

Def 1.1 A ring is a nonempty set R with two binary operations $+$ and \cdot satisfying

- (1) $(R, +)$ is an abelian group
- (2) (R, \cdot) is a semigroup
- (3) $a(b+c) = ab+ac$ for all $a, b, c \in R$.
 $(a+b)c = ac+bc$

If multiplication is commutative, R is called a commutative ring

If (R, \cdot) is a monoid, R is called a unital ring or ring with 1 or a ring with unity

Ex \mathbb{Z} is a commutative ring with 1.

Ex \mathbb{Z}_n is a commutative ring with 1.

Ex $M_n(\mathbb{R})$ is a non-commutative ring with 1.

Thm 1.2 Let R be a ring.

- (i) $0 \cdot a = a \cdot 0 = 0$ for all $a \in R$
- (ii) $(-a)b = a(-b) = -(ab)$ for all $a, b \in R$
- (iii) $(-a)(-b) = ab$ for all $a, b \in R$
- (iv) $(na)b = a(nb) = n(ab)$ for all $n \in \mathbb{Z}$, $a, b \in R$.
- (v) $\left(\sum_{i=1}^n a_i\right)\left(\sum_{j=1}^m b_j\right) = \sum_{i=1}^n \sum_{j=1}^m a_i b_j$ for all $a_i, b_j \in R$

Pf (i) $0 \cdot a = (0+0) \cdot a = 0a + 0a$, so $0 = 0a$

(ii) $ab + (-a) \cdot b = (a + (-a))b = 0 \cdot b = 0$, so $(-a)b = -(ab)$

(iii) $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$

(iv) $(na) \cdot b = (a + \dots + a)b = ab + \dots + ab = n(ab)$

(v) Distributive property

□

Def 1.3 Let R be a ring. $a \in R$ is called a left zero divisor if $ab=0$ for some $b \in R$. A zerodivisor is an element that is both a left and right zero divisor.

Ex 2 is a zero divisor in \mathbb{Z}_6 .

Ex $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ is a zero divisor in $M_2(\mathbb{R})$
 since $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

Def 1.4 Let R be a ring with 1. $a \in R$ is called left invertible if there exists $b \in R$ with $ba=1$. An element that is both left and right invertible is called a unit. The group of units is (usually) denoted R^* .

Ex $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in M_2(\mathbb{R})$ is a unit (since $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$)

Def 1.5 A commutative ring with $1 \neq 0$ and no zero divisors is called an integral domain. A ring with $1 \neq 0$ in which every nonzero element is a unit is called a division ring.
 A commutative division ring is called a field.

Ex \mathbb{Z} is an integral domain.

Def 1.7 Let R, S be rings. A function $f: R \rightarrow S$ is called a homomorphism if $f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$ for all $a, b \in R$.

Def 1.8 Let R be a ring. If there is a least positive integer n s.t. $na=0$ for all $a \in R$, n is called the characteristic of R , written $\text{char } R = n$. Otherwise, say R has characteristic 0.
Ex $\text{char } \mathbb{Z}_n = n$

Thm 1.9 Let R be a unital ring with $\text{char } R = n > 0$

(i) Let $\phi: \mathbb{Z} \rightarrow R$ be the map given by $\phi(m) = m \cdot 1$.

ϕ is a homomorphism with $\text{Ker } \phi = \langle n \rangle$

(ii) n is the least positive integer such that $n \cdot 1 = 0$

(iii) If R has no zero divisors, then n is prime.

Pf (i) If $m \in \text{Ker } \phi$, $ma = 0 \cdot m \cdot 1 \cdot a = 0 \cdot a = 0$ for all $a \in R$.

By assumption, $m > n$. Write $m = Kn + r$ for some $0 \leq r < n$.

Then $ra = 0$ for all $a \in R$, so $r = 0$, i.e. $m \in \langle n \rangle$.

(ii) If $K \cdot 1 = 0$, then $K \cdot a = K \cdot 1 \cdot a = 0 \cdot a = 0$ for all $a \in R$.

(iii) Suppose $n = Kr$ for some $K, r \in \mathbb{N}$.

Then $0 = n \cdot 1 = Kr \cdot 1 = K(r \cdot 1)$

□

~~Section 2~~

§2 Ideals

Observe: If $x, y \in \text{Ker } \phi$, $x+y, xy \in \text{Ker } \phi$

But also If $a \in R$, $x \in \text{Ker } \phi$, $ax \in \text{Ker } \phi$

Def 2.1 Let R be a ring. A subring is a subset that is itself a ring.

A left ideal I is a subring satisfying if $x \in R$, $a \in I$, $xa \in I$

A right ideal I is a subring satisfying if $a \in I$, $x \in R$, $ax \in I$

A (two-sided) ideal is a subring that is both a left and right ideal.

Ex $\langle n \rangle$ is an ideal of \mathbb{Z}

Ex Let $I = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \mid a, b \in \mathbb{R} \right\} \subset M_2(\mathbb{R})$. This is a left-sided ideal but not a right ideal.

Ex For any ring R , $\{0\}$ and R are ideals

Cor 2.3 The intersection of ideals is an ideal.

Def 2.4 Let $X \subset R$ be a subset. Let $\{A_i\}_{i \in I}$ be the collection of all ideals containing X .
Then $(X) = \bigcap_{i \in I} A_i$ is called the ideal generated by X .

If $X = \{x_1, \dots, x_n\}$, we write (x_1, \dots, x_n) and say it is finitely generated.

A principal ideal is an ideal generated by a single element.

A principal ideal domain (PID) is an integral domain in which all ideals are principal.

Ex In \mathbb{Z} , $(3) = \langle 3 \rangle = 3\mathbb{Z}$

Ex \mathbb{Z} is a PID. $(a, b) = (d)$ where $d = \gcd(a, b)$, since $d = ma + nb$ for some $m, n \in \mathbb{Z}$.

Thm 2.6 Let I, J be (left) ideals of a ring R .

(i) $I + J = \{x + y \mid x \in I, y \in J\}$ is a (left) ideal

(ii) $IJ = \{ \sum x_i y_i \mid x_i \in I, y_i \in J \}$ is a (left) ideal.

Thm 2.7 Let R be a ring, I an ideal. Then the additive quotient group R/I is a ring with multiplication $(a+I)(b+I) = ab+I$

pf well defined: Suppose $a+I = a_0+I$, $b+I = b_0+I$
 $a = a_0 + x$ for some $x \in I$ $b = b_0 + y$ for some $y \in I$

$$\text{Then } a_0 b_0 + I = (a - x)(b - y) + I = ab - ax - xb + xy + I = ab + I.$$

$\uparrow \quad \quad \uparrow \quad \quad \uparrow$
 $I \quad \quad I \quad \quad I$

□

Thm 2.8 If $\varphi: R \rightarrow S$ is a ring homomorphism, $Ker \varphi$ is an ideal.

pf If $a, b \in Ker \varphi$, $\varphi(a+b) = \varphi(a) + \varphi(b) = 0 + 0 = 0$, so $a+b \in Ker \varphi$

If $a \in Ker \varphi$, $x \in R$, $\varphi(ax) = \varphi(a)\varphi(x) = 0\varphi(x) = 0$, so $ax \in Ker \varphi$

$\varphi(xa) = \varphi(x)\varphi(a) = \varphi(x)0 = 0$, so $xa \in Ker \varphi$ \square

~~Thm 2.9~~

Thm 2.9 (First Isomorphism Theorem) Let $\varphi: R \rightarrow S$ be a ring homomorphism.

Then $R/Ker \varphi \cong Im \varphi$

pf Let $\bar{\varphi}: R/Ker \varphi \rightarrow Im \varphi$ be the well-defined abelian group isomorphism
 $a + Ker \varphi \mapsto \varphi(a)$

check: $\bar{\varphi}(a + Ker \varphi) \bar{\varphi}(b + Ker \varphi) = \varphi(a)\varphi(b) = \varphi(ab)$

$\bar{\varphi}(ab + Ker \varphi) = \varphi(ab)$

so $\bar{\varphi}$ is a ring isomorphism. \square

Thm 2.13 Let $I \subset R$ be an ideal. There is a one-to-one correspondence between
 ideals of R/I and ideals of R containing I .

Def A prime ideal P of a ring R is a proper ideal satisfying

~~$RS \subset P \Rightarrow R \subset P$ or $S \subset P$~~

$IS \subset P \Rightarrow I \subset P$ or $S \subset P$ for all ideals $I, S \subset R$

Thm 2.15 Let P be a proper ideal of a ring R .

~~1) If R is prime, then $R \setminus P$ is multiplicatively closed,
 or if $a, b \in R$ then $ab \in P$ or $b \in P$.~~

~~2) If R is commutative and P is prime,~~

1) If $R \setminus P$ is multiplicatively closed, then P is prime.

2) If R is commutative and P is prime, then $R \setminus P$ is multiplicatively closed.

Remark $R \setminus P$ multiplicatively closed \Leftrightarrow If $a, b \in R$ with $ab \in P$, either $a \in P$ or $b \in P$

PF (i) Let $I, J \subset R$ be ideals with $I \subset J \subset P$.

Suppose $I \not\subset P$ (so we will show $J \subset P$).

Let $x \in I \setminus P$. Let $y \in J$.

Then $xy \in I \subset P$, so $y \in P$ (since $x \notin P$).

This holds for all $y \in J$, so $J \subset P$.

(ii) Let $a, b \in R$ with $ab \in P$

Claim ~~(a) or (b) \subset P~~

If $x \in (a)(b)$, $x = ar_1br_2$ for some $r_1, r_2 \in R$
 $= (ab)r_1r_2 \in P$.

P prime $\Rightarrow (a) \subset P$ (so $a \in P$) or $(b) \subset P$ (so $b \in P$)

Cor Let R be a commutative unit ring. Then (0) is prime iff R is an integral domain.

PF Let $a, b \in R \setminus (0)$. Then (0) is prime iff $ab=0$ implies $a=0$ or $b=0$ if R is an integral domain. \square

Ex The prime ideals of \mathbb{Z} are precisely (p) for primes p .

Thm 2.16 Let R be a commutative unit ring. An ideal P is prime iff R/P is an integral domain.

PF \Rightarrow Let $a+P, b+P \in R/P$.
If $(a+P)(b+P) = 0+P$, $ab+P = P$, i.e. $ab \in P$.
Then $a \in P$ or $b \in P$, so $a+P = 0+P$ or $b+P = 0+P$.
Thus R/P is an integral domain.

\Leftarrow Suppose R/P is an integral domain. Let $a, b \in R$ with $ab \in P$.
Then $(a+P)(b+P) = 0+P$, so $a+P = 0+P$ or $b+P = 0+P$
i.e. $a \in P$ or $b \in P$.

Thus P is prime \square

Def 2.17 Let R be a ring. A proper ideal M is called maximal if it is not contained in any other proper ideal.

Ex (3) is maximal in \mathbb{Z} . (6) is not maximal since $(6) \subset (2)$.

Thm 2.18 Let R be a unital ring. Then R contains a maximal ideal. Moreover, every proper ideal is contained in some maximal ideal.

Pf Let \mathcal{P} be the poset of proper ideals of R ordered by inclusion.

Let $\mathcal{C} = \{C_i \mid i \in I\}$ be a chain of ^{proper} ideals.

Claim $C := \bigcup_{i \in I} C_i$ is an upper bound for \mathcal{C}

(1) C is a proper ideal: Let $a, b \in C$, so $a \in C_i, b \in C_j$.
Since \mathcal{C} is a chain, wlog $C_i \subset C_j$, so $a, b \in C_j \subset C$.

If $r \in R$, $ra \in C_i \subset C$.

Note $1 \notin C_i$ for all $i \in I$, so $1 \notin C$.

(2) $C_i \subset C$ for all $i \in I$: By construction.

Then Zorn $\Rightarrow \mathcal{P}$ has a maximal element. \square

Thm 2.19 Let R be a ~~commutative~~ commutative unital ring. Every maximal ideal is a prime ideal.

Pf Let M be a maximal ideal, and $a, b \in R \setminus M$.

Then $M + (a) = M + (b) = R$, so

$$1 = m_1 + ar_1 = m_2 + br_2$$

for some $m_1, m_2 \in M, r_1, r_2 \in R$.

$$\text{Then } 1 = (m_1 + ar_1)(m_2 + br_2) = \underbrace{m_1 m_2 + m_1 br_2 + m_2 ar_1}_{\in M} + ab r_1 r_2$$

If $ab \in M$, then $1 \in M$ \downarrow so $ab \notin M$, thus M is prime. \square

Thm 2.20 Let R be a unital ring.

(i) If R/M is a division ring, then M is maximal.

(ii) If R is commutative, then M is maximal $\Leftrightarrow R/M$ is a field.

PF (i) Let N be an ideal with $M \subsetneq N$.

Let $a \in N \setminus M$. Then there exists $b \in N \setminus M$ with $(a+M)(b+M) = 1+M$

so $ab - 1 \in M \subset N$. But $ab \in N$, so $1 \in N$, i.e. $N = R$.

Thus M is maximal.

(ii) \Leftarrow Follows from (i)

\Rightarrow Suppose M is maximal. Then M is prime, so R/M is an integral domain.

Let $a+M \neq 0+M$, (so $a \notin M$).

Then $(a+M)R/M = R/M$, so $1 = ar + m$ for some $r \in R, m \in M$.

Then $(a+M)(r+M) = ar + M = 1 + M$

Thus every non-zero element of R/M has a multiplicative inverse,

So R/M is a field.

Cor 2.21 Let R be a commutative unital ring. TFAE

(i) R is a field

(ii) R has exactly two ideals, 0 and R .

(iii) 0 is a maximal ideal

(iv) Every non-zero homomorphism of rings $R \rightarrow S$ is injective.

PF Thm 2.20 gives ~~(i) \Leftrightarrow (ii)~~ (i) \Leftrightarrow (iii). Clearly (ii) \Leftrightarrow (iii)

(iv) \Leftrightarrow Either $\ker \varphi = 0$ or $\ker \varphi = R \Leftrightarrow$ (ii)

□

Thm 2.22, 2.23 Let $\{R_i\}_{i \in I}$ be a collection of rings. Then $\prod_{i \in I} R_i$ is a ring (with component wise multiplication) that is ~~the~~ a product in the category of rings.

Thm 2.24 Let R be a ring, ~~and~~ $I_1, \dots, I_n \subset R$ ideals. Suppose

(i) $I_1 + \dots + I_n = R$

(ii) $I_k \cap (I_1 + \dots + I_{k-1} + I_{k+1} + \dots + I_n) = 0$ for each $1 \leq k \leq n$.

Then $R \cong I_1 \times \dots \times I_n$.

pf $\varphi: I_1 \times \dots \times I_n \rightarrow R$ given by $\varphi(x_1, \dots, x_n) = x_1 + \dots + x_n$ is an abelian group isomorphism.

