PMATH 446 - Introduction to Commutative Algebra

2015 01 C

R commutative ring, $1 \in R$

Should know
1) What a ring is
2) What an ideal is
3) units, zero divisors, idempotents ($e^2 = e$)
4) prime ideals ($ab \in P \Rightarrow a \in P$ or $b \in P$ and $P \subsetneq R$)
5) Maximal ideal
$M \trianglelefteq R$ maximal $\iff M \subsetneq R$ & $M \trianglelefteq I \trianglelefteq R \Rightarrow I \in \{M, R\}$

Recall: $P \trianglelefteq R$ is prime $\iff R/P$ is an integral domain
$M \trianglelefteq R$ is maximal $\iff R/M$ is a field

E.g. $(0) \trianglelefteq \mathbb{Z}$ prime $(0) \subsetneq 2\mathbb{Z} \subsetneq \mathbb{Z}$

6) Zorn's lemma
$(\mathcal{S}, \leq)$ $(S_\alpha)_{\alpha \in J}$ $\alpha <_J \beta \Rightarrow S_\alpha \leq_S S_\beta$
if $\exists s \in S$ st $s \geq S_\alpha$ $\forall \alpha \in J$
$\Rightarrow \mathcal{S}$ has a maximal element

For us
We'll use Zorn's lemma mostly with $\mathcal{S}$ = collection of ideals in a ring R, $\leq$ given by $\subseteq$

Application
If R is a ring ($0 \neq 1$), then R has a maximal ideal.
In fact if $I \trianglelefteq R$ then $\exists$ a maximal ideal $M \supseteq I$.

Proof: Let
$$\mathcal{S} = \{J \trianglelefteq R \,;\, J \supseteq I,\ J \subsetneq R\},$$
If $I \trianglelefteq R \Rightarrow I \in \mathcal{S}$, so $\mathcal{S} \neq \emptyset$. Notice that if X is a totally ordered set & $\{I_\alpha\}_{\alpha \in X}$ is a chain in $\mathcal{S}$ (ie $\alpha < \beta \Rightarrow I_\alpha \subseteq I_\beta$) then

$$\bigcup_{\alpha \in X} I_\alpha =: J \supseteq I$$

If $a, b \in J \Rightarrow \exists\, \alpha, \beta \in X$ st $a \in I_\alpha$, $b \in I_\beta$. Either $I_\alpha \subseteq I_\beta \Rightarrow a, b \in I_\beta \Rightarrow a + b \in I_\beta \subseteq J$ or $\beta \leq_X \alpha \Rightarrow I_\beta \subseteq I_\alpha$

so $b, a \in I_\alpha \Rightarrow b + a \in I_\alpha \subseteq J$.
If $a \in J$, $r \in R \Rightarrow \exists \alpha \in X$ st $a \in I_\alpha \Rightarrow ra \in I_\alpha \subseteq J$

the rest will be on 2015 01 12

So J is an ideal & $J \supseteq I$. To show $J \in \mathcal{S}$ we must show that $J \subsetneq R$. But this follows from the fact that if $J = R \Rightarrow 1 \in J \Rightarrow \exists \alpha$ st $1 \in I_\alpha$ $\not\Rightarrow$ $\therefore J_\alpha \subsetneq R$.
Conclusion: Every chain in $\mathcal{S}$ has an upper bound.
Zorn's lemma $\Rightarrow \exists M \in \mathcal{S}$ maximal element of $\mathcal{S}$. So $M \supseteq J$.
If $\exists M'$ st $M \subsetneq M' \subsetneq R$ then $M' \in \mathcal{S}$ & $M \not\supseteq M$, contradicting maximality. So M is maximal, as required. ∎

This fact requires R to have 1.
Ex Take R to be an abelian group that does not have a maximal proper subgroup
Ex $R = \{\alpha \in \mathbb{C}^*;\ \exists m \geq 1 \text{ st } \alpha^{2^m} = 1\}$.
Exercise R has no maximal proper subgroups
Define $r \odot s = 1$ (zero of R) } R has no maximal ideals
$r \oplus s = r \cdot s$

Chinese remainder theorem for rings.
Set up: R is a ring, $I_1, \ldots, I_k \trianglelefteq R$ s.t.
1) $\bigcap_{i=1}^{k} I_i = \emptyset$ & 2) the I_i are pairwise comaximal, ie $i \neq j \Rightarrow I_i + I_j = R$.

