overset{1}{N(u)}N(\alpha) = N(\alpha)$

$\Leftarrow$) $\alpha|\beta \Rightarrow \beta = \alpha\gamma \Rightarrow \underset{N(\alpha)}{N(\beta)} = N(\alpha\gamma) = N(\alpha)N(\gamma)$

$\Rightarrow N(\gamma) = 1 \Rightarrow \gamma \in \mathcal{U}(\mathbb{Z}[\sqrt{m}])$

$\Rightarrow \alpha \sim \beta$

Examples

① $m=-1 \Rightarrow \mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i]$

i.e. $N(z) = |a^2+b^2| = 1$

$U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$

② $m<-1 \Rightarrow \mathbb{Z}[\sqrt{m}] = \mathbb{Z}[\sqrt{-d}]$

$m=-d,\ d>1$

$N(a+b\sqrt{-d}) = |a^2-(-d)b^2|$

$= |a^2+b^2d| = a^2+b^2d \quad , d>1$

$\alpha = (a+b\sqrt{-d}) \in U(\mathbb{Z}[\sqrt{-d}]) \Leftrightarrow a^2+db^2=1$

$\Rightarrow \begin{cases} a=\pm 1 \Rightarrow b=0 \\ \text{or} \\ a=0 \Rightarrow db^2=1 \end{cases}$

no sol^n as $d>1$ and $b \in \mathbb{Z}$

So, $U(\mathbb{Z}[\sqrt{-d}]) = \{\pm 1\}$

③ If $m \geq 2$ [remember, $m \notin \{0,1,4,9,\dots\}$]

$\Rightarrow \mathbb{Z}[\sqrt{m}]$ ~~[illegible]~~ , $N(a+b\sqrt{m}) = 1$

$a^2-mb^2 = \pm 1$

↳ infinite sol^n

[Famous example,

$x^2-dy^2 = \pm 1$ Pell's eq^n

Infinite no° sol^n]

e.g. $\mathbb{Z}[\sqrt{2}]$, $a^2-2b^2 = \pm 1$

$a=1, b=1$

$1+\sqrt{2} = \alpha$

or

$a=3, b=2$

$9-2\cdot 4 = \beta$

$N(\alpha^2) = 1$
$N(\alpha^3) = 1$
$\vdots$

$x_0 = 1, \quad y_0 = 1$
$x_1 = 3, \quad y_1 = 2$
$\vdots \qquad \vdots$
$x_n \qquad y_n$
$x_{n+1} = x_n + 2y_n \qquad y_{n+1} = x_n + y_n$

$$(1+\sqrt{2})^2 = 1 + 2 + 2\sqrt{2} = 3 + 2\sqrt{2}$$

$$(x_n + y_n\sqrt{2})(1+\sqrt{2}) = (x_n + 2y_n) + (x_n + y_n)\sqrt{2}$$

e.g.

$R = \mathbb{Z}[\sqrt{-5}]$

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

$2, 3, \quad 1 \pm \sqrt{5}$ irreds

$\alpha = (2, 3, 1 \pm \sqrt{5})$ irreds

$N(\alpha) \in \{4, 9, 6\}$
If $\alpha = \beta\gamma$ proper divisions
then $N(\beta) \in \{2, 3\}$

$\beta = a + b\sqrt{-5}$ s.t. $a^2 + 5b^2 = 2, 3$ $\times$

$\Rightarrow \mathbb{Z}[-\sqrt{-5}]$ is NOT a UFD

2 is irred, but NOT prime
why? because $2 | 6$ but $2 \nmid (1+\sqrt{-5})$ and $2 \nmid (1-\sqrt{-5})$

$\mathbb{Z}[\sqrt{-7}]$, $8 = 2 \cdot 2 \cdot 2 = (1+\sqrt{-7})(1-\sqrt{-7})$

irred

Prop^n 2.14

$\mathbb{Z}[\sqrt{m}]$ satisfies ACC (on principal ideals)

Proof

Take $(a_1) \subseteq (a_2) \subseteq \ldots \subseteq (a_n) \subseteq \ldots$

$a_n | a_{n-1}$, $a_{n-1} | a_{n-2}$, $\ldots$, $a_2 | a_1$

$\Rightarrow N(a_n) | N(a_{n-1})$, $\ldots$, $N(a_2) | N(a_1)$

So, $N(a_1) \geq N(a_2) \geq \ldots \geq N(a_n) \geq \ldots$

$\Rightarrow \exists\, k \in \mathbb{N}$ s.t $N(a_n) = N(a_k)$, $a_n | a_k$ $\forall n \geq k$

$\Leftrightarrow a_n \sim a_k$ $\forall n \geq k$

$\Downarrow$

$(a_n) = (a_k)$ $\forall n \geq k$ $\square$

gcd and lcm

Def^n 2.14

R UFD , $a, b \in R$, we say that d is a gcd of a and b if:

i/ $d | a$, $d | b$ ($\Leftrightarrow (a) \subseteq (d), (b) \subseteq (d)$ $\Leftrightarrow (a)+(b) \subseteq (d)$)

ii/ $\forall e \in R$ s.t $e | a$, $e | b$ we have $e | d$ ($\forall e$ s.t $(a)+(b) \subseteq (e) \Rightarrow (d) \subseteq (e)$)

Examples

① If R ED we can compute $\gcd(a,b)$ using the Euclidean algorithm

$\mathbb{Z}$, $60 = 2^2 \cdot 3 \cdot 5$
$28 = 2^2 \cdot 7$
$90 = 2 \cdot 3^2 \cdot 5$

$\gcd(60,28)$ is 4

$\gcd(60,90)$ is 30
why? take prime with lowest exponent, i.e. 2, 3, 5 and multiply, $2 \times 3 \times 5 = 30$

Remark: gcd is only defined up to associates

② R is a UFD, $a = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$
$b = p_1^{\beta_1} \cdots p_r^{\beta_r}$, $\alpha_i, \beta_i \geq 0$

$\Rightarrow d = p_1^{\gamma_1} \cdots p_r^{\gamma_r}$ w/ $\gamma_i = \min(\alpha_i, \beta_i)$

$d = \gcd(a,b)$

③ If R PID, $a, b \in R$

$\underbrace{(a)+(b)}_{\substack{\shortparallel \\ (d)}} \trianglelefteq R$

(d) as R PID $\Rightarrow d = \gcd(a,b)$

as $(a) \subseteq (d)$, $(b) \subseteq (d)$
any e s.t $(a) \subseteq (e)$
$\Rightarrow \underbrace{(a)+(b)}_{\substack{\shortparallel \\ (d)}} \subseteq (e)$

$(d) = (a) + (b) = \{ha + kb \mid h, k \in R\}$
$\Rightarrow \exists\, h, k \in R$ s.t $d = ha + kb$

Bezout's Identity

Note from Sheet 4: $(a) \cap (b) = \mathrm{lcm}(a,b)$

$\gcd(ca, cb) = c\gcd(a,b)$
pretty much all the stuff we know about gcd holds here

Fields of Fractions

R ID, $S \subseteq R$ multiplicatively closed (submonoid)

$\begin{cases} 1 \in S, \; 0 \notin S \\ s,t \in S \Rightarrow st \in S \end{cases}$

$R \times S = \{(a,s) \mid a \in R, s \in S\}$

define $(a,s) \sim (b,t) \iff at = bs$

$\sim$ is an equivalence relation (Exercise to check: $as \sim as$, $as \sim sa$, $as \sim bt$ and $bt \sim cu \Rightarrow as \sim cu$)

Define $\frac{a}{s} := \{(a',s') \mid (a',s') \sim (a,s)\}$

$R \times S/_{\sim} := \{\frac{a}{s} \mid a \in R, s \in S\}$

contained in set

$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}$

$\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$

$\Rightarrow R \times S/_{\sim} = S^{-1}R$ is a ring

Examples

1/ $\mathbb{Z}_{(p)} = \mathbb{Z}[\frac{1}{p}] = \{ \frac{a}{b} \mid p \nmid b \} = S^{-1}\mathbb{Z}$

w/ $S = \{ b \in \mathbb{Z} \mid p \nmid b \} = R \setminus (p)$
$\{ c \in \mathbb{Z} \mid p \mid c \} = (p)$

2/ R ID $P \trianglelefteq R$ prime ideal $S = R \setminus P$

mult. closed as P prime ideal if $a, b \in P$, $ab \in P \Rightarrow ab \notin S$

$S^{-1}R = \{ \frac{a}{s} \mid a \in R, s \notin P \} = R_P$ localisation of R at P

3/ R ID ($ab = 0 \Rightarrow a = 0$ or $b = 0$
or/ $a \neq 0, b \neq 0 \Rightarrow ab \neq 0$)

$S = R^* = R \setminus \{0\}$ is mult. closed

$S^{-1}R = \{ \frac{a}{b} \mid a, b \in R, b \neq 0 \} = Q(R)$

for ring of Quotients, NOT the Quotient ring

Properties

1/ $S^{-1}R$ ring
2/ There is an injective ring homomorphism, (If R ID, though R ID is only one of relevance to us)
$\varphi : R \longrightarrow S^{-1}R$
$r \longmapsto \frac{r}{1}$

3/ $\forall s \in S$, $\varphi(s) = \frac{s}{1}$,

$$\frac{s}{1} \cdot \frac{1}{s} = 1 \Rightarrow \varphi(s) \in \mathcal{U}(R)$$

In particular, if $S = R^*$, $S^{-1}R = Q(R)$

$\forall s \in S$, s.t. $s \neq 0 \Rightarrow s \in \mathcal{U}(Q(R)) \Rightarrow Q(R)$ field

$Q(R) \equiv$ field of fractions of R

Examples

$Q(\mathbb{Z}) = \mathbb{Q}$

$Q(\mathbb{F}[x]) = \left\{ \frac{f(x)}{g(x)} \mid g(x) \neq 0 \right\} \equiv$ rational functions

---

R UFD $\longrightarrow Q = Q(R)$

$R[x] \leq Q[x]$

Polynomial Rings over Domains

Goal: R UFD $\Rightarrow R[x]$ UFD

Strategy: R UFD $\Rightarrow R$ ID, $Q = Q(R)$ field

$R[x] \leq Q[x]$ ED

$f(x) = 2x^2+4 \in \mathbb{Z}[x]$

$= 2(x^2+4)$

$f(x)$ irred in $\mathbb{Q}[x]$

Def^n 2.15

R UFD, $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$

we say that f is primitive if $\gcd(a_0, a_1, \ldots, a_n) = 1$
i.e. $\nexists\, p$ prime s.t $p \mid a_i \ \forall i = 0, \ldots, n$

Example

i/ $2x+1$ primitive in $\mathbb{Z}[x]$

ii/ If $f(x)$ is monic $\Rightarrow$ f is primitive

iii/ If $f(x)$ is irred $\Rightarrow$ f is primitive

Lemma 2.1

R UFD, $Q = Q(R)$
$f \in Q[x] \Rightarrow \exists\ \lambda \in Q^*$ $\tilde{f} \in R[x]$ primitive
$f \neq 0$ s.t $\boxed{f = \lambda \cdot \tilde{f}}$
Moreover, λ and $\tilde{f}$ are unique up to multiplication by a unit of R.

Proof

$f(x) \in Q[x]$, $f \neq 0 \Rightarrow f(x) = \frac{a_0}{b_0} + \frac{a_1}{b_1} x + \cdots + \frac{a_n}{b_n} x^n$

$a_i, b_i \in R$, $b_i \neq 0$

$r = b_0 \ldots b_n$, $a_i' = \frac{a_i r}{b_i} = a_i b_0 b_1 \cdots b_{i-1} b_{i+1} \cdots b_n \in R$

$d = \gcd(a_0', \ldots, a_n')$, $c_i = \frac{a_i'}{d} \in R$

$d \mid a_0', \ldots, a_n'$

35

$\tilde{f} = c_0 + c_1 x + \dots + c_n x^n$, $f = \frac{d}{r}\tilde{f}$

$$\gcd(c_0, \dots, c_n) = \gcd\left(\frac{a_0'}{d}, \dots, \frac{a_n'}{d}\right)$$
$$= \frac{1}{d}\gcd(a_0', \dots, a_n') = \frac{1}{d} \cdot d = 1$$

$\Rightarrow \tilde{f}$ is primitive

Uniqueness
Assume $f = \lambda \tilde{f} = \mu \tilde{g}$ for $\lambda, \mu \in \mathbb{Q}^*$
$\tilde{f}, \tilde{g} \in R[x]$ primitive

[a, b, c, d etc independent of first part of proof]

$$\lambda = \frac{a}{b} \ (b \neq 0) \ , \quad \mu = \frac{c}{d} \ (d \neq 0)$$

$\tilde{f} = a_0 + \dots + a_n x^n$, $\tilde{g} = b_0 + b_1 x + \dots + b_n x^n$

$$\frac{a}{b}(a_0 + \dots + a_n x^n) = \frac{c}{d}(b_0 + \dots + b_n x^n)$$

$\Leftrightarrow a\frac{a_i}{b} = c\frac{b_i}{d} \quad \forall i = 0, \dots, n$

$\Leftrightarrow a d a_i = b c b_i \quad \forall i = 0, \dots, n$

$$ad = ad \cdot 1 \overset{\tilde{f} \text{ primitive}}{(\sim)=} (ad) \cdot \gcd(a_0, \dots, a_n)$$
$$(\sim)= \gcd(ad a_0, \dots, ad a_n)$$
$$(\sim)= \gcd(bc b_0, \dots, bc b_n)$$
$$(\sim)= bc \gcd(b_0, \dots, b_n)$$
$$(\sim)= bc \cdot 1 = bc$$
$(\sim)$

after this, we lose equality. We have equality up to associates. So, should write $(\sim)$

$\therefore$ $ad = bc$ up to associates

i.e. $ad \sim bc \Rightarrow \exists u \in U(R)$ s.t $bc = uad$

$$\Leftrightarrow \frac{c}{d} = u \cdot \frac{a}{b}$$

$$\Leftrightarrow \mu = u \cdot \lambda$$

$$ad\, a_i = bc\, b_i$$

$$\frac{a}{b} a_i = \frac{c}{d} b_i = u \cdot \frac{a}{b} b_i$$

$$\Leftrightarrow a_i = u b_i$$

$$\Leftrightarrow b_i = u^{-1} a_i \quad \forall i = 0, \dots, n$$

$$\boxed{\hat{g} = u^{-1} \tilde{f}}$$

$\square$

Def^n 2.16

If $f \in \mathbb{Q}[x]$, $f(x) = \lambda \tilde{f}$ as before.
We call λ the content of f $(\lambda = c(f))$
$\tilde{f}$ the primitive part of f

Example

$$f(x) = \frac{4}{3} + \frac{8}{21} x + 2x^2 \in \mathbb{Q}[x]$$

$$f(x) = \frac{1}{3 \cdot 21} (21 \cdot 4 + 3 \cdot 8x + 63 \cdot 2x^2)$$

$$= \frac{1}{63} (2^2 \cdot 3 \cdot 7 + 2^3 \cdot 3x + 2 \cdot 3 \cdot 21 x^2)$$

$$= \frac{6}{63} (14 + 4x + 21x^2)$$

$$= \frac{2}{21} \tilde{f}$$

$\gcd(14, 4, 21) = 1$

<u>Prop^n 2.15</u>

R UFD, $Q = Q(R)$, $f \in Q[x]$, $f \neq 0$,

then:

1. If $\lambda \in Q^* \Rightarrow$ $c(\lambda f) = \lambda c(f)$, $(\widetilde{\lambda f}) = \tilde{f}$ $\Big\}$ $\lambda f = c(\lambda f)(\widetilde{\lambda f})$
2. $f \in R[x] \iff c(f) \in R$
3. $f \in R[x]$ then f is primitive $\iff c(f) = 1$
4. $f, g \in R[x]$ primitive and $f \sim g$ in $Q[x]$ $\Rightarrow f \sim g$ in $R[x]$

<u>Proof</u>

1. $$\left.\begin{array}{l} \lambda f = c(\lambda f) \cdot (\widetilde{\lambda f}) \\ \quad \| \\ \lambda c(f)\tilde{f} \text{ primitive} \\ \quad \neq \\ \quad 0 \end{array}\right\} \Rightarrow \begin{array}{l} c(\lambda f) = \lambda c(f) \\ (\widetilde{\lambda f}) = \tilde{f} \end{array}$$

2. <u>$\Rightarrow$|</u> Trivial $f = \overset{\in R}{\gcd(a_0 \ldots a_n)}\underbrace{\left(\frac{a_0}{d} + \cdots + \frac{a_n}{d}x^n\right)}_{\text{primitive}}$