Observe: If $x \in I_i$, $y \in I_j$, then $xy \in I_i \cap I_j = 0$

Let $(a_1, \dots, a_n), (b_1, \dots, b_n) \in I_1 \times \dots \times I_n$

then $\varphi(a_1, \dots, a_n) \varphi(b_1, \dots, b_n) = (a_1 + \dots + a_n)(b_1 + \dots + b_n)$

$$= a_1 b_1 + \dots + a_n b_n$$

$$= \varphi(a_1, \dots, a_n) \varphi(b_1, \dots, b_n) \quad \square$$

Thm 2.25 ("Chinese Remainder Theorem" - Sun-Tsz'e, ~400 AD)

Let $I_1, \dots, I_n \subset R$ be ideals such that $R^2 + I_i = R$ for all i

and $I_i + I_j = R$ for all $i \neq j$ (I_1, \dots, I_n called pairwise comaximal)

Let $b_1, \dots, b_n \in R$. Then there exists $b \in R$ such that

$$b \equiv b_i \pmod{I_i} \quad \text{for each } 1 \leq i \leq n.$$

Moreover, b is uniquely determined up to congruence modulo $I_1 \cap \dots \cap I_n$

PF Claim $R = I_k + \bigcap_{i \neq k} I_i$ for each $1 \leq k \leq n$

PF wlog $k=1$. Prove by induction $R = I_1 + \bigcap_{2 \leq i \leq n} I_i$

$n=2$: $R = I_1 + I_2$ ✓

$n \geq 2$: By induction, $R = I_1 + (I_2 \cap \dots \cap I_{n-1})$

$$R^2 = (I_1 + (I_2 \cap \dots \cap I_{n-1}))(I_1 + I_n) \subset I_1 + (I_2 \cap \dots \cap I_n)$$

$$\text{Since } R = R^2 + I_1, \quad R = I_1 + (I_2 \cap \dots \cap I_n)$$

Now let $b_1, \dots, b_n \in R$.

Then $b_k = q_k + r_k$ for some $q_k \in I_k$, $r_k \in \bigcap_{i \neq k} I_i$

In particular $r_k \equiv b_k \pmod{I_k}$ and $r_k \equiv 0 \pmod{I_i}$ for all $i \neq k$.

Let $b = r_1 + \dots + r_n$. Then $b \equiv r_k \equiv b_k \pmod{I_k}$ □

Cor 2.26 Let m_1, \dots, m_n be pairwise coprime positive integers.

Let $b_1, \dots, b_n \in \mathbb{Z}$. Then there is a solution to

$$x \equiv b_1 \pmod{m_1} \quad \dots \quad x \equiv b_n \pmod{m_n}$$

that is uniquely determined modulo $m_1 m_2 \dots m_n$.

PF Let $I_i = (m_i)$. Since $\gcd(m_i, m_j) = 1$, $1 = a m_i + b m_j$ for some $a, b \in \mathbb{Z}$
i.e. $\mathbb{Z} = (m_i) + (m_j)$. □

Apply thm 2.25.

§ 5 Polynomial rings

Def Let R be a ring. The ring of polynomials over R , denoted $R[x]$ is

- (1) The set of all sequences (a_0, a_1, a_2, \dots) such that $a_i \in R$, only finitely many non-zero
- (2) Addition is component wise
- (3) Multiplication given by

$$(a_0, a_1, \dots) \cdot (b_0, b_1, \dots) = (a_0 b_0, a_0 b_1 + a_1 b_0, a_0 b_2 + a_1 b_1 + a_2 b_0, \dots)$$

(n^{th} component is $\sum_{i+j=n} a_i b_j$)

Thm 5.1 $R[x]$ is a ring. If R is commutative or unital, so is $R[x]$

PF need to check multiplication is associative

Let $(a_i), (b_i), (c_i) \in R[x]$

$$\begin{aligned} (a_i) ((b_i) \cdot (c_i)) &= (a_i) \cdot \left(\sum_{j+k=i} b_j c_k \right) \\ &= \left(\sum_{r+s=i} a_r \sum_{j+k=s} b_j c_k \right) \\ &= \left(\sum_{r+j+k=i} a_r b_j c_k \right) \end{aligned}$$

$$\begin{aligned} ((a_i) \cdot (b_i)) \cdot (c_i) &= \left(\sum_{j+k=i} a_j b_k \right) \cdot (c_i) \\ &= \left(\sum_{r+s=i} \left(\sum_{j+k=r} a_j b_k \right) c_s \right) \\ &= \left(\sum_{j+k+s=i} a_j b_k c_s \right) \end{aligned}$$

If $1 \in R$, $(1, 0, 0, \dots)$ is multiplicative identity. □

Thm 5.2 Let R be a unital ring. Let $x \in R[x]$ be the element $(0, 1, 0, 0, \dots)$

(i) $x^n = (0, 0, \dots, 0, 1, 0, 0, \dots)$
 \uparrow
 $n+1$ -st spot

(ii) If $a \in R$, $ax^n = x^n a = (0, \dots, 0, a, 0, \dots)$

(iii) $\sum_{i=0}^n a_i x^i = (a_0, a_1, \dots, a_n, 0, \dots)$

Thm 5.3 Let R be a ring. Then $R[x][y] \cong R[y][x]$, so there are isomorphisms $R[x, y]$ (or more generally, $R[x_1, \dots, x_n]$)

pf If $f \in R[x][y]$, write $f = \sum_{i=0}^m (\sum_{j=0}^n a_{ij} x^j) y^i = \sum_{j=0}^n (\sum_{i=0}^m a_{ij} y^i) x^j$ □

Remark Sometimes use notation $R^{[n]} = R[x_1, \dots, x_n]$

Observe: $R \hookrightarrow R^{[n]}$

Thm 5.5 Let $\phi_0: R \rightarrow S$ be a homomorphism of commutative unital rings with $\phi_0(1) = 1$. Let $s_1, \dots, s_n \in S$. Then there is a unique homomorphism

$\phi: R[x_1, \dots, x_n] \rightarrow S$ s.t. $\phi|_R = \phi_0$ and $\phi(x_i) = s_i$.

In other words, ϕ is completely determined by ϕ_0 and the choice of $\phi(x_i)$.

pf ~~$\phi(\sum_{i=0}^n a_i x^i) = \sum_{i=0}^n \phi(a_i) \phi(x^i)$~~

It suffices to assume $n=1$.

If $\sum_{i=0}^n a_i x^i \in R[x]$, set $\phi(\sum_{i=0}^n a_i x^i) = \sum_{i=0}^n \phi_0(a_i) s^i$

(This is the only choice that makes ϕ a homomorphism)

This is called the evaluation map or substitution map □

§3 Factorization in commutative rings

Def 3.1 Let R be commutative, we say $a|b$ (a "divides" b) if $b = ax$ for some $x \in R$. If $a|b$ and $b|a$, then a and b are called associates.

Thm 3.2 Let R be commutative, unital, let $a, b \in R$.

- (i) $a|b \Leftrightarrow (b) \subset (a)$
- (ii) a and b are associates $\Leftrightarrow (a) = (b)$
- (iii) $u \in R^* \Leftrightarrow u|r$ for all $r \in R$.
- (iv) $u \in R^* \Leftrightarrow (u) = R$
- (v) If R is a domain, a and b are associates $\Leftrightarrow a = bu$ for some $u \in R^*$

pf (i) $a|b \Leftrightarrow \exists b \in (a) \Leftrightarrow (b) \subset (a)$

(ii) Immediate from (i)

(iii) $\Rightarrow r = u(u^{-1}r)$

\Leftarrow If $u|1$, $1 = ux$ for some $x \in R$, i.e. $u \in R^*$

(iv) note (iii) says $u \in R^* \Leftrightarrow u|1 \Leftrightarrow R \subset (u)$ by (i)

(v) \Leftarrow (Domain not needed) $a = bu \Rightarrow b|a$, $b = au^{-1} \Rightarrow a|b$

$\Rightarrow a = bx$ and $b = ay$

then $a = ayx \Leftrightarrow a(1 - yx) = 0 \Rightarrow x, y \in R^*$ \square

Def Let R be commutative, unital. Let $x \in R \setminus R^*$ be nonzero.

(i) x is called irreducible if whenever $x = ab$, then $a \in R^*$ or $b \in R^*$.

(ii) x is called prime if whenever $x|ab$, then $x|a$ or $x|b$.

Ex In \mathbb{Z} , prime numbers are irreducible and prime.

Ex $\Rightarrow R = \mathbb{Z}[x, y]/(x^2 - y^3)$

y is irreducible

But $y(y^2) = x^2$, so $y \nmid x^2$. But $y \nmid x$, so y is not prime.

Thm 3.4 Let R be an integral domain, $x \in R \setminus \{0\}$

- (i) x is prime $\Leftrightarrow (x)$ is a prime ideal
- (ii) x is irreducible $\Leftrightarrow (x)$ is maximal among proper principal ideals
- (iii) If x is prime then x is irreducible.
- (iv) If R is a PID, then x is prime $\Leftrightarrow x$ is irreducible.
- (v) Associates of primes are prime. Associates of irreducibles are irreducible.
- (vi) If x is irreducible and $a \mid x$, either $a \in R^*$ or $x \mid a$ (i.e. a is an associate).

Pf (i) Immediate

(ii) \Rightarrow Suppose $(x) \subset (y)$. Then $x = ay$ for some $a \in R$. x irreducible $\Rightarrow a \in R^*$ or $y \in R^*$.
If $a \in R^*$, then $(x) = (y)$. If $y \in R^*$, then $(y) = R$.

\Leftarrow Suppose $x = ab$ for some $a, b \in R$. ~~It follows that~~ $(x) \subset (a)$,
so $(x) = (a)$ (i.e. $b \in R^*$) or $(a) = R$ (i.e. $a \in R^*$).

(iii) Let x be prime, suppose $x = ab$. Then $x \mid ab$, so $x \mid a$ or $x \mid b$.

Then $a = xy$, so $x = (xy)b$. Then $x(1 - yb) = 0$, so $b \in R^*$.

(iv) Assume R is a PID, let $x \in R$ be irreducible. Then by (ii) (x) is a maximal ideal, hence prime.

(v) Follows from (i) & (ii). Since associates generate the same ideal.

(vi) Definition

Q: When are prime + irreducible the same?

Problem with $\mathbb{Z}[x]/(x^2-y^3)$: $x^2=y^3$

i.e. x^2 can be factored two different ways

Def 3.5 An integral domain is called a unique factorization domain if every element factors uniquely (upto units) as a product of irreducibles

Ex \mathbb{Z} is a UFO

$$6 = 2 \cdot 3 = (-2)(-3)$$

Observe: If R a UFO and x irreducible, x is prime.

~~top is irreducible~~

$x|ab \Rightarrow x|a$ or $x|b$ (factor into irreducibles)
so x is prime.

Thm 3.7 Every PID is a UFO.

Lemma 3.6 A PID is Noetherian, i.e. every chain of ideals

$$(a_1) \subset (a_2) \subset (a_3) \subset \dots$$

stabilizes (i.e. for some n , $j \geq n \Rightarrow (a_j) = (a_n)$.)

Pf Let $I = \bigcup_{i=1}^{\infty} (a_i)$. This is an ideal, so $I = (x)$.

For some n , $x \in (a_n)$, so $(x) \subset (a_n) \subset I = (x)$. Q

Pf of 3.7 Lemma If a is reducible, $a = pq$ for some irreducible p .

Pf (a) is contained in some maximal (prime) ideal (p) .

Let $x \in R$. Then $x = p_1 q_1$ for some irreducible p_1 .

$$x = p_1 p_2 q_2$$

$$= p_1 p_2$$

$$x = p_1 p_2 p_3 q_3$$

\vdots

(70)

Chain of ideals: $(q_1) \subset (q_2) \subset (q_3) \subset \dots$

Must terminate, so x can be factored as product of irreducibles.

Suppose $x = p_1 \dots p_r = q_1 \dots q_s$ for irreducibles p_i, q_j .

Since R a PID, (p_i) is maximal, so $R/(p_i)$ a field.

Then $q_1 \dots q_s \equiv x \equiv 0$ in $R/(p_1)$, so wlog $q_1 \equiv 0$, i.e. $q_1 \in (p_1)$, i.e.

q_1, p_1 are associates

Then since domain, cancel, $p_2 \dots p_r = q_2 \dots q_s$. Induct. \square

— x —

Division algorithm: Let $a, b \in R$. Then there exists $q, r \in R$ s.t. $a = qb + r$ and $r < b$.

Def 3.8 ~~Approximate~~ An integral domain R is called a Euclidean domain if there exists a function $\phi: R \setminus \{0\} \rightarrow \mathbb{N}$ such that

(i) If $a, b \in R$ are nonzero, then $\phi(a) \leq \phi(ab)$

(ii) If $a, b \in R$ are nonzero, then exist $q, r \in R$ s.t. $a = qb + r$ and either $r = 0$ or $\phi(r) < \phi(b)$

Ex \mathbb{Z} is a Euclidean domain with $\phi(x) = |x|$.

Ex Let $\mathbb{Z}[i] = \mathbb{Z}[x]/(x^2+1)$ (the ring of Gaussian integers)

Define $\phi(a+bi) = a^2 + b^2$.

$$\begin{aligned} \text{Ex } \frac{3+4i}{1+2i} &= \frac{(3+4i)(1-2i)}{\underset{\phi(1+2i)}{\uparrow} 5} = \frac{11}{5} - \frac{2}{5}i \\ &= 2 + \frac{1}{5} - \frac{2}{5}i \end{aligned}$$

$$\begin{aligned} (3+4i) &= 2(1+2i) + (\frac{1}{5} - \frac{2}{5}i)(1+2i) \\ &= 2(1+2i) + 1 \end{aligned}$$

More generally: Let $\alpha = a+bi$, $\beta = c+di$

$$\frac{\alpha}{\beta} = \frac{a+bi}{c+di} = \frac{(a+bi)(c-di)}{q(\beta)} = \frac{ac+bd}{q(\beta)} + \frac{(bc-ad)i}{q(\beta)}$$

With $ac+bd = q_1 q(\beta) + r_1$ with $|r_1| \leq \frac{1}{2}q(\beta)$ $(bc-ad)i = q_2 q(\beta) + r_2$ with $|r_2| \leq \frac{1}{2}q(\beta)$

Then $\frac{\alpha}{\beta} = \frac{q_1 q(\beta) + r_1}{q(\beta)} + \frac{(q_2 q(\beta) + r_2)i}{q(\beta)} = (q_1 + q_2 i) + \frac{r_1 + r_2 i}{q(\beta)}$

So $\alpha = (q_1 + q_2 i)\beta + \frac{(r_1 + r_2 i)\beta}{q(\beta)}$

Now $q\left(\frac{(r_1 + r_2 i)\beta}{q(\beta)}\right) = q\left(\frac{r_1 + r_2 i}{\beta}\right) \cdot \frac{q(r_1 + r_2 i)}{q(\beta)} = \frac{r_1^2 + r_2^2}{q(\beta)} \leq \frac{(\frac{1}{2}q(\beta))^2 + (\frac{1}{2}q(\beta))^2}{q(\beta)} = \frac{1}{2}q(\beta)$

Ex $\mathbb{A}[x]$ is Euclidean with $q(f) = \deg f$

Do Ex first:

Let $f = \sum_{i=0}^n a_i x^i$ $g = \sum_{i=0}^m b_i x^i$ assume $n \geq m$.

Induct on $\deg f - \deg g = n - m$

If $n=m$, $f = \underbrace{\frac{a_n}{b_m} g}_{\uparrow q} + \underbrace{\sum_{i=0}^{m-1} (a_i - \frac{a_n}{b_m} b_i) x^i}_{\uparrow r}$

If $n > m$: ~~$f = \frac{a_n}{b_m} g$~~ Let $q = \frac{a_n}{b_m} x^{n-m}$

Then $\deg(f - qg) < \deg f$.

If $\deg(f - qg) < \deg g$, done.

