

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

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  $\phi(m) = m \cdot 1$ .

$\phi$  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  $0 = n \cdot 1 = K \cdot r \cdot 1 = K \cdot (r \cdot 1)$

□

~~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)  $IJ = \left\{ \sum x_i y_i \mid x_i \in I, y_i \in J \right\}$  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: since  $a+I = a_0+I$ ,  $b+I = b_0+I$   
 $a = a_0 + x$  for some  $x \in I$        $b = b_0 + y$  for some  $y \in I$

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

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

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  $b=0$  i.e.  $R$  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 <sup>proper</sup> 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

$$1 = m_1 + a r_1 = m_2 + b r_2$$

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

$$\text{Then } 1 = (m_1 + a r_1)(m_2 + b r_2) = \underbrace{m_1 m_2 + m_1 b r_2 + m_2 a r_1}_{\in M} + a b r_1 r_2$$

If  $ab \in M$ , then  $1 \in M$   $\downarrow$  so  $ab \notin M$ ,  $\therefore M$  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  $I_i = \langle m_i \rangle$ . Since  $\gcd(m_i, m_j) = 1$ ,  $1 = a m_i + b m_j$  for some  $a, b \in \mathbb{Z}$   
i.e.  $\mathbb{Z} = \langle m_i \rangle + \langle m_j \rangle$ . □

Apply thm 2.25.

## § 5 Polynomial rings

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

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

( $n^{\text{th}}$  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  $(a_i), (b_i), (c_i) \in R[X]$

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

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

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 these are isomorphic  $R[x, y]$  (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,  $\phi$  is completely determined by  $\phi_0$  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  $\phi$  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  $\Rightarrow R = \mathbb{A}[x, y] / (x^2 - y^3)$

$y$  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 (up to 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  $\phi(a+bi) = a^2 + b^2$ .

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

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



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  $n \geq m$ .

Indet 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,  $f - qg = q_0 g + \overset{\deg < \deg g}{\downarrow q_1 \text{ into } r}$

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

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

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

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

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

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

$$= (x^2 - 2x + 3)g + r_3$$

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  $\varphi(r) < \varphi(y)$

$$\cancel{x - qy} + r = x - qy \in I \Rightarrow r = 0$$

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

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

$$sadtf - tdesb = 0$$

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

$\uparrow$   
 $s$

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

□

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

(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  $S=R^{\times}$ , 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  $y \in S$

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

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

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

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

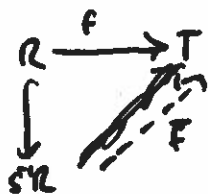
$$\varphi(a+b) = \frac{(a+b)s^2}{s^2} = \frac{as}{s} + \frac{bs}{s} = \varphi(a) + \varphi(b)$$

If  $s \in S$ ,  $\varphi(s) = \frac{s \cdot s}{s} = s$  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  $\varphi$  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,  ~~$S \cap P \neq \emptyset$~~  and  ~~$S \cap P \neq \emptyset$~~ , 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)  $J = \tilde{S}'I$  :

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

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

(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  $ab \in P$ .

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

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

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

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)  $r \cdot f(a) = f(r \cdot a)$  for all  $r \in R, a \in M$ .

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

The map  $Q: R[x] \rightarrow R[x]$  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  $\forall r \in R, n \in N$ .

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 <sup>unital</sup>  $R$ -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~~  $\{B_i\}_{i \in I}$  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

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

"   
  $N/\text{Im } f$

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  $\alpha$  and  $\gamma$  are both injective, so is  $\beta$ .
- (ii) If  $\alpha$  and  $\gamma$  are both surjective, so is  $\beta$ .
- (iii) If  $\alpha$  and  $\gamma$  are both isomorphisms, so is  $\beta$ .

Pf "Diagram chasing"

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

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

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

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

(ii) Let  $x \in B$ .