   <u>$\Leftarrow$|</u> $c(f) \in R$

   $\tilde{f} \in R[x] \Rightarrow c(f)\hat{f} \in R[x] \Rightarrow f \in R[x]$

3. f primitive $\iff f = \hat{f} \iff c(f) = 1$

4. f, g primitive $\Rightarrow c(f) = c(g) = 1$

   $f \sim g$ in $Q[x] \Rightarrow \exists\, \lambda \in Q^*$ s.t $g = \lambda f$

   $1 = c(g) = c(\lambda f) = \lambda c(f) = \lambda$ (up to unit of R)

   $\Rightarrow f \sim g$ in $R[x]$

   $\square$

__Lemma 2.2__ (Gauss' Lemma)

f, g primitive $\Rightarrow$ fg primitive

__Proof__

$f = a_0 + a_1 x + \dots + a_n x^n, \quad g = b_0 + b_1 x + \dots + b_n x^n$

$\Rightarrow \forall p$ prime $\quad \exists i$ s.t $p | a_0, p | a_1, \dots, p | a_{i-1}, p \nmid a_i$

$\exists j$ s.t $p | b_0, p | b_1, \dots, p | b_{j-1}, p \nmid b_j$

$\Rightarrow fg = \underline{\qquad} + c_{i+j} x^{i+j} + \underline{\qquad}$

$$c_{i+j} = \underbrace{a_0 b_{i+j} + a_1 b_{i+j-1} + \dots +}_{A} a_i b_j \underbrace{+ \dots + a_{i+j} b_0}_{B}$$

$p | A, \quad p | B, \quad p \nmid a_i b_j$

$\Rightarrow p \nmid c_{i+j}$

$\Rightarrow fg$ primitive

Consequence of Gauss' Lemma: $c(fg) = c(f)c(g)$

__Proof__

$f = c(f)\tilde{f}, \quad g = c(g)\tilde{g}$

$\Rightarrow fg = c(f)c(g)\tilde{f}\tilde{g}$

$= c(f)c(g)\widetilde{fg}$ by Gauss

$\underset{\text{consequence}}{\Rightarrow}$ $c(f)c(g) = c(fg)$

$\square$

39

Prop^n 2.16

$f \overset{\neq 0}{\in} R[x]$

- If $\deg f = 0$
  f irred in $R[x] \iff f$ irred in R
- If $\deg f \geq 1$, f primitive
  f irred in $R[x] \iff f$ irred in $Q[x]$

Proof

① $\deg f = 0 \implies f \in R$

Suppose f is reducible in $R[x]$, $f = gh$

$$\underbrace{\underset{\substack{\text{\rotatebox{90}{$\leq$}}\\0}}{\deg(g)} + \underset{\substack{\text{\rotatebox{90}{$\leq$}}\\0}}{\deg(h)}} = \deg f = 0$$

because f and hence $g, h \neq 0$

$\deg h = \deg g = 0 \implies h, g \in R$

f irred in $R \implies f$ irred in $R[x]$
Converse is trivial $\square$

[$f = 2x \in Q[x]$, f is irred as 2 is a unit
$\in \mathbb{Z}[x]$, f is not irred as 2 is not a unit in $\mathbb{Z}[x]$]

② f primitive. Suppose f is irreducible in $R[x]$
Suppose $f = gh$ in $Q[x]$
$g = c(g)\hat{g}$, $h = c(h)\hat{h}$

primitive

So,

$$f = c(g)c(h)\underbrace{\hat{g}\hat{h}}_{\text{primitive by Gauss}}$$

$c(g)c(h) = 1$

$\Rightarrow f = \tilde{g}\tilde{h}$ $\times$ as we supposed f is irred in $R[x]$

We showed: f irred in $R[x] \Rightarrow f$ irred in $Q[x]$
Converse is trivial

$\square$

Example we had does not contradict this as the example is not primitive

Theorem 2.1
R UFD $\Rightarrow R[x]$ UFD

Proof
$f \in R[x]$ $\quad f \neq 0$

If $\deg f = 0$ then R UFD, f has a unique factorisation into irreducibles. $f = p_1 \dots p_r$, p_i's irred

If $\deg f \geq 1$, in $Q[x]$, $f = f_1 \dots f_r$, $f_i \in Q[x]$

$f = c(f) \cdot \tilde{f}$, $\quad \tilde{f} \in R[x]$ primitive

$c(f) = c(f_1) \dots c(f_r)$ (Gauss)
$f_i = c(f_i)\tilde{f}_i$, $\quad \tilde{f}_i$ primitive

$\therefore f = c(f_1) \dots c(f_r)\tilde{f}_1 \dots \tilde{f}_r$
$\tilde{f}_i$'s are primitive irred in $Q[x] \Rightarrow \tilde{f}_i$ irred in $R[x]$

$c(f_1), \dots, c(f_r) \in R$, $\quad R$ UFD
It has a factor into irred in R (hence in $R[x]$)

This shows the existence.

<u>Uniqueness:</u>

Suppose $f = \underbrace{p_1 \dots p_s}_{\in R} \underbrace{f_1 \dots f_k}_{\deg \geqslant 1} = q_1 \dots q_{s'} g_1 \dots g_{k'}$

f_i's, g_i's are irred in $R[x]$, hence primitive (because $f_i = c(f_i)\tilde{f}_i \Rightarrow c(f_i) = 1$ because f_i irred)

By Gauss, $f_1 \dots f_k$ and $g_1 \dots g_{k'}$ are primitive
$\Rightarrow p_1 \dots p_s = c(f) = q_1 \dots q_{s'}$
up to a unit

R UFD $\Rightarrow$ $s = s'$
$p_i = q_i$ after permutation

$f_1 \dots f_k = g_1 \dots g_{k'}$

f_i's, g_i's primitive irred in $R[x]$ and $Q[x]$ (just shown)

$Q[x]$ UFD $\Rightarrow$ $k = k'$
$f_i = g_i$ after permutation $\square$

<u>Examples</u>

$\mathbb{Z}[x]$ is UFD, <u>NOT</u> a PID
$(2, x)$ is not principal

k field, $k[x_1, \dots, x_n]$ UFD
why? More generally
R UFD, then $R[x_1, \dots, x_n] = \underbrace{R[x_1, \dots, x_{n-1}]}_{UFD}[x_n]$

42

$\mathbb{R}[x,y]$ UFD , not a PID
(x,y) not principal

$\mathbb{Z}[\sqrt{-5}] = \mathbb{Z}[x]/(x^2+5)$ NOT a UFD

$9 = 3\cdot 3 = (2+\sqrt{-5})(2-\sqrt{-5})$
Two really different factorisations

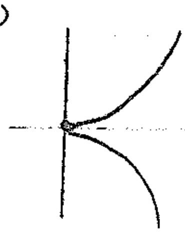
i/ $\mathbb{Z}[i] = \mathbb{Z}[x]/(x^2+1)$ is a UFD

ii/ $R = \mathbb{R}[x,y]/(y^2-x^3)$
$\Downarrow$
$f = y^2 = x^3$ $\bar{x}, \bar{y}$ images of x & y in R

Suppose $\bar{x} = u\cdot\bar{y}$
$\bar{x}^3 = u^3\,\bar{y}^3$
$\quad \overset{\shortparallel}{v}$
$= v\,\bar{y}\cdot\bar{y}^2$
$= v\,\bar{y}\,\bar{x}^3$
$\Rightarrow 1 = v\bar{y}$ $\Rightarrow$ $\bar{y}$ is a unit

$y\cdot v(x,y) = 1 + f(y^2-x^3)$
not possible because : make $y=0 \Rightarrow 0=1$

So, $R = \mathbb{R}[x,y]/(y^2-x^3)$ is not a UFD



43

iii/ $R = \mathbb{R}[x,y]/(y-x^2) \cong \mathbb{R}[x]$ $\therefore$ UFD

$$\mathbb{R}[x] \longrightarrow \mathbb{R}[x,y] \longrightarrow \mathbb{R}[x,y]/(y-x^2)$$

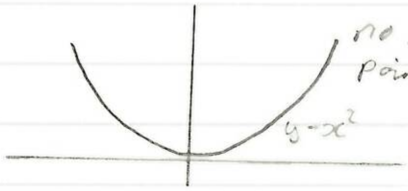
φ

$$\overset{\in}{f} = q(y-x^2) + r, \quad r \in \mathbb{R}[x]$$

Euclidean division

clearly surjective
$\therefore$ any $f \in \mathbb{R}[x,y]$, $\varphi(r) = f$ φ is surjective

φ injective as r is unique
$\therefore \varphi$ is an isomorphism



Chapter 3: Modules

Def^n 3.1 commutative unless otherwise stated

R ring, a module over R (R-mod) is an abelian group $(M, +)$ together with an operation

no mult on M

$$R \times M \longrightarrow M$$
$$(r, m) \longmapsto r * m = rm$$

do not confuse with mult on ring as m does not need to be an element on the ring

satisfying:

M1 : Distributivity — $r(m+n) = rm + rn$

M2 : Distributivity wrt addition on ring — $(r+s)m = rm + sm$

M3 : Pseudo-associativity — $\underbrace{(rs)}_{\text{product on ring}}m = r(sm)$

$\forall m, n \in M$
$\forall r, s \in R$

M4 : Modularity — $1 \cdot m = m$

Examples

1/ If $\mathbb{F}$ is a field, modules / $\mathbb{F}$ are precisely vector spaces / $\mathbb{F}$ $\boxed{\mathbb{F}\text{-mods} \equiv \text{v.s} / \mathbb{F}}$

2/ $R = \mathbb{Z}$ $(G, +)$ abelian group

$$\mathbb{Z} \times G \longrightarrow G$$
$$(n, g) \longmapsto n \cdot g = \begin{cases} \overbrace{g + g + \dots + g}^{n}, & \text{if } n > 0 \\ 0, & \text{if } n = 0 \\ \underbrace{(-g) + (-g) + \dots + (-g)}_{-n}, & \text{if } n < 0 \end{cases}$$

$\Rightarrow$ G is a $\mathbb{Z}$-module

$\boxed{\Rightarrow \mathbb{Z}\text{-mods} \equiv \text{Abelian groups}}$

2

$\mathbb{R}^3$

$\mathbb{R}[x]_2 = \{p(x) \in \mathbb{R}[x] \mid deg(p) \leq 2\}$ } isomorphic as same dim

G-abelian group (f.g) $\Rightarrow G = \mathbb{Z}^s \oplus \mathbb{Z}/_{d_1\mathbb{Z}} \oplus \mathbb{Z}/_{d_2\mathbb{Z}} \oplus \dots \oplus \mathbb{Z}/_{d_r\mathbb{Z}}$

3/ $\mathbb{F}[x]$ $\quad M$ $\mathbb{F}[x]$-module $\Rightarrow M$ $\mathbb{F}$-mod

$\Rightarrow M = V$ v.s $/\mathbb{F}$

$\mathbb{F}[x] \times M \longrightarrow M \quad \rightsquigarrow \quad \mathbb{F} \times M \longrightarrow M$

V v.s$/\mathbb{F}$ $\quad \mathbb{F}[x] \times V \longrightarrow V$

define $\quad \alpha : V \longrightarrow V$

$\qquad v \longmapsto \alpha(v) = x \cdot v$

$\alpha(v+w) = x(v+w) = xv + xw = \alpha(v) + \alpha(w)$

$\alpha(\lambda v) = x(\lambda v) = (x\lambda)v = (\lambda x)(v) = \lambda(xv) = \lambda\alpha(v)$ $\Big|$ $\Rightarrow \alpha$ linear map

So, to each $\mathbb{F}[x]$-mod we can associate a pair (V, α) where V v.s$/\mathbb{F}$

$\alpha : V \to V$ (linear map)

Conversely, given (V, α) we can define

$$\mathbb{F}[x] \times V \longrightarrow V$$
$$(p(x), v) \longmapsto p(x)v$$

e.g.

$$(x^3 - 2x + 3)v = \underbrace{x^3 v}_{\alpha^3(v)} - \underbrace{2xv}_{-2\alpha(v)} + 3v$$ fine as V v.s

$$= \underbrace{\alpha^3(v)}_{\alpha(\alpha(\alpha(v)))} - 2\alpha(v) + 3v$$

$\mathbb{F}[x]$-mods $= (V, \alpha)$ $\quad$ V v.s $/\mathbb{F}$

$\alpha : V \longrightarrow V$ linear

If $V = \mathbb{C}^n$, $\quad \alpha : \mathbb{C}^n \longrightarrow \mathbb{C}^n$

$v \longmapsto \alpha(v) = Av$

$\alpha \rightsquigarrow A \in M_n(\mathbb{C})$

by change of basis $\quad A \longrightarrow P^{-1}AP$

and here we come to JNF over $\mathbb{C}$. However, we cannot expect to find JNF over an arbitrary ring. So, we shall come to Rational Canonical Form.

The guiding theory to this part of the course is to mimic Linear Algebra with fields.

Example

R ring $\qquad R \times R \longrightarrow R$

$(r, s) \longmapsto rs$

$\Rightarrow$ R is an R-mod, ${}_R R$

Notation: If M R-mod, sometimes we write ${}_R M$

Def^n 3.2

M R-mod, $P \subseteq M$, we say that P is a submodule of M if $P \leq M$ subgroup of M and $\forall p \in P$, $\forall r \in R$ $\Rightarrow rp \in P$

looks like absorbency

<u>Examples</u>

① R ring, $M = {}_R R$

subgroup satisfying $rP \subseteq P$ (absorbency)

$P \leq {}_R R$ submodule $\iff$ $P \trianglelefteq R$ ideal

② M R-mod $\Rightarrow$ $0 = \{0\} \leq M$ zero submodule
$M \leq M$ total submodule

③ $R = \mathbb{Z}$, G abelian group ($\equiv \mathbb{Z}$-mod)
$H \leq G$ submodule $\iff$ $H \leq G$ subgroup

④ $R = \mathbb{F}$ field, $M = V$ v.s/$\mathbb{F}$

$W \leq V$ submodule $\iff$ $W \leq V$ subvector sp

⑤ R, S rings $\varphi : R \to S$ ring hom
M S-module
$\Rightarrow$ The map $R \times M \to M$

$S \times M$

$(r, m) \longmapsto r * m := \underbrace{\varphi(r)\, m}_{\in M}$

gives an R-mod structure on M

In particular, if $R \leq S$ subring, then every S-mod is also an R-mod - Restriction of Scalars

<u>Prop^n 3.1</u>
R ring, M R-mod, $A, B \leq M$ submods.
Then

i) $A \cap B$ is a submodule
ii) $A + B = \{a + b \mid a \in A, b \in B\} \leq M$ submod

Proof

Exercise □

Cyclic Modules and Finitely Generated Modules

Defⁿ 3.3

R ring, M R-mod, $x \in M$, then we define $Rx := \{rx \mid r \in R\}$ the cyclic submodule of M generated by x

Example

$M = {}_R R$, $x \in R \Rightarrow Rx = (x)$

If $A \leq M$ submod s.t $A = Rx$ for some $x \in M$, we say that A is a cyclic module (generated by x).

e.g.