Else, $f - qg = q_0 g + \overset{\deg < \deg g}{\downarrow \text{int}} r$

so $f = (q + q_0)g + r$

Ex $f = x^4 + 7x$, $g = x^2 + 2x + 1$

$$f = x^2 g + r_1 \quad r_1 = (x^4 + 7x) - x^2(x^2 + 2x + 1) = -2x^3 - x^2 + 7x$$

$$r_1 = -2x g + r_2 \quad r_2 = (-2x^3 - x^2 + 7x) + 2x(x^2 + 2x + 1) = 3x^2 + 9x$$

$$r_2 = 3g + r_3 \quad r_3 = 3x^2 + 9x - 3(x^2 + 2x + 1) = 3x - 3$$

$$f = x^2 g + r_1 = x^2 g + (-2xg + r_2) = x^2 g - 2xg + 3g + r_3 \\ = (x^2 - 2x + 3)g + r_3$$

Th 3.9 Euclidean rings are PIDs.

Pf Let $I \subset R$. Choose $x \in I$ with $\varphi(x)$ minimal.

If $y \in I$, write $x = qy + r$ with $\varphi(r) < \varphi(y)$

$$\text{If } x = qy + r \text{ then } r = x - qy \in I \Rightarrow r = 0$$

So $x = qy$

Thus $I = (y)$. □

Euclidean domains \subset PIDs \subset UFDs \subset Integral domains

§4 Rings of quotients + localization

Ex What is \mathbb{Q} ? Is $\mathbb{Q} = \mathbb{Z} \times \mathbb{Z}$?

$$(a, b) \sim (c, d) \text{ iff } ad - bc = 0$$

Def 4.1 A nonempty subset $S \subset R$ is called multiplicative if it is ~~multiplicative~~ closed under multiplication, i.e. if $a, b \in S$, then $ab \in S$.

Ex If R is a ring, R^\times is multiplicative

Ex If R is an integral domain, R^\times is multiplicative.

Ex More generally, if $P \subset R$ is a prime ideal, $R \setminus P$ is multiplicative

(Why should S be multiplicative? If $\frac{1}{s}, \frac{1}{t}$ exist, so should $\frac{1}{st}$)

Thm 4.2 Let R be a commutative ring, and $S \subset R$ multiplicative. Define \sim on $R \times S$ by

$$(a, b) \sim (c, d) \text{ if } s(ad - bc) = 0 \text{ for some } s \in S.$$

\sim is an equivalence relation

pf Reflexive & symmetric ✓

Transitive: Suppose $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$

$$s(ad - bc) = 0$$

$$t(cf - de) = 0$$

for some $s, t \in S$

$$sad = sbc$$

$$tcf = bde$$

make sense

$$sad(tf) = sbctf \quad sbtcf = tde(sb)$$

$$sadtf - tde sb = 0$$

$$\underline{std}(af - be) = 0$$

$$\Rightarrow (a, b) \sim (e, f)$$

□

Note If R has no zero divisors and $0 \notin S$, then $(a,b) \sim (c,d) \Leftrightarrow ad-bc=0$

Typically write $\frac{a}{b}$ for elements of $R+S/\sim$. write $S^{-1}R$ for $R+S/\sim$.

observe: (i) $\frac{a}{b} = \frac{c}{d} \Leftrightarrow s(ad-bc)=0$ for some $s \in S$.

(ii) $\frac{ts}{ts} = \frac{t}{s}$ for all $t \in S$.

(iii) If $0 \in S$, then $S^{-1}R = \{0\}$

Thm 4.3 (i) $S^{-1}R$ is a commutative unital rds with operations

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \quad \text{and} \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

(ii) If R is an integral domain and $0 \notin S$, then $S^{-1}R$ is an integral domain.

(iii') If R is an integral domain and $S=R^*$, then $S^{-1}R$ is a field.
 $\text{frac } R$ (or sometimes $\text{quot } R$), the field of fractions of R , is a field.

pf (i) Well-defined: Suppose $\frac{a}{b} = \frac{A}{B}$ and $\frac{c}{d} = \frac{C}{D}$.

$s(ab-bA)=0$ and $t(cd-dC)=0$ for some $s, t \in S$.

we want: $\frac{ad+bc}{bd} = \frac{Ad+Bc}{BD}$, so $((ad+bc)BD - (Ad+Bc)bd) \neq 0$ for some $y \in S$

$$tdDs(ab-bA) + tBb(cd-dC)=0$$

$$st((ad+bc)BD - (Ad+Bc)bd)=0 \quad \checkmark$$

we want: $\frac{ac}{bd} = \frac{Ac}{Bd}$ so $(acBD - Acbd) \neq 0$ for some $y \in S$.

$$(tcd)s(ab-bA) + (sbA)(t)(cd-dC)=0$$

$$st(acBD - bAdC)=0 \quad \checkmark$$

(ii) Note $\frac{0}{s} \in S^{-1}R$ is the additive identity for any $s \in S$. Fix one such $s \in S$.

$$\text{since } \frac{0}{s} = \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}, \text{ so } 0 \cdot bd - sac = 0 \\ sac = 0$$

$$\Rightarrow a=0 \text{ or } c=0$$

$$\Rightarrow \frac{a}{b} = \frac{0}{s} \text{ or } \frac{c}{d} = \frac{0}{s}$$

(iii) Let $\frac{a}{b} \in S^{-1}R$. Then $\frac{b}{a} \in S^{-1}R$, and $\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = \frac{ab}{ab}$

(note $\frac{s}{s} \in S^{-1}R$ is m.u. identity for any $s \in S$).

□

Ex $\mathbb{Q} = \text{frac } \mathbb{Z}$

Ex $\mathbb{C}(x) = \text{frac } \mathbb{C}[x] = \left\{ \frac{p(x)}{q(x)} \mid p, q \in \mathbb{C}[x], q \neq 0 \right\} / \sim$

Ex Let $S = \{1, x, x^2, \dots\} \subset \mathbb{C}[x]$

$$S^{-1}\mathbb{C}[x] = \mathbb{C}[x, x^{-1}]$$

Thm 4.4 Let R be commutative, $S \subset R$ multiplicative.

(i) the map $Q: R \longrightarrow S^{-1}R$

is a well defined homomorphism

$$r \longmapsto \frac{rs}{s} \text{ for any } s \in S$$

and if $s \in S$, $Q(s) \in (S^{-1}R)^*$

(ii) If $0 \notin S$ and S contains no zero divisors, Q is injective.

In particular, every integral domain may be embedded in its field of fractions

(iii) If R is unital and $S \subset R^*$, then Q is an isomorphism.

pf (i) well defined: need $\frac{rs}{s} = \frac{r' b}{t}$ for any $s, t \in S$

$$\bullet \quad rs - r's = 0 \quad \checkmark$$

homomorphism: Let $a, b \in R$. $\varphi(a) = \frac{as}{s}$ $\varphi(b) = \frac{bs}{s}$

$$\varphi(ab) = \frac{ab s^2}{s^2} = \frac{a}{s} \cdot \frac{b}{s} = \varphi(a) \varphi(b)$$

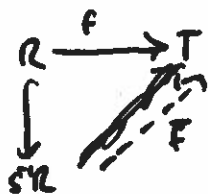
$$\varphi(a+b) = \frac{(a+b)s^2}{s^2} = \frac{a}{s} + \frac{b}{s} = \varphi(a) + \varphi(b)$$

If $s \in S$, $\varphi(s) = \frac{s \cdot s}{s} = \frac{s^2}{s}$ has inverse $\frac{s}{s^2}$

(ii) suppose $\varphi(a) = \frac{as}{s} = 0$. Then $as = 0$, so $a s = 0 \Rightarrow a = 0$.
Thus φ is injective.

(iii) Suppose $s \in R^* \cap S$ and $\frac{r}{s} \in S^{-1}R$. Then $\varphi(\frac{r}{s}) = \frac{rs^2}{s^3} = \frac{r}{s}$

Thm 4.5 Let R be commutative, $S \subset R$ multiplicative. Let T be a commutative unital rds.
Let $f: R \rightarrow T$ be a homomorphism with $f(s) \in T^*$. Then there exists a
unique homomorphism $\bar{f}: S^{-1}R \rightarrow T$ s.t. diagram commutes



pf Define $\bar{f}(\frac{r}{s}) = f(r)f(s)^{-1}$

well defined: suppose $\frac{r}{s} = \frac{r_0}{s_0}$, so $t(rs_0 - sr_0) = 0$ for some $t \in S$
 $f(t)(f(r)f(s_0) - f(s)f(r_0)) = 0$
 $f(r)f(s_0) - f(s)f(r_0) = 0 \cdot f(t)^{-1} = 0$

$$f(r)f(s_0) = f(s)f(r_0)$$

$$f(r)f(s)^{-1} = f(r_0)f(s_0)^{-1}$$

$$\bar{f}(\frac{r}{s}) = \bar{f}(\frac{r_0}{s_0})$$

homomorphism: Let $\frac{r}{s}, \frac{r_0}{s_0} \in S^{-1}R$

$$\begin{aligned} \bar{f}\left(\frac{r}{s}\right) &= f(r)f(s)^{-1} = f(r_0)f(s)^{-1}f(s_0)f(s_0)^{-1} = \bar{f}\left(\frac{r_0}{s_0}\right)\bar{f}\left(\frac{s_0}{s}\right) \\ \bar{f}\left(\frac{r}{s} + \frac{r_0}{s_0}\right) &= \bar{f}\left(\frac{rs_0 + r_0s}{ss_0}\right) = f(rs_0 + r_0s)f(ss_0)^{-1} \\ &= (f(r)f(s_0) + f(r_0)f(s))f(s)^{-1}f(s_0)^{-1} \\ &= f(r)f(s)^{-1} + f(r_0)f(s)^{-1}f(s_0)^{-1} \\ &= \bar{f}\left(\frac{r}{s}\right) + \bar{f}\left(\frac{r_0}{s_0}\right) \end{aligned}$$

Thm 4.7 Let R be commutative, SCR multiplicative.

If $I \subset R$ is an ideal, then $S^{-1}I = \{\frac{a}{s} \mid a \in I, s \in S\}$ is an ideal of $S^{-1}R$.

pf Let $\frac{a}{s}, \frac{b}{t} \in S^{-1}I$ (so $a, b \in I, s, t \in S$)

$$\text{Then } \frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st} \in S^{-1}I \text{ since } at + bs \in I$$

$$\text{If } \frac{x}{u} \in S^{-1}R, \quad \frac{x}{u} \cdot \frac{a}{s} = \frac{xa}{us} \in S^{-1}I \text{ since } xa \in I. \quad \square$$

Thm 4.8 Let R be commutative, unit ring, SCR multiplicative, $I \subset R$ an ideal

Then $S^{-1}I = S^{-1}R$ iff $S \cap I \neq \emptyset$

pf Idea: ideal is the whole ring if it has a unit.

\Leftarrow If $s \in S \cap I$, then $1 = \frac{s}{s} \in S^{-1}I$, so $S^{-1}I = S^{-1}R$

\Rightarrow ~~Let $s \in S$, so $\frac{s}{s}$ is identity in $S^{-1}R$.~~

Let $s \in S$, so $\frac{s}{s}$ is identity in $S^{-1}R$.

Then $\frac{s}{s} \in S^{-1}I$, so $\frac{s}{s} = \frac{a}{t}$ for some $a \in I, t \in S$

$$t_0(st - as) = 0 \text{ for some } t_0 \in S$$

$$\text{Then } \underbrace{as}_{\in I} \underbrace{t_0}_{\in S} = \underbrace{t_0}_{\in S} \underbrace{st}_{\in I} \in I \cap S. \quad \square$$

Lemma 4.9 Let R be commutative, unital, SCR multiplicative.

(i) Every ideal in $\tilde{S}'R$ is of form $\tilde{S}'I$ for some ideal $I \subset R$.

(ii) If $P \subset R$ is a prime ideal, ~~$S \not\subset P$ and $S \cap P = \emptyset$~~ , then $\tilde{S}'P$ is a prime ideal.
 $S \cap P = \emptyset$

Pr (i) Let $J \subset \tilde{S}'R$ be an ideal. Fix some $e \in S$, so $\frac{e}{e}$ is identity in $\tilde{S}'R$.

$$\text{Set } I = J \cap R = \{r \in R \mid \frac{re}{e} \in J\}$$

(1) I is an ideal: Let $r, s \in I$

$$\text{Then } \frac{re}{e}, \frac{se}{e} \in J, \text{ so } \frac{re}{e} + \frac{se}{e} = \frac{re^2 + se^2}{e^2} = \frac{(r+s)e^2}{e^2} = \frac{(r+s)e}{e} \in J, \\ \text{so } r+s \in I.$$

$$\text{If } a \in R, \text{ then } \frac{ae}{e} \cdot \frac{re}{e} = \frac{are^2}{e^2} = \frac{are}{e} \in J, \text{ so } ar \in I.$$

(2) $J = \tilde{S}'I$:

$$\text{If } \frac{a}{s} \in J, \text{ then } \frac{a}{s} \cdot \frac{se}{e} = \frac{ae}{e} \in J, \text{ so } a \in I \text{ and } \frac{a}{s} \in \tilde{S}'I.$$

$$\text{If } \frac{a}{s} \in \tilde{S}'I, a \in J, \text{ so } \frac{ae}{e} \in J, \text{ then } \frac{ae}{e} \cdot \frac{s}{s} = \frac{a}{s} \cdot \frac{s}{s} = \frac{a}{s} \in J$$

(ii) Let $\frac{a}{s}, \frac{b}{t} \in \tilde{S}'R \setminus \tilde{S}'P$, ~~$a, b \in R$~~ , so $a, b \in R \setminus P$.

$$\text{Need to show } \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st} \notin \tilde{S}'P.$$

Suppose $\frac{ab}{st} \in \tilde{S}'P$: we claim $ab \in P$.

$$\frac{ab}{st} = \frac{c}{u} \text{ for some } c \in P, u \in S.$$

$$\text{Then } v(abu - cst) = 0 \text{ for some } v \in S$$

$$\underbrace{ab}_{\notin P} \underbrace{uv}_{\in P} = \underbrace{cst}_{\in P} v \quad \text{requires } S \cap P = \emptyset$$

thus $ab \in P$. This contradicts P being prime. \square

Thm 4.10 Let R be commutative, unital, and let $S \subset R$ be multiplicative.
 There is a one-to-one correspondence between prime ideals of R
 disjoint from S , and prime ideals of $S^{-1}R$ given by

$$P \longrightarrow S^{-1}P$$

PF Our proof of 4.9 (i) shows this is injective.
 Let Q be a prime ideal of $S^{-1}R$. Then $Q = S^{-1}I$ for some ideal $I \subset R$.

claim I is prime.

Let $a, b \in R \setminus I$.

Then $\frac{a}{s}, \frac{b}{s} \in S^{-1}R \setminus Q$

so $\frac{a}{s} \cdot \frac{b}{s} = \frac{ab}{s^2} = \frac{ab}{s} \in S^{-1}R \setminus Q$ since Q prime
 $\frac{ab}{s} \in S^{-1}R \setminus S^{-1}I$
 then $ab \notin I$.

claim $I \cap S = \emptyset$
 If $x \in I \cap S$, $\frac{x}{1} \in S^{-1}I = Q \Rightarrow Q = S^{-1}R$ \downarrow

Def Let R be a commutative, unital ring, $P \subset R$ a prime ideal.
 The localization of R at P , denoted R_P , is the ring $S^{-1}R$ for the set $S = R \setminus P$.
 If $I \subset R$ is an ideal, $S^{-1}I$ is denoted I_P .

Idea from algebraic geometry! R represents regular functions from variety $V \rightarrow k$
 To restrict attention locally, need functions that don't vanish \Rightarrow can be inverted.

Thm 4.11 Let R be commutative, unital, $P \subset R$ prime.

(i) There is a one-to-one correspondence between prime ideals of R contained in P
 and prime ideals of R_P

(ii) In R_P , P_P is the unique maximal ideal.

Pf (c) follows from 4.10.

(ii) (i) implies P_p is maximal.