$$\Rightarrow R \cong \prod_{i=1}^{k} R/I_i$$

Modules

Let R be a ring. An R-module M is just an abelian group $0_M \to (M,+)$ endowed with a map

$$R \times M \to M$$
$$(r,m) \mapsto r \cdot m$$

s.t. 1) $r \cdot (s \cdot m) = (rs) \cdot m$; 2) $r(m+n) = r \cdot m + r \cdot n$ 3) $(r+s) \cdot m = r \cdot m + s \cdot m$
4) $1_R \cdot m = m$.

ex 1) $R = F$ a field; V is an F-module $\Leftrightarrow$ V is an F-v.s.
2) $R = \mathbb{Z}$, M = an abelian group

3) $R = \mathbb{R}[x]$, $M = \mathbb{C}$

Define $p(x) \cdot \lambda = p(i) \cdot \lambda$
($p(x) \in R$, $\lambda \in M$)

Def'n Let R be a ring & let M be an R-module. We define

$$\underset{\text{annihilator of } M}{\text{Ann}_R(M)} = \{r \in R;\ r \cdot m = 0 \ \ \forall m \in M\}$$

Remark: $\text{Ann}_R(M)$ is an ideal of R: If $r, s \in \text{Ann}_R(M) \Rightarrow$
$(r+s) \cdot m = r \cdot m + s \cdot m = 0_M + 0_M = 0_M \quad \forall m \in M$
If $a \in \text{Ann}_R(M)$ & $r \in R \Rightarrow (ra) \cdot m = r(am) = r \cdot 0_M = 0_M$

Remark: If $S = R/\text{Ann}_R(M)$ then M has the structure of an S-module.

$s \in S$, $s = r + \text{Ann}_R(M)$

$s \cdot m = r \cdot m$ well-defined by annihilator property

2015 01 08

$I = \text{Ann}_R(M)$, M ~~admits~~ inherits a structure as an R/I-module

$r \equiv s \pmod I \iff r - s \in I \iff (r-s) \cdot m = 0 \ \ \forall m \in M$

$\iff r \cdot m = s \cdot m \ \ \forall m \in M$

So M gets an R/I-module structure via the rule

$$(r+I) \cdot m = r \cdot m.$$

Def'n An R-module M is <u>faithful</u> if $\text{Ann}_R(M) = (0)$.

Remark: If $I = \text{Ann}_R(M)$ then M is a faithful R/I-module.

Def'n If $N \subseteq M$ & M is an R-module and N is an R-module then we'll call N an <u>R-submodule</u> of M if

$n_1, n_2 \in N \Rightarrow n_1 + n_2 \in N$

$n \in N, r \in R \Rightarrow r \cdot n \in N$

$0_M \in N$

Remarks:

1) R is an R-module
2) $I \trianglelefteq R \Rightarrow I$ is a R-submodule of R
3) If M is an R-module & $I \trianglelefteq R$
   we can construct an R-submodule IM of M,
   $$IM = \{\sum_{i=1}^{n} x_i m_i \,;\, x_i \in I,\ m_i \in M\}$$
4) If $N \subseteq M$ is an R-submodule of M, we can form a quotient module
   $$M/N = \{m + N \,;\, m \in M\}$$
   $$(m_1 + N) + (m_2 + N) = (m_1 + m_2) + N$$
   $$r(m + N) = rm + N$$

If R is a ring & M, N are two R-modules we say that a map $f: M \to N$ is an <u>R-module homomorphism</u> if
① $f(m_1 + m_2) = f(m_1) + f(m_2) \quad \forall m_1, m_2 \in M$
② $f(r \cdot m) = r \cdot f(m) \quad \forall r \in R,\ m \in M$

Facts:

1) $\ker(f) = \{m \in M \,;\, f(m) = 0\} \subseteq M$ is a submodule
2) $\operatorname{im}(f) = \{f(m) \,;\, m \in M\} \subseteq N$ is a submodule
3) $\ker(f) = (0) \iff f$ is 1-1
4) $\operatorname{im}(f) = N \iff f$ is onto
5) if $f: M \to M'$ is an onto R-module homomorphism then
   $$M/\ker(f) \cong M'$$