Since  $\gamma$  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  $f'(w) = x - \beta(z)$

$\alpha$  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

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

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

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

(3)  $\Rightarrow$  (2)

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

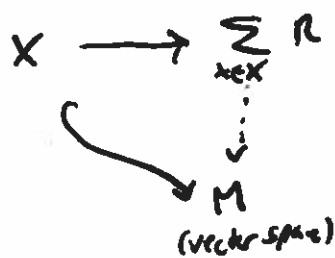
where  $\tilde{f}$  has kernel map  $\sum_{x \in X} xR \rightarrow F$   
 $x \mapsto i(x)$

(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  $r_1x_1 + \dots + r_nx_n + r_{n+1}a = 0$  for some  $r_i \in k$ , not all zero.

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

so  $a = -\frac{1}{r_{n+1}}(r_1x_1 + \dots + r_nx_n) \in N$  ↓

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,  $I \subset R$  <sup>proper</sup> 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  $\pi$  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  $\pi: R \rightarrow R/m$

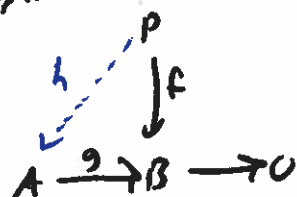
is a nonzero surjection, and  $R/m$  is a field, thus has IBN.  $\square$

### §3 Projective and Injective modules

#### Motivations

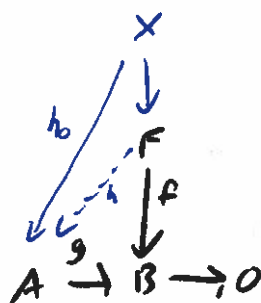
- 1) Projective modules are almost as nice as free modules
  - (i) Direct summands of free modules
  - (ii) Locally free
- 2) Algebraic ~~over~~ analogue of vector bundles - locally trivial  
(Ex: Infinitely long Möbius strip)

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

- (1)  $P$  is projective
- (2) Every short exact sequence  $0 \rightarrow A \rightarrow B \rightarrow P \rightarrow 0$  splits  
(so  $B \cong A \oplus P$ )
- (3) 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!

$$A \rightarrow B \rightarrow 0$$

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

□

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

$$A \rightarrow B \rightarrow 0$$

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

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)

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

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

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



$\Leftarrow$  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  $\phi$  is an  $R$ -module homomorphism

By assumption,  $\phi$  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  $A \cong F/K \xrightarrow{f} F(F)$   
 $A \cong F/K \cong F(F)/K(F) \hookrightarrow \sum \mathbb{Q}/K(F)$   
 $\uparrow$   
 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,

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

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

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

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

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!  
 $\downarrow$

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

(99)

$\square$

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

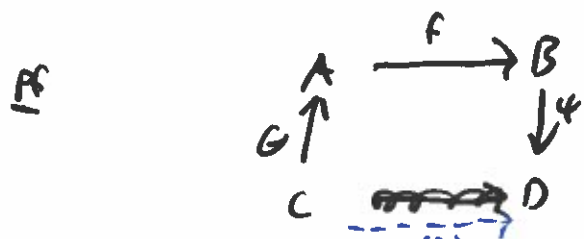
Def Let  $A, B$  be  $R$ -mods.

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

This is an  $R$ -module<sup>\*</sup>:  $\exists f, g \in \text{Hom}_R(A, B)$   $f+g \in \text{Hom}_R(A, B)$  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  $\varphi$  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  $\varphi$  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  $\text{Im } \varphi \supset \text{Ker } \psi$ .

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

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

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  $\text{Ker } \psi \xrightarrow{j} B$

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

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

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

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

□

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.

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

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

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

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  $\varphi$  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  $\tilde{\phi} \tilde{\psi}(\text{id}) = \psi \circ \phi$ , 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  $f \in \text{Hom}_R(P, C)$

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

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

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

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

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

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

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

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

$M \otimes_R N := F/K$  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  $\text{Im}(\omega \otimes f) \subset K \otimes (\text{Im } f)$

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

Suffices to show  $\alpha$  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  $\beta$  is bilinear, so we obtain

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

For any generator  $k \otimes m \in K \otimes_R M$

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

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

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

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

□

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  $\beta \alpha = \text{id}$ ,  $\alpha \beta = \text{id}$ . □

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  $\alpha_2 = i_2 \otimes id$

$\alpha_1, \alpha_2$  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.