$\mathbb{F}$ field, $\mathbb{F}v = \text{span}\{v\}$ $v \in V$, $v \neq 0$

Defⁿ 3.4

M R-mod, $x_1, \dots, x_n \in M$

$\Rightarrow Rx_1 + Rx_2 + \dots + Rx_n = \{r_1x_1 + r_2x_2 + \dots + r_nx_n \mid r_i \in R\}$ submodule generated by $\{x_1, \dots, x_n\}$

If $M = Rx_1 + \dots + Rx_n$ we say that M is finitely generated and that $\{x_1, \dots, x_n\}$ is a generating set of M

N.B. think of finitely generated being kind of like finite dimensional

Def^n 3.5

M R-mod, $P \leq M$ submod, for any $x \in M$ define $x + P = \bar{x} := \{x + y \mid y \in P\}$

$$M/P = \{x + P \mid x \in M\}$$

$$(x+P) + (y+P) = (x+y) + P$$

$$r \cdot (x+P) = rx + P$$

not rP as we have ~~ab~~ absorbing, $rp \in P$

with these operations, M/P is an R-mod, called the quotient of M by P

Remark: $x + P = y + P \iff x - y \in P$
$x + P = 0 \ (= 0 + P) \iff x \in P$

Prop^n 3.2

M R-mod s.t $M = Rx_1 + \dots + Rx_n$
$P \leq M$ submod $\Rightarrow$ M/P is finitely generated and $\{\bar{x}_1, \bar{x}_2, \dots, \bar{x}_n\}$ is a generating set for M/P

Proof

$$M/P = \{m + P \mid m \in M\}$$

take $m \in M \Rightarrow \exists r_1, \dots, r_n$ s.t $m = r_1 x_1 + \dots + r_n x_n$

$$\begin{aligned} \Rightarrow m + P &= (r_1 x_1 + \dots + r_n x_n) + P \\ &= ((r_1 x_1) + P) + \dots + ((r_n x_n) + P) \\ &= r_1 \underbrace{(x_1 + P)}_{\bar{x}_1} + \dots + r_n \underbrace{(x_n + P)}_{\bar{x}_n} \end{aligned}$$

$= r_1\bar{x}_1 + \dots + r_n\bar{x}_n$

$\Rightarrow M/P = R\bar{x}_1 + \dots + R\bar{x}_n$ $\square$

Corollary 3.1

If $M = Rx$ cyclic, $P \leq M$
$\Rightarrow M/P$ is cyclic (and $M/P = R\bar{x}$)

Module Homomorphisms

Defn 3.6

R ring, M, N R-mods. A map $\varphi: M \to N$ is a mod homomorphism if it satisfies

also called R-linear map

$$\left.\begin{array}{l} 1/\ \varphi(m+m') = \varphi(m) + \varphi(m') \\ \quad \varphi(0) = 0 \\ \quad [\varphi(-m) = -\varphi(m)] \end{array}\right\} \varphi \text{ group homo}$$

never really need to check this as $\varphi(-m) = (-1)\varphi(m)$

$11/\ \varphi(rm) = r\varphi(m)$

Examples

1/ $Id: M \to N$ mod homomorphism

11/ $\mathbb{F}$ field V, W v.s $/\mathbb{F}$ mod$/\mathbb{F}$

$\alpha: V \to W$ mod homomorphism $\Leftrightarrow$ α is a linear map

111/ R M, N R mods, $0: M \to N$ mod homo
$m \mapsto 0$

iv/ $R = \mathbb{Z}$, $M = {}_{\mathbb{Z}}\mathbb{Z} = N$ $\quad {}_{\mathbb{Z}}\mathbb{Z} \longrightarrow {}_{\mathbb{Z}}\mathbb{Z}$

$x \longmapsto 2x$

mod homomorphism BUT
not a ring homomorphism as $1 \not\mapsto 1$

v/ $R = \mathbb{Z}$, $M = G$, $N = H$
$\alpha : G \longrightarrow H$ mod hom $\iff$ α is a group hom

Def^n 3.7
R ring M, N R-mods, $\alpha : M \to N$ mod homs
i/ If α injective, we say that α is a monomorphism
ii/ If α surjective, we say that α is an epimorphism
iii/ If α bijective, we say that α is an isomorphism

We define $\mathrm{Hom}_R(M, N) = \{ \alpha : M \to N \text{ s.t } \alpha \text{ mod hom} \}$

Property
$\alpha \in \mathrm{Hom}_R(M, N)$, $\beta \in \mathrm{Hom}_R(N, P)$
$\Rightarrow \beta \circ \alpha \in \mathrm{Hom}_R(M, P)$

Proof
Exercise $\square$

Def^n 3.8
$\alpha \in \mathrm{Hom}_R(M, N)$,
we define:
$$\ker(\alpha) = \{ m \in M \text{ s.t } \alpha(m) = 0 \}$$
$$\mathrm{Im}(\alpha) = \{ n \in N \text{ s.t } \exists m \in M \text{ s.t } \alpha(m) = n \}$$
$$= \{ \alpha(m) \mid m \in M \}$$

Prop^n 3.3

$$\begin{array}{l} \operatorname{Ker}\alpha \le M \\ \operatorname{Im}\alpha \le N \end{array} \quad \Bigg| \text{ Submodule}$$

Proof

Exercise $\square$

Example

i/ $Id : M \to M \implies \operatorname{Ker} Id = 0$

$\operatorname{Im} Id = M$

ii/ $0 : M \to M \implies \operatorname{Ker}(0) = M$

$\operatorname{Im}(0) = 0$

iii/ $P \le M$, $\underset{\text{Canonical projection}}{\pi_p} : M \to M/P$

$m \mapsto m + P$

$\implies \pi_p \in \operatorname{Hom}_R(M, M/P)$

$\operatorname{Ker}\pi_p = P$

$\operatorname{Im}\pi_p = M/P$

So, $\alpha : M \to N$ R-mod hom $\iff \alpha(a_1 m_1 + a_2 m_2) = a_1\alpha(m_1) + a_2\alpha(m_2)$

$\forall a_1, a_2 \in R$

$\forall m_1, m_2 \in M$

Theorem 3.1 (First Isomorphism Theorem for Modules)

R ring,

M, N R-mods, $\alpha \in \operatorname{Hom}_R(M, N)$

$\implies M/_{\operatorname{Ker}\alpha} \cong \operatorname{Im}\alpha$

10

Proof

Take the map $\varphi : M/_{\ker\alpha} \longrightarrow \operatorname{Im}\alpha$

$m + \ker\alpha \longmapsto \alpha(m)$

i) φ well defined
ii) φ module homomorphism
iii) φ bijective

i) $m + \ker\alpha = m' + \ker\alpha \iff m - m' \in \ker\alpha$
$\iff \alpha(m-m') = 0$
$\iff \alpha(m) = \alpha(m')$
$\iff \varphi(m+\ker\alpha) = \varphi(m'+\ker\alpha)$

$\therefore$ φ well defined and injective

ii) $\varphi((m+\ker\alpha)+(m'+\ker\alpha)) = \varphi((m+m')+\ker\alpha)$
$= \alpha(m+m')$
$= \alpha(m) + \alpha(m')$
$= \varphi(m+\ker\alpha) + \varphi(m'+\ker\alpha)$

$\varphi(r(m+\ker\alpha)) = \varphi((rm)+\ker\alpha)$
$= \alpha(rm)$
$= r\alpha(m)$
$= r\varphi(m+\ker\alpha)$

iii) $\forall n \in \operatorname{Im}\alpha$
$\exists m \in M$ s.t $n = \alpha(m) = \varphi(m+\ker\alpha)$
$\square$

<u>Theorem 3.2</u> we normally work with commutative, but our def^n, theorems etc usually work for non-commutative (after some tweaking) - this won't

R <u>commutative</u> ring, ${}_RM$ R-mod, then M is cyclic $\iff$ $\exists\ I \trianglelefteq R$ ideal s.t

$$M \cong {}_R(R/I)$$

moreover, I is unique

<u>Proof</u>

<u>$\Leftarrow$)</u> ${}_RR$ is cyclic, ${}_RR = R.1$

$\Rightarrow \forall\ I \trianglelefteq R$ ideal, $I \leqslant_R R$ submod

$\overset{\text{corollary}}{\Rightarrow}$ ${}_R(R/I)$ is cyclic, generated by $1+I$ $\square$

$\underset{M}{\overset{\shortparallel}{}}$

<u>$\Rightarrow$)</u>

M cyclic $\Rightarrow$ $\exists\ x \in M$ s.t $M = Rx$

Consider the (module) homomorphism

$$\varphi :\ {}_RR \longrightarrow M = Rx$$
$$r \longmapsto rx$$

φ surjective as $\operatorname{Im}\varphi = M$

$\ker\varphi \leqslant_R R$ submod, then $I = \ker\varphi \trianglelefteq R$

$\overset{\text{1st Iso Thm}}{\Rightarrow}$ $R/I \cong M$

Assume $M \cong R/_I \cong R/_J$ for $I, J \trianglelefteq R$

$\Rightarrow \exists \beta : R/_I \xrightarrow{\sim} R/_J$ module isomorphism

$\Rightarrow \exists r \in R$ s.t $\beta(r+I) = 1+J$

For any $i \in I \subseteq R$

$$i(r+I) = ir + I = \underline{0 + I}$$

$$\beta(i(r+I)) = \beta(0+I) = 0+J$$

BUT we also see $\beta(i(r+I)) = i\,\beta(r+I)$
$$= i(1+J)$$
$$= i + J$$

$$i + J = 0 + J \Rightarrow i \in J$$
$$\Rightarrow I \subseteq J$$

If we consider $\beta^{-1} : R/_J \to \frac{R}{I}$

and do the same thing, we get $J \subseteq I$

$$\Rightarrow \underline{I = J}$$

$\square$

<u>Defn 3.9</u>

${}_R M$, R-mod, $X \subseteq M$ (non-empty) subset of M, we define the <u>annihilator of X</u> by

$$\text{ann}(X) := \{ r \in R \mid r \cdot x = 0 \quad \forall x \in X \}$$

N.B. In vector spaces this would only be 0. So, this is something new.

Examples

① $R = \mathbb{Z}$, $G = \mathbb{Z}/16\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{15}\}$

Pick $\bar{4} \in G$, $X = \{\bar{4}\}$

$\therefore ann(\bar{4}) = \{n \in \mathbb{Z} \mid n \cdot \bar{4} = \bar{0}\}$

$= \{n \in \mathbb{Z} \mid \overline{4n} = \bar{0}\}$

means $16 \mid 4n$

$\Rightarrow 4n = 4 \cdot 4k$

$\Rightarrow n = 4k$

$\Rightarrow 4 \mid n$

$\therefore ann(\bar{4}) = \{n \in \mathbb{Z} \mid 4 \mid n\} = (4)$

N.B. We actually find that, by doing this, we will always get an ideal

Prop^n 3.4

(I) $ann(X) \trianglelefteq R$ ideal

(II) $ann(X) = \bigcap_{x \in X} ann(x)$

Proof

(I) $0 \in ann(X)$

$r, s \in ann(X) \Rightarrow \forall x \in X \quad (r+s)x = \underset{0}{\underset{\shortparallel}{rx}} + \underset{0}{\underset{\shortparallel}{sx}} = 0$

$\Rightarrow r + s \in ann(X)$

$r \in \operatorname{ann}(X), \quad r' \in R$

$$\Rightarrow \forall x \in X \quad (r'r)\cdot x = r'(r\cdot x)$$
$$= r\cdot 0 = 0$$

$$\Rightarrow r'r \in \operatorname{ann}(X)$$

$\therefore$ ideal $\square$

Example

R ID $\quad M = {}_R R$, $x \in M$ s.t. $x \neq 0$

$$\operatorname{ann}(x) = \{ r \in R \mid rx = 0 \} = \{0\}$$

$x \neq 0 \Rightarrow r = 0$ as R ID

Remark: ${}_R M$ R-mod, $x \in M$

$R\cdot x$ cyclic $\quad Rx \cong R/I$, where $I = \operatorname{ann}(x)$

Theorem 3.3 (2nd Isomorphism Theorem)

M R-mod, $A, B \leq M$ submods

$$\Rightarrow \boxed{\frac{A+B}{A} \cong \frac{B}{A\cap B}}$$

Proof

Same as that for rings $\square$

15

What we know as Correspondence Thm

Theorem 3.4 (3rd Isomorphism Theorem) M R-mod, $P \leq M$ submod, then there is a byection

$$\{Q \leq M \mid P \leq Q\} \xleftrightarrow{1:1} \{\text{submods of } M/P\}$$
$$Q \longmapsto Q/P$$

3rd IT as we know it

and moreover $\boxed{{}^{M/P}\!/_{Q/P} \cong M/Q}$

Proof

Same as that for rings $\square$

Direct Sum of Modules

Def^n 3.10

$M_1, \ldots, M_n$ R-mods

Define $M = \{(m_1, m_2, \ldots, m_n) \mid m_i \in M_i\}$ $(= M_1 \times \ldots \times M_n)$

set - $(m_1, \ldots, m_n) + (m_1', \ldots, m_n') = (m_1 + m_1', m_2 + m_2', \ldots, m_n + m_n')$

- $-(m_1, \ldots, m_n) := (-m_1, \ldots, -m_n)$

- $0 := (0_{m_1}, \ldots, 0_{m_n})$

- $r(m_1, \ldots, m_n) := (rm_1, \ldots, rm_n)$

with these operations, M becomes an R-module called the (external) direct sum of the M_i's and we can write

$$M = M_1 \oplus \ldots \oplus M_n = \bigoplus_{i=1}^{n} M_i$$

If we take $M_i' = \{(0, \ldots, 0, \underset{\uparrow i}{m_i}, 0, \ldots, 0) \mid m_i \in M_i\}$

$\Rightarrow M_i' \leq M$ submodule, and $M_i \cong M_i'$

So, we can identify M_i with M_i' and look at M_i as a submodule of M.

Q: If M R-mod, $M_1, \ldots, M_n \leq M$ submodules

what conditions on the M_i's ensure that
$M = \bigoplus_{i=1}^{n} M_i$?

Here, we want to 'break up' M and want to know how.

Assume $M = M_1 \oplus M_2 \oplus \ldots \oplus M_n = \{(m_1, \ldots, m_n) \mid m_i \in M_i\}$
For each $m \in M$ $\exists$ $m_1 \in M_1, \ldots, m_n \in M_n$
s.t $m = (m_1, \ldots, m_n)$
and $(m_1, \ldots, m_n) = (m_1, 0, \ldots, 0) + (0, m_2, 0, \ldots, 0) + \ldots + (0, \ldots, 0, m_n)$
$$m = m_1 + m_2 + \ldots + m_n$$
i.e. each m can be written as a sum of m_i's
$$\Rightarrow M = M_1 + \ldots + M_n$$

Moreover, if $m_i \in M_i$, $m_i = (0, \ldots, 0, m_i, 0, \ldots, 0)$

$$\Rightarrow m_1 + \ldots + m_n = (m_1, m_2, \ldots, m_n) = 0$$
$$\Leftrightarrow (m_1, m_2, \ldots, m_n) = (0, 0, \ldots, 0)$$
$$\Leftrightarrow m_1 = 0, m_2 = 0, \ldots, m_n = 0$$

[Looks similar to LI - needs some tweaking, though]

Defn 3.11
M R-mod, $M_1, \ldots, M_n \leq M$ submods
We say that $\{M_1, \ldots, M_n\}$ is an independent set of modules if $m_1 + \ldots + m_n = 0 \Rightarrow m_1 = \ldots = m_n = 0$

Remark

We just showed that:

if $M = \bigoplus_{i=1}^{n} M_i \Rightarrow \begin{cases} M = M_1 + \dots + M_n \\ \{M_1, \dots, M_n\} \text{ independent set of mods} \end{cases}$

Our goal now is to show the reverse.
If we asked if 2 modules are independent, we cannot answer that question. This is because we can ~~may~~ see any module as a sum of others and only then can we relate some sort of 'independence'.

Prop^n 3.5

M R-mod, $M_1, \dots, M_n \leq M$ submods.
Then the following are equivalent:

1/ $\{M_1, \dots, M_n\}$ is an independent set of mods

2/ Every $m \in M_1 + \dots + M_n$ can be written as

$$m = m_1 + \dots + m_n$$

in a unique way

omit the M_i

3/ $\forall i = 1, \dots, n$ one has $M_i \cap (M_1 + \dots + M_{i-1} + M_{i+1} + \dots + M_n) = 0$

this is equiv to 2 vectors in direct sum iff $v_1 \cap v_2 = 0$

Proof

1=>2/

Let $m \in M_1 + \dots + M_n$, $m = m_1 + \dots + m_n$
$= m_1' + \dots + m_n'$

$\therefore 0 = \underbrace{(m_1 - m_1')}_{M_1} + \dots + \underbrace{(m_n - m_n')}_{M_n}$

$$\left.\begin{aligned} \Rightarrow m_1 - m_1' &= 0 \\ m_2 - m_2' &= 0 \\ &\vdots \\ m_n - m_n' &= 0 \end{aligned}\right\} \Rightarrow m_i = m_i' \quad \forall i$$

QED(1=>2)

2=>3)

Take $m \in M_i \cap (M_1 + \dots + M_{i-1}, M_{i+1} + \dots + M_n)$

$m \in M_i \Rightarrow m = m_i$

and

$m \in M_1 + \dots + M_{i-1} + M_{i+1} + \dots + M_n \Rightarrow m = m_1 + \dots + m_{i-1} + m_{i+1} + \dots + m_n$

$$m_i = m_1 + \dots + m_{i-1} + m_{i+1} + \dots + m_n$$

$$\Rightarrow 0 = m_1 + \dots + m_{i-1} - m_i + m_{i+1} + \dots + m_n$$
$$= 0 + 0 + \dots + 0$$

$\therefore$ by uniqueness,
$$\left.\begin{aligned} m_1 &= 0 \\ m_2 &= 0 \\ &\vdots \\ m_i &= 0 \\ &\vdots \\ m_n &= 0 \end{aligned}\right\} \Rightarrow m = 0$$

QED(2=>3)

3=>1)

Take $m_1 + m_2 + \dots + m_n = 0$

$$\Rightarrow \underbrace{m_2 + \dots + m_n}_{\in M_2} = \underbrace{-m_1}_{\in M_1} = x \in M_1 \cap (M_2 + \dots + M_n)$$