If M & N are two R-modules then
$$\operatorname{Hom}_R(M,N) = \{f: M \to N \,;\, f \text{ is an } R\text{-module homomorphism}\}$$
Notice that $\operatorname{Hom}_R(M,N)$ is itself an R-module
$f, g \in \operatorname{Hom}_R(M,N)$, $(f+g)(m) = f(m) + g(m)$
$0_{\operatorname{Hom}}(m) = 0_N$
if $f \in \operatorname{Hom}_R(M,N)$, $r \in R$, $(rf)(m) = rf(m) = f(rm)$

Ex. $R = \mathbb{C}$, $M = \{\begin{bmatrix} a \\ b \end{bmatrix}, a, b \in \mathbb{C}\} = \mathbb{C}^{2\times 1}$, $N = \mathbb{C}^{3\times 1}$
$\operatorname{Hom}_{\mathbb{C}}(\mathbb{C}^2, \mathbb{C}^3) = M_{3\times 2}(\mathbb{C})$

If $f: M \to M$ we call f an endomorphism.

$\mathrm{Hom}_R(M,M) = \mathrm{End}_R(M)$ ← is actually a ring

$(f+g)(m) = f(m)+g(m)$

$M \xrightarrow{f} M \xrightarrow{g} M$, $M \xrightarrow[\text{null}]{f-g} M$

Ex $R = \mathbb{C}$, $M = \mathbb{C}^{2\times 1}$

$\mathrm{End}_{\mathbb{C}}(\mathbb{C}^2) \cong M_{2\times 2}(\mathbb{C})$

A module M is <u>simple</u> if (0) & M are it's only R-submodules

Schur's lemma: If M is a simple R-module then $\mathrm{End}_R(M)$ is a division ring, ie every non-zero element has an inverse

Direct Sum & Direct Product

If X is an index set & $\{M_\alpha\}_{\alpha\in X}$ is a collection of R-modules then we have

(direct sum) $\bigoplus_{\alpha\in X} M_\alpha = \{(m_\alpha)_{\alpha\in X};\ m_\alpha \in M_\alpha \ \&\ \{\alpha\in X;\ m_\alpha \neq 0\} \text{ finite}\}$

(direct product) $\prod_{\alpha\in X} M_\alpha = \{(m_\alpha)_{\alpha\in X};\ m_\alpha \in M_\alpha\}$

Ex $R = \mathbb{Z}$, $M_1 = \bigoplus_{\mathbb{N}} \mathbb{Z}$, $M_2 = \prod_{\mathbb{N}} \mathbb{Z}$

Q: Is $M_1 \cong M_2$ as an R-module

A: No, M_1 countable, M_2 uncountable

<u>Def</u> An R-module M is <u>free</u> if there exists a set X such that

$$M \cong \bigoplus_{i\in X} R$$

More intuitively, M is free if there exists a subset

$$B = \{m_x;\ x\in X\} \subseteq M$$

such that every element of M has a unique expression

$$m = \sum_{x\in X} r_x m_x,\ r_x = 0 \text{ for all but finitely many } x\in X$$

To see the equivalence, let $e_y \in \bigoplus_{x \in X} R$, $y \in X$ be the sequence with a 1 in the y^{th} coordinate & zeroes everywhere else.

$$f: \bigoplus_{x \in X} R \to M, \quad f((r_x)_{x \in X}) = \sum_{x \in X} r_x e_x$$

Hard question: Is $\prod_{i=1}^{\infty} \mathbb{Z}$ a free $\mathbb{Z}$-module?

Remark: If R is a field every R-module is free (Zorn's lemma)

Eg if $R = \mathbb{Z}$, $M = \mathbb{Z}/2\mathbb{Z}$, M is not free
$2 \cdot m = 0 \cdot m \quad \forall m \in M$

Notation: We'll write R^X for $\bigoplus_{x \in X} R$ & if $|X| = n < \infty$, we'll write R^n for $\bigoplus_{i=1}^{n} R$.
If $M = R^X$, we call $|X|$ the rank of the free module M.
rank = dimension, for v.s.
We don't know yet whether rank is unique.
ie can we have, say, $R^2 \cong R^3$?
We'll show rank is well-defined & we can't have $R^n \cong R^m$ unless $n = m$.