Suppose $M \subset R_p$ is some other maximal ideal. By (i), $M = Q_p$

for some prime ideal $Q \subset P$. But $Q \subset P \Rightarrow Q_p \subset P_p$

and Q_p maximal $\Rightarrow Q_p = P_p$.

Def 4.12 A commutative, unital ring is called a local ring if it has a unique maximal ideal. If this maximal ideal is \mathfrak{m} , then write (R, \mathfrak{m}) is local

Idea: If you localize, you get a local ring.

Ex $\mathbb{Z}/p^n\mathbb{Z}$ is local for primes p .

Maximal ideal is (p)

Thm 4.13 Let R be a commutative unital ring. TFAE

(i) (R, \mathfrak{m}) is local

(ii) $R \setminus R^*$ is a max ideal

(iii) $R \setminus R^*$ is an ideal

Pf (i) \Rightarrow (ii) Take $\mathfrak{m} \subset R \setminus R^*$
If $x \in R \setminus R^*$, $x \notin R$, so $x \in \mathfrak{m}$
Thus $R \setminus R^* \subset \mathfrak{m}$, so $R \setminus R^* = \mathfrak{m}$.

(ii) \Rightarrow (iii) \checkmark

(iii) \Rightarrow (i) Any proper ideal must be contained in $R \setminus R^*$ \square

Ex $\mathbb{C}[[x]]$ is local

Ex $k[x]/(x^n)$ is local

Ch. IV Modules

Two ways to think about modules

- 1) Like vector spaces, but with scalars from a ring
- 2) Like ideals, but live outside of ring

Def 1.1 Let R be a ring. A (left) R -module M is an additive abelian group together with a multiplication operation $R \times M \rightarrow M$ satisfying
for all $r, s \in R$ $a, b \in M$

- 1) $r \cdot (a+b) = r \cdot a + r \cdot b$
- 2) $(r+s) \cdot a = r \cdot a + s \cdot a$
- 3) $r(s \cdot a) = (rs) \cdot a$
- 4) If R is unital, $1 \cdot a = a$

Ex A vector space is a module over a field

Ex An abelian group is a \mathbb{Z} -module

Ex An ideal is a module.

Ex Let $\phi: R \rightarrow S$ be a ring homomorphism. If M is an S -module, it is also an R -module with multiplication $r \cdot m = \phi(r) \cdot m$ for all $r \in R, m \in M$.

Def 1.2 Let M, N be R -modules. An R -module homomorphism is a function $f: M \rightarrow N$

- 1) $f(a+b) = f(a) + f(b)$ for all $a, b \in M$
- 2) $r \cdot f(a) = f(ra)$ for all $r \in R, a \in M$.

Ex Let R be a ring. $R[x]$ is an R -module.

The map $\phi: R[x] \rightarrow R[x]$ is a module homomorphism but not a ring homomorphism
$$f \mapsto xf$$

Def 1.3 Let M be an R -module. A subgroup $N \subset M$ is called a submodule if $rn \in N$ for all $r \in R, n \in N$.

Ex A ring is a module over itself. ~~Also submodule over itself.~~ Its submodules are its ideals.

Ex x^2R is an R -submodule of $R[x]$

Def 1.4 Let M be an R -module. Let $X \subset M$ be a subset.

The submodule generated by X is the intersection of all submodules containing X .

If X is finite, the module it generates is called finitely generated.

Def If $\{B_i\}_{i \in I}$ is a family of submodules, the submodule generated by their union is called the sum of the B_i . If I is finite, it is denoted $B_1 + \dots + B_n$.

Ex $xR + x^2R \subset R[x]$

Thm 1.5 Let R be ^{unital} R -module.

(i) If $a \in R$, the submodule generated by $\{a\}$ is $Ra = \{ra \mid r \in R\}$

(ii) If $X \subset M$ is a set, the submodule generated by X is

$$RX = \left\{ \sum_{i=1}^s r_i a_i \mid s \in \mathbb{N}, r_i \in R, a_i \in X \right\}$$

(iii) If ~~the set~~ $\{B_i\}_{i \in I}$ is a family of submodules, the sum

$$\text{is } \left\{ \sum_{i=1}^s b_{i_k} \mid s \in \mathbb{N}, b_{i_k} \in B_{i_k} \right\}$$

(finite sums of elements of B_i 's)

Thm 1.6 Let M be an R -module and $N \subseteq M$ a submodule.
 Then M/N is an R -module with multiplication

$$r \cdot (a+N) = ra+N \quad \text{for all } r \in R.$$

pf M/N is an abelian group.

check multiplication well defined: Suppose $a+N = b+N$, so $a-b = n \in N$.

$$\text{Then } ra+N = r(b+n)+N = rb+N.$$

Straightforward to check submodule properties.

Remark Straightforward to verify that isomorphism theorems hold for modules.

Thm 1.11 Let R be a ring, $\{M_i\}_{i \in I}$ a family of R -modules

(i) $\prod_{i \in I} M_i$ is an R -module (direct product)

(ii) $\sum_{i \in I} M_i$ is a submodule of $\prod_{i \in I} M_i$ (direct sum)

If I is finite then consider direct sum $M_1 \oplus M_2 \oplus \dots \oplus M_n$.

Ex Let R be a ring. $R[x] \oplus R[x]$ is an R -module.

Def A sequence of R -module homomorphisms $A \xrightarrow{f} B \xrightarrow{g} C$ is called exact (at B) if $\text{Im } f = \text{Ker } g$. A (possibly infinite) sequence

$\dots \xrightarrow{f_{i-1}} A_{i-1} \xrightarrow{f_i} A_i \xrightarrow{f_{i+1}} A_{i+1} \xrightarrow{f_{i+2}} \dots$ is called exact if

every subsequence $A_{i-1} \xrightarrow{f_i} A_i \xrightarrow{f_{i+1}} A_{i+1}$ is exact.

Ex If M, N are R -modules

$0 \rightarrow M \rightarrow M \oplus N \rightarrow N \rightarrow 0$ is exact.

Ex If $N \subset M$ is a submod

$$0 \rightarrow N \rightarrow M \rightarrow M/N \rightarrow 0 \text{ is exact.}$$

Ex Let $f: M \rightarrow N$ be a homomorphism

$$0 \rightarrow \text{Ker } f \rightarrow M \xrightarrow{f} N \rightarrow \text{Coker } f \rightarrow 0 \text{ is exact.}$$

\parallel
 $N/\text{Im } f$

Lemma 1.17 (Short Five Lemma) Let

$$\begin{array}{ccccccc} 0 & \rightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C \rightarrow 0 \\ & & \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma \\ 0 & \rightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' \rightarrow 0 \end{array}$$

be a commutative diagram

Suppose the rows are both exact.

- (i) If α and γ are both injective, so is β .
- (ii) If α and γ are both surjective, so is β .
- (iii) If α and γ are both isomorphisms, so is β .

Pf "Diagram chasing"

(i) Let $x \in \text{Ker } \beta$

then $\gamma g(x) = g' \beta(x) = g'(0) = 0$, i.e. $g(x) \in \text{Ker } \gamma$

γ is injective, so $g(x) = 0$, i.e. $x \in \text{Ker } g = \text{Im } f$

write $x = f(y)$ for some $y \in A$.

then $f' \alpha(y) = \beta f(y) = \beta(x) = 0$, so $\alpha(y) \in \text{Ker } f' = \{0\}$

So $y \in \text{Ker } \alpha$, α injective $\Rightarrow y = 0$.

then $x = f(y) = f(0) = 0$. Thus β is injective.

(ii) Let $x \in B$.

Since γ is surjective, there exists $y \in C$ with $\gamma(y) = g'(x)$.

Since g is surjective, there exists $z \in B$ with $g(z) = y$

$$\text{so } \gamma g(z) = g'(x)$$

$$\gamma''(y) = g'(x)$$

Then $g'(x - \beta(z)) = 0$, so $x - \beta(z) \in \text{Ker } g' = \text{Im } f'$

Let $w \in A'$ with $f'(w) = x - \beta(z)$

α is surjective, so there exists $v \in A$ with $\alpha(v) = w$.

$$x - \beta(z) = f'(w) = f' \alpha(v) = \beta f(v)$$

$$x - \beta(z) = \beta f(v)$$

$$x = \beta(z + f(v))$$

□

Def If case (iii) occurs, we say the exact sequences are isomorphic. Sequence of R-modules

Thm 1.18 Let $0 \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow 0$ be exact. TFAE

(i) The sequence is right split: There exists $h: C \rightarrow B$ with $gh = \text{id}$

(2) The sequence is left split: There exists $k: B \rightarrow A$ with $kf = \text{id}$

(3) The sequence is isomorphic to the sequence $0 \rightarrow A \rightarrow A \oplus C \rightarrow C \rightarrow 0$

Pf (1) \Rightarrow (3)

$$\begin{array}{ccccccc}
 0 & \rightarrow & A & \xrightarrow{i} & A \oplus C & \xrightarrow{\pi} & C \rightarrow 0 \\
 & & \downarrow \text{id} & & \downarrow f+h & & \downarrow \text{id} \\
 0 & \rightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C \rightarrow 0
 \end{array}$$

Let $a \in A$: $(f+h)(i(a)) = (f+h)(a, 0) = f(a) + h(0) = f(a)$

$f(\text{id}(a)) = f(a)$ ✓

Let $(a, c) \in A \oplus C$

$$g((fk)(a, c)) = g(f(a) + k(c)) = g(f(a)) + g(k(c)) = 0 + c = c$$

$$id(\pi(a, c)) = id(c) = c \quad \checkmark$$

So the diagram commutes. Five lemma $\Rightarrow f+k$ is an isomorphism.

(ii) \Rightarrow (iii)

$$\begin{array}{ccccccc} 0 & \rightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C \rightarrow 0 \\ & & \downarrow id & & \downarrow (k, g) & & \downarrow id \\ 0 & \rightarrow & A & \xrightarrow{i} & A \oplus C & \xrightarrow{\pi} & C \rightarrow 0 \end{array}$$

Let $a \in A$: $(k, g)(f(a)) = (kf(a), g(f(a))) = (a, 0)$

$$i(id(a)) = i(a) = (a, 0) \quad \checkmark$$

Let $b \in B$: $\pi((k, g)(b)) = \pi(k(b), g(b)) = g(b)$

$$id(g(b)) = g(b) \quad \checkmark$$

So the diagram commutes. Five lemma $\Rightarrow (k, g)$ is an isomorphism.

(iii) \Rightarrow (i, ii)

$$\begin{array}{ccccccc} 0 & \rightarrow & A & \xrightarrow{i_1} & A \oplus C & \xrightarrow{\pi_2} & C \rightarrow 0 \\ & & \downarrow & \nearrow \pi_1 & \downarrow \varphi & \nearrow i_2 & \downarrow \\ 0 & \rightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C \rightarrow 0 \end{array}$$

Let $h = \varphi i_2$

$$k = \pi_1 \varphi^{-1}$$

19

§2 Free modules

Def Let M be an R -module, $X \subset M$ a subset. X is called linearly independent if whenever $x_1, \dots, x_n \in X$, $r_1, \dots, r_n \in R$,

$$r_1 x_1 + \dots + r_n x_n = 0 \Rightarrow r_1 = \dots = r_n = 0.$$

A linearly independent generating set is called a basis

Thm 2.1 Let R be unital, F an R -module. TFAE

(1) F has a non-empty basis X

$$(2) F \cong \sum_{x \in X} xR \cong \sum_{x \in X} R$$

(3) There is a non-empty set X and a function $i: X \rightarrow F$ such that given any R -module M and a function $f: X \rightarrow M$, there exists a unique $\tilde{f}: F \rightarrow M$

$$\begin{array}{ccc} X & \xrightarrow{i} & F \\ & \searrow f & \downarrow \tilde{f} \\ & & M \end{array} \quad \text{commutes}$$

Pf (1) \Rightarrow (3) Let X be a basis, $i: X \rightarrow F$ the inclusion map.

Since X is linearly independent, every $u \in F$ can be written uniquely

$$u = r_1 x_1 + \dots + r_n x_n \quad \text{for some } r_i \in R, x_i \in X$$

$$\text{Define } \tilde{f}: F \rightarrow M \quad \text{by} \quad \tilde{f}(r_1 x_1 + \dots + r_n x_n) = r_1 f(x_1) + \dots + r_n f(x_n)$$

Straightforward to verify this is a homomorphism with $\tilde{f} \circ i = f$

(3) \Rightarrow (2)

$$\begin{array}{ccc} X & \xrightarrow{i} & F \\ & \searrow f & \downarrow \tilde{f} \\ & & \sum_{x \in X} xR \end{array}$$

$$\text{Note } \tilde{f} \text{ has inverse map } \sum_{x \in X} xR \rightarrow F$$

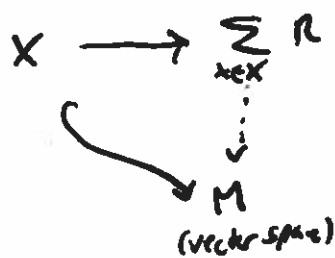
$$x \mapsto i(x)$$

(2) \Rightarrow (1) If X linearly dependent, the vectors don't span. (Thm 1.15)
 Clearly X generates F . □

Ex $R[x]$ is a free R -module with basis $\{1, x, x^2, x^3, \dots\}$

Corollary Let R be unital, M an R -module. Then M is the homomorphic image of a free module.

PF Let X be a generating set for M .



Thm 2.4 Every module over a field (or division ring) is free, □

Lemma 2.3 Let k be a field, M a k -module (vector space). A maximal linearly independent set is a basis of M .

PF Let X be a maximal linearly independent set, let $N = \sum_{x \in X} kx$.

Then X is a basis of M .

Suppose $a \in M \setminus N$. Claim $X \cup \{a\}$ is linearly independent.

If $r_1 x_1 + \dots + r_n x_n + r_{n+1} a = 0$ for some $r_i \in k$, not all zero.

note $r_{n+1} \neq 0$ (since X linearly independent),

so $a = -\frac{1}{r_{n+1}} (r_1 x_1 + \dots + r_n x_n) \in N$ ↓

Claim contradicts maximality, so $M = N$.

PF of Thm 2.4 Let $S = \{X \subset M \mid X \text{ is linearly independent}\}$.

so $\{C_i \mid i \in I\}$ is a chain in S , $C = \bigcup_{i \in I} C_i$ is lin indep, so $C \in S$.

Zorn \Rightarrow S has a maximal element, which is a basis by Lemma 2.3.

Thm 2.5 Every spanning set of a vector space contains a basis.

Pf Apply Zorn to linearly independent subsets of the spanning set.

Recall: Free abelian groups (i.e. free \mathbb{Z} -modules) have a well-defined rank

Def 2.8 Let R be unital. If for every free module F , two bases of F have the same cardinality, we say R has the invariant basis number (IBN) property or the invariant dimension property. The rank (dimension) of a free module (vector space) is the cardinality of any basis.

Ex \mathbb{Z} has IBN property.

Thm 2.7 Fields have the IBN property; i.e., if k is a field, V a k -vector space, and X, Y are bases of V , then $|X| = |Y|$.

Pf If X, Y both finite: row reduction + count pivots
Now, we suppose X is infinite.

Claim 1 Y is infinite.