$\Rightarrow x = 0$ (by 3) $\Rightarrow m_1 = 0$

Now $\underbrace{0 + m_3 + \dots + m_n}_{\in M_1 + M_3 + \dots + M_n} = -m_2 \implies m_2 = 0$ as before

In general,

$$\underbrace{m_1 + \dots + m_{i-1} + m_{i+1} + \dots + m_n}_{\in M_1 + \dots + M_{i-1} + M_{i+1} + \dots + M_n} = -m_i \in M_i$$

$\implies m_i = 0$

QED

Example

M R-mod $A, B \leq M$ submods

$\implies \{A, B\}$ independent $\iff A \cap B = 0$

N.B. If we had $A, B, C \leq M$ submods,
it is not enough to check $A \cap B \cap C = 0$!
We need to check $A \cap (B + C) = 0$

Prop^n 3.6

M R-mod, $M_1, \dots, M_n \leq M$ submods,
then

$M = M_1 \oplus M_2 \oplus \dots \oplus M_n \iff \left\{ \begin{array}{l} M = M_1 + \dots + M_n \\ \text{and} \\ \{M_1, \dots, M_n\} \text{ independent set of mods} \end{array} \right.$

Proof

$\Rightarrow$) Already done

$\Leftarrow$)

$$\left.\begin{array}{l} M = M_1 + \dots + M_n \\ \{M_i\}_{i=1}^n \text{ indeps} \end{array}\right\} \Rightarrow \begin{array}{l} \forall m \in M \text{ there are unique} \\ m_1 \in M_1, \dots, m_n \in M_n \text{ s.t.} \\ m = m_1 + \dots + m_n \end{array}$$

Define $\alpha : M \longrightarrow \bigoplus_{i=1}^{n} M_i$

$m \longmapsto (m_1, \dots, m_n)$ ← these exist and are unique : well defined

α module hom (easy)

$\ker \alpha = \{ m \mid \alpha(m) = 0 = (0, \dots, 0) \} \Rightarrow m = 0 + 0 + \dots + 0 = 0$
$= \{0\}$

$\operatorname{Im} \alpha = \{ \alpha(m) \mid m \in M \} = \bigoplus_{i=1}^{n} M_i$

Take $(m_1, \dots, m_n) \in \bigoplus_{i=1}^{n} M_i$, $m_i \in M_i \leq M$

$\alpha(m_i) = (0, \dots, 0, m_i, 0, \dots, 0)$
$\alpha(m_1 + \dots + m_n) = (m_1, \dots, m_n)$
$\Rightarrow \operatorname{Im} \alpha = \bigoplus_{i=1}^{n} M_i$

α is surjective $\Rightarrow \alpha$ isomorphism

$\Rightarrow M \cong \bigoplus_{i=1}^{n} M_i$ □

N.B. Often we will say two things are equal and show they are isomorphic, this is as good as we can get here

Notation: If $M_1 = M_2 = \ldots = M_n = M$

$$\Rightarrow \bigoplus_{i=1}^{n} = M \oplus M \oplus \ldots \oplus M = M^n$$

Free Modules

Def^n 3.12

Let R be a ring, a module of the form
$$F = ({}_R R)^n = {}_R R \oplus {}_R R \oplus \ldots \oplus {}_R R$$

no confusion as no direct product of rings. To be super precise, include subscript R

will ~~initiale~~ be called a free module (of rank n) over R

In a sense, these will be the easiest modules we can construct (apart from 0-mod and trivial-mod)

Def^n 3.13

M R-mod, $\{e_1, \ldots, e_n\} \subseteq M$ subset.

We say that $\{e_1, \ldots, e_n\}$ is a basis of M if $\forall m \in M$ $\exists$ unique $r_1, \ldots, r_n \in R$ s.t

$$m = r_1 e_1 + \ldots + r_n e_n$$

Remark: If $\{e_1, \ldots, e_n\}$ basis of M and $r \in R$ s.t

$r \cdot e_i = 0 \implies r = 0$

$\implies \operatorname{ann}(e_i) = 0$

$$Re_i \cong R/\underbrace{\operatorname{ann}(e_i)}_{0} = R$$

$$\therefore Re_i \cong R$$

Theorem 3.5

R ring, M R-mod, then ~~has~~
M has a basis $\iff$ M is free

Proof

$\implies$| $\{e_1, \ldots, e_n\} \subseteq M$ basis $\implies \forall m \in M \; \exists \overset{\text{unique}}{!}$

$r_i \in R$ s.t $m = r_1 e_1 + \ldots + r_n e_n$

Define $\alpha : M \longrightarrow R^n$
$m \longmapsto (r_1, \ldots, r_n)$

α is a mod hom (easy)

$\operatorname{Ker} \alpha = 0$
$\operatorname{Im} \alpha = R^n$ $\quad (r_1, \ldots, r_n) = \alpha(r_1 e_1 + \ldots + r_n e_n)$
$\implies \operatorname{Im} \alpha = R^n$

$\implies M \cong R^n \implies M$ is free

$\Longleftarrow$| $M = R^n = \{(r_1, \ldots, r_n) \mid r_i \in R\}$

$e_1 = (1, 0, \ldots, 0)$, $e_2 = (0, 1, 0, \ldots, 0)$, $\ldots$, $e_n = (0, \ldots, 0, 1)$
$\implies \{e_1, \ldots, e_n\}$ basis of R^n $\square$

Prop^n 3.6

$F = R^n$ free R-mod with basis $\{e_1, \dots, e_n\}$
M R-mod, then $\forall m_1, \dots, m_n \in M$ there is a unique module homomorphism $\varphi : R^n \to M$
s.t $\varphi(e_i) = m_i$

Proof
Assume $\varphi : R^n \to M$ mod hom s.t $\varphi(e_i) = m_i$
$\forall x \in R^n$ there are unique $r_1, \dots, r_n \in R$ s.t

$$x = r_1 e_1 + \dots + r_n e_n$$

$$\begin{aligned} \varphi(x) = \varphi(r_1 e_1 + \dots + r_n e_n) &= \varphi(r_1 e_1) + \dots + \varphi(r_n e_n) \\ &= r_1 \varphi(e_1) + \dots + r_n \varphi(e_n) \\ &= r_1 m_1 + \dots + r_n m_n \end{aligned}$$

$\Rightarrow \varphi$ is unique

Now, define $\varphi(x) = r_1 m_1 + \dots + r_n m_n$, where $x = \sum_{i=1}^{n} r_i e_i$

φ is a mod hom (easy)

$$\varphi(e_i) = 0 \cdot m_1 + \dots + 0 \cdot m_{i-1} + 1 \cdot m_i + 0 \cdot m_{i+1} + \dots + 0 \cdot m_n$$
$$= m_i \quad \square$$

Prop^n 3.7

M finitely generated R-mod
$\Rightarrow \exists$ F free R-mod and $P \leq F$ submod
s.t $M = F/P$

Proof
M finitely generated $\Rightarrow \exists\, m_1, \dots, m_n \in M$ s.t
$M = Rm_1 + Rm_2 + \dots + Rm_n$

Take $F = R^n \Rightarrow F$ has a basis $\{e_1, \dots, e_n\}$
By prop^n 3.6 $\exists\, \varphi . F \longrightarrow M$ mod hom
s.t $\varphi(e_i) = m_i$

$\forall m \in M \quad \exists\, r_1 \dots r_n \in R$ s.t $m = r_1 m_1 + \dots + r_n m_n$
why? Because $M = Rm_1 + Rm_2 + \dots + Rm_n$

$\Rightarrow \varphi(r_1 e_1 + \dots + r_n e_n) = m$
$\Rightarrow \operatorname{Im} \varphi = M$

$\operatorname{Ker} \varphi$ may not be 0 as $m = r_1 m_1 + \dots + r_n m_n$
may not be unique.

BUT $P = \operatorname{Ker} \varphi \leq F \xRightarrow[\text{Thm}]{\text{1st Iso}} M \cong F/P$ □

Theorem 3.6
R PID
If $R^m \cong R^n \Rightarrow m = n$

Proof ⌜Sketch of last year's proof - online ⌝

$I \trianglelefteq R$ maximal, R/I field
⌞$\varphi \cdot R^m \xrightarrow{\sim} R^n \longrightarrow \tilde{\varphi} : (R/I)^m \xrightarrow{\sim} (R/I)^n$⌟

Let Q = field of fractions of R

Q^m, Q^n v.s $/Q$

Assume $\varphi: R^m \to R^n$ isomorphism of R-mods

Define $\psi: Q^m \to Q^n$
x

$x = (q_1, \dots, q_m)$, $q_i \in Q = \mathrm{Frac}(R)$

$\Rightarrow q_i = \frac{a_i}{b_i}$, $a_i, b_i \in R$, $b_i \neq 0$

~~xx~~ $x = \left(\frac{a_1}{b_1}, \frac{a_2}{b_2}, \dots, \frac{a_m}{b_m}\right) = \frac{1}{\underbrace{b_1 b_2 \cdots b_m}_{d}}(a_1c_1, a_2c_2, \dots, a_mc_m)$

$c_i = b_1 \cdots b_{i-1} b_{i+1} \cdots b_m$

$\psi(x) = \psi\left(\frac{1}{d}(a_1c_1, \dots, a_mc_m)\right)$

$\psi(x) := \frac{1}{d}\varphi(a_1c_1, \dots, a_mc_m)$

Show:

- ψ linear map ✓ (easy)
- ψ isomorphism

  $\psi(x) = 0$

  " $\frac{1}{d}\varphi(a_1c_1, \dots, a_mc_m) \Rightarrow \varphi(a_1c_1, \dots, a_mc_m) = (0, \dots, 0)$

$$\Rightarrow (a_1 c_1, \dots, a_m c_m) = (0, 0, \dots, 0)$$

$\Rightarrow a_1 c_1 = 0$

$a_2 c_2 = 0$ $\qquad\qquad c_i \neq 0$ as b_j's $\neq 0$

$\vdots$

$a_m c_m = 0$

$\Rightarrow a_1 = a_2 = \dots = a_m = 0 \Rightarrow x = 0$

$\therefore \psi$ injective.

φ surjective $\Rightarrow \exists x_1 \in R^m$ s.t. $\varphi(x_1) = (1, 0, \dots 0)$

$\vdots$

$x_i \in R^m$ s.t. $\varphi(x_i) = (0, \dots, 1, \dots, 0)$

$\vdots$

$x_n \in R^m$ s.t. $\varphi(x_n) = (0, \dots, 0, 1)$

$\forall (s_1/t_1, \dots, s_n/t_n) \in Q^n$

$= \varphi(s_1/t_1 x_1 + s_2/t_2 x_2 + \dots + s_n/t_n x_n) \Rightarrow \varphi$ surjective

ψ isomorphism $\Rightarrow Q^m \cong Q^n \underset{\text{Theorem}}{\overset{\text{basis}}{\Rightarrow}} m = n$ $\square$

<u>Def^n 3.14</u>

F free R-mod (R PID)

$\Rightarrow \underset{\text{rank}}{\underline{rk}}(F) =$ no$^{\circ}$ elements in a basis of F

Free Modules, Finitely Generated Modules and PIDs

Generators and Relations

A discription of a module by generators and relations is,

$$M = \langle e_1, \dots, e_n \mid \underbrace{\sum_{i=1} a_{ij} e_i = 0}_{f}, \ a_{ij} \in R \ \text{ for } j = 1, \dots, m \rangle$$

$$M = \langle e_1, \dots, e_n \mid f_1 = 0, f_2 = 0, \dots, f_m = 0 \rangle$$

F = free mod with basis $e_1, \dots, e_n$

$f_1, \dots f_m \in F$, $P = \langle f_1, \dots, f_m \rangle \leq F$

$M = F/P$

If we had,

$$G = \langle x, y, z \mid xy = yx,\ xz = zx,\ yz = zy,\ x^8 y^7 = z^2,\ x^{11} = 1 \rangle$$

could we discuss what this group is? How it behaves? Not yet!

Def^n 3.15

We say that M is finitely presented if $M \simeq F/P$ with F finitely generated free module, $P \leq F$ finitely generated submodule

Prop^n 3.8

R ring, M R-mod, $P \leq M$ submod

If P and M/P are finitely generated $\Rightarrow M$ is also finitely gen

Proof

If we were in vector spaces, this would be simple, just notice a mapping $\varphi: V \to V/W$, $\ker\varphi = W$, $\operatorname{Im}\varphi = V/W$ and apply Rank-Nullity Theorem.

Now,

M/P finitely generated $\Rightarrow \exists\, \bar{x}_1, \ldots, \bar{x}_k$ generators for M/P

P finitely generated $\Rightarrow \exists\, y_1, \ldots, y_l$ generators for P

$m \in M \Rightarrow \bar{m} = \overline{m + P} \in M/P$

$\Rightarrow \bar{m} = r_1\bar{x}_1 + \ldots + r_k\bar{x}_k$

$\Rightarrow m = r_1x_1 + \ldots + r_kx_k + p$, for some $p \in P$

$\Rightarrow \exists\, s_1, \ldots, s_l \in R$ s.t $p = s_1y_1 + \ldots + s_ly_l$

$\Rightarrow m = r_1x_1 + \ldots + r_kx_k + s_1y_1 + \ldots + s_ly_l$

So, $\{x_1, \ldots, x_k, y_1, \ldots, y_l\}$ is a finitely generating set for M $\square$

Prop^n 3.9

R PID, then every submod of a finitely generated free mod is finitely generated.

In particular, every finitely generated mod is finitely presented

Proof

F = free mod with basis $e_1 \ldots e_n$

By induction on n,

<u>$n=1$</u> $\Rightarrow \quad F = Re_1 \cong_R R \quad , \quad P \leq F \Rightarrow P \leq_R R$

$$\Rightarrow P \trianglelefteq \text{ideal} \overset{R \text{ PID}}{\Rightarrow} P = (a) \Rightarrow P \text{ is finitely generated}$$

Assume every submod of a free mod of rank n is finitely generated. F free mod with basis $\{e_1, \dots, e_{n+1}\}$ $P \leq F$.

Define the mapping $\alpha : F \longrightarrow R$

$$e_i \longrightarrow \delta_{i,n+1} = \begin{cases} 0, & i \neq n+1 \\ 1, & i = n+1 \end{cases}$$

So, $\alpha : F \longrightarrow R$

$$(r_1, \dots, r_{n+1}) \longmapsto r_{n+1}$$

α is a mod hom

$\ker \alpha$ = free module generated by $\{e_1, \dots e_n\}$

$$\begin{tikzcd} F \arrow[r, "\alpha"] & R \\ P \arrow[u, hook, "\text{inclusion map}"] \arrow[ur, dotted, "\beta"'] & \end{tikzcd}$$

$\beta = \alpha_{|P}$ mod hom

$\ker \beta = P \cap \ker \alpha \leq \ker \alpha$ free of rank n

$\Rightarrow \ker \beta$ finitely generated

$\operatorname{Im} \beta \leq_R R$ free of rank 1 $\quad \therefore \operatorname{Im} \beta$ finitely generated

Apply 1st Isomorphism Theorem:

$$\frac{P}{\ker \beta} \cong \operatorname{Im} \beta \qquad \text{finitely generated}$$

So, we have $\ker \beta \leq P$ and finitely generated $\overset{\text{Prop}^n}{\Rightarrow}$ P finitely gen $\square$

N.B. Thanks to this, we can now 'forget' the abstract modular nature and work with matrices

R PID

M finitely generated R-mod $\Rightarrow M = F/P$

$F = R^n$ free

$P \leq F \Rightarrow P$ finitely generated
$\Rightarrow P = Rf_1 + \dots + Rf_m$

$M = \langle \underbrace{r_1 e_1 + \dots + r_n e_n}_{e_1 \dots e_n} \mid f_1 = 0, f_2 = 0, \dots f_m = 0 \rangle$

$$f_j = \sum_{i=1}^{n} a_{ij} e_i \rightsquigarrow A = [M] = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & & \ddots & \vdots \\ a_{n1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

$\in M_{m \times n}(R)$

presentation matrix of M

So, M f.g / R PID $\Rightarrow M = F/P$ F free, $P \leq F$ f.g
$\Rightarrow M$ has presentation matrix $A = [a_{ij}]$
given by $f_i = \sum a_{ij} e_i$ for $\{f_1 \dots f_m\}$ generators of P

$M \rightsquigarrow A$

Q: What matrices are presentation matrices for M?

N.B. Pretty much everything we know for matrices will work here, with the exception of one theorem which we must be careful with - we will see this later.