Exactness

M, M', M'' be three R-modules
$f: M'' \to M$, $g: M \to M'$
write this as $M'' \xrightarrow{f} M \xrightarrow{g} M'$
We say this is exact at M if $\operatorname{im}(f) = \ker(g)$.
More generally, if we have

$$M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \xrightarrow{f_3} \cdots \xrightarrow{f_n} M_{n+1}$$

then we say this is exact if it is exact at each M_i, $i \in \{2, \ldots, n\}$.

2015 01 09

An exact sequence of the form

$$0 \longrightarrow M'' \xrightarrow{f} M \xrightarrow{g} M' \longrightarrow 0$$

is called a <u>short exact sequence</u>.
What does it mean?

$0 \longrightarrow M'' \xrightarrow{f} M$ is exact $\iff$ f is injective
$M'' \xrightarrow{f} M \xrightarrow{g} M'$ is exact $\iff$ $\operatorname{im}(f) = \ker(g)$
$M \xrightarrow{g} M' \longrightarrow 0$ is exact $\iff$ g is surjective

Remark: If $0 \longrightarrow M'' \xrightarrow{f} M \xrightarrow{g} M' \longrightarrow 0$ is a short exact sequence then $M/\ker(g) \cong M'$ as R-modules.
Why? g onto, so 1st iso. thm $\Rightarrow M/\ker(g) \cong \operatorname{im}(g)$

<u>Ex</u> If M and N are R-modules

$\iota : M \to M \oplus N$ $\quad$ $\pi_2 : M \oplus N \to N$
$\iota(m) = (m, 0)$ $\quad$ $\pi_2(m, n) = n$

short exact sequence

$$0 \longrightarrow M \xrightarrow{\iota} M \oplus N \xrightarrow{\pi_2} N \longrightarrow 0$$

<u>Ex</u>

$$0 \longrightarrow \mathbb{Z} \xrightarrow{f} \mathbb{Z} \xrightarrow{g} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

$n \xmapsto{g} n + 2\mathbb{Z}$
$n \xmapsto{f} 2n$

Splitting

A short exact sequence

$$0 \longrightarrow M'' \xrightarrow{f} M \xrightarrow{g} M' \longrightarrow 0$$

is said to split if there exists an R-module homomorphism

$$\tau : M' \to M$$

such that

$$g \circ \tau = \mathrm{id}_{M'}.$$

(Sometimes τ is called a <u>section</u>)

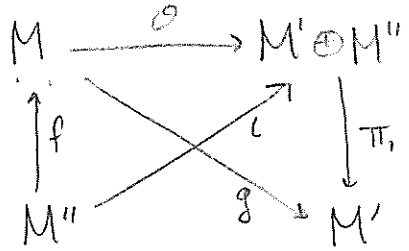
Splitting Lemma:

Let

$$0 \longrightarrow M'' \xrightarrow{f} M \xrightarrow{g} M' \longrightarrow 0$$

be a short exact sequence. Then the following are equivalent:

1) there exists an R-module isomorphism $\theta: M \to M' \oplus M''$ such that $\theta \circ f(m'') = (0, m'')$ for all $m'' \in M''$ and $\pi_1(\theta(m)) = g(m)$ for all $m \in M$



2) there exists $\tau: M' \to M$ such that $g \circ \tau = id_{M'}$

3) there exists $\sigma: M \to M''$ such that $\sigma \circ f = id_{M''}$

$$0 \longrightarrow M'' \underset{\sigma}{\overset{f}{\rightleftarrows}} M \underset{\tau}{\overset{g}{\rightleftarrows}} M' \longrightarrow 0$$

Proof:

(1)$\Rightarrow$(2): Suppose we have the map $\theta: M \xrightarrow{\cong} M' \oplus M''$. We want to construct a map $\tau: M' \to M$. Do this via $\tau(m') = \theta^{-1}(m', 0)$. What is $g \circ \tau$?

$$g \circ \tau(m') = g(\theta^{-1}(m', 0)) = \pi_1(\theta(\theta^{-1}(m', 0))) = \pi_1(m', 0) = m'.$$

(1)$\Rightarrow$(3): We have θ. Want to construct $\sigma: M \to M''$. Define $\sigma(m) = \pi_2(\theta(m))$. Need to show $\sigma \circ f = id_{M''}$:

$$\sigma(f(m'')) = \pi_2(\theta(f(m''))) = \pi_2(\iota(m'')) = \pi_2(0, m'') = m''.$$

(3)$\Rightarrow$(1): Want to define $\theta: M \to M' \oplus M''$. Define $\theta(m) = (g(m), \sigma(m))$:

$$\pi_1(\theta(m)) = \pi_1(g(m), \sigma(m)) = g(m),$$
$$\theta(f(m'')) = (g(f(m'')), \sigma(f(m''))) = (0, m'').$$

(2)$\Rightarrow$(1): Define instead $\psi: M' \oplus M'' \to M$ by $\psi(m', m'') = \tau(m') + f(m'')$.