Pf If not, $Y = \{y_1, \dots, y_n\}$

$$\text{write } y_1 = a_{11}x_1 + \dots + a_{1n}x_n$$

$$\vdots$$

$$y_n = a_{n1}x_1 + \dots + a_{nn}x_n$$

$$\Rightarrow \{x_1, \dots, x_n\} \text{ spans } V$$

$$\Rightarrow X \text{ linearly dependent. } \downarrow$$

Now we may assume Y is infinite as well: write $Y = \{y_i\}_{i \in I}$.

$$\text{write each } y_i = \sum_{j \in E_i} a_{ij}x_j \quad \text{for some finite } E_i \subset X, \quad x_j \in E_i$$

$$\text{Then } |\bigcup_{i \in I} E_i| = |I| = |Y| \quad \text{and } \bigcup_{i \in I} E_i \text{ spans } V.$$

$$\text{If } |X| > |Y|, \text{ then exists } x \in X \setminus \bigcup_{i \in I} E_i$$

$$\text{Since } \bigcup_{i \in I} E_i \text{ spans, } x = b_1x_1 + \dots + b_nx_n \text{ for some } x_i \in X$$

$$\Rightarrow X \text{ linearly dependent}$$

$$\text{So } |X| \leq |Y|.$$

$$(\text{Similarly, } |Y| \leq |X|)$$

(90)

□

Prop 2.9 If R has IBN property and F, F' free R -mod's, then $E \cong F$ iff E and F have the same rank.

Lemma 2.10 Let R be unital, $I \subset R$ ^{proper} ideal. Let F be a free module with basis X , and $\pi: F \rightarrow F/IF$ the quotient map. Then F/IF is a free R/I -module with basis $\pi(x)$. Moreover, $|\pi(x)| = |x|$.

Pf Claim 1 $\pi(x)$ generates F/IF .

Let $u + IF \in F/IF$ for some $u \in F$.

Then $u = \sum_{j=1}^n r_j x_j$ for some $r_j \in R$.

$$\begin{aligned} \text{So } u + IF &= \left(\sum_{j=1}^n r_j x_j \right) + IF = \sum_{j=1}^n (r_j x_j + IF) = \sum_{j=1}^n (r_j + IF)(x_j + IF) \\ &= \sum_{j=1}^n (r_j + IF) \pi(x_j). \end{aligned}$$

Claim 2 $\pi(x)$ is linearly independent.

Suppose $\sum_{j=1}^n (r_j + I) \pi(x_j) = 0$ for some $r_j + I \in R/I$, $\pi(x_j) \in \pi(X)$ distinct.

$$\sum_{j=1}^n (r_j + I)(x_j + IF)$$

$$\left(\sum_{j=1}^n r_j x_j \right) + IF \Rightarrow \sum_{j=1}^n r_j x_j \in IF$$

$$\text{So } \sum_{j=1}^n r_j x_j = \sum_{k=1}^m s_k u_k \text{ for some } s_k \in I, u_k \in F.$$

$$= \sum_{i=1}^p \tilde{s}_i \tilde{x}_i \text{ for some } \tilde{s}_i \in I, \tilde{x}_i \in X \text{ s.t. } X \text{ a basis of } F.$$

After reindexing, since X linearly independent we must have $r_j = \tilde{s}_j$, $x_j = \tilde{x}_j$,
 So $r_j + I = I$ for all j .

Claim 3 π is injective

Suppose $\pi(x_1) = \pi(x_2)$ for $x_1, x_2 \in X$.

Then $(1+I)\pi(x_1) - (1+I)\pi(x_2) = 0$

$$\overset{11}{x_1 + x_2 + IF} \quad \overset{11}{\tilde{s}_i \in I}$$

So $x_1 - x_2 = \sum \tilde{s}_i \tilde{x}_i$ as above, implying $1 \in I$ or $x_1 - x_2 = 0$ \square

Prop 2.11 Let $f: R \rightarrow S$ be a nonzero surjection of unital rings.
If S has IBN property, then so does R .

Pf Let $I = \ker f$, so $S \cong R/I$.

Let F be a free R -module, with two bases X and Y .

Then F/IF is a free S -module with bases $\pi(X)$ and $\pi(Y)$, and $|X| = |\pi(X)|$
 $|Y| = |\pi(Y)|$

S has IBN $\Rightarrow |\pi(X)| = |\pi(Y)|$, so $|X| = |Y|$ \square

Cor 2.12 Let R be a commutative unital ring. Then R has IBN property

Pf. Let $m \in R$ be a nonunit idel. Then $\pi: R \rightarrow R/m$

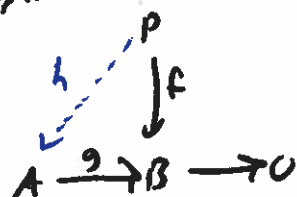
is a nonzero surjection, and R/m is a field, thus has IBN. \square

§3 Projective and Injective modules

Motivations

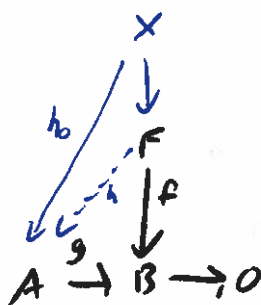
- 1) Projective modules are almost as nice as free modules
 - (i) Direct summands of free modules
 - (ii) Locally free
- 2) Algebraic ~~over~~ analogue of vector bundles - locally trivial
(Ex: Infinitely long Möbius strip)

Def 3.1 An R -module P is called projective if for any surjection $g: A \rightarrow B$ and homomorphism $f: P \rightarrow B$ there exists $h: P \rightarrow A$ s.t. $f = gh$



Thm 3.2 Free modules are projective.

PF Let F be a free module, and suppose



Let X be a basis for F . For each $x \in X$, choose $y_x \in A$ with $g(y_x) = f(x)$

Define $h_0: X \rightarrow A$ by $h_0(x) = y_x$.

Apply universal property of F .

□

Thm 3.4 Let P be an R -module. TFAE

- (i) P is projective
- (ii) Every short exact sequence $0 \rightarrow A \rightarrow B \rightarrow P \rightarrow 0$ splits
(so $B \cong A \oplus P$)
- (iii) There is a free module F and a (projective) module K
such that $F = K \oplus P$.

PF (i) \Rightarrow (ii)

$$0 \rightarrow A \rightarrow B \rightarrow P \rightarrow 0$$

\swarrow (dashed arrow from B to P)
 $\downarrow P$

(ii) \Rightarrow (iii) There is free module F

$$0 \rightarrow K \rightarrow F \rightarrow P \rightarrow 0$$

Let $K = \text{Kernel of this map.}$

Then $F \cong K \oplus P$

(iii) \Rightarrow (i) Suppose $F \cong K \oplus P$

F projective!

$$\begin{array}{ccc}
 & F \cong K \oplus P & \\
 & \pi \downarrow \uparrow i & \\
 A & \rightarrow B \rightarrow 0 &
 \end{array}$$

\swarrow (dashed arrow from $F \cong K \oplus P$ to A)
 $\downarrow P$

□

Ex \mathbb{Z}_2 and \mathbb{Z}_3 are \mathbb{Z}_6 modules

$\mathbb{Z}_6 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3$, \mathbb{Z}_6 is free \mathbb{Z}_6 -module $\Rightarrow \mathbb{Z}_2, \mathbb{Z}_3$ projective \mathbb{Z}_6 -modules.

Prop 3.5 A direct sum of R -modules $\sum_{i \in I} P_i$ is projective if and only if each P_i is projective

PF \Rightarrow Suppose $\sum_{i \in I} P_i$ is projective

$$\begin{array}{ccc}
 & \sum P_i & \\
 & \pi \downarrow \uparrow i & \\
 A & \rightarrow B \rightarrow 0 &
 \end{array}$$

\swarrow (dashed arrow from $\sum P_i$ to A)
 $\downarrow P_i$

Thus P_i is projective

L Suppose P_i each projective

$$\begin{array}{ccc} & P_i & \\ & \downarrow & \\ & \Sigma P_i & \\ \swarrow & \downarrow & \\ A & \rightarrow B & \rightarrow 0 \end{array}$$

Since we have maps $P_i \rightarrow A$ for all $i \in I$, we get a map $\Sigma P_i \rightarrow A$

□

Def An R -module J is called injective if whenever (top row exact)

$$\begin{array}{ccccc} 0 & \rightarrow & A & \xrightarrow{f} & B \\ & & \downarrow f & & \downarrow h \\ & & J & \xleftarrow{g} & J \end{array} \quad \text{there exists } h: B \rightarrow J \text{ s.t. } hg = f.$$

Prop 3.7 A direct product of R -modules $\prod_{i \in I} J_i$ is injective if and only if each J_i is injective.

Pf Reverse arrows in proof of Prop 3.5

Prop 3.12 Every R -module can be embedded in an injective R -module
(Takes a bit of work to get here!)

Lemma 3.8 Let R be unital, J an R -module. J is injective iff for every (left) ideal $I \subset R$, every R -module homomorphism $I \rightarrow J$ extends to a homomorphism $R \rightarrow J$.

Pf \Rightarrow Suppose J is injective. Let $I \subset R$ be an ideal

$$\begin{array}{ccc} 0 & \rightarrow & I & \rightarrow & R \\ & & \downarrow & & \swarrow \\ & & J & & J \end{array}$$

\Leftarrow Suppose we are given $0 \rightarrow A \xrightarrow{g} B$

$$\downarrow f$$

J

Let $S = \{h: C \rightarrow J \mid \text{Im } g \subset C \subset B, h_g = f\}$

S is nonempty, since $A \cong \text{Im } g$, so $fg': \text{Im } g \rightarrow J$

S is partially ordered by extension/restriction

Let $h: H \rightarrow J$ be a maximal element (Zorn!)

Claim $H = B$ (If true, then J is injective!)

Suppose $H \subsetneq B$. Let $b \in B \setminus H$.

Let $I = \{r \in R \mid rb \in H\}$ a (left) ideal of R .

Then $\phi: I \rightarrow J$
 $r \mapsto h(rb)$

Observe: if $a \in R$, $\phi(ar) = h(arb) = ah(rb) = a\phi(r)$

so ϕ is an R -module homomorphism

By assumption, ϕ extends to $\kappa: R \rightarrow J$ with $\kappa(r) = h(rb)$ for all $r \in I$.

Let $K = H + Rb$

Define $\bar{h}: K \rightarrow J$ by $\bar{h}(a + rb) = h(a) + \kappa(r)$ for $a \in H, r \in R$

well-defined: Suppose $a_1 + r_1 b = a_2 + r_2 b$ $a_i \in H, r_i \in R$.

Then $a_1 - a_2 = (r_2 - r_1)b \in H \cap Rb$

In particular, $(r_2 - r_1)b \in H$, so $r_2 - r_1 \in I$.

Then $h(a_1) - h(a_2) = h((r_2 - r_1)b) = \kappa(r_2 - r_1) = \kappa(r_2) - \kappa(r_1)$

so $\bar{h}(a_1 + r_1 b) = h(a_1) + \kappa(r_1) = h(a_2) + \kappa(r_2) = \bar{h}(a_2 + r_2 b)$

Then $\bar{h} \in S$ extends h , contradicting maximality $\downarrow \square$

~~Def 3.4~~

Def An abelian group D is called divisible if for every $y \in D$ and $n \in \mathbb{Z} \setminus \{0\}$, there exists $x \in D$ with $nx = y$.

In other words, the map $D \xrightarrow{x \mapsto nx} D$ is surjective.

Ex \mathbb{Q} is divisible. \mathbb{Z} is not.

Easy Lemma Homomorphic image of a divisible group is divisible.

Lemma 3.4 A \mathbb{Z} -module is divisible if and only if it is injective.

Pf \Leftarrow Let D be an injective \mathbb{Z} -module. Fix $n \in \mathbb{Z} \setminus \{0\}$.

Note that $\langle n \rangle \subset \mathbb{Z}$ is a free \mathbb{Z} -module.

Let $y \in D$.

Define $f: \langle n \rangle \rightarrow D$ by $f(n) = y$ (since $\{n\}$ is a basis)

$$\begin{array}{ccc} 0 & \rightarrow & \langle n \rangle & \xrightarrow{\quad} & \mathbb{Z} \\ & & \downarrow f & \nearrow h & \\ & & D & & \end{array}$$

Since D is injective, there exists $h: \mathbb{Z} \rightarrow D$

Now $nh(1) = h(n) = f(n) = y$. This D is divisible.
 \swarrow Ideal of \mathbb{Z}

\Rightarrow Suppose D is divisible. Let $f: \langle n \rangle \rightarrow D$ be a homomorphism.

Choose $x \in D$ with $nx = f(n)$, and define $h: \mathbb{Z} \rightarrow D$ by $h(1) = x$.

Then h extends f , so by Lemma 3.8 D is injective. \square

Lemma 3.10 Every abelian group can be embedded in a divisible abelian group.

Pf Let A be an abelian group.

There is a free group F s.t. $F/K \cong A$ for some subgroup $K \subset F$.

Since $F \cong \sum \mathbb{Z}$, and $\mathbb{Z} \subset \mathbb{Q}$, $F \xrightarrow{f} \sum \mathbb{Q}$

Note \mathbb{Q} divisible, hence injective, so $\sum \mathbb{Q}$ is injective.

Then $A \cong F/K \xrightarrow{f} F(F) \xrightarrow{f} \sum \mathbb{Q} / f(K)$
 $A \cong F/K \cong F(F)/f(K) \xrightarrow{f} \sum \mathbb{Q} / f(K)$
 \uparrow
 Homomorphic image of a divisible group, thus divisible. \square

Lemma 3.11 Let R be unital, J a divisible abelian group.

Then $\text{Hom}_{\mathbb{Z}}(R, J)$ is an injective R -module.

Pf Let $I \subset R$ be an ideal, and $f: I \rightarrow \text{Hom}_{\mathbb{Z}}(R, J)$

Define $g: I \rightarrow J$ by $g(i) = (f(i))(1)$

Since J injective,

$$\begin{array}{ccccc} 0 & \rightarrow & I & \rightarrow & R \\ & & g \downarrow & \swarrow \tilde{g} & \\ & & J & & \end{array}$$

Now define $h: R \rightarrow \text{Hom}_{\mathbb{Z}}(R, J)$
 $r \mapsto h(r)$

$h(r): R \rightarrow J$
 $x \mapsto \tilde{g}(xr)$

Check: Is $h(r) \in \text{Hom}_{\mathbb{Z}}(R, J)$?

Let $x, y \in R$. $[h(r)](x+y) = \tilde{g}((x+y)r) = \tilde{g}(xr + yr) = \tilde{g}(xr) + \tilde{g}(yr) = [h(r)](x) + [h(r)](y)$

Check: Is h a homomorphism?

Let $r, s \in R$. Is $h(rs) = h(r)h(s)$?

$$[h(rs)](x) = \tilde{g}(xrs)$$

$$\textcircled{QED} [h(s)](x) = [h(s)](xr) = \tilde{g}(xrs)$$

\uparrow R -module structure of $\text{Hom}_Z(R, J)$ \uparrow Def'n of h

Check: Does h extend f ?

Let $r \in I$. Is $h(r) = f(r)$?

Let $x \in R$ $[h(r)](x) = \tilde{g}(xr) = g(xr) = [f(xr)](1)$ since f is an R -mod hom,

$$= [xf(r)](1)$$

since $\text{Hom}_Z(R, J)$ is an R -module

$$= f(r)(1x)$$

$$= f(r)(x)$$

So h extends f , and Lemma 3.8 shows $\text{Hom}_Z(R, J)$ is injective. \square

Prop Let R be unital. Every R -module can be embedded in an injective R -module.

Pf Let A be an R -module. It can be embedded in a divisible abelian group J via an \uparrow injective group homomorphism $f: A \rightarrow J$

This induces a map $\bar{f}: \text{Hom}_Z(R, A) \rightarrow \text{Hom}_Z(R, J)$

$$\bar{f}(g) \longmapsto fg$$

$$\begin{array}{ccc} R & \rightarrow & A \\ \downarrow & \swarrow f & \\ J & & \end{array}$$

Note: \bar{f} is injective, since if $fg = 0$, then $\text{Im } g \subseteq \ker f = \{0\}$ since f is injective.