Matrices over PIDs

R PID , $M_n(R) \equiv n \times n$ matrices w/ coefficents in R

$GL_n(R) \equiv$ invertible $n \times n$ matrices

$$A \in M_n(R) \Rightarrow \det(A) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma)\, a_{1\sigma(1)} \cdots a_{n\sigma(n)}$$

Warning! : If $R = \mathbb{F}$, by Cramer's Rule

$$A \in GL_n(R) \iff \det A \neq 0$$

and $$A^{-1} = \frac{1}{\det A} (\operatorname{adj}(A))^t$$

In rings, we cannot do this in general. Just because something is non-zero does not mean we can divide by it

! (New) Cramer's Rule

$$A \in M_n(R) \Rightarrow A \cdot (\operatorname{adj}(A))^t = \det A \, I_n$$

In particular, $A \in GL_n(R) \iff \det(A) \in \mathcal{U}(R)$ and in that case, $A^{-1} = (\det(A))^{-1} (\operatorname{adj}(A))^t$

N.B. this is what happens with $R = \mathbb{F}$

N.B. ~~Beware~~ Beware! Over rings we cannot divide. We can subtract, multiply but not divide - unless we are dealing with units. Remember, if all non-zero elements are a unit (i.e. a field) we have a division Ring

Examples

① $A = \begin{bmatrix} 1 & 2 \\ 2 & 2 \end{bmatrix} \in M_2(\mathbb{Z})$,

$A \notin GL_2(\mathbb{Z})$ as $\det(A) = -2 \notin \mathcal{U}(\mathbb{Z})$

② $B = \begin{bmatrix} -2 & -1 \\ 1 & 1 \end{bmatrix} \in M_2(\mathbb{Z})$,

$\det(B) = -1 \in \mathcal{U}(\mathbb{Z}) \Rightarrow B \in GL_2(\mathbb{Z})$

$M = R^m$ free mod of rank m w/ basis $\{e_1, \dots, e_m\}$
$N = R^n$ free mod of rank n w/ basis $\{f_1, \dots, f_n\}$

$\forall x \in M$, $x = \sum_{i=1}^{m} r_i e_i \rightsquigarrow [x]_e = \begin{bmatrix} r_1 \\ \vdots \\ r_m \end{bmatrix}$

$\alpha : M \to N$ mod hom
α is determined by $\alpha(e_i) = \sum_{j=1}^{n} a_{ji} f_j$, $a_{ji} \in R$

$$A = [a_{ji}] = \begin{bmatrix} \uparrow & & \uparrow \\ [\alpha(e_1)]_f & \cdots & [\alpha(e_m)]_f \\ \downarrow & & \downarrow \end{bmatrix} = [\alpha]_f^e$$

So, we get a correspondence,

$\alpha \longmapsto [\alpha]_f^e$: fix the bases

this provides a module isomorphism , $Hom_R(M, N) \simeq M_{n \times m}(R)$

Some properties

i) $[\alpha(m)]_f = [\alpha]_f^e [m]_e$ $\qquad \alpha : M^e \to N^f$

ii) $[\beta \circ \alpha] = [\beta]_g^f [\alpha]_f^e$ $\qquad \beta : N \to P_g$

iii) α is an isomorphism
$\iff m = n$
and $[\alpha]_f^e \in GL_m(R)$

$$\begin{tikzcd} {}^eM \arrow[r, "\alpha"] \arrow[dr, "\beta\circ\alpha"'] & N_f \arrow[d, "\beta"] \\ & P_g \end{tikzcd}$$

iv/ If e, e' bases of M $\quad$ & $M \xrightarrow{Id_M} M$ e'

$\Rightarrow \underbrace{[Id]^{e}_{e'}}_{} \in GL_n(R)$

transition matrix from e to e'

$$\begin{tikzcd} \overset{e'}{M} \arrow[r, "Id_M"] \arrow[rrr, bend right, "\alpha"'] & \overset{e}{M} \arrow[r, "\alpha"] & \overset{f}{N} \arrow[r, "Id_N"] & \overset{f'}{N} \end{tikzcd}$$

$$\Rightarrow \boxed{\underbrace{[\alpha]^{e'}_{f'}}_{A'} = \underbrace{[Id_N]^{f}_{f'}}_{X} \cdot \underbrace{[\alpha]^{e}_{f}}_{A} \underbrace{[Id_M]^{e'}_{e}}_{Y}}$$

$A' = XAY$ $\quad$ w/ $\quad X \in GL_n(R)$
$\qquad\qquad\qquad\qquad Y \in GL_m(R)$

Defⁿ 3.16

$A, B \in M_{n\times m}(R)$, we say that A and B are equivalent $(A \sim B)$ if $\exists\ X \in GL_n(R)$, $Y \in GL_m(R)$

s.t $B = XAY$

Back to finitely presented modules

M R-mod, $M = F/P$ $\qquad$ F has basis $e = \{e_1, \dots, e_n\}$
P has a generating set $\{f_1 \dots f_m\}$
$P \leq F$

N.B. P does not need to be free, $\{f_1, \dots, f_m\}$ is not a basis so we cannot use anything we just did

$$f_j = \sum_{i=1}^{n} a_{ij} e_i \quad , \quad A = [a_{ij}] \text{ presentation matrix}$$
$$A \in M_{n\times m}(R)$$

G free module ~~of~~ of rank m w/ basis $g = \{g_1, \dots, g_m\}$

Take $\alpha : G \to F$
the mod hom given by
$$\alpha(g_j) = f_i$$

$$[\alpha]_e^g = A$$

$\operatorname{Im} \alpha = P$ Why? Must be submodule of F and, as we are dealing with f and rank $m \Rightarrow P$

Take $e' = \{e_1' \dots e_n'\}$ basis of F
$g' = \{g_1' \dots g_m'\}$ basis of G

P doesn't change because we changed basis of F, G just the representation

<u>N.B.</u> Can only change basis with free modules

So,
$$\forall p \in P \ , \ p \in \operatorname{Im}\alpha \Rightarrow p = \alpha(r_1 g_1' + \dots + r_m g_m') \text{ for some } r_j \in R$$
$$= \sum_{j=1}^{m} r_j \alpha(g_j')$$

$\Rightarrow \{\alpha(g_1') \dots \alpha(g_m')\}$ is a generating set for P

$$\alpha(g_j') = \sum_{i=1}^{n} a_{ij}' e_i' \quad , \quad A' = [a_{ij}'] = [\alpha]_{e'}^{g'}$$
is also a presentation matrix for M

$$A' = [\alpha]_{e'}^{g'} = \underbrace{[Id_F]_{e'}^{e}}_{X} \underbrace{[\alpha]_{e}^{g}}_{A} \underbrace{[Id_G]_{g}^{g'}}_{Y}$$

$$\Rightarrow \boxed{A \sim A'}$$

Theorem 3.7

Let $A, B \in M_{m\times n}(R)$, then A and B are presentation matrices for the same module $\Leftrightarrow$ $A \sim B$

N.B. multiplying by invertible matrix on left means column op.

multiplying by invertible matrix on right means row op

Over $\mathbb{F}$, doing this leads to reduced row echelon form and reduced column echelon form. Which will lead to:

$$\left(\begin{array}{c|c} \begin{matrix} 1 & 0 & \cdots & 0 \\ 0 & \ddots & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{matrix} & 0 \\ \hline 0 & 0 \end{array}\right) = \text{Hermite Normal Form}$$

Goal: Find a "nice" form for matrices under equivalence

Elementary row / column ops

I. Swapping two rows / columns $\left(\begin{matrix} R_i \longleftrightarrow R_j \\ C_i \longleftrightarrow C_j \end{matrix} \right)$

II. Multiply a row / column by a UNIT $\lambda \in U(R)$

λR_i, λC_j

most useful → III. Add to a row/column another row or column, multiplied by any element, $\lambda \in R$,

$$\left. \begin{matrix} R_i + \lambda R_j \\ C_i + \lambda C_j \end{matrix} \right\}$$

$A \in M_{m\times n}(R)$ is diagonal if $a_{ij} = 0$ whenever $i \neq j$

i.e.

$$\left[\begin{array}{ccc|c} a_{11} & & 0 & \\ & \ddots & & 0 \\ 0 & & a_{mm} & \end{array}\right] \quad (\text{if } n \geq m)$$

or

$$\left[\begin{array}{ccc} a_{11} & & 0 \\ & \ddots & \\ 0 & & a_{nn} \\ \hline & 0 & \end{array}\right] \quad (\text{if } m \geq n)$$

<u>Theorem</u> 3.8 (Smith Normal Form)

R PID, then $\forall A \in M_{m\times n}(R)$ there is a diagonal matrix $D = D(d_1, \dots, d_r)$, where $r = \min(m, n)$ s.t $A \sim D$ and $d_1 | d_2 | d_3 | \dots | d_r$

Moreover, the elements d_i are unique up to associates, i.e. the ideals (d_i) are unique.

The matrix D is called the <u>Smith Normal Form (SNF)</u> of A and the d_i's are called the <u>invariant factors of A</u>

<u>N.B.</u> The proof is even more important

<u>Examples</u>

① $A = \begin{bmatrix} 4 & -3 \\ -2 & 1 \end{bmatrix} \in M_2(\mathbb{Z})$

(want the smallest number up to divisibility, i.e. 1, in the top left).

So,
$$A \underset{C_1 \leftrightarrow C_2}{\overset{R_1 \leftrightarrow R_2}{\sim}} \begin{bmatrix} 1 & -2 \\ -3 & 4 \end{bmatrix} \overset{R_2 + 3R_1}{\sim} \begin{bmatrix} 1 & -2 \\ 0 & -2 \end{bmatrix}$$
$$-1 \in U(\mathbb{Z}) \overset{-R_2}{\sim} \begin{bmatrix} 1 & -2 \\ 0 & 2 \end{bmatrix}$$
$$\overset{R_1 + R_2}{\sim} \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$$

Is this SNF? They are equivalent as we used only elementary ops. $1 \mid 2$ and $1, 2$ unique up to associates.

$\therefore \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$ SNF of A

<u>N.B.</u> If we didn't do $-R_2$ and instead did $r_1 - r_2$, we would get
$$\begin{bmatrix} 1 & 0 \\ 0 & -2 \end{bmatrix}.$$
which is also SNF as $2 \sim -2$, i.e. $-2 = (-1) \cdot 2$ s.t. $-1 \in U(\mathbb{Z})$

(2) $B = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & -2 \end{bmatrix} \in M_3(\mathbb{Z})$

Not SNF as $2 \nmid 3 \nmid -2$

So, $B \underset{}{\overset{R_3+R_2}{\sim}} \begin{bmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 3 & -2 \end{bmatrix} \overset{C_3+C_2}{\sim} \begin{bmatrix} 2 & 0 & 0 \\ 0 & 3 & 3 \\ 0 & 3 & 1 \end{bmatrix}$

$\underset{\substack{C_1 \leftrightarrow C_3 \\ R_1 \leftrightarrow R_3}}{\sim} \begin{bmatrix} 1 & 3 & 0 \\ 3 & 3 & 0 \\ 0 & 0 & 2 \end{bmatrix} \underset{C_2 - 3C_1}{\sim} \begin{bmatrix} 1 & 0 & 0 \\ 3 & -6 & 0 \\ 0 & 0 & 2 \end{bmatrix}$

$\underset{R_2 - 3R_1}{\sim} \begin{bmatrix} 1 & 0 & 0 \\ 0 & -6 & 0 \\ 0 & 0 & 2 \end{bmatrix} \underset{\substack{C_2 \leftrightarrow C_3 \\ R_2 \leftrightarrow R_3}}{\sim} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -6 \end{bmatrix}$

$1 \mid 2 \mid -6$ and $1, 2, 6$ unique up to associates
$\Rightarrow$ SNF

(3) $C = \begin{bmatrix} 0 & 6 \\ 3 & 8 \\ 9 & 18 \end{bmatrix} \in M_{3\times 2}(\mathbb{Z})$

$C \underset{R_2 \leftrightarrow R_1}{\sim} \begin{bmatrix} 3 & 8 \\ 0 & 6 \\ 9 & 18 \end{bmatrix} \underset{C_2 - 3C_1}{\sim} \begin{bmatrix} 3 & -1 \\ 0 & 6 \\ 9 & -9 \end{bmatrix} \underset{\substack{C_2 \leftrightarrow C_1 \\ -C_1}}{\sim} \begin{bmatrix} 1 & 3 \\ -6 & 0 \\ 9 & 9 \end{bmatrix}$

$\underset{C_2 - 3C_1}{\sim} \begin{bmatrix} 1 & 0 \\ -6 & 18 \\ 9 & 36 \end{bmatrix} \underset{\substack{R_2 + 6R_1 \\ R_3 - 9R_1}}{\sim} \begin{bmatrix} 1 & 0 \\ 0 & 18 \\ 0 & 36 \end{bmatrix} \underset{R_3 - 2R_2}{\sim} \begin{bmatrix} 1 & 0 \\ 0 & 18 \\ 0 & 0 \end{bmatrix}$ SNF of C

General Strategy

1. Put the "smallest" element in position $(1,1)$

2. a) For each $j \neq 1$, if $a_{11} \mid a_{j1}$ then apply
$$R_j - \frac{a_{j1}}{a_{11}} R_1 \quad : \quad \text{make } a_{j1} = 0$$

   b) If $a_{11} \nmid a_{j1} \longrightarrow$ find $\gcd(a_{11}, a_{j1})$ and put it in R_1

$$\begin{bmatrix} 3 & 8 \\ \vdots & \vdots \end{bmatrix}$$

$$8 = 3 \cdot 2 + 2$$
$$\downarrow$$
$$8 - 2 \cdot 3 = 2$$

If we have Euclidean division
$ha + kb = d = \gcd(a, b)$
$\underbrace{(a) + (b)}_{(a,b)} = (d)$

So,

if R PID, $A \in M_{m \times n}(R)$
$\Rightarrow \exists \; D = D(d_1, \dots, d_r)$ diagonal s.t
$A \sim D$, $d_1 \mid d_2 \mid \dots \mid d_r$
and $D \equiv$ SNF of A
d_i's $\equiv$ invariant factors of A (unique up to associates)

Proof of Existence

Case 1 (R, N) ED

→ Goal: Show that $A \sim \left(\begin{array}{c|c} d_1 & 0 \\ \hline 0 & A' \end{array}\right)$

s.t d_1 divides all entries in A'

→ Do it by elementary ops.

* Step 0

Pick a_{ij} s.t $N(a_{ij})$ minimal

Assume $A \neq 0$, if $A = 0$ we are done

Apply $R_1 \longleftrightarrow R_i$, $C_1 \longleftrightarrow C_j$

* Step I

Suppose $\exists$ a_{1j} (in first row) s.t $a_{11} \nmid a_{1j}$

By euclidean division, $a_{1j} = q a_{11} + r$, $r \neq 0 \Rightarrow N(r) < N(a_{11})$

Apply $C_j - q C_1$ (r is now in pos $(1, j)$)

$C_j \longleftrightarrow C_1$ (r is in pos $(1,1)$)

* Start over

After a finite no° steps, this process is over

* Step II

Suppose $\exists$ a_{i1} (in first column) s.t $a_{11} \nmid a_{i1}$

By euclidean division, $a_{i1} = q a_{11} + r$, $r \neq 0 \Rightarrow N(r) < N(a_{11})$

Apply $R_i - q R_1$ (r is now in pos $(i, 1)$)

$R_i \longleftrightarrow R_1$ (r is now in pos $(1,1)$)

* Start over

After a finite no° steps, this process is over

→ When we do these two steps, we are getting gcd of $\left(\begin{array}{c|c} d_1 & 0 \\ \hline 0 & A' \end{array}\right)$

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

after steps I and II

$a_{11} \mid a_{1j} \quad \forall j$

$a_{11} \mid a_{i1} \quad \forall i$

* Step III

a) $\forall j$ apply $C_j - \frac{a_{1j}}{a_{11}} C_1$ (0 in position $(1,j)$)

b) $\forall i$ apply $R_i - \frac{a_{i1}}{a_{11}} R_1$ (0 in position $(i,1)$)

$$\left(\begin{array}{c|c} a_{11} & 0 \\ \hline 0 & A' \end{array}\right) \xrightarrow{\text{step IV } (*)} \left(\begin{array}{c|ccccc} a_{11} & a_{i2} & \cdots & a_{ij} & \cdots & a_{in} \\ \hline 0 & & & A' & & \end{array}\right)$$

* Step IV

Find a_{ij} s.t $a_{11} \nmid a_{ij}$

Apply $R_1 + R_i$ (or $C_1 + C_j$) (*)

Go back to Step I

N.B. for theoretical purposes, doesn't matter if we choose columns or rows. For practical purposes, choose one which will have fewer non-zero elements

* Step V

Now, $a_{11} \mid a_{ij} \quad \forall i j \Rightarrow d_1 = a_{11}$

$$\left(\begin{array}{c|c} a_{11} & 0 \\ \hline 0 & A' \end{array}\right)$$

Forget about first row and first column.
Apply some process to A'

Eventually:

$$\left(\begin{array}{c|c|cccc|c} d_1 & 0 & & \cdots & & & 0 \\ \hline 0 & d_2 & 0 & \cdots & & & 0 \\ \hline \vdots & 0 & \underline{d_3} & \ddots & & & \vdots \\ \vdots & \vdots & & & \ddots & & \vdots \\ 0 & 0 & \cdots & & & d_r & 0 \end{array}\right)$$

which is SNF.