Claim: ψ is an isomorphism.

$$\ker(\psi) = \{(m', m'') \,;\, \tau(m') + f(m'') = 0\}$$

Notice $\tau(m') + f(m'') = 0 \to g(\tau(m')) + g(f(m'')) = 0 \Rightarrow m' + 0 = 0 \to m' = 0$. Also $f(m'') = 0$ now implies $m'' = 0$.

To show ψ is onto, let $m \in M$. Apply g to figure out $m_1 = g(m)$. Now $m - \tau(m') \in \ker(g) = \text{im}(f)$, so $\exists! m''$ with desired property. Check rest. ∎

Warning: If $M \cong M'' \oplus M'$ and $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ is a short exact sequence, then we do not necessarily have a section for g or f.

Eg. $R = \mathbb{Z}$ $M'' = \mathbb{Z}$, $M = \mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^{\omega}$, $M' = (\mathbb{Z}/2\mathbb{Z})^{\omega} = \bigoplus_{i=1}^{\infty} (\mathbb{Z}/2\mathbb{Z})$
Then $M \cong M'' \oplus M'$. Let $f: M'' \to M$, $g: M \to M'$
$f(n) = (2n, 0, 0, \ldots)$ $g(n, \varepsilon_1, \varepsilon_2, \ldots) = (n + 2\mathbb{Z}, \varepsilon_1, \ldots)$
Then $0 \to M'' \xrightarrow{f} M \xrightarrow{g} M' \to 0$ is exact.
Notice that g does not have a section, ie $\nexists \tau: M' \to M$ s.t. $g \circ \tau = id_{M'}$.
Why not? Let's think!

$$\tau(\varepsilon_1, \ldots) = (\underbrace{0}_{\text{must be } 0}, ? \ldots)$$

So $(1,0,0,\ldots) \xmapsto{\tau} (0, *, \ldots)$
$\downarrow g$
$(0, *, \ldots)$
id ↘ ↙ impossible

Structure theorem for modules over a PID

Recall: An R-module M is called <u>cyclic</u> if there is an $m \in M$ such that $M = Rm$

Eg. $R = \mathbb{Z}$, $M = \mathbb{Z} \oplus \mathbb{Z}$ is not cyclic
$N = \mathbb{Z}/5\mathbb{Z}$ is cyclic

Remark: If M is cyclic with $M = Rm$. We have an R-module homomorphism $\varphi: R \to M$ given by $\varphi(r) = rm$.
$I = \ker(\varphi) \trianglelefteq R$, the 1st iso. thm. $\Rightarrow M \cong R/I$, $I = \mathrm{Ann}(M)$.

Let R be a ring & let M be an R-module. Recall that M is a finitely generated (f.g.) R-module if $\exists \ell = 1$ & $m_1, \ldots, m_\ell \in M$ s.t. $M = Rm_1 + \cdots + Rm_\ell$.

Theorem: Let R be a PID & let M be a f.g. R-module. Then $\exists d \geq 0$ (unique) ~~such that~~ & some prime elements $\pi_1, \dots, \pi_s \in R$, $s \geq 0$ distinct not nec. unique but unique up to reord.

such that

$$M \cong R^d \oplus R/(\pi_1^{r_1}) \oplus \cdots \oplus R/(\pi_s^{r_s})$$

Proof: By induction on the number of generators d needed for M.

Base case. $d=1 \iff M$ is cyclic $\iff M \cong R/I$.

~~Inductive case: case I.~~

Two cases. Case 1: $I=(0) \Rightarrow M \cong R^1$

Case 2: $I \neq (0) \Rightarrow I = (a)$, $a \neq 0$. PID $\Rightarrow$ UFD so

$a = u\pi_1^{r_1} \cdots \pi_s^{r_s}$ u unit, π_i prime distinct

So $I = (\pi_1^{r_1} \cdots \pi_s^{r_s})$. For $k=1,\dots,s$ let $J_k = (\pi_k^{r_k})$.