\bar{f} is an R -module homomorphism

Also observe $\text{Hom}_R(R, A) \subset \text{Hom}_Z(R, A)$

And $A \hookrightarrow \text{Hom}_R(R, A)$

$$a \longmapsto f_a$$

$$\text{where } f_a(r) = ra$$

Injective!
 \downarrow

$$\text{So } A \hookrightarrow \text{Hom}_R(R, A) \hookrightarrow \text{Hom}_Z(R, A) \hookrightarrow \text{Hom}_Z(R, J)$$

Prop 3.13 Let R be unital, J an R -module. TFAE

(i) J is injective

(ii) Every short exact sequence $0 \rightarrow J \rightarrow B \rightarrow C \rightarrow 0$ splits (so $B \cong J \oplus C$)

(iii) J is a direct summand of any module of which it is a submodule.

PF (i) \Rightarrow (ii)

$$\begin{array}{ccccccc} 0 & \rightarrow & J & \rightarrow & B & \rightarrow & C \rightarrow 0 \\ & & \downarrow & \swarrow & & & \\ & & J & & & & \end{array}$$

(ii) \Rightarrow (iii) Suppose J is a submodule of B

then $0 \rightarrow J \rightarrow B \rightarrow B/J \rightarrow 0$ splits by (ii), so $B \cong J \oplus B/J$.

(iii) \Rightarrow (i) J is a submodule of an injective module Q .

Prop 3.7 $\Rightarrow J$ is injective.

□

§4 Hom

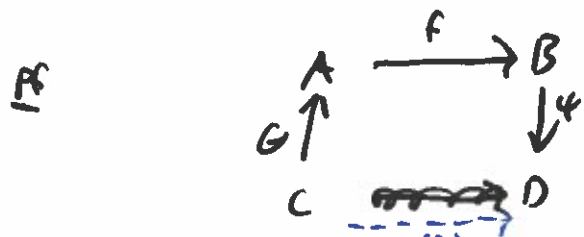
Def Let A, B be R -mods.

$$\text{Hom}_R(A, B) = \{ f: A \rightarrow B \mid f \text{ is an } R\text{-module homomorphism} \}$$

This is an R -module^{*}: $\exists f, g \in \text{Hom}_R(A, B)$ $f+g \in \text{Hom}_R(A, B)$ is given by $(f+g)(x) = f(x) + g(x)$
 $r f \in \text{Hom}_R(A, B)$ given by $(rf)(x) = r f(x)$.
 $r \in R$

* If R noncommutative, need not be an R -module, but is always an abelian group.

Thm 4.1 Let A, B, C, D be R -modules. Let $\varphi: C \rightarrow A$ and $\psi: B \rightarrow D$ be R -module homomorphisms. Then there is a natural map $\Theta: \text{Hom}_R(A, B) \rightarrow \text{Hom}_R(C, D)$ given by $\Theta(f) = \psi f \varphi$



If $f, g \in \text{Hom}_R(A, B)$ $\Theta(f+g) = \psi(f+g)\varphi = \psi(f\varphi + g\varphi) = \psi f\varphi + \psi g\varphi = \Theta(f) + \Theta(g)$
 If $r \in R$, $\Theta(rf) = \psi(rf)\varphi = r\psi f\varphi = r\Theta(f)$. □

Two important examples:

(1) $A=C$, $\Theta = \text{id}$

$A \text{ mod } \varphi: B \rightarrow D$ gives a map $\text{Hom}_R(A, B) \rightarrow \text{Hom}_R(A, D)$
 $f \mapsto \psi f$

" $\text{Hom}(A, -)$ is a covariant functor"

(2) $B=D$, $\psi = \text{id}$ $A \text{ mod } \Theta: C \rightarrow A$ gives a map $\text{Hom}_R(A, B) \rightarrow \text{Hom}_R(C, B)$
 $f \mapsto f\varphi$

" $\text{Hom}(-, B)$ is a contravariant functor"

Thm 4.2 $\text{Hom}_R(D, -)$ is left exact.

i.e. Let $0 \rightarrow A \xrightarrow{\varphi} B \xrightarrow{\psi} C$ be a sequence of R -modules.

This is an exact sequence if and only if for every R -module D ,

the sequence $0 \rightarrow \text{Hom}_R(D, A) \xrightarrow{\bar{\varphi}} \text{Hom}_R(D, B) \xrightarrow{\bar{\psi}} \text{Hom}_R(D, C)$ is exact.

Pf \Rightarrow

(i) we first show $\bar{\varphi}$ is injective.

Let $f \in \text{Ker } \bar{\varphi}$, so $0 = \bar{\varphi}(f) = \varphi f$

i.e. $\varphi f(x) = 0$ for all $x \in D$

Since φ is injective, $f(x) = 0$ for all $x \in D$, i.e. $f = 0$.

So $\text{Ker } \bar{\varphi} = 0$

(ii) claim $\text{Im } \bar{\varphi} = \text{Ker } \bar{\psi}$

Let $g \in \text{Im } \bar{\varphi}$, so $g = \bar{\varphi}(f) = \varphi f$ for some $f \in \text{Hom}_R(D, A)$

then $\bar{\psi}(g) = \psi g = (\psi \varphi) f = 0$ since $\psi \varphi = 0$

Thus $g \in \text{Ker } \bar{\psi}$. So $\text{Im } \bar{\varphi} \subset \text{Ker } \bar{\psi}$.

Now let $g \in \text{Ker } \bar{\psi}$, so $0 = \bar{\psi}(g) = \psi g$

In other words, $\text{Im } g \subset \text{Ker } \psi = \text{Im } \varphi$

$0 \xrightarrow{g} \text{Im } g \subset \text{Im } \varphi \xrightarrow{\varphi^{-1}} A$

Let $h: D \rightarrow A$ be $h = \varphi^{-1}g$

then $\bar{\varphi}(h) = \varphi h = \varphi \varphi^{-1}g = g$, so $g \in \text{Im } \bar{\varphi}$

Thus $\text{Ker } \bar{\psi} \subset \text{Im } \bar{\varphi}$

\Leftarrow (i) we first show φ is injective

By assumption, $0 \rightarrow \text{Hom}(D, A) \xrightarrow{\bar{\varphi}} \text{Hom}(D, B) \xrightarrow{\bar{\psi}} \text{Hom}(D, C)$ is exact

Let $i \in \text{Hom}(D, A)$ be the inclusion map $D \hookrightarrow A$

Then $\bar{\varphi}(i) = \varphi i = 0$ (since $\text{Im } i = D \subset \text{Ker } \varphi$)

Since $\bar{\varphi}$ is injective, $i = 0$ map, i.e. $\text{Ker } \varphi = 0$

(ii) Claim $\text{Im } \varphi \supset \text{Ker } \psi$.

$$0 \rightarrow \text{Hom}(A, A) \xrightarrow{\varphi} \text{Hom}(A, B) \xrightarrow{\psi} \text{Hom}(A, C) \text{ is exact}$$

$\varphi = \varphi(\text{id}) \in \text{Im } \varphi = \text{Ker } \psi$, so $\psi(\varphi) = \psi\varphi = 0$, i.e. $\text{Im } \varphi \subset \text{Ker } \psi$

For other containment,

$$0 \rightarrow \text{Hom}(\text{Ker } \psi, A) \xrightarrow{\varphi} \text{Hom}(\text{Ker } \psi, B) \xrightarrow{\psi} \text{Hom}(\text{Ker } \psi, C) \text{ is exact}$$

Let $j \in \text{Hom}(\text{Ker } \psi, B)$ be inclusion map $\text{Ker } \psi \hookrightarrow B$

Note $\psi(j) = \psi j = 0$, so $j \in \text{Ker } \psi = \text{Im } \varphi$

Thus $j = \varphi f$ for some $f \in \text{Hom}(\text{Ker } \psi, A)$

Now if $x \in \text{Ker } \psi$, $x = j(x) = \varphi f(x) \in \text{Im } \varphi$

So $\text{Ker } \psi \subset \text{Im } \varphi$

□

Prop 4.3 $\text{Hom}_R(-, D)$ is ~~not~~ left exact

i.e. Let $A \xrightarrow{\varphi} B \xrightarrow{\psi} C \rightarrow 0$ be a sequence of R -modules

This is an exact sequence if and only if for every R -module D ,

$$0 \rightarrow \text{Hom}_R(C, D) \xrightarrow{\bar{\psi}} \text{Hom}_R(B, D) \xrightarrow{\bar{\varphi}} \text{Hom}_R(A, D) \text{ is exact.}$$

PF \Rightarrow (i) First show $\bar{\varphi}$ is injective.

Let $f \in \text{Ker } \bar{\varphi}$, so $0 = \bar{\varphi}(f) = f\varphi$

Now let $y \in C$. Then φ surjective $\Rightarrow y = \varphi(x)$ for some $x \in B$

then $f(y) = f\varphi(x) = 0$. Thus $f = 0$

So $\bar{\varphi}$ is injective.

(ii) Claim $\text{Im } \bar{\varphi} = \text{Ker } \bar{\psi}$

Let $f \in \text{Ker } \bar{\psi}$. We want to construct $g \in \text{Hom}_R(B, D)$ with $f = \bar{\varphi}(g)$
so that $f \in \text{Im } \bar{\varphi}$.

$$\text{Ker } \varphi \hookrightarrow B \xrightarrow{\varphi} C \rightarrow 0$$

$$\downarrow f$$

$$D$$

$$B/\text{Ker } \varphi \xrightarrow{\bar{\varphi}} C \rightarrow 0$$

$$\downarrow \bar{f}$$

$$0$$

Claim $\text{Ker } \varphi \subset \text{Ker } f$

If $x \in \text{Ker } \varphi$, $x = \varphi(y)$ for some $y \in A$.

Then $f(x) = f(\varphi(y)) = \varphi(f(y)) = 0$ since $f \in \text{Ker } \vartheta$

Now $f = \varphi(\bar{f}) = \bar{f} \circ \varphi$, since $\bar{f} \circ \varphi(x) = \bar{f}(x + \text{Ker } \varphi) = f(x)$ for all $x \in B$.

Thus $\text{Ker } \vartheta \subset \text{Im } \bar{\varphi}$.

Now let $g \in \text{Im } \bar{\varphi}$, so $g = \bar{\varphi}(f) = f \circ \varphi$ for some $f \in \text{Hom}_R(C, D)$

Then $\vartheta(g) = g \circ \vartheta = f \circ \varphi \circ \vartheta = 0$ since $\varphi \circ \vartheta = 0$

Thus $\text{Im } \bar{\varphi} \subset \text{Ker } \vartheta$.

\Leftarrow (i) First we show φ is surjective.

By assumption, $0 \rightarrow \text{Hom}(C, C/\text{Im } \varphi) \xrightarrow{\bar{\varphi}} \text{Hom}(B, C/\text{Im } \varphi) \xrightarrow{\vartheta} \text{Hom}(A, C/\text{Im } \varphi)$ is exact.

Let $\pi: C \rightarrow C/\text{Im } \varphi$ be quotient map.

Then $\bar{\varphi}(\pi) = \pi \circ \varphi = 0$, so since $\bar{\varphi}$ is injective $\pi = 0$, i.e. $C = \text{Im } \varphi$.

(ii) Claim $\text{Im } \vartheta = \text{Ker } \varphi$

By assumption $0 \rightarrow \text{Hom}(C, B/\text{Im } \vartheta) \xrightarrow{\bar{\varphi}} \text{Hom}(B, B/\text{Im } \vartheta) \xrightarrow{\vartheta} \text{Hom}(A, B/\text{Im } \vartheta)$ is exact.

Let $\pi: B \rightarrow B/\text{Im } \vartheta$ be quotient map.

Now $\vartheta(\pi) = \pi \circ \vartheta = 0$, so $\pi \in \text{Ker } \vartheta = \text{Im } \bar{\varphi}$.

So $\pi = \bar{\varphi}(g) = g \circ \varphi$ for some $g \in \text{Hom}(C, B/\text{Im } \vartheta)$

Now if $x \in \text{Ker } \varphi$, then $\pi(x) = g(\varphi(x)) = 0$, so $x \in \text{Ker } \pi = \text{Im } \vartheta$.

Thus $\text{Ker } \varphi \subset \text{Im } \vartheta$

By assumption, $0 \rightarrow \text{Hom}(C, C) \xrightarrow{\tilde{\psi}} \text{Hom}(B, C) \xrightarrow{\tilde{\phi}} \text{Hom}(A, C)$ is exact

The $\tilde{\phi} \tilde{\psi}(\text{id}) = \psi \phi$, so $\text{Im } \tilde{\phi} \subseteq \text{Ker } \tilde{\psi}$. □

Thm 4.5 Let P be an R -module. P is projective if and only if $\text{Hom}(P, -)$ is (right) exact.

PF \Rightarrow Suppose P is projective.

Let $0 \rightarrow A \xrightarrow{\phi} B \xrightarrow{\psi} C \rightarrow 0$ be an exact sequence of R -modules.

Consider $0 \rightarrow \text{Hom}_R(P, A) \xrightarrow{\tilde{\phi}} \text{Hom}_R(P, B) \xrightarrow{\tilde{\psi}} \text{Hom}_R(P, C) \rightarrow 0$

By Thm 4.2, suffices to show $\tilde{\psi}$ is surjective.

Let $f \in \text{Hom}_R(P, C)$

$$\begin{array}{ccc} & P & \\ \nearrow g & \downarrow f & \\ B & \xrightarrow{\psi} & C \rightarrow 0 \end{array}$$

Since P is projective, there exists $g \in \text{Hom}_R(P, B)$ with $f = \psi g = \tilde{\psi}(g)$

\Leftarrow Suppose

$$\begin{array}{c} P \\ \downarrow f \\ 0 \rightarrow K \rightarrow B \rightarrow C \rightarrow 0 \end{array}$$

The $0 \rightarrow \text{Hom}(P, K) \rightarrow \text{Hom}(P, B) \rightarrow \text{Hom}(P, C) \rightarrow 0$ is exact

The $f \in \text{Hom}(P, C)$ lifts to $g \in \text{Hom}(P, B)$ □

Prop 4.6 Let J be an R -mod. J is injective if and only if $\text{Hom}(-, J)$ is (right) exact.

PF \Rightarrow Suppose J is injective.

Let $0 \rightarrow A \xrightarrow{q} B \xrightarrow{r} C \rightarrow 0$ be exact.

Consider $0 \rightarrow \text{Hom}(C, J) \xrightarrow{\bar{r}} \text{Hom}(B, J) \xrightarrow{\bar{q}} \text{Hom}(A, J) \rightarrow 0$

By Prop 4.3, it suffices to show \bar{q} is surjective.

Let $f \in \text{Hom}(A, J)$

$$\begin{array}{ccc} 0 & \rightarrow & A & \xrightarrow{q} & B \\ & & \downarrow f & \searrow \bar{q} & \\ & & J & & \end{array}$$

Since J is injective, the (diag) $g \in \text{Hom}(B, J)$ will $f = g \circ q = \bar{q}(g)$

\Leftarrow Suppose $0 \rightarrow A \rightarrow B \rightarrow B/\text{Im} \rightarrow 0$

$$\begin{array}{ccc} & & \downarrow f \\ & & J \end{array}$$

The $0 \rightarrow \text{Hom}(B/\text{Im}, J) \rightarrow \text{Hom}(B, J) \rightarrow \text{Hom}(A, J) \rightarrow 0$ is exact.