Case 2 $\qquad ED \Rightarrow PID \Rightarrow UFD$

R PID but not an ED

Defn 3.17

R UFD we define the length map, $\lambda : R^* \to \mathbb{N}$ by

$$\lambda(a) = \begin{cases} 0 & , \text{ if } a \in U(R) \\ r & , \text{ if } a = p_1 \dots p_r \text{ , with } p_i \text{ irred} \end{cases}$$

Ex

$\underset{2\times 1}{\lambda(\overset{\shortparallel}{2})} = 1 \quad , \quad \lambda(\underset{5\times 3\times 2\times 1}{\overset{\shortparallel}{30}}) = 3 = \lambda(\underset{2\times 2\times 2}{\overset{\shortparallel}{8}})$

$$\left.\begin{array}{l} a = p_1 \dots p_r \\ b = q_1 \dots q_s \end{array}\right\} ab = p_1 \dots p_r q_1 \dots q_s$$

Prop^n 3.10

1. If $a, b \in R^*$ $\Rightarrow$ $\lambda(ab) = \lambda(a) + \lambda(b)$
2. If $a | b$ $\Rightarrow$ $\lambda(a) \leq \lambda(b)$
3. If $a \sim b$ $\Rightarrow$ $a | b$ and $\lambda(a) = \lambda(b)$

* Step 0'

Pick a_{11} with minimal length

* Step I'

Suppose $a_{11} \nmid a_{1j}$ (assume $j = 2$) ; $a_{11} \nmid a_{12}$

$d = \gcd(a_{11}, a_{12})$, $d \neq 0$ $\quad a_{11} = d \cdot y_1$

$a_{12} = d \cdot y_2$

$$R \text{ PID} \Rightarrow (a_{12}) + (a_{11}) = d$$
$$\Rightarrow d = x_1 a_{11} + x_2 a_{12}$$
$$\Rightarrow d = d x_1 y_1 + d x_2 y_2$$
$$\Rightarrow 1 = x_1 y_1 + x_2 y_2$$

$$Y = \left[\begin{array}{cc|c} x_1 & -y_2 & 0 \\ x_2 & y_1 & \\ \hline \multicolumn{2}{c|}{0} & I_{n-2} \end{array}\right] \in M_n(R)$$

, $\det(Y) = 1$ $\Rightarrow Y \in GL_n(R)$ $\Rightarrow AY \sim A$, $X = Id$

[$A \sim B \iff \exists X \in GL_n(R)$ $\exists Y \in GL_n(R)$ s.t. $B = XAY$]

$$A \cdot Y = \left[\begin{array}{cc|c} a_{11} & a_{12} & ? \\ a_{21} & a_{22} & \\ \hline \multicolumn{2}{c|}{?} & ? \end{array}\right] \cdot Y$$

$$= \left[\begin{array}{c|c} x_1 a_{11} + x_2 a_{12} & ? \\ \hline ? & ? \end{array}\right]$$

$$= \left[\begin{array}{c|c} d & ? \\ \hline ? & ? \end{array}\right]$$

$$D = XAY \ , \ \left.\begin{matrix} d \mid a_{11} \\ a_{11} \nmid a_{12} \end{matrix}\right\} \Rightarrow \lambda(d) < \lambda(a_{11})$$

* Start over

* Step II'

Same as before, modifying step II as we did for step I (i.e. assume $a_{11} \nmid a_{21}$)

$$X = \begin{bmatrix} x_1 & x_2 & 0 \\ -y_2 & y_1 & \\ 0 & & I_{n-2} \end{bmatrix} \in GL_n(R)$$

$XA \sim A$

$$\begin{bmatrix} d & \cdots \\ \vdots & \end{bmatrix}$$

Replace A by XA and start over

* Steps III, IV, V remain unchanged

At the end we get SNF_D

N.B What we just did is not very practical in rather, unless we are in a ED

Uniqueness of SNF

$A \in M_{m\times n}(R)$ $\quad (R \text{ PID})$

Defn 3.18

An $i\times i$ minor of A is an element of R of the form $\det(K)$, where K is an $i\times i$ submatrix of A

Defn 3.19

The i-th fitting ideal of A is

$J_i(A) =$ Ideal generated by all $i\times i$ minors of A

Examples

$$A = \begin{bmatrix} 1 & 2 & -1 \\ 3 & 4 & -1 \end{bmatrix} \in M_{2\times 3}(\mathbb{Z})$$

max is an $i\times i$ minor

$$J_1(A) = (1, 2, -1, 3, 4, -1) = (1) = \mathbb{Z}$$

N.B. generally, if we have an ideal generated by multiple elements, it is the ideal generated by the gcd. As we have a 1 here, it is generated by 1

$$J_2(A) = \left(\begin{vmatrix} 1 & 2 \\ 3 & 4 \end{vmatrix}, \begin{vmatrix} 1 & -1 \\ 3 & -1 \end{vmatrix}, \begin{vmatrix} 2 & -1 \\ 4 & -1 \end{vmatrix} \right)$$

$$= (-2, 2, 2) = (2)$$

Prop^n 3.11

If $A = D(d_1, \dots, d_r)$, $d_1 | d_2 | \dots | d_r$
$\Rightarrow J_i(A) = (d_1 \dots d_i)$

Proof

$$\left[\begin{array}{cc|c} d_1 & 0 & 0 \\ 0 & d_r & 0 \end{array}\right]$$

the only non-zero $i \times i$ minors are

$$\det \begin{bmatrix} d_{\alpha_1} & & 0 \\ & d_{\alpha_2} & \\ 0 & & d_{\alpha_i} \end{bmatrix} = d_{\alpha_1} d_{\alpha_2} \dots d_{\alpha_i}$$

$1 \leq \alpha_1 \leq \alpha_2 < \alpha_3 \dots < \alpha_i \leq r$ i.e. not changing the order

as
$$\left.\begin{array}{l} \alpha_1 \geq 1 \\ \alpha_2 \geq 2 \\ \alpha_3 \geq 3 \\ \vdots \\ \alpha_k \geq k \end{array}\right\} \Rightarrow d_k | d_{\alpha_k} , \forall k = 1, \dots, i$$

$\Rightarrow d_1 \dots d_i \mid d_{\alpha_1} \dots d_{\alpha_k}$

multiple of

$\Rightarrow d_{\alpha_1} \dots d_{\alpha_k} \in (d_1 \dots d_i)$

$\Rightarrow J_i(A) \subseteq (d_1 \dots d_i)$

Conversely,

$d_1 \dots d_i \in J_i(A)$

$\Rightarrow (d_1 \dots d_i) \subseteq J_i(A)$

$\Rightarrow (d_1 \dots d_i) = J_i(A)$

$\square$

Remark: $K = [a_{ij}] \in M_n(R)$
$\underline{a}_j = j$th columns of K

Assume $\underline{a}_1 = \lambda \underline{b} + \mu \underline{c}$

i.e. $K = \begin{bmatrix} \lambda b_1 + \mu c_1 & a_{12} & \cdots & a_{1n} \\ \lambda b_2 + \mu c_2 & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ \lambda b_n + \mu c_n & a_{n2} & \cdots & a_{nn} \end{bmatrix}$

$$\therefore \det K = \sum_{i=1}^{n} (\lambda b_i + \mu c_i) K_{i,1}$$

$(i,1)$-cofactor

det if we delete ith row, 1st column and include sign $\begin{pmatrix} + & - & + & \cdots \\ - \\ + \end{pmatrix}$

$$= \lambda \sum_{i=1}^{n} b_i K_{i,1} + \mu \sum_{i=1}^{n} c_i K_{i,1}$$

$$= \lambda \det \begin{bmatrix} b_1 & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & & \\ b_n & a_{n2} & \cdots & a_{nn} \end{bmatrix} + \mu \det \begin{bmatrix} c_1 & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & & \\ c_n & a_{n2} & \cdots & a_{nn} \end{bmatrix}$$

So, if $\underline{a}_1 = \lambda \underline{b} + \mu \underline{c}$

$\Rightarrow \det(K)$ is an R-linear combination of $\det[\underline{b}, \underline{a}_2, \ldots, \underline{a}_n]$ and $\det[\underline{c}, \underline{a}_2, \ldots, \underline{a}_n]$

By induction, same true for $\underline{a}_1 = \lambda_1 \underline{b}_1 + \lambda_2 \underline{b}_2 + \ldots + \lambda_r \underline{b}_r$

Prop^n 3.12
$A \in M_{m \times n}(R)$, $Y \in M_n(R) \Rightarrow J_i(AY) \subseteq J_i(A)$

Proof
Consider AY
The jth column of AY is:

$$\begin{bmatrix} \uparrow & \uparrow & & \uparrow \\ \underline{a}_1 & \underline{a}_2 & \cdots & \underline{a}_n \\ \downarrow & \downarrow & & \downarrow \end{bmatrix} \begin{bmatrix} y_{11} & \cdots & y_{1j} & \cdots & y_{n1} \\ \vdots & & & & \\ y_{n1} & \cdots & y_{nj} & \cdots & y_{nn} \end{bmatrix}$$

jth column

is $y_{1j}\underline{a}_1 + \dots + y_{nj}\underline{a}_n$

K $i \times i$ submatrix of AY

jth column of K will be of the form,

$$Y_{1\alpha_j}\bar{a}_1 + \dots + Y_{n\alpha_j}\bar{a}_n$$

where $\bar{a}_i$ is a "partial column" of A

remark

$\Rightarrow$ $\det K$ is an R-linear combination of $i \times i$ minors of A

$\Rightarrow$ $\det K \in J_i(A)$

$\Rightarrow$ $J_i(AY) \subseteq J_i(A)$

as $\det K$ ~~are~~ is the generator of $J_i(AY)$ $\square$

Prop^n 3.13

$A \in M_{m \times n}(R)$, $X \in M_m(R) \Rightarrow J_i(XA) \subseteq J_i(A)$

Prop^n 3.14

If $A \sim B \Rightarrow J_i(A) = J_i(B)$ $\forall i = 1, \dots, r$

Proof

$$A \sim B \iff \left.\begin{array}{l} \exists X \in GL_m(R) \\ \exists Y \in GL_n(R) \end{array}\right\} \text{ s.t } B = XAY$$

$$J_i(B) = J_i(XAY) \subseteq J_i(AY) \subseteq J_i(A)$$

Now, as X, Y invertible, we get $A = X^{-1}BY^{-1}$

49

$\Rightarrow J_i(A) \subseteq J_i(B)$ using same technique as before.

$\therefore J_i(A) \subseteq J_i(B) \subseteq J_i(A) \Rightarrow J_i(A) = J_i(B)$ $\square$

Uniqueness of SNF

$D = D(d_1 \ldots d_r)$, $d_1 | d_2 | \ldots | d_r$
$E = D(e_1 \ldots e_r)$, $e_1 | e_2 | \ldots | e_r$ } s.t $D \sim E$

We want to show that each $d_i = u_i e_i$
i.e. $d_i \sim e_i$
i.e. $(d_i) = (e_i)$ $\forall i = 1, \ldots, r$

$$\left.\begin{matrix} J_1(D) = J_1(E) \\ (d_1) = (e_1) \end{matrix}\right\} \Rightarrow d_1 = u_1 e_1$$

Assume $d_j = u_j e_j$ $\forall j = 1, \ldots, i-1$

$$\left.\begin{matrix} J_i(D) = J_i(E) \\ (d_1 \ldots d_i) = (e_1 \ldots e_i) \end{matrix}\right\} \exists u \in \mathcal{U}(R) \text{ s.t } d_1 \ldots d_i = u e_1 \ldots e_i$$

BUT, $d_1 \ldots d_i = u e_1 \ldots e_i$
$d_1 \ldots d_i = u_1 e_1 u_2 e_2 \ldots u_{i-1} e_{i-1} d_i$

$$(u_1 \ldots u_{i-1}) \boxed{(e_1 \ldots e_{i-1})} d_i = u \boxed{(e_1 \ldots e_{i-1})} e_i$$

- If $e_{i-1} \neq 0$ $\quad (\Rightarrow e_1 \neq 0, \ldots, e_{i-2} \neq 0)$

$$\Rightarrow \underbrace{(u_1 \ldots u_{i-1})}_{v \in U(R)} d_i = u\, e_i$$

$$\Rightarrow \quad d_i = (v^{-1}u)\, e_i$$

$$\Rightarrow \quad e_i \sim d_i$$

- If $e_{i-1} = 0$ and $e_{i-1} \mid e_i \Rightarrow e_i = 0$

$$\left.\begin{array}{l} e_{i-1} = 0 \text{ and } e_{i-1} \mid e_i \Rightarrow e_i = 0 \\ \quad ? \\ d_{i-1} = 0 \text{ and } d_{i-1} \mid d_i \Rightarrow d_i = 0 \end{array}\right\} \Rightarrow e_i \sim d_i$$

1

Chapter IV: Finitely Generated Modules over PIDs

R PID throughout chapter

Prop^n 4.1

$_RF$ free mod of rank n
$P \leq F \Rightarrow P$ free and $\operatorname{rank} P \leq \operatorname{rank}(F)$

More precisely, $\exists \{e_1, \dots, e_n\}$ basis of F and elements $d_1 \dots d_m \in R^*$ s.t $\{d_1 e_1 \dots d_m e_m\}$ is a basis of P and $d_1 | d_2 | \dots | d_m$

Proof

$n = \operatorname{rank}(F) \Rightarrow P$ f.g
$\Rightarrow \exists f_1 \dots f_s \in F$ s.t $\{f_1 \dots f_s\}$ gen P

G free module of rank S, $\{g_1' \dots g_s'\}$ basis of G

$\Rightarrow \exists$ unique $\alpha: G \to F$ mod hom
s.t $\alpha(g_i') = f_i$

$\operatorname{Im} \alpha = P$

Pick g, e bases of G, F s.t

$[\alpha]_e^g$ is in SNF
$= D(d_1 \dots d_t)$, $d_1 | d_2 | \dots | d_t$

$g = \{g_1 \dots g_s\}$, $\alpha(g_j) = \begin{cases} d_j e_j & , 1 \leq j \leq t \\ 0 & , t \leq j \leq s \end{cases}$

$\operatorname{Im} \alpha = P$ still
submod of F

$\Rightarrow P$ is generated by $\{d_1e_1 \dots d_te_t\}$
$\Rightarrow P = \sum R \cdot \alpha(g_j)$
$= \sum_{j=1}^{t} Rd_je_j$

Now, need to prove it is a direct sum, i.e. remove one element and compute intersection.

$$\underset{Re_j}{\underset{\cap\!|}{(Rd_je_j)}} \cap \underset{Re_k}{\underset{\cap\!|}{\left(\sum_{k\neq j} Rd_ke_k\right)}} \subseteq \underset{0}{\underset{\|}{(Re_j) \cap \left(\sum_{k\neq j} Re_k\right)}}$$

$\therefore (Rd_je_j) \cap \left(\sum_{k\neq j} Rd_ke_k\right) = 0$

$$\Rightarrow P = \bigoplus_{j=1}^{t} Rd_je_j = \bigoplus_{j=1}^{m} Rd_je_j,$$

where d_m is the last non-zero element in the SNF

$\{d_1e_1 \dots d_me_m\}$ generates P, $d_j \neq 0$

$d_1 | d_2 | \dots | d_m$

Assume $a_1d_1e_1 + \dots + a_md_me_m = b_1d_1e_1 + \dots + b_md_me_m$ and want to show $a_i = b_i \;\forall i$

$\Rightarrow a_1d_1e_1 = b_1d_1e_1$

$\vdots$

$a_md_me_m = b_md_me_m$

working in ID $\Rightarrow$ cancellation and $d_m \neq 0$

$\Rightarrow a_i e_i = b_i e_i \quad \forall i = 1, \dots, n$

$\Rightarrow a_i = b_i$

$\Rightarrow \{d_1 e_1 \dots d_m e_m\}$ basis of P $\square$

Theorem 4.1 (Classification of f.g mods over a PID) Let R be PID, ${}_R M$ f.g module, then there are elements $d_1 \dots d_r \in R^* \setminus U(R)$ and $s \in \mathbb{N}$ s.t $d_1 | d_2 | \dots | d_r$ and

$$\boxed{M \cong \left(\bigoplus_{i=1}^{r} \frac{R}{(d_i)} \right) \oplus R^s}$$

Moreover, r and s, and the ideals (d_i), are unique

N.B. This is the most important theorem and proof in the course.