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

$\beta$  is identity on generators, so  $\beta$  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  $\alpha$  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  $\alpha$  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  $\beta$  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  $a \in A, \sum a_i \otimes m_i \in A \otimes_R M$ .

$$\text{Then } a \cdot \sum a_i \otimes m_i = \sum (aa_i) \otimes m_i$$

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  $\{x_j \mid j \in J\}$  be a basis of  $F$ , so  $F = \sum_{j \in J} Rx_j$ .  
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, if  $r_j \neq 0$ , then there exists  $c_j \in \overline{F}_{(j)} \cap G$  with  $f_j(c_j) = r_j$ .

Claim  $\{c_j \mid j \in J, r_j \neq 0\}$  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~~ <sup>projective</sup>  $R$ -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  $\varphi: R \xrightarrow{\varphi} R_a$   $\varphi$  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,  $\phi_r$  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  $x_i \in M(p_{i1}) \oplus \dots \oplus M(p_{in})$  for some primes  $p_{i1}, \dots, p_{in} \in R$ .

$\Rightarrow M \subseteq \bigoplus_{i=1}^n M(p_{i1}) \oplus \dots \oplus M(p_{in})$

□

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  $x, y \in R$ .

$$\text{Then } b = s x b + \hat{p}^j y b = s x b \in R a \quad \text{since } \hat{p}^j M = 0$$

$$\text{Then } \hat{p}^{j-1} c = b + r \hat{p}^{k-1} a \in R a$$

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,  $M_{\text{tor}}(p_i) = Ra_{i_1} \oplus \dots \oplus Ra_{i_{k_i}}$

□

## Ch. 8 Commutative Rings and Modules

Assume all rings are commutative unital.

### §1 Chain Conditions

Def 1.1 An  $R$ -module  $M$  is called Noetherian if ~~to~~ every chain of submodules  $M_1 \subset M_2 \subset \dots$  stabilizes; i.e. there is some  $n$  such that  $M_n = M_{n+1} = M_{n+2} = \dots$ . (Ascending chain condition)

$M$  is called Artinian if every chain of submodules  $M_1 \supset M_2 \supset M_3 \dots$  stabilizes (Descending chain condition)

Def 1.2 A ring is Noetherian (Artinian) if it is Noetherian (resp. Artinian) as a module over itself (i.e. its ideals satisfy ascending (resp. descending) chain condition).

Ex  $\mathbb{Z}$  is Noetherian, but not Artinian  
 $\Rightarrow (m) \subset (n) \iff n \mid m$   
Note  $(2) \supset (4) \supset (8) \supset (16) \supset \dots$

Ex Every PID is Noetherian

Ex An Artinian integral domain  $R$  is a field.  
Let  $a \in R$ . Then  $(a) \supset (a^2) \supset (a^3) \supset \dots$  stabilizes, so  $(a^n) = (a^{n+1})$  for some  $n \in \mathbb{N}$ .  
Then  $a^n \in (a^{n+1})$ , so  $a^n = ba^{n+1}$  for some  $b \in R$ , so  $1 = ba$ .

Thm 1.5 Let  $0 \rightarrow L \xrightarrow{f} M \xrightarrow{g} N \rightarrow 0$  be a short exact sequence.  
Then  $M$  is Noetherian (resp. Artinian) if and only if  $L$  and  $N$  are Noetherian (resp. Artinian).

PF  $\Rightarrow$  Submodules of  $L$  are submodules of  $M$ , so  $L$  is Noetherian

Let  $N_1 \subset N_2 \subset \dots$  be a chain of submodules of  $M$ .

Then  $g'(N_1) \subset g'(N_2) \subset \dots$  is a chain of submodules of  $M$

So  $g'(N_i) = g'(N_n)$  for all  $i \geq n$  for some  $n \in \mathbb{N}$ .

Then  $N_i = g(g'(N_i)) = g(g'(N_n)) = N_n$  for all  $i \geq n$ , so  $M$  is Noetherian.

L Suppose  $L, M$  Noetherian

Let  $M_1 \subset M_2 \subset \dots$  be a chain of submodules of  $M$ .

Let  $L_i = f^{-1}(f(L) \cap M_i)$   $N_i = g(M_i)$

Then  $0 \rightarrow L_i \rightarrow M_i \rightarrow N_i \rightarrow 0$  is exact

Since  $L, M$  Noetherian, there exists  $n$  s.t.  $L_i = L_n$  and  $N_i = N_n$  for all  $i \geq n$ .