The $f \in \text{Hom}(A, J)$ lifts to $g \in \text{Hom}(B, J)$ \square

Thm 4.9 Let R be unital, A an R -module. The $\text{Hom}_R(R, A) \cong A$.

PF Define $\phi: \text{Hom}_R(R, A) \rightarrow A$

$$f \mapsto f(1)$$

$$\psi: A \rightarrow \text{Hom}_R(R, A)$$

$$a \mapsto (r \mapsto ra)$$

check $\phi\psi = \text{id}$ \square

Remark $\text{Hom}_R(A, R)$ is called the dual of A , denoted A^*

§ 5 Tensor Products

Motivation Let R be commutative, with 1 rts.
How are $R[x]$, $R[y]$, $R[x, y]$ related as modules?

$R[x]$ free on $\{1, x, x^2, x^3, \dots\}$

$R[y]$ free on $\{1, y, y^2, y^3, \dots\}$

$R[x] \oplus R[y]$ free on $\{1, x, y, x^2, y^2, x^3, y^3, \dots\}$ No mixed terms!

How to formally "multiply" things from two different modules?

Def Let M, N be R -modules.

Let F be free module with basis $M \times N$

Let $K \subset F$ be generated by

$$(m, m_2, n) - (m, n) - (m_2, n)$$

$$(m, m_1, m_2) - (m, m_1) - (m, m_2)$$

$$r(m, n) - (rm, n)$$

$$r(m, n) - (m, rn)$$

$M \otimes_R N := F/K$ is the tensor product of M and N .

Ex $R[x] \otimes_R R[y] \cong R[x, y]$ (as R -modules)

Def Let A, B, C be R -modules. A bilinear map $f: A \times B \rightarrow C$ is a function satisfying

(i) $f(a, a_2, b) = f(a, b) + f(a_2, b)$

(ii) $f(a, b, b_2) = f(a, b) + f(a, b_2)$

(iii) $f(a, b) = f(a, rb) = rf(a, b)$

for all $a, a_2, a_3 \in A$
 $b, b_2, b_3 \in B$
 $r \in R$

~~Def 5.5~~

Ex There is a canonical bilinear map

$$\begin{aligned} M \times N &\longrightarrow M \otimes N \\ (m, n) &\longmapsto m \otimes n \end{aligned}$$

"Elementary tensors"

As a set, $M \otimes N$ consists of (not necessarily distinct) linear combinations of elementary tensors.

Thm 5.6 Let M, N, L be R -modules and $g: M \times N \rightarrow L$ a bilinear map. There is a unique R -module homomorphism $\bar{g}: M \otimes N \rightarrow L$

$$\begin{array}{ccc} M \times N & \xrightarrow{g} & L \\ \downarrow & \nearrow \bar{g} & \\ M \otimes N & & \end{array}$$

pf

$$\begin{array}{ccc} M \times N & \xrightarrow{g} & L \\ \downarrow F & \nearrow g_0 & \\ F & & \\ \downarrow & \nearrow \bar{g} & \\ F/K = M \otimes N & & \end{array}$$

Suffice to show $K \subset \text{Ker } g_0$

But this is precisely the bilinearity of g !

□

Remark $M \otimes N$ is uniquely determined by this property.

Remark If R commutative, $M \otimes_R N \cong N \otimes_R M$.

Cor 5.3 Let $f: M \rightarrow M'$, $g: N \rightarrow N'$ be R -module homomorphisms. There is a unique homomorphism $M \otimes N \rightarrow M' \otimes N'$ such that

This homomorphism is denoted $f \otimes g$

pf

The map $f \otimes g: M \times N \rightarrow M' \otimes N'$ is bilinear

Thm 5.6 obtain unique homomorphism $M \otimes N \rightarrow M' \otimes N'$

□

Prop 5.4 The tensor product is right exact, i.e. if

$$L \xrightarrow{f} M \xrightarrow{g} N \rightarrow 0 \text{ is exact,}$$

$$K \otimes_R L \xrightarrow{\omega \otimes f} K \otimes_R M \xrightarrow{\omega \otimes g} K \otimes_R N \rightarrow 0 \text{ is exact.}$$

PF Claim 1 $\omega \otimes g$ is surjective.

Suffices to show $K \otimes n \in \text{Im}(\omega \otimes g)$ for all $K \in K, n \in N$.

g surjective $\Rightarrow n = g(m)$ for some $m \in M$.

$$\text{Then } K \otimes n = K \otimes g(m) = (\omega \otimes g)(K \otimes m) \in \text{Im}(\omega \otimes g)$$

Claim 2 $\text{Im}(\omega \otimes f) \subset K \otimes (\text{Im } f)$

$$\text{Note } (\omega \otimes g) \circ (\omega \otimes f) = \omega \otimes (g \circ f) = \omega \otimes 0 = 0 \quad \text{since } g \circ f = 0.$$

Claim 3 $\text{Ker}(\omega \otimes g) \subset \text{Im}(\omega \otimes f)$

~~Since~~ Since $\text{Im}(\omega \otimes f) \subset K \otimes (\text{Im } f)$

$$\begin{array}{ccc} K \otimes_R M & \xrightarrow{\omega \otimes g} & K \otimes_R N \\ \pi \downarrow & \nearrow \alpha & \\ K \otimes_R M / \text{Im}(\omega \otimes f) & & \end{array}$$

Suffices to show α is an isomorphism

Define $\beta: K \times N \rightarrow K \otimes_R M / \text{Im}(\omega \otimes f)$ by

$$\beta(K, n) = \pi(K \otimes m) \quad \text{where } m \in M \text{ s.t. } g(m) = n$$

well defined: since $g(m_0) = n$ as well.

The $g(m - m_0) = 0$, so $m - m_0 \in \text{Ker } g = \text{Im } f$.

The $K \otimes (m - m_0) \in \text{Im}(\omega \otimes f)$, so $\pi(K \otimes (m - m_0)) = 0$

$$\text{so } \pi(K \otimes m) = \pi(K \otimes m_0)$$

Straightforward to verify that β is bilinear, so we obtain

$$\bar{\alpha}: K \otimes_R N \rightarrow K \otimes_R M / \text{Im}(\text{id} \otimes f)$$

For any generator $k \otimes n \in K \otimes_R N$

$$\alpha \bar{\beta}(k \otimes n) = \alpha \beta(k, n) = \alpha \pi(k \otimes m) = (\text{id} \otimes g)(k \otimes n) = k \otimes n.$$

$$\text{So } \alpha \bar{\beta} = \text{id}$$

Similarly, for any generator $\pi(k \otimes m)$ of $K \otimes_R M / \text{Im}(\text{id} \otimes f)$

$$\bar{\beta} \alpha(\pi(k \otimes m)) = \bar{\beta}(\text{id} \otimes g)(k \otimes n) = \bar{\beta}(k \otimes g(n)) = \beta(k, g(n)) = \pi(k \otimes m)$$

Thm 5.7 Let R be commutative, M an R -module. Then $A \otimes_R R \cong A$

PF Define bilinear map $A \times R \rightarrow A$
 $(a, r) \mapsto ra$

This gives homomorphism $\alpha: A \otimes_R R \rightarrow A$

Construct $\beta: A \rightarrow A \otimes_R R$
 $a \mapsto a \otimes 1$

check $\beta \alpha = \text{id}$, $\alpha \beta = \text{id}$. \square

Thm 5.8 Let R be commutative, L, M, N R -modules.

Then $(L \otimes_R M) \otimes_R N \cong L \otimes_R (M \otimes_R N)$

PF Fix $x \in L$. Define $\gamma_x: M \times N \rightarrow (L \otimes_R M) \otimes N$ by
 $(m, n) \mapsto (x \otimes m) \otimes n$

This is bilinear, so we obtain $\bar{\gamma}_x: M \otimes N \rightarrow (L \otimes_R M) \otimes N$

Now define $\alpha: L \times (M \otimes_R N) \rightarrow (L \otimes_R M) \otimes N$ by

$$(x, y) \mapsto \bar{\gamma}_x(y).$$

This is also bilinear, so we obtain $\bar{\alpha}: L \otimes_R (M \otimes_R N) \rightarrow (L \otimes_R M) \otimes_R N$.

Note by construction, $\bar{\alpha}(\ell \otimes (m \otimes n)) = (\ell \otimes m) \otimes n$.

Construction is the same way. □

Thm 5.9 Let L, M, N be R -modules.

$$(L \otimes M) \otimes N \cong (L \otimes N) \otimes (M \otimes N)$$

PF Construct $\alpha, \beta: L \otimes N \rightarrow (L \otimes N) \otimes N$ by $\alpha = i_1 \otimes id$

$\alpha_2: M \otimes N \rightarrow (L \otimes N) \otimes N$ by $\alpha_2 = i_2 \otimes id$

α_1, α_2 give $\alpha: (L \otimes N) \oplus (M \otimes N) \rightarrow (L \otimes N) \otimes N$

Define $\beta_0: (L \otimes M) \otimes N \rightarrow (L \otimes N) \otimes (M \otimes N)$

$$(\ell, m) \otimes n \mapsto (\ell \otimes n, m \otimes n)$$

This is bilinear, so we obtain $\beta: (L \otimes M) \otimes N \rightarrow (L \otimes N) \otimes (M \otimes N)$

Let $(\ell, m) \otimes n \in (L \otimes M) \otimes N$

$$\begin{aligned} \alpha\beta((\ell, m) \otimes n) &= \alpha(\ell \otimes n, m \otimes n) \\ &= (\ell, 0) \otimes n + (0, m) \otimes n \\ &= ((\ell, 0) + (0, m)) \otimes n \\ &= (\ell, m) \otimes n \end{aligned}$$

$\alpha\beta$ is identity on generators, so is identity.

$$\begin{aligned}
\beta((l \otimes n_1, m \otimes n_2)) &= \beta((l, 0) \otimes n_1 + (0, m) \otimes n_2) \\
&= \beta((l, 0) \otimes n_1) + \beta((0, m) \otimes n_2) \\
&= (l \otimes n_1, 0 \otimes n_1) + (0 \otimes n_2, m \otimes n_2) \\
&= (l \otimes n_1, 0) + (0, m \otimes n_2) \\
&= (l \otimes n_1, m \otimes n_2)
\end{aligned}$$

β is identity on generators, so β is id.

□

Thm 5.10 Let L, M, N be R -modules.

$$\text{Hom}_R(L \otimes M, N) \cong \text{Hom}(L, \text{Hom}(M, N))$$

pf Define $\alpha: \text{Hom}_R(L \otimes M, N) \longrightarrow \text{Hom}(L, \text{Hom}(M, N))$ by

$$\text{or } f \in \text{Hom}_R(L \otimes M, N), \quad \alpha(f): L \longrightarrow \text{Hom}(M, N)$$

$$[\alpha(f)(l)](m) = f(l \otimes m)$$

(1) Is $\alpha(f)(l)$ a homomorphism $M \rightarrow N$?

$$\begin{aligned}
[\alpha(f)(l)](m_1 + m_2) &= f(l \otimes (m_1 + m_2)) = f(l \otimes m_1) + f(l \otimes m_2) \\
&= [\alpha(f)(l)](m_1) + [\alpha(f)(l)](m_2)
\end{aligned}$$

$$[\alpha(f)(l)](rm) = f(l \otimes rm) = f(r(l \otimes m)) = rf(l \otimes m) = r[\alpha(f)(l)](m)$$

(2) Is α a homomorphism?

$$[\alpha(f+g)(l)](m) = (f+g)(l \otimes m) = f(l \otimes m) + g(l \otimes m) = [\alpha(f)(l)](m) + [\alpha(g)(l)](m)$$

$$[\alpha(rf)(l)](m) = (rf)(l \otimes m) = r(f(l \otimes m)) = r[\alpha(f)(l)](m)$$

(1) Is α a homomorphism?

(2) Is $\alpha(f)$ a homomorphism?

$$\begin{aligned} [\alpha(f)(l_1 + l_2)](m) &= f((l_1 + l_2) \otimes m) = f(l_1 \otimes m + l_2 \otimes m) \\ &= f(l_1 \otimes m) + f(l_2 \otimes m) \\ &= [\alpha(f)(l_1)](m) + [\alpha(f)(l_2)](m) \end{aligned}$$

$$\begin{aligned} [\alpha(f)(rl)](m) &= f(rl \otimes m) = f(r(l \otimes m)) = r f(l \otimes m) \\ &= r [\alpha(f)(l)](m) \end{aligned}$$

Define $\beta: \text{Hom}(L, \text{Hom}(M, N)) \rightarrow \text{Hom}_R(L \otimes M, N)$

If $g \in \text{Hom}(L, \text{Hom}(M, N))$

$$[\beta(g)](l \otimes m) = [g(l)](m)$$

(4) Is β a homomorphism?

$$\begin{aligned} [\beta(g_1 + g_2)](l \otimes m) &= [(g_1 + g_2)(l)](m) = [g_1(l) + g_2(l)](m) \\ &= [g_1(l)](m) + [g_2(l)](m) \\ &= [\beta(g_1)](l \otimes m) + [\beta(g_2)](l \otimes m). \end{aligned}$$

$$\begin{aligned} [\beta(rg)](l \otimes m) &= [(rg)(l)](m) = [r g(l)](m) \\ &= r [g(l)](m) \\ &= r [\beta(g)](l \otimes m) \end{aligned}$$

(5) Is $\beta \alpha$ identity?

$$[\beta \alpha(f)](l \otimes m) = [\alpha(f)(l)](m) = f(l \otimes m), \text{ so } \beta \alpha(f) = f$$

(6) Is $\alpha \beta$ identity?

$$[\alpha \beta(g)(l)](m) = [\beta(g)](l \otimes m) = [g(l)](m), \text{ so } \alpha \beta(g) = g.$$

□

§7 Algebras

Def 7.1 Let R be a commutative, unital ring. A ring A is called an R -algebra if

1) A is an R -module

2) $r \cdot (ab) = (r \cdot a)b = a(r \cdot b)$ for all $r \in R, a, b \in A$.

Ex $R[x]$ is an R -algebra.

Ex \mathbb{Q} is a \mathbb{Z} -algebra

Ex \mathbb{C} is an \mathbb{R} -algebra.

Thm Let A be an R -algebra, and M an R -module.

Then $A \otimes_R M$ is an A -module

(this is called change of base)

Pf $A \otimes_R M$ is an abelian group since it is an R -module

Let $a \in A, \sum a_i \otimes m_i \in A \otimes_R M$.

Then $a \cdot \sum a_i \otimes m_i = \sum (aa_i) \otimes m_i$

Ex $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}[x] = \mathbb{Q}[x]$

Ex If S is an R -algebra, $S \otimes_R R^n \cong S^n$

Ex $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}^n \cong \mathbb{C}^n$

§6 Modules over a PID

Thm 6.1 Let R be a PID, F a free R -module, $G \subset F$ a submodule.
Then G is a free R -module and $\text{rank } G \leq \text{rank } F$.

PF Let $\{x_i | i \in J\}$ be a basis of F , so $F = \sum_{i \in J} Rx_i$.
By the well ordering principle, assume J is well ordered (every nonempty set has a minimal element).

Set

$$\overline{F}_{(j)} = \sum_{i < j} Rx_i \quad \text{and} \quad \overline{F}_{(j)} = \sum_{i < j} Rx_i = \overline{F}_{(j)} \oplus Rx_j \quad \text{for each } j \in J.$$

Note if $x \in \overline{F}_{(j)}$, $x = b + rx_j$ for some $b \in \overline{F}_{(j)}$, $r \in R$.