Proof

M f.g module over R PID

$\Rightarrow \exists$ F free, $P \leq F$ s.t $M \cong F/P$

$\Rightarrow \exists \{e_1, \dots, e_n\}$ basis of F, $d_1 \dots d_m \in R^*$ s.t $d_1 | \dots | d_m$ and s.t $\{d_1 e_1 \dots d_m e_m\}$ basis of P;

$F = Re_1 \oplus \dots \oplus Re_n$

$P = Rd_1 e_1 \oplus \dots \oplus Rd_m e_m$

$$M = \frac{F}{P} = \frac{Re_1 \oplus \dots \oplus Re_n}{Rd_1 e_1 \oplus \dots \oplus Rd_m e_m \oplus R \cdot 0 e_{m+1} \oplus \dots \oplus R \cdot 0 e_n}$$

4

as $P = Rd_1e_1 \oplus \ldots \oplus Rd_me_m$

$$\therefore M = \bigoplus_{i=1}^{n} \frac{Re_i}{Rd_ie_i}$$

$$\cong \frac{R}{(d_1)} \oplus \ldots \oplus \frac{R}{(d_m)} \underbrace{\oplus \frac{R}{(0)} \oplus \ldots \oplus \frac{R}{(0)}}_{R^s}$$

if $d_i \in U(R) \Rightarrow R/(d_i) = 0$

$$\therefore M = \frac{R}{(d_1)} \oplus \ldots \oplus \frac{R}{(d_r)} \oplus R^s = \left(\bigoplus_{i=1}^{r} \frac{R}{(d_i)} \right) \oplus R^s$$

$\square$

Def^n 4.1

R PID, M R-mod, we say that $m \in M$ is a torsion element if $\exists\, r \in R^\#$ s.t. $rm = 0$, i.e. if $\mathrm{ann}(m) \neq 0$.

$T(M) = \{ m \in M \mid \mathrm{ann}(m) \neq 0 \} \leq M$, submod is the torsion submodule of M

If $M = T(M)$ then we say that M is a torsion module
$T(M) = 0$ we say that M is torsion-free

Examples

1/ $M = R^s$ free $\Rightarrow T(M) = 0$ (Exercise)

2/ ${}_{\mathbb{Z}}\mathbb{Q}$ is torsion free, but ${}_{\mathbb{Z}}\mathbb{Q}$ is not free

3/ R ID, $I \trianglelefteq R$, ${}_R\left(R/I\right)$

$T(R/I) = R/I$ torsion module

Prop^n 4.2

$$R \text{ PID}, \quad M = \left(\bigoplus_{i=1}^{r} R/(d_i) \right) \oplus R^s$$

N.B. every time we write this we know $d_1 | d_2 | \dots | d_r$ from theorem 4.1

$$\Rightarrow T(M) = \bigoplus_{i=1}^{r} R/(d_i)$$

and $\dfrac{M}{T(M)} \cong R^s$

Proof

Take $m = (a, b)$, $a \in \bigoplus_{i=1}^{r} \dfrac{R}{(d_i)}$

$b \in R^s$, $r \in R^*$

s.t $r \cdot m = 0$, $rm = (ra, rb) \Rightarrow ra = 0$

$\underbrace{rb = 0}_{\text{because } b \in R^s \text{ free}} \Rightarrow b = 0$

$$\Rightarrow m = (a, 0) \in \bigoplus_{i=1}^{r} R/(d_i)$$

$T(M) \subseteq \bigoplus_{i=1}^{r} \dfrac{R}{(d_i)} \ni a = (a_1, \dots, a_r)$

$\therefore d_i \cdot a_i = 0$, as $d_i \in (d_i)$

BUT as $d_1 | d_2 | \dots | d_r$

$\underset{\neq 0}{d_r} \cdot a = 0$

$\Rightarrow a \in T(M)$

$\therefore T(M) \subseteq \bigoplus_{i=1}^{r} \dfrac{R}{(d_i)} \subseteq T(M) \Rightarrow T(M) = \bigoplus_{i=1}^{r} \dfrac{R}{(d_i)}$

$$M \cong A \oplus B \iff \begin{array}{l} M = A + B \\ A \cap B = 0 \end{array}$$

$$\frac{M}{A} = \frac{A+B}{A} \underset{\substack{\text{2nd} \\ \text{I.T}}}{\cong} \frac{B}{\underbrace{A \cap B}_{=0}} \cong B$$

$$\therefore \frac{M}{\underset{\| \atop A}{T(M)}} \cong \underset{\| \atop B}{R^s}$$

$\square$

<u>Prop^n 4.3</u> If
$$M \cong \left(\bigoplus_{i=1}^{r} \frac{R}{(d_i)} \right) \oplus R^s$$
$$\cong \left(\bigoplus_{s=1}^{r'} \frac{R}{(d_j')} \right) \oplus R^{s'}$$
$$\Rightarrow \bigoplus \frac{R}{(d_i)} \cong \bigoplus \frac{R}{(d'_j)} \quad \text{and} \quad s = s'$$

<u>Proof</u>
$$\underline{\bigoplus_{i=1}^{r}} \frac{R}{(d_i)} = T(M) = \underline{\bigoplus_{i=1}^{r'}} \frac{R}{(d_j')}$$

$$R^s \cong \frac{M}{T(M)} \cong R^{s'} \Rightarrow s = s'$$

$\square$

Invariant Factors and Elementary Divisors

Prop^n 4.4

R commutative ring, $a, b \in R$ s.t
$(a)+(b)=R$
$\Rightarrow (a)\cap(b)=(ab)$
and
$$_R\left(\frac{R}{(ab)}\right) \cong \frac{R}{(a)} \oplus \frac{R}{(b)}$$

Proof
Exercise - hint: Use 2nd Isomorphism Theorem

Corollary 4.1
R PID, $d \in R^* \setminus U(R)$
$\Rightarrow d = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$, where p_i are different primes
$$\Rightarrow \frac{R}{(d)} \cong \frac{R}{(p_1^{\alpha_1})} \oplus \cdots \oplus \frac{R}{(p_s^{\alpha_s})}$$

If $M = \frac{R}{(d_1)} \oplus \cdots \oplus \frac{R}{(d_r)}$ (torsion) R-mod

We can write $d_i = p_1^{\alpha_{1,i}} p_2^{\alpha_{2,i}} \cdots p_s^{\alpha_{s,i}}$

1/ For each $j=1,\dots,s$, $0 \le \alpha_{j,1} \le \alpha_{j,2} \le \cdots \le \alpha_{j,r}$

d_2 d_r

exponent of p_j in d_1

11/ For each $j=1,\dots,s$, $\alpha_{j,r} > 0$

111/ $\exists i$ s.t $\alpha_{i,1} \geq 1$

8

$$\begin{aligned}
d_1 &= p_1^{\alpha_{1,1}} \; p_2^{\alpha_{2,1}} \cdots p_s^{\alpha_{s,1}} \\
d_2 &= p_1^{\alpha_{1,2}} \; p_2^{\alpha_{2,2}} \cdots p_s^{\alpha_{s,2}} \\
&\vdots \\
d_r &= p_1^{\alpha_{1,r}} \; p_2^{\alpha_{2,r}} \cdots p_s^{\alpha_{s,r}}
\end{aligned}$$

elementary divisors

$M = \bigoplus_{i=1}^{r} \frac{R}{(d_i)}$ — Invariant Factor decomposition

$= \bigoplus_{i=1}^{r} \left(\bigoplus_{j=1}^{s} \frac{R}{(p_j^{\alpha_{j,i}})} \right)$ — Elementary Divisor decomposition

Each of the $\frac{R}{(p_j^{\alpha_{j,i}})}$ is called an elementary divisor of M

<u>Example</u>

$R = \mathbb{Z}$, $A = \mathbb{Z}_2 \oplus \mathbb{Z}_{20} \oplus \mathbb{Z}_{60} \oplus \mathbb{Z}_{120}$

$\mathbb{Z}_{120} = \mathbb{Z}/(120)$

$2 \mid 20 \mid 60 \mid 120$

$\therefore$ Invariant Factor Decomposition

So,

$$\begin{aligned}
2 &= 2^1 \cdot 3^0 \cdot 5^0 \\
20 &= 2^2 \cdot 3^0 \cdot 5^1 \\
60 &= 2^2 \cdot 3^1 \cdot 5^1 \\
120 &= 2^3 \cdot 3^1 \cdot 5^1
\end{aligned}$$

elementary divisors

$$A = \underbrace{\mathbb{Z}_2 \oplus \mathbb{Z}_{2^2} \oplus \mathbb{Z}_{2^2} \oplus \mathbb{Z}_{2^3}}_{\text{First column}} \oplus \underbrace{\mathbb{Z}_3 \oplus \mathbb{Z}_3}_{\text{2nd column}} \oplus \underbrace{\mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5}_{\text{3rd column}}$$

Note that we can rearrange this so that,

$$\bigoplus_{i=1}^{r}\left(\bigoplus_{j=1}^{s}\frac{R}{(p_j^{\alpha_{j,i}})}\right)=\bigoplus_{j=1}^{s}\left(\bigoplus_{i=1}^{r}\frac{R}{(p_j^{\alpha_{j,i}})}\right)$$

So, in this way we can get groups of same primes.
So, we can label,

A_2 = 1st column
A_3 = 2nd column
A_5 = 3rd column

To prove uniqueness of Invariant Factor Decomposition and Elementary Divisor Decomposition, we need:

1. Prove that Elementary divisors are uniquely determined
2. Show how to recover Invariant Factors from Elementary divisors.

<u>Def^n 4.2</u>

R PID, M R-mod, $p \in R$ prime.
We say that $m \in M$ is p-torsion if there is some $t \in \mathbb{N}$ s.t. $p^t \cdot m = 0$ (i.e. $p^t \in \mathrm{ann}(m)$).
equiv to saying $p \in \mathrm{ann}(m)$
The set,

$$M_p = \{m \in M \mid m \text{ is } p\text{-torsion}\} \leq M \text{ submod}$$

p-primary component of M

<u>Prop^n 4.5</u>

M finitely generated (torsion) R-mod,

$$M=\bigoplus_{i=1}^{s}\left(\bigoplus_{j=1}^{r}\frac{R}{(p_i^{\alpha_{i,j}})}\right) \Rightarrow M_{p_i}=\bigoplus_{j=1}^{r}\frac{R}{(p_i^{\alpha_{i,j}})}$$

and $M = M_{p_1} \oplus M_{p_2} \oplus \cdots \oplus M_{p_s}$

10

Proof

Let $N_i = \bigoplus_{j=1}^{r} \frac{R}{(p_i^{\alpha_{i,j}})}$, $\alpha_{i,j} \leq \alpha_{i,r}$ $\forall j = 1, \dots, r$

$\Rightarrow p_i^{\alpha_{i,r}} \frac{R}{(p_i^{\alpha_{i,j}})} = 0$ $\forall j = 1, \dots, r$

$\Rightarrow p_i^{\alpha_{i,r}} \cdot N_i = 0$

$\Rightarrow N_i \subseteq M_{p_i}$

We have $M = N_1 \oplus N_2 \oplus \dots \oplus N_s$

Pick $m \in M$, $m = (a_1, a_2, \dots, a_s)$, $a_i \in N_i$

If $m \in M_{p_i}$ $\Rightarrow \exists t \in \mathbb{N}$ s.t $p_i^t m = 0$

$\Rightarrow (p_i^t a_1, p_i^t a_2, \dots, p_i^t a_s) = 0$

$\Rightarrow p_i^t a_1 = 0, \dots, p_i^t a_s = 0$

$\Rightarrow \forall_j$, $p_i^t \in \text{ann}(a_j)$ $\Big\} \Rightarrow$ $(p_i^t) \subseteq \text{ann}(a_j)$

$\Rightarrow p_j^{\alpha_{j,r}} \in \text{ann}(a_j)$ $\qquad (p_j^{\alpha_{j,r}}) \subseteq \text{ann}(a_j)$

$(p_i^t) + (p_j^{\alpha_{j,r}}) \subseteq \text{ann}(a_j)$

If $j \neq i$ $\Rightarrow$ $\gcd(p_i^t, p_j) = 1$

$\left.\begin{array}{l} a \mid p_i^t \Rightarrow a = p_i \\ a \mid p_j \Rightarrow a = p_j \end{array}\right\} p_i \neq p_j$

$\Rightarrow (p_i^t) + (p_j^{\alpha_{j,r}}) = (1) = R$

$\Rightarrow R \subseteq \text{ann}(a_j)$

$\Rightarrow a_j = 0$

$\Rightarrow m = (0, 0, \dots, 0, a_i, 0, \dots, 0) \in N_i$

$\Rightarrow M_{p_i} \subseteq N_i$

and proven $N_i \leq M_{p_i}$

$\Rightarrow N_i = M_{p_i}$ $\square$

M f.g torsion R-mod (R PID)

Assume $M \cong \bigoplus_{i=1}^{s} \left(\bigoplus_{j=1}^{r} R/(p_i^{\alpha_{ij}}) \right) = \bigoplus_{i=1}^{s} \bigoplus_{k=1}^{r'} \frac{R}{(p_i^{\alpha_{ik}})}$

$\Rightarrow \forall i = 1, \dots, s$

$$M_{p_i} \cong \bigoplus_{j=1}^{r} \frac{R}{(p_i^{\alpha_{ij}})}$$
$$\cong$$
$$\bigoplus_{k=1}^{r'} \frac{R}{(p_i^{\alpha_{ik}})}$$

Prop^n 4.6
M R-mod, $x \in R$ s.t $x \cdot M = 0$, i.e. $x \in \operatorname{ann}(M)$

$\Rightarrow$ we can get an $R/(x)$ module structure on M by

setting $(r + (x))m = rm$ $(+\underbrace{xm}_{0})$

i.e. M is an $\frac{R}{(x)}$-module

Proof

If $r+(x)=r'+(x)$, $(r+(x))m=rm$
$(r'+(x))m=r'm$

$r-r'\in(x) \iff r-r'=s\cdot x$ for some s

$(r-r')m = rm - r'm$

$(sx)m = s(xm) = 0$

$\Rightarrow rm=r'm$

So, the action is well defined.
Rest is an exercise $\square$

Prop^n 4.7
A R-mod, $x\in R \Rightarrow xA=\{xa \mid a\in A\}\leq A$ submod

Moreover, $x\left(\dfrac{A}{xA}\right)=0$

$[\, r(a+xA)=ra+xA$
$x(a+xA)=xa+xA=0 \,]$

$\Rightarrow \forall A$ R-mod, $\forall x\in R$
$\dfrac{A}{xA}$ is an $\dfrac{R}{(x)}$-module

Proof
trivial $\square$

Let $M=M_p$, p-torsion module, $p\in R$ prime

$$M_p=\frac{R}{(p^{\alpha_1})}\oplus\frac{R}{(p^{\alpha_2})}\oplus\cdots\oplus\frac{R}{(p^{\alpha_r})}$$

$1\leq\alpha_1\leq\alpha_2\leq\cdots\leq\alpha_r$

$\forall i \in \mathbb{N}$, $p^i M \leq M$ - by prop^n 4.7
and we see $p(p^i M) \leq p^i M$

$$p^{i+1} M \leq p^i M$$

$p \dfrac{p^i M}{p^{i+1} M} = 0 \implies \dfrac{p^i M}{p^{i+1} M}$ is an $\dfrac{R}{(p)}$ - module

$\implies \dfrac{p^i}{p^{i+1} M}$ is an $\mathbb{F}$-vector space,
$\mathbb{F} = R/(p)$

$\mathbb{F}$, field
as (p) maximal
as R PID and
$R/(p) \implies$ I.D as
p prime.
so, (p) prime ideal
and I.D/maximal ideal $\implies \mathbb{F}$

- If $\alpha \leq i$, $p^i\left(\dfrac{R}{(p^\alpha)}\right)$

$$p^{\alpha+j} \frac{R}{(p^\alpha)} = p^j\left(p^\alpha \frac{R}{(p^\alpha)}\right) = 0$$

- If $i < \alpha$ $\quad p^i \dfrac{R}{(p^\alpha)} = \dfrac{p^i R}{(p^\alpha)} = \dfrac{(p^i)}{(p^\alpha)}$

By 3rd Isomorphism Theorem

$$\frac{p^i\left(R/(p^\alpha)\right)}{p^{i+1}\left(R/(p^\alpha)\right)} = \frac{(p^i)/(p^\alpha)}{(p^{i+1})/(p^\alpha)} \cong \frac{(p^i)}{(p^{i+1})}$$

$$= \frac{Rp^i}{Rp^i p}$$

$$= \frac{R}{(p)} = \mathbb{F}$$

$$\frac{p^i M}{p^{i+1} M} = \frac{p^i\left(\frac{R}{(p^{\alpha_1})} \oplus \dots \oplus R/(p^{\alpha_r})\right)}{p^{i+1}\left(\frac{R}{(p^{\alpha_1})} \oplus \dots \oplus R/(p^{\alpha_r})\right)}$$

$$= \frac{p^i \, R/(p^{\alpha_1}) \oplus \dots \oplus p^i \, R/(p^{\alpha_r})}{p^{i+1} R/(p^{\alpha_1}) \oplus \dots \oplus p^{i+1} R/(p^{\alpha_r})}$$

$$= \frac{p^i R/(p^{\alpha_1})}{p^{i+1} R/(p^{\alpha_1})} \oplus \dots \oplus \frac{p^i R/(p^{\alpha_r})}{p^{i+1} R/(p^{\alpha_r})} = \mathbb{F}^{n_i}$$

where n_i = number of $\{\alpha_j \mid \alpha_j > i\}$

as $\frac{p^i M}{p^{i+1} M}$ is a vector space,

$$n_i = \text{no}^{\circ}\{\alpha_j \mid \alpha_j > i\} = \dim_{\mathbb{F}} \frac{p^i M}{p^{i+1} M}$$

dim over $\mathbb{F}$

N.B. Never have to compute this, just using it to prove

$$M = \frac{R}{(p^{\alpha_1})} \oplus \dots \oplus R/(p^{\alpha_r})$$

$$r = \text{no}^{\circ}\{\alpha_j \mid \alpha_j > 0\} = n_0 = \dim_{\mathbb{F}} \frac{M}{pM}$$

The number of $\frac{R}{(p^i)}$ in the decomposition is

$n_i = \text{no}^{\circ}\{\alpha_j \mid \alpha_j > i\}$

$n_{i-1} = \text{no}^{\circ}\{\alpha_j \mid \alpha_j > i-1\}$

$\therefore \text{no}^{\circ}\{\alpha_j \mid \alpha_j = i\} = n_{i-1} - n_i$

$$= \dim \frac{p^{i-1} M}{p^i} - \dim \frac{p^i M}{p^{i+1} M}$$

$\Rightarrow \alpha_j$ are uniquely determined

$\Rightarrow$ the elementary divisor decomposition is unique

2/ How to recover d_i's from $p_j^{\alpha_{j,i}}$'s ?