Claim: J_k's are comaximal, ie $k \neq \ell \Rightarrow J_k + J_\ell = R$ & $\bigcap_{k=1}^s J_k = I$ (CRT $\Rightarrow$)

$$\hookrightarrow R/I \cong \prod_{i=1}^s R/J_i = \prod_{k=1}^s R/(\pi_k^{r_k})$$

Verification: 1) $k \neq \ell \rightarrow J_k + J_\ell = (\pi_k^{r_k}, \pi_\ell^{r_\ell}) = (b)$ as R is a PID

$(b) \geq (\pi_k^{r_k}) \Rightarrow b \mid \pi_k$

$(b) \geq (\pi_\ell^{r_\ell}) \Rightarrow b \mid \pi_\ell$ $\Rightarrow b$ unit

2) As $I \leq J_k$ $\forall k$, $I \leq \bigcap J_k$.

if $b \in J_k$ $\forall k$ then $\pi_k^{r_k} \mid b$ $\forall k \rightarrow \pi_1^{r_1} \cdots \pi_s^{r_s} \mid b \rightarrow b \in I$.

Inductive Case: Now suppose the result holds whenever M is generated by less than d elements.

Consider $M = \langle m_1, \dots, m_d \rangle = Rm_1 + \cdots + Rm_d$

Case I: $r_1 m_1 + \cdots + r_d m_d = 0 \rightarrow r_i = 0 \ \forall i : \Rightarrow M \cong R^d$.

Case II: $\exists (r_1, \dots, r_d) \neq (0, \dots, 0)$ s.t. $r_1 m_1 + \cdots + r_d m_d$.

Consider the set $\mathcal{S}$ of all d-tuples $(m_1, \dots, m_d) \in M^d$ ~~s.t.~~ s.t. $M = Rm_1 + \cdots + Rm_d$.

Given $(n_1, \dots, n_d) \in \mathcal{S}$. Let $J_{(n_1,\dots,n_d)} \leq R$

Trick: Pick $(n_1, \dots, n_d) \in \mathcal{S}$ such that $\{r \in R : rn_1 \in Rn_2 + \cdots + Rn_d\}$ that $J_{(n_1,\dots,n_d)}$ is maximal in the collection of ideals $\{J_{(n_1,\dots,n_d)} : (n_1, \dots) \in \mathcal{S}\}$.

Sometimes you're in the zone, and you realize the zone is an illusion

2015 01 13 (2)

Fact: If $\mathcal{J}$ is a non-empty collection of ideals in a PID then $\exists J \in \mathcal{J}$ that is maximal in $\mathcal{J}$. (wrt inclusion)

Proof: Pick $(a_1) \in \mathcal{J}$. If (a_1) is maximal in $\mathcal{J}$, stop.
Otherwise, $\exists (a_2) \in \mathcal{J}$ st $(a_2) \supsetneq (a_1)$, . . .
We see that either we'll eventually produce a maximal element of $\mathcal{J}$, or we'll produce an infinite ascending chain

2015 01 15

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

of ideals in $\mathcal{J}$. Let, as R is a PID,

$$J = \bigcup_{i=1}^{\infty} (a_i) = (b).$$

So $\exists j$ st $b \in (a_j) \Rightarrow (b) \subseteq (a_j)$. This is a contradiction as

$$(b) \supseteq (a_{j+1}) \supsetneq (a_j) \supseteq (b).$$

□

(Pf cont.) As R is a PID,

$$J_{(n_1,\ldots,n_d)} = (r).$$

Claim: If $r_1 m_1 + r_2 m_2 + \cdots + r_d m_d = 0 \Rightarrow r \mid r_2, \ldots, r \mid r_d$.
Once we have the claim, we are done!
Why? Let $N_1 = Rn_1' \subseteq M$ and $N_2 = Rn_2' + \cdots + Rn_d' \subseteq M$.
By induction hypothesis, N_1 and N_2 have a decomposition of the desired form. So does $N_1 \oplus N_2$ then.