For  $i \geq n$ :

$$\begin{array}{ccccccc} 0 & \rightarrow & L_n & \rightarrow & M_n & \rightarrow & N_n \rightarrow 0 \\ & & \downarrow \text{id} & & \downarrow i & & \downarrow \text{id} \\ 0 & \rightarrow & L_i & \rightarrow & M_i & \rightarrow & N_i \rightarrow 0 \end{array}$$

Five Lemma  $\Rightarrow M_n = M_i$  for all  $i \geq n$ . □

Cor 1.6 Let  $N \subset M$  be  $R$ -modules. Then  $M$  is Noetherian (resp. Artinian) iff  $N$  and  $M/N$  are Noetherian (resp. Artinian)

Ex  $\mathbb{Z}/n\mathbb{Z}$  is Noetherian

Cor 1.7 Let  $M_1, \dots, M_n$  be modules. Then  $M_1 \oplus \dots \oplus M_n$  is Noetherian (resp. Artinian) iff all  $M_i$  are Noetherian (resp. Artinian)

PF  $0 \rightarrow (M_1 \oplus \dots \oplus M_{n-1}) \rightarrow M_1 \oplus \dots \oplus M_n \rightarrow M_n \rightarrow 0$

Thm 1.8 If  $R$  is Noetherian (resp. Artinian), then every finitely generated  $R$ -module is Noetherian (resp. Artinian)

PF Let  $M$  be a f.g.  $R$ -module.

Then  $M \cong R^n/K$ , and  $R^n$  Noetherian, so  $M$  is Noetherian.

Thm 1.9 A module is Noetherian iff every submodule is finitely generated.  
A ring is Noetherian iff every ideal is finitely generated

PF  $\Rightarrow$  Let  $M$  be Noetherian,  $N \subseteq M$  a submodule.

Let  $S = \{ L \subseteq N \mid L \text{ is finitely generated} \}$ .

note: if  $L_1 \subseteq L_2 \subseteq L_3 \subseteq \dots$  is a chain in  $S$ ,

then  $\bigcup_{i=1}^{\infty} L_i = \bigcup_{i=1}^{\infty} L_n = L_n$  for some  $n$ , hence  $\bigcup_{i=1}^{\infty} L_i \in S$ .

Then  $\Rightarrow S$  has a maximal element  $K$

If  $K \neq N$ , let  $x \in N \setminus K$ . Then  $K + Rx$  is f.g., and  $K \subsetneq K + Rx$ .

So  $K = N$ , i.e.  $N$  is f.g.

$\Leftarrow$  Let  $M_1 \subseteq M_2 \subseteq M_3 \subseteq \dots$  be a chain of submodules of  $M$ .

Let  $N = \bigcup_{i=1}^{\infty} M_i$ .  $N = Rx_1 + \dots + Rx_n$  by assumption.

Let  $m$  be minimal s.t.  $x_1, \dots, x_n \in M_m$ .

then  $M_m \supseteq N = \bigcup_{i=1}^{\infty} M_i$ , so  $M_i = M_m$  for all  $i \geq m$ .  $\square$

Ex  $A[x_1, x_2, \dots]$  is not Noetherian

Thm 4.9 (Hilbert Basis Theorem) If  $R$  is Noetherian, so is  $R[x_1, \dots, x_n]$

## §2 Prime and primary ideals

Motivation: Let  $R$  be a UFD,  $d \in R$ .

Then  $d = p_1^{a_1} \cdots p_k^{a_k}$  for some primes  $p_i \in R$

so  $(d) = (p_1^{a_1}) \cap \cdots \cap (p_k^{a_k})$

$\uparrow$   
Not prime ideal!

But if  $ab \in (p_i^{a_i})$  and  $a \notin (p_i^{a_i})$ , then  $b^{a_i} \in (p_i^{a_i})$  for some  $k$

So  $(d)$  is the intersection of primary ideals.

Big goal: In a Noetherian ring, every ideal is the intersection of primary ideals

~~Def 2.5~~

Def 2.5 Let  $I \subset R$  be an ideal. The radical of  $I$  is

$$\text{rad}(I) = \bigcap_{\substack{P \supset I \\ P \text{ prime}}} P \quad (\text{Sometimes denoted } \sqrt{I})$$

Thm 2.6  $\text{rad}(I) = \{r \in R \mid r^n \in I \text{ for some } n \in \mathbb{N}\}$

PF Trivial if  $I=R$ , so assume  $I$  a proper ideal.

Suppose  $r^n \in I$ , and  $P \supset I$  is prime. Then  $r^n \in P$ , so  $r \in P$ .

Thus  $r \in \text{rad}(I)$

Conversely, suppose  $r \in \text{rad}(I)$ , and suppose for contradiction that  $r^n \notin I$  for all  $n \in \mathbb{N}$ .

Let  $S = \{J \subset R \mid J \text{ ideal, } r^n \notin J \text{ for all } n \in \mathbb{N}\}$

$S$  nonempty (since  $I \in S$ ) ; apply Zorn

Maximal element  $P \in S$  (and  $P \supset I$ )

Note  $P$  is prime: if  $x, y \notin P$ , then  $r^n \in P + xR$  for some  $n \in \mathbb{N}$   
 $r^n \in P + yR$  for some  $n \in \mathbb{N}$

and  $r^{2n} \in P + xyR$ , so  $xy \in P$

(as  $xy \notin P \Rightarrow r^{2n} \in P$ , contradicting  $P \in S$ )

Let  $P$  prime,  $P \supset I \Rightarrow r \in P$   $\downarrow$

□

Thm 2.7 Let  $I, J \subset R$  be ideals

(i)  $\text{Rad}(\text{Rad } I) = \text{Rad } I$

(ii)  $\text{Rad}(IJ) = \text{Rad}(I \cap J) = \text{Rad}(I) \cap \text{Rad}(J)$

(iii)  $\text{Rad}(I^n) = \text{Rad}(I)$

Pf (i) Let  $r \in \text{Rad}(\text{Rad } I)$ , so  $r^n \in \text{Rad } I$ , so  $(r^n)^m \in I$   
 $\overset{r^{nm}}{\parallel} \Rightarrow r \in \text{Rad}(I)$ .

(ii) Let  $r \in \text{Rad}(I) \cap \text{Rad}(J)$ , so  $r^n \in I$ ,  $r^m \in J$  for some  $n, m \in \mathbb{N}$ .

Then  $r^{n+m} = r^n r^m \in IJ$ , so  $r \in \text{Rad}(IJ)$

and  $r^{nm} \in I \cap J$ , so  $r \in \text{Rad}(I \cap J)$

Note  $IJ \subset I \cap J$ , so  $\text{Rad}(IJ) \subset \text{Rad}(I \cap J)$

~~Also  $r \in \text{Rad}(IJ)$ ,  $r^n \in IJ$  for some  $n \in \mathbb{N}$~~

Also  $IJ \subset I$ ,  $IJ \subset J$ , so  $\text{Rad}(IJ) \subset \text{Rad}(I) \cap \text{Rad}(J)$  □

Def An ideal  $I \subset R$  is called radical if  $I = \text{Rad}(I)$

Ex For any ideal,  $\text{rad}(I)$  is radical.

Ex Every prime ideal is radical

Def 2.8 An ideal  $\mathcal{A} \subset R$  is called primary if whenever  $ab \in \mathcal{A}$  and  $a \notin \mathcal{A}$ , then  $\hat{b} \in \mathcal{A}$  for some  $n \in \mathbb{N}$

Ex If  $R$  is a UFD,  $p$  prime,  $(p^n)$  is primary

Ex In  $k[x, y]$ ,  $(x^2, y)$  is primary

Let  $a, b \in k[x, y]$  so  $\bar{a}, \bar{b} \in k[x, y]/(y) \cong k[x]$



If  $ab \in (x^2, y)$ , then  $\bar{a}\bar{b} \in (x^2)$

with  $\bar{a} = a_0 + a_1x + x^2\tilde{a}(x)$  for some  $a_0, a_1 \in R$   $\tilde{a}, \tilde{b} \in R[x]$   
 $\bar{b} = b_0 + b_1x + x^2\tilde{b}(x)$

If  $a \notin (x^2, y)$ ,  $\bar{a} \notin (x^2)$  so either  $a_0 \neq 0$  or  $a_1 \neq 0$

If  $ab \in (x^2, y)$ ,  $\bar{a}\bar{b} \in (x^2)$

$$\bar{a}\bar{b} = a_0b_0 + (a_0b_1 + a_1b_0)x + x^2(*)$$

so  $a_0b_0 = 0$  and  $a_0b_1 + a_1b_0 = 0$

Case 1  $a_0 \neq 0$ , so  $b_0 = 0$ , i.e.  $\bar{b} \in (x)$ , so  $(\bar{b})^2 \in (x^2)$ , so  $b^2 \in (x^2, y)$

Case 2  $a_0 = 0$ , so  $a_1 \neq 0$ , so  $b_0 = 0$   $\uparrow$

(More generally,  $(x^i, y^j) \subset R[x, y]$  is primary)

Thm 2.9 Let  $Q \subset R$  be primary. Then  $\text{rad}(Q)$  is prime.

Pf Let  $a, b \in R$  with  $ab \in \text{rad}(Q)$  and  $a \notin \text{rad}(Q)$

Then  $(ab)^n \in Q$  for some  $n \in \mathbb{N}$ .

so  $a^n b^n$

Since  $a \notin \text{rad}(Q)$ ,  $a^n \notin Q$ , so  $Q$  primary  $\Rightarrow (b^n)^m \in Q$  for some  $m \in \mathbb{N}$

so  $b \in \text{rad}(Q)$ .

Thus  $Q$  is prime.

Def Let  $Q \subset R$  be primary,  $P = \text{rad}(Q)$ .

$P$  is called the associated prime ideal of  $Q$

$Q$  is called  $P$ -primary.

Thm 2.10 Let  $Q, P \subset R$  be ideals. Then  $Q$  is  $P$ -primary iff

- (i)  $Q \subset P \subset \text{rad } Q$  and  
(ii) If  $ab \in Q$  and  $a \notin Q$ , then  $b \in P$ .

PF  $\Leftarrow$  Suppose (i) and (ii). Let  $a, b \in R$  with  $ab \in Q$  and  $a \notin Q$ .

Then  $b \in P \subset \text{rad } Q$ , so  $b^n \in Q$  for some  $n \in \mathbb{N}$ . Thus  $Q$  is primary.

We still need to show  $P = \text{rad } Q$ .

Let  $b \in \text{rad } Q$ , so  $b^n \in Q$  for some minimal  $b$ .

If  $n=1$ ,  $b \in Q \subset P$  and we are done.

If  $n > 1$ ,  $b \cdot b^{n-1} \in Q$  and  $b^{n-1} \notin Q$ , so by (ii),  $b \in P$ .

$\Rightarrow$  (i) Trivial since  $P \supset \text{rad } Q$ .

(ii) By def of primary,  $ab \in Q$  and  $a \notin Q \Rightarrow b^n \in Q$ , then  $b \in \text{rad } Q = P$   $\square$

Thm 2.11 A finite intersection of  $P$ -primary ideals is  $P$ -primary.

PF Since  ~~$Q_1, Q_2$~~   $Q_1, Q_2$  are  $P$ -primary.

Then  $\text{Rad}(Q_1 \cap Q_2) = \text{Rad}(Q_1) \cap \text{Rad}(Q_2) = P \cap P = P$

Let  $a, b \in R$  with  $ab \in Q_1 \cap Q_2$

If  $a \notin Q_1 \cap Q_2$ , then  $a \notin Q_1$  or  $a \notin Q_2$ .

Then either  $b \in P$  or  $b \in P$ , so  $b \in P$ .

By Thm 2.10,  $Q_1 \cap Q_2$  is  $P$ -primary.  $\square$

Def Let  $I \subset R$  be an ideal. A minimal prime over  $I$  is a prime ideal  $P \supset I$  s.t. if  $Q$  prime and  $I \subset Q \subset P$ , then  $Q = P$ .

Thm Every proper ideal is contained in a minimal prime ideal.

PF Let  $I \subset R$  be a proper ideal.

Let  $S = \{P \supset I \mid P \text{ prime}\}$

$I$  contained in a maximal ideal, so  $S \neq \emptyset$

Let  $P_1 \supset P_2 \supset \dots$  is a chain in  $S$ ,  $\bigcap_{i=1}^{\infty} P_i \in S$

Zorn  $\Rightarrow S$  has a minimal element  $P$ , which is minimal over  $I$ .

(Really: If  $P$  prime,  $I \subset P$ , there is a minimal prime  $P_0$  with  $I \subset P_0 \subset P$ )

Thm If  $R$  is Noetherian, every proper ideal has finitely many minimal primes

PF Suppose not. Since  $R$  Noetherian, there is a maximal counterexample ideal  $I$ .

Note  $I$  is not prime, so let  $f, g \in R \setminus I$  with  $fg \in I$

If  $P$  is a minimal prime over  $I$ , then  $fg \in P$ , so  $f \in P$  or  $g \in P$

$\Rightarrow P$  is minimal prime over  $I + fR$  or  $I + gR$ .

$\Rightarrow I + fR$  (or  $I + gR$ ) is a bigger counterexample  $\downarrow \square$

Def An ideal  $I$  is called irreducible if whenever  $I = J \cap K$ , then  $I = J$  or  $I = K$ .

Lemma Irreducible ideals are primary

PF Let  $I \subset R$  be an irreducible ideal.

Let  $a, b \in R$  with  $ab \in I$ . We will show either  $a \in I$  or  $b^m \in I$  for some  $m$ .

Set  $J_k = \{c \in R \mid cb^k \in I\}$ . Note  $a \in J_1$ .

$I = J_0 \subset J_1 \subset J_2 \subset \dots$

$R$  Noetherian  $\Rightarrow$  for some  $N$ ,  $J_n = J_N$  for  $n \geq N$ .

Claim  $I \supseteq J_N \cap (I + (b^N))$

pf  $\subset \checkmark$

$\supset$  Let  $c \in J_N \cap (I + (b^N))$

so  $c = x + b^N y$  for some  $x \in I, y \in R$

and  $c b^N \in I$

so  $c b^N = x b^N + b^{2N} y$

$\uparrow \quad \uparrow \quad \Rightarrow b^{2N} y \in I$ , so  $y \in J_{2N} = J_N$

$\Rightarrow b^N y \in I$

Thus  $c = x + b^N y \in I$ .

~~so rather~~

Now  $I$  irreducible  $\Rightarrow I = J_N$  or  $I = I + (b^N)$

Case 1  $I = I + (b^N) \Rightarrow b^N \in I$

Case 2  $I = J_N \supset J_1 \supset J_0 = I$ , so  $J_1 = I$

Let  $a \in J_1$ , so  $a \in I$ .

□

Lasker-Noether Theorem In a Noetherian ring, every ideal is an intersection of finitely many primary ideals.

pf By lemma, it suffices to show every ideal is a finite intersection of irreducible ideals.

Let  $S = \{ I \in R \mid I \text{ is not a finite intersection of irreducible ideals} \}$

Suppose  $S$  is nonempty: Choose  $I_0 \in S$ .

We must have  $I_0 = J_1 \cap K_1$  for some ideals  $J_1, K_1$  different from  $I_0$   
(otherwise  $I_0$  is irreducible)

Note where  $J_1 \in S$  (if  $J_1, K_1$  both not in  $S$ , their intersection is not in  $S$ !)

Let  $I_1 = J_1$ .

Repeat to produce

$$I_0 \subset I_1 \subset I_2 \subset \dots \quad \text{with } I_{i+1} \neq I_i \text{ at each step}$$

This contradicts  $R$  being Noetherian!

So  $S$  had to be empty. □

Corollary In a Noetherian ring, every radical ideal is a finite intersection of minimal prime ideals

PF Let  $I \subset R$  be radical.

By Lasker-Noether, write  $I = Q_1 \cap \dots \cap Q_n$  for some primary ideals  $Q_i$ .

$$\text{Then } I = \text{rad}(I) = \text{rad}(Q_1 \cap \dots \cap Q_n) = \text{rad}(Q_1) \cap \dots \cap \text{rad}(Q_n)$$

$\uparrow \qquad \qquad \qquad \nearrow$   
all prime!

Each  $\text{rad}(Q_i)$  can be replaced by a minimal prime  $I \subset P_i \subset \text{rad}(Q_i)$ .

## S4 Noetherian Rings & Modules

Prop 4.1 A ring is Noetherian if and only if every prime ideal is finitely generated.

Pf  $\Rightarrow$  R Noetherian  $\Leftrightarrow$  every ideal finitely generated.

$\Leftarrow$  Let  $S = \{I \subset R \mid I \text{ is not finitely generated}\}$

Suppose  $S$  is not empty.

Zorn  $\Rightarrow$   $S$  has a maximal element  $P$

Claim  $P$  is prime

(This contradicts assumption, so  $S$  is empty, so all ideals f.g., so  $R$  is Noetherian.)

Pf of Claim Suppose for contradiction that  $a, b \notin P$  and  $ab \in P$ .

Then  $P + aR, P + bR$  are bigger than  $P$ , hence f.g.

Write  $P + aR = (p_1 + ar_1, \dots, p_n + ar_n)$

$p_i, r_i \in P$

$P + bR = (p_1 + br_1, \dots, p_n + br_n)$

$r_i, s_i \in R$

$(q_1 + bs_1, \dots, q_m + bs_m)$

Now let  $J = \text{Ann}_{R/P}(\{a\}) = \{r \in R \mid ra \in P\}$ , an ideal ("annihilator")

observe  $(q_i + bs_i)a = q_i a + abs_i \in P$ , ~~and~~  $\uparrow \quad \uparrow$   
 $P \quad P$

so  $P \subsetneq P + bR \subset J$ . So  $J$  also bigger than  $P$ , so a f.g.

write  $J = (j_1, \dots, j_k)$  for some  $j_i \in R$ .

Let  $x \in P \subset P + aR$  be arbitrary.

then  $x = \sum_{i=1}^n (p_i + ar_i) y_i$  for some  $y_i \in R$

Rearranging,  $a \sum_{i=1}^n r_i y_i = x - \sum_{i=1}^n p_i y_i \in P$

so by definition  $\sum_{i=1}^n r_i y_i \in J$ , so  $\sum_{i=1}^n r_i y_i = \sum_{i=1}^k j_i z_i$  for some  $z_i \in R$ .

then  $x = \sum_{i=1}^n p_i y_i + \sum_{i=1}^k j_i z_i a$

this implies  $P \subset (p_1, \dots, p_n, j_1 a, \dots, j_k a)$   $\downarrow$

$\square$

Def Let  $M$  be an  $R$ -module,  $S \subset M$  any nonempty subset.

$\text{Ann}_R(S) = \{r \in R \mid rs = 0 \text{ for all } s \in S\}$  is an ideal of  $R$ .

Lemma 4.2 Let  $M$  be a f.g.  $R$ -module, and  $I = \text{Ann}_R(M)$ .  
Then  $M$  is Noetherian (resp. Artinian) if and only if  $R/I$  is a Noetherian (resp. Artinian) ring.

pf  $\Rightarrow$  Write  $M \cong R x_1 + \dots + R x_n$

Let  $I_i = \text{Ann}_R(\{x_i\})$ , so  $I = I_1 \cap \dots \cap I_n$

We have an injective map  $\phi: R/I \hookrightarrow R/I_1 \oplus \dots \oplus R/I_n$

Claim  $R/I_i \cong R x_i$

$r + I_i \mapsto r x_i$

Injective: If  $r x_i = 0$ ,  $r \in I_i$

Surjective:  $r + I_i \mapsto r x_i$

well defined since  $I_i = \text{Ann}_R(\{x_i\})$

$M$  Noetherian  $\Rightarrow R x_i$  Noetherian  $\Rightarrow R/I_i$  Noetherian.  $\Rightarrow R/I$  is Noetherian  $R$ -module.

Finally, ideals in  $R/I$  are also  $R$ -submodules, so  $R/I$  is Noetherian.

$\Leftarrow$  Suppose  $R/I$  is Noetherian ring.

Then  $M$  is a f.g.  $R/I$  module, hence Noetherian.  