If the elementary divisors are

$p_1^{\alpha_{1,1}}, \ldots, p_1^{\alpha_{1,r_1}}, p_2^{\alpha_{2,1}}, \ldots, p_2^{\alpha_{2,r_2}}, \ldots, p_s^{\alpha_{s,1}}, \ldots, p_s^{\alpha_{s,r_s}}$

$\Rightarrow d_r = p_1^{\alpha_{1,r_1}} p_2^{\alpha_{2,r_2}} \ldots p_s^{\alpha_{s,r_s}}$

$d_{r-1} = p_1^{\alpha_{1,r_1-1}}, p_2^{\alpha_{2,r_2-1}}, \ldots, p_s^{\alpha_{s,r_s-1}}$

$d_1 = p_1^{\alpha_{1,1}} p_2^{\alpha_{2,1}}, \ldots, p_s^{\alpha_{s,1}}$

[gcd every single prime highest power]

Example

$A = \mathbb{Z}_2 \oplus \mathbb{Z}_{2^2} \oplus \mathbb{Z}_{2^2} \oplus \mathbb{Z}_{2^3} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$

$2, \; 2^2, \; 2^2, \; 2^3, \; 3, \; 3, \; 5, \; 5, \; 5$

$d_4 = 2^3 \cdot 3 \cdot 5 = 120$

$d_3 = 2^2 \cdot 3 \cdot 5 = 60$

$d_2 = 2^2 \cdot 5 = 20$

$d_1 = 2 = 2$

$A = \mathbb{Z}_2 \oplus \mathbb{Z}_{20} \oplus \mathbb{Z}_{60} \oplus \mathbb{Z}_{120}$

This is how you recover the Invariant Factor decomp!

Which concludes the proof of the biggest theorem in the course.

Applications

1. Finitely Generated Abelian Groups ($R = \mathbb{Z}$)

Theorem 4.2 (Classification of f.g abelian groups)

If A f.g abelian group
$\Rightarrow \exists\ d_1 \mid d_2 \mid \dots \mid d_r$ in $\mathbb{N}$
and $s \in \mathbb{N}$ (unique) s.t $A \cong (\mathbb{Z}_{d_1} \oplus \dots \oplus \mathbb{Z}_{d_r}) \oplus \mathbb{Z}^s$

Prop^n 4.8
A f.g abelian group is torsion free
$\Leftrightarrow$ it is free
torsion $\Leftrightarrow$ it is finite

Examples
① $(\mathbb{Q}, +)$ abelian (mod over $\mathbb{Z}$), torsion free
but it is NOT free
why? $\frac{1}{2}$ and $\frac{1}{5}$ (say)

then
$$2 \cdot \frac{1}{2} - 5 \cdot \frac{1}{5} = 0$$

why does prop^n 4.8 fail? Because $\mathbb{Q}$ is not f.g $/\mathbb{Z}$

17

(2) ${}_{\mathbb{Z}}\left(\mathbb{R}/\mathbb{Z}\right)$ i.e. ignore integer part
i.e. decimal parts only

torsion module but it is NOT free
(because it is NOT f.g)

Goal: Classify all abelian groups of order n

1. (p-torsion) $A = \mathbb{Z}_{p^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{n_t}}$

$$|A| = |\mathbb{Z}_{p^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{n_t}}|$$
$$= |\mathbb{Z}_{p^{n_1}}||\mathbb{Z}_{p^{n_2}}| \cdots |\mathbb{Z}_{p^{n_t}}|$$
$$= p^{n_1} p^{n_2} \cdots p^{n_t} = p^{n_1+n_2+\cdots+n_t}$$

Can assume $n_1 \leq n_2 \leq \cdots \leq n_t$

If A p-torsion, $|A| = n \Rightarrow n = n_1 + \cdots + n_t$

$\Rightarrow$ no. $\{$p-torsion abelian groups of order $p^n\}$
= no. $\{$decompositions $n = n_1 + \cdots + n_t$ s.t $n_1 \leq \cdots \leq n_t\}$
= no. $\{$partitions of $n\}$
= $\wp(n)$ — very important function
— not to be confused with p prime

N.B. Look up on Wiki to see what this looks like, mammoth of a beastie!

Very difficult to compute as n increases,

$p(1) = 1$

$p(2) = 2$ 2 or 1+1

$p(3) = 3$ 3, 1+2, 1+1+1

$p(4) = 5$ 4, 1+3, 2+2, 1+1+2, 1+1+1+1

$p(5) = 7$ 5, 2+3, 1+4, 1+1+3, 1+2+2, 1+1+1+2, 1+1+1+1+1

$p(6) = 11$ 6, 1+5, 2+4, 1+1+4, 3+3, 1+2+3, 1+1+1+3, 2+2+2, 1+1+2+2, 1+1+1+1+2, 1+1+1+1+1+1

$p(7) = 15$

$p(10) = 42$

⋮

So, all abelian groups of order n,

A abelian group, $|A| = n = p_1^{n_1} \dots p_t^{n_t}$

$|A| = |A_{p_1} \oplus A_{p_2} \oplus \dots \oplus A_{p_t}| = |A_{p_1}| \dots |A_{p_t}| = p_1^{n_1} \dots p_t^{n_t}$

So, we only need choose among all possible A_{p_i} s.t $|A_{p_i}| = p_i^{n_i}$

<u>Example</u>

Find all abelian groups of order 600,

$600 = 2^3 \cdot 3 \cdot 5^2$, $|A| = 600 \Rightarrow A = A_2 \oplus A_3 \oplus A_5$

$|A_2| = 2^{3}$

A_2: $3 = 3 \longrightarrow \mathbb{Z}_{2^3}$

$3 = 1+2 \longrightarrow \mathbb{Z}_2 \oplus \mathbb{Z}_{2^2}$

$3 = 1+1+1 \longrightarrow \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

19

$|A_3| = 3^{1}$

A_3: $1 = 1 \longrightarrow \mathbb{Z}_3$

$|A_5| = 5^{2}$

A_5: $2 = 2 \longrightarrow \mathbb{Z}_{5^2}$

$2 = 1+1 \longrightarrow \mathbb{Z}_5 \oplus \mathbb{Z}_5$

$$\begin{aligned}\therefore A &= \mathbb{Z}_{2^3} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{5^2} \\ &= \mathbb{Z}_{2^3} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \\ &= \mathbb{Z}_2 \oplus \mathbb{Z}_{2^2} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{5^2} \\ &= \mathbb{Z}_2 \oplus \mathbb{Z}_{2^2} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \\ &= \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{5^2} \\ &= \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5\end{aligned}$$

$A = \mathbb{Z}_2 \oplus \mathbb{Z}_{2^2} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 = \mathbb{Z}_{10} \oplus \mathbb{Z}_{60}$

$\underline{\underline{2}}$ $\underline{2^2}$ $\underline{3}$ $\underline{\underline{5}}$ $\underline{5}$

<u>Groups given by gens and relations</u>

$A = \langle x, y, z, w \mid 2x + 2y = 0,\ 3z = 0,\ 4w = 0 \rangle$

Presentation matrix: write as columns:

20

$$\begin{bmatrix} 2 & 0 & 0 \\ 2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 4 \end{bmatrix} \underset{\substack{C_1 \leftrightarrow C_3 \\ R_1 \leftrightarrow R_3}}{\rightsquigarrow} \begin{bmatrix} 3 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 4 \end{bmatrix} \underset{\substack{R_1 + R_2 \\ R_3 - R_2}}{\rightsquigarrow} \begin{bmatrix} 3 & 2 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 4 \end{bmatrix}$$

$$\underset{\substack{C_1 - C_2 \\ R_3 \leftrightarrow R_4}}{\rightsquigarrow} \begin{bmatrix} 1 & 2 & 0 \\ -2 & 2 & 0 \\ 0 & 0 & 4 \\ 0 & 0 & 0 \end{bmatrix} \underset{R_2 + 2R_1}{\rightsquigarrow} \begin{bmatrix} 1 & 2 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 4 \\ 0 & 0 & 0 \end{bmatrix} \underset{C_2 - 2C_1}{\rightsquigarrow} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 4 \\ 0 & 0 & 0 \end{bmatrix}$$

$$\underset{R_2 + R_3}{\rightsquigarrow} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 6 & 4 \\ 0 & 0 & 4 \\ 0 & 0 & 0 \end{bmatrix} \underset{C_2 - C_3}{\rightsquigarrow} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 4 \\ 0 & -4 & 4 \\ 0 & 0 & 0 \end{bmatrix} \underset{R_3 + 2R_2}{\rightsquigarrow} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 4 \\ 0 & 0 & 12 \\ 0 & 0 & 0 \end{bmatrix}$$

$$\underset{C_3 - 2C_2}{\rightsquigarrow} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 12 \\ 0 & 0 & 0 \end{bmatrix} \qquad \begin{pmatrix} x \\ y \\ z \\ w \end{pmatrix}$$

only consider diag
ignore columns with 1

$$A \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{12}$$
$$\cong \mathbb{Z}_2 \oplus \mathbb{Z}_{2^2} \oplus \mathbb{Z}_3$$

cyclic group of order 2, the $(x+y)$, could call $(x+y) = x'$

cyclic group of order 4, should have element of order 4, the w

cyclic group of order 3, should have element of order 3, the z

and write,

$$A = \langle x', z, w \mid 2x' = 0, 3z = 0, 4w = 0 \rangle$$

21

Matrices under similarity

$A, B \in M_n(R)$ are similar if $\exists P \in GL_n(R)$ s.t $B = P^{-1}AP$

N.B. under $\mathbb{C}$, we solved this with JNF

$A \in M_n(\mathbb{F})$, $\alpha : \mathbb{F}^n = V \longrightarrow V$
$\underline{v} \longmapsto A.\underline{v}$

$\iff \mathbb{F}[x]$ - mod structure on V
$(f(x) \cdot \underline{v} = f(\alpha)\underline{v})$

submods of $V \iff W \leq_{\mathbb{F}} V$ subspace s.t $\alpha(W) \leq W$

Lemma 4.1
If $V = V_1 \oplus V_2 \oplus \dots \oplus V_t$
and e_i basis of $V_i \Rightarrow e = e_1 \cup e_2 \cup \dots \cup e_t$

Defn 4.3
We say that $A \in M_n(\mathbb{F})$ is block diagonal if,

$$A = \begin{bmatrix} A_1 & & & O \\ & A_2 & & \\ & & \ddots & \\ O & & & A_t \end{bmatrix}, \quad \text{where } A_k \in M_{n_k}(\mathbb{F})$$

$n = n_1 + \dots + n_t$

$$= A_1 \oplus A_2 \oplus \dots \oplus A_t$$

V v.s/$\mathbb{F}$ $\alpha : V \longrightarrow V$ linear map
$V = V_1 \oplus V_2 \oplus \dots \oplus V_t$
where $\alpha(V_i) \leq V_i \Rightarrow \alpha_i = \alpha|_{V_i} : V_i \longrightarrow V_i$

linear maps
e_i basis of V_i
$e = e_1 \cup \dots \cup e_t$

$\Rightarrow [\alpha]_e^e = [\alpha_1]_{e_1}^{e_1} \oplus \dots \oplus [\alpha_t]_{e_t}^{e_t}$

(V, α) $\quad \mathbb{F}[x]$-mod

$$\begin{aligned} \operatorname{ann}_{\mathbb{F}[x]}(V) &= \{ f(x) \in \mathbb{F}[x] \mid f(x) \cdot \underline{v} = 0 \quad \forall \underline{v} \in V \} \\ &= \{ f(x) \in \mathbb{F}[x] \mid f(\alpha)(\underline{v}) = 0 \quad \forall \underline{v} \in V \} \\ &= \{ f(x) \in \mathbb{F}[x] \mid f(\alpha) = 0 \} \\ &= (m_\alpha(x)) \end{aligned}$$

minimal polynomial

$\Rightarrow$ V is a finite torsion over $\mathbb{F}[x]$, (finite as can take any basis)

$\Rightarrow V = \bigoplus_{i=1}^{t} \dfrac{\mathbb{F}[x]}{(d_i)}$, where $d_1 \mid d_2 \mid \dots \mid d_t \in \mathbb{F}[x]$

$\oplus V_i$

d_i's unique up to associates (as all non-zero, constants are units - make d_i monic and we find they are unique)

Each $V_i = \dfrac{\mathbb{F}[x]}{(d_i)}$ is an α-invariant subspace of V

$\left[V \cong \dfrac{\mathbb{F}[x]}{m_\alpha(x)} \right]$

Restrict ourselves to study $V = \dfrac{\mathbb{F}[x]}{(d)}$, $d \in \mathbb{F}[x]$ monic

$\operatorname{ann}(V) = (d) = (m_\alpha(x))$

$d = x^n + \lambda_{n-1} x^{n-1} + \dots + \lambda_1 x + \lambda_0$

$\mathcal{E}$

Assume we have a basis $\{\alpha^{n-1}(\underline{v}), \ldots, \alpha^2(\underline{v}), \alpha(\underline{v}), \underline{v}\}$ which is constructed in the exact same way that we construct the basis for JNF.

$$[\alpha]_e^e = \begin{bmatrix} -\lambda_{n-1} \cdot 1 & & 0 & 0 \\ -\lambda_{n-2} \cdot 0 & & \vdots & \vdots \\ -\lambda_{n-3} \cdot 0 & & \vdots & \vdots \\ \vdots & & & \\ -\lambda_1 \cdot 0 & & 1 & 0 \\ -\lambda_0 \cdot 0 & & 0 & 1 \\ & & 0 & 0 \end{bmatrix} = C_d$$

Strict upper diag of 1s

companion matrix of d

$d(\alpha) = 0$ so $\alpha^n = -\lambda_0 - \lambda_1 \alpha - \ldots - \lambda_{n-1}\alpha^{n-1}$

Theorem 4.3 (Rational Canonical Form - RCF)

$A \in M_n(\mathbb{F})$, then A is similar to a unique matrix of the form, $C_{d_1} \oplus \cdots \oplus C_{d_n}$, where C_{d_i} companion matrix of d_i

and $d_1 | d_2 | \ldots | d_t$ monic polynomials

$C_{d_1} \oplus \cdots \oplus C_{d_t}$ is what we call the Rational Canonical Form of A

Moreover, A and B are similar $\iff$ $RCF(A) = RCF(B)$

Benefits here are that this does not require factorisation. This is particularly useful as there is a formula for factorising degree 2, a really complicated formula for factorising deg 3, a really really long formula for factorising deg 4 but no formula for factorising deg ≥ 5