So write $r_i = ra_i$ and let
$n_1' = n_1 + a_2 n_2 + \cdots + a_d n_d$
$n_i' = n_i$ $i \neq 1$

Claim 2: $M \cong N_1 \oplus N_2$.
Why? To show this, we need $M = N_1 + N_2$ (obvious) and $N_1 \cap N_2 = (0)$.
If $a \in N_1 \cap N_2$ then $a = un_1'$ and $a = u_2 n_2' + \cdots + u_d n_d'$.
Notice $rn_1' = r(n_1 + a_2 n_2 \cdots + a_d n_d) = rn_1 + ra_2 n_2 + \cdots = rn_1 + \cdots = 0$
So if $a \in N_1 \cap N_2$ & $a \neq 0$ then $r \nmid u$. So $(u, r) \supsetneq (r)$ if $a \neq 0$.
But $un_1' = u_2 n_2' + \cdots \in Rn_2' + \cdots + Rn_d'$
& $rn_1' = 0 \in Rn_2' + \cdots + Rn_d'$
$\Rightarrow J_{(n_1', \ldots, n_d')} \supseteq (u, r) \supsetneq (r) = J_{(n_1, \ldots, n_d)}$
Contradicting the maximality of $J_{(n_1, \ldots, n_d)}$.

Proof of claim: Suppose $r_1 n_1 + \cdots + r_d n_d = 0$ & $\exists i > 1$ st $r \nmid r_i$. Wlog $i = 2$. Let $s = \gcd(r, r_2)$ & $(s) \supsetneq (r)$. Write $r = sa$, $r_2 = sb$, $\gcd(a, b) = 1$. ie $\exists c, d \in R$ st $ca + db = 1$

$\begin{bmatrix} a & b \\ -d & c \end{bmatrix}$ with $\det \neq 0$

Take the relation $r_1 n_1 + r_2 n_2 + \cdots + r_d n_d = s(an_1 + bn_2) + r_3 n_3 + \cdots + r_d n_d = 0$
Make a new spanning set for M:

$$\begin{cases} n_1' = an_1 + bn_2 \\ n_2' = -dn_1 + cn_2 \end{cases} \qquad \begin{cases} n_3' = n_3 \\ n_4' = n_4 \end{cases}$$

Why does it span M?

$cn_1' - bn_2' = \quad = n_1$

$dn_1' + an_2' = \quad = n_2$

Now what?

$s(an_1 + bn_2) + r_3 n_3 + \cdots + r_d n_d = 0$

$\Rightarrow sn_1' + r_3 n_3' + \cdots = 0 \Rightarrow J(n_1', \ldots, n_d') \supseteq (s) \ni (1)$ ⊥ ∎

Tensor Products

$$m : R \times R \to R$$
$$m(r+s, u) = m(r,u) + m(s,u)$$
$$m(ar, u) = am(r,u)$$

Let R be a ring & let M & N be two R-modules. We will create a module $M \otimes_R N$ called the tensor product of M & N (over R).
How do we build this?
Start by building a free module F with basis $\{e_{(m,n)} ; (m,n) \in M \times N\}$.
We'll take a submodule $G \subseteq F$, G will be the R-submodule of F spanned by all elements of the following form:

$$e_{(rm,n)} - re_{(m,n)}, \quad e_{(m_1+m_2,n)} - e_{(m_1,n)} - e_{(m_2,n)},$$
$$e_{(m,rn)} - re_{(m,n)}, \quad e_{(m,n_1+n_2)} - e_{(m,n_1)} - e_{(m,n_2)}$$

Define $M \otimes_R N := F/G$. We write $m \otimes n := e_{(m,n)} + G$.
Warning: Not every element of $M \otimes_R N$ need be expressible as $m \otimes n$.

Ex What is $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} (\mathbb{Z}/3\mathbb{Z})$?
Solution: Write $\mathbb{Z}/2\mathbb{Z} = \{[0]_2, [1]_2\}$, $\mathbb{Z}/3\mathbb{Z} = \{[0]_3, [1]_3, [2]_3\}$

$F = \mathbb{Z}e_{([0]_2,[0]_3)} \oplus \cdots \oplus \mathbb{Z}e_{([1]_2,[2]_3)}$.

Claim $G = F$, ie $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z} = (0)$

$e_{([i]_2,[j]_3)} = ie_{([1]_2,[j]_3)} = ije_{([0]_2,[0]_3)}$ mod G

So $e_{([0]_2,[0]_3)}$ generates. But this is $= e_{[3]_2,[1]_3} = 3e_{[1]_2,[1]_3} = e_{[1]_2,[0]_3}$

$= 0\, e_{[1]_2,[1]_3} = 0$ mod