Define $f_j : \overline{F}_{(j)} \cap G \longrightarrow R$
 $b + rx_j \longmapsto r$

Note $\text{Ker } f_j = \overline{F}_{(j)} \cap G$, so we have an exact sequence

$$0 \rightarrow \overline{F}_{(j)} \cap G \xrightarrow{f_j} \text{Im } f_j \rightarrow 0$$

Note $\text{Im } f_j \subset R$ is an ideal, so $\text{Im } f_j = (r_j)$ for some $r_j \in R$.

Moreover, ~~there exist~~ if $r_j \neq 0$, then there $c_j \in \overline{F}_{(j)} \cap G$ with $f_j(c_j) = r_j$.

Claim $\{c_j | j \in J, r_j \neq 0\}$ is a basis of G .

(i) Linear independence: Suppose $s_1 c_{j_1} + \dots + s_n c_{j_n} = 0$ for some j_1, \dots, j_n

$$\text{then } 0 = f_{j_n}(s_1 c_{j_1} + \dots + s_n c_{j_n}) = s_n f_{j_n}(c_{j_n}) = s_n r_{j_n}$$

Thus $s_n = 0$. By induction, all $s_i = 0$.

(ii) G -generators:

Let $i \in J$ be smallest such that $a \in F_{(i)} \cap G$ is not generated by C .

Let $J' = \{j \mid r_j \neq 0\}$ (so $C = \{c_j \mid j \in J'\}$)

Suppose $i \notin J'$: Then the map $\overline{F}_{(i)} \cap G \rightarrow F_{(i)} \cap G$ is equality,

so $a \in \overline{F}_{(i)} \cap G$.

But then there is a $k < i$ with $a \in F_{(k)} \cap G$, contradicting minimality of i .

So we must have $i \in J'$. Write $f_i(a) = sr_i$ for some $s \in R$.

Let $b = a - sc_i$. Since $a \notin \text{span}(C)$, $b \in \text{span}(C)$.

Also, $f_i(b) = f_i(a) - f_i(sc_i) = 0$, so $b \in \overline{F}_{(i)} \cap G$.

This contradicts minimality of i . □

Cor 6.2 Let R be a PID. If M is a finitely generated R -module generated by n elements, then every submodule of M is generated by at most n elements.

pf Let $N \subset M$ be a submodule.

$$\pi: R^n \longrightarrow M$$

$\pi^{-1}(N)$ is a submodule of R^n , hence free with basis $\{x_1, \dots, x_m\}$, $m \leq n$.

Then N is generated by $\{\pi(x_1), \dots, \pi(x_m)\}$ □

Cor 6.3 A projective module over a PID is free

pf Let M be a ~~free~~ ^{projective} R -module.

$$0 \rightarrow K \rightarrow F \rightarrow M \rightarrow 0, \text{ so } F \cong M \oplus K$$

∴ M is isomorphic to a submodule of F , hence is free. □

Thm 6.4 Let R be a PID, A an R -module.

(i) $\mathcal{O}_a := \{r \in R \mid ra = 0\}$ is an ideal of R for each $a \in A$.

This is called the order ideal of $a \in A$.
If $\mathcal{O}_a = (r)$, a is said to have order r .

(ii) $A_{\text{tor}} = \{a \in A \mid \mathcal{O}_a \neq 0\}$ is a submodule of A .

This is called the torsion submodule of A .

If $A = A_{\text{tor}}$, A is called a torsion module. If $A_{\text{tor}} = 0$, A is called torsion free.

(iii) For each $a \in A$, $R/\mathcal{O}_a \cong R_a = \{ra \mid r \in R\}$ as R -modules.

(iv) Let $p \in R$ be prime. If $(p^i) \subset \mathcal{O}_a$, then $\mathcal{O}_a = (p^j)$ for some $0 \leq j \leq i$.

(v) Let $p \in R$ be prime. If $(p^i) = \mathcal{O}_a$, then $p^j \notin \mathcal{O}_a$ for all $0 \leq j < i$.

PF (i) Let $a \in A$.

If $r_1, r_2 \in \mathcal{O}_a$, $r_1 a = 0, r_2 a = 0$, so $(r_1 + r_2)a = r_1 a + r_2 a = 0 + 0 = 0$, so $r_1 + r_2 \in \mathcal{O}_a$.

If $s \in R$, $(sr_1)a = s(r_1 a) = s \cdot 0 = 0$, so $sr_1 \in \mathcal{O}_a$.

(ii) Let $a_1, a_2 \in A_{\text{tor}}$. Then there exist nonzero $r_1, r_2 \in R$ such that $r_1 a_1 = 0, r_2 a_2 = 0$.
Then $r_1 r_2 (a_1 + a_2) = r_2 r_1 a_1 + r_1 r_2 a_2 = 0 + 0 = 0$. So $a_1 + a_2 \in A_{\text{tor}}$.

(iii) If $r \in R$, then $r_1 (ra_1) = r(r_1 a_1) = r \cdot 0 = 0$, so $ra_1 \in A_{\text{tor}}$.

(iii) Define $\varphi: R \xrightarrow{\varphi} R_a$ φ is surjective.
 $r \mapsto ra$

Let $\ker \varphi = \mathcal{O}_a$, so $R/\mathcal{O}_a \cong R_a$

(iv) Since R a PID, $\mathcal{O}_a = (r)$ for some $r \in R$.

Then since $p^i \in \mathcal{O}_a = (r)$, $r \mid p^i$.

Since R a UFD, $r = p^j u$ for some $u \in R^*$, $j \leq i$. Then $\mathcal{O}_a = (r) = (p^j)$.

(v) Suppose for contradiction that $p^j \in \mathcal{O}_i$ for some $0 \leq j < i$.

Then $p^j = p^i \gamma$ with $j < i$, contradicting unique factorization. \square

Thm 6.6 Let R be a PID, A a f.g. R -module. Then $A = A_{\text{tor}} \oplus F$ for some free module F .

Thm 6.5 Every f.g. torsion free module over a PID is free.

PF Let R be a PID, A a f.g. R -module generated by a finite set X .

Since A is torsion free, Rx is a free submodule of A for each $x \in X$.

Let $S = \{x_1, \dots, x_n\} \subset X$ be a minimal subset, for which

$F = Rx_1 + \dots + Rx_n$ is a free submodule.

If $y \in X \setminus S$, then $ry \in F$ for some $r \in R$. (otherwise, $S \cup \{y\}$ is linearly independent)

Taking a (finite) product of these r 's for each $y \in X \setminus S$, obtain nonzero $r \in R$

s.t. $rX \subset F$.

Since X generates A , $rA \subset F$.

Define $\phi_r : A \rightarrow A$ (clearly $\text{Im } \phi_r = rA \subset F$ is a free module)
 $a \mapsto ra$

But since A is torsion free, ϕ_r is injective, so $A \cong \text{Im } \phi_r$ \square

PF of 6.6 Set $F = A/A_{\text{tor}}$, free by Thm 6.5

$0 \rightarrow A_{\text{tor}} \rightarrow A \rightarrow F \rightarrow 0$ is exact, splits since F is free, hence projective.

Th, $A \cong A_{\text{tor}} \oplus F$ \square

Thm 6.12 Let M be a f.g. module over a PID R .

Then $M \cong R^{\hat{n}} \oplus \underbrace{R_{x_1} \oplus \dots \oplus R_{x_k}}_{M_{\text{tor}}}$ where x_i has order $p_i^{s_i}$ for some prime p_i , positive integer s_i .

Thm 6.7 Let R be a PID, M a torsion R -module. For $p \in M$ a prime, set

$$M(p) = \{a \in M \mid a \text{ has order } \leq p^s \text{ for some } s\}$$

(i) $M(p)$ is a submodule for each prime $p \in M$

(ii) $M = \sum_{\substack{p \in R \\ \text{prime}}} M(p)$. If M is f.g., this sum is finite.

Pf (i) Let $a, b \in M(p)$. Then $\mathcal{O}_a = (p^r)$, $\mathcal{O}_b = (p^s)$ for some $r, s \in \mathbb{N}$

Setting $k = \max(r, s)$, we see $p^k(a+b) = 0$, so $(p^k) \subset \mathcal{O}_{a+b}$, hence $\mathcal{O}_{a+b} = (p^i)$ for some $0 \leq i \leq k$ (Thm 6.4 (iv))

Thus, $a+b \in M(p)$

Let $x \in R$. Then $p^r(xa) = 0$, so $(p^r) \subset \mathcal{O}_{xa}$, hence $\mathcal{O}_{xa} = (p^j)$ for some $0 \leq j \leq r$

Then, $xa \in M(p)$

(ii) Claim 1 $\{M(p) \mid p \in M \text{ prime}\}$ generates M

Let $a \in M \setminus \{0\}$, so $\mathcal{O}_a = (r)$ for some $r \in R$.

R a PID \Rightarrow UFD, so $r = p_1^{n_1} \dots p_k^{n_k}$ for p_i distinct primes p_i

$$\text{Let } r_i = p_1^{n_1} \dots p_{i-1}^{n_{i-1}} p_{i+1}^{n_{i+1}} \dots p_k^{n_k}$$

Then r_1, \dots, r_k are coprime, so $\gcd(r_1, \dots, r_k) = 1$

Then $1 = s_1 r_1 + \dots + s_k r_k$ for some $s_i \in R$.

$$a = s_1 r_1 a + \dots + s_k r_k a$$

$$\text{Note } p_i^{n_i}(s_i r_i a) = s_i r_i a = 0$$

for each i , so $s_i r_i a \in M(p_i)$.

Then $a \in M(p_1) + \dots + M(p_k)$

Claim 2 The sum is direct
 Fix $p \in R$ a prime, and let M_i be submodule generated by $M(q_i)$ for primes $q_i \neq p$.
 we need to show $M(p) \cap M_i = \{0\}$

Suppose $a \in M(p) \cap M_i$, so $p^k a = 0$ for some $k \in \mathbb{N}$.

Also, $a = a_1 + \dots + a_k$ for some $a_i \in M(q_i)$ for primes q_i distinct from p .

Then $q_i^{k_i} a_i = 0$ for some $k_i \in \mathbb{N}$.

Then $(q_1^{k_1} \dots q_k^{k_k}) a = 0$ Let $d = q_1^{k_1} \dots q_k^{k_k}$.

Note p^k, d coprime, so $1 = rp^k + sd$ for some $r, s \in R$.

Then $a = rp^k a + sd a = 0$

Claim 3 If M is f.s., this sum is finite.

Suppose $M = Rx_1 + \dots + Rx_n$

~~x_i are annihilated by $M(q_i)$~~

Then $x_i \in M(p_{i1}) \oplus \dots \oplus M(p_{in_i})$ for some primes $p_{i1}, \dots, p_{in_i} \in R$.

$\Rightarrow M \subseteq \bigoplus_{i=1}^n M(p_{i1}) \oplus \dots \oplus M(p_{in_i})$

□

Lemma 6.8 Let R be a PID, M an R -module such that $p^n M = 0$ and $p^{n-1} M \neq 0$
 for some prime $p \in R$, $n \in \mathbb{N}$. Let $a \in M$ have order p^n .

(i) If $M \neq Ra$, there exists nonzero $b \in M$ s.t. $Ra \cap Rb = 0$

(ii) $M = Ra \oplus C$ for some submodule C .

pf (i) Let $c \in M \setminus Ra$. Since $p^n M = 0$, $p^n c = 0 \in Ra$

Let $j \in \mathbb{N}$ be minimal such that $p^j c \in Ra$

so $p^{j-1} c \notin Ra$, and $p^j c = r_1 a$ for some $r_1 \in R$.

Write $r_1 = p^k r$ for some $k \geq 0$
 maximal, so $p \nmid r$

Then $0 = \hat{p}^j c = \hat{p}^{n-j}(\hat{p}^j c) = \hat{p}^{n-j}(\hat{p}^k r a)$, so $n-j+k \geq n$, thus $k \geq j \geq 1$

$$\text{Set } b = \hat{p}^{j-1} c - r \hat{p}^{k-1} a$$

As $\hat{p}^{j-1} c \notin R a$, so $b \neq 0$, and $\hat{p} b = \hat{p}^j c - r \hat{p}^k a = 0 - 0 = 0$

We claim $R a \cap R b = 0$.

If not, there exists $s \in R$ with $s b \in R a$ and $s b \neq 0$.

Since $s b \neq 0$, $\hat{p} \nmid s$, so s and \hat{p} are coprime

thus $s x + \hat{p}^j y = 1$ for some $x, y \in R$.

$$\text{Then } b = s x b + \hat{p}^j y b = s x b \in R a \text{ since } \hat{p}^j M = 0$$

$$\text{Then } \hat{p}^{j-1} c = b + r \hat{p}^{k-1} a \in R a$$

Recall j was minimal s.t. $\hat{p}^j c \in R a$, so we must have $j-1 > 0$, so $c \in R a$ \downarrow

(ii) wlog, $M \neq R a$.

$$\text{Let } S = \{B \in M \mid R a \cap B = 0\}$$

Zorn \Rightarrow S has a maximal element $C \in M$ with $R a \cap C = 0$

Since $R a \cap C = 0$, suffices to show $M = R a + C$.

Claim $M/C = R(a+c)$

$$\text{Since } \hat{p}^n A = 0, \quad \hat{p}^n(A/C) = 0$$

$$\text{But } \hat{p}^{n-1}(a+c) = \hat{p}^{n-1} a + C \neq C, \text{ since } \hat{p}^{n-1} a + C = C \Rightarrow \hat{p}^{n-1} a \in C \cap R a = 0$$

and $\hat{p}^n a \neq 0$ by assumption

So $\hat{p}^{n-1}(A/C) \neq 0$, and we can apply part (i) to A/C

So either $M/C = R(a+c)$, or there exists $b \in M/C$ with $R(a+c) \cap R(b+C) = C$

Suppose latter

Then $R a \cap (R b + C) \neq 0$. But $C \not\subseteq R b + C$, contradiction.

Thus $M/C = R(a+c)$, so $M = R a + C$

□

Thm 6.9 Let R be a PID, M a f.g. R -module such that every element has order a power of p for some fixed prime $p \in R$.
 Then $M = Ra_1 \oplus \dots \oplus Ra_k$, where a_i has order p^{n_i} for some $n_i \in \mathbb{N}$.

PF ~~Proof~~ Suppose $M = Ra_1 + \dots + Ra_k$. Induction on k , $k=1$ trivial.

Let a_i have order p^{n_i} for some $n_i \in \mathbb{N}$.

wlog, $n_1 \geq n_i$ for all $1 \leq i \leq k$.

Then $p^{n_1} M = 0$ and $p^{n_1-1} M \neq 0$

By Lemma 6.8, $M = Ra_1 \oplus C$

Moreover, letting $\pi: M \rightarrow C$ be quotient map,

C is generated by $\pi(a_1), \dots, \pi(a_k)$

Moreover, $p^{n_i} \pi(a_i) = \pi(p^{n_i} a_i) = \pi(0) = 0$, so $\mathcal{O}_{\pi(a_i)} = (p^{n_i})$ for some $n_i \leq n_1$.

Now apply induction hypothesis $\Rightarrow C = Ra_{n_2} \oplus \dots \oplus Ra_{n_k}$

□

Thm 6.12 Let R be a PID, M a f.g. R -module.

$$M = R^n \oplus Ra_1 \oplus \dots \oplus Ra_k$$

where a_i has order $p_i^{n_i}$ for some prime $p \in R$.

PF By thm 6.6, $M = R^n \oplus M_{\text{tor}}$

By thm 6.7, $M_{\text{tor}} = M_{\text{tor}}(p_1) \oplus \dots \oplus M_{\text{tor}}(p_k)$

By thm 6.9, $M_{\text{tor}}(p_i) = Ra_{i_1} \oplus \dots \oplus Ra_{i_{k_i}}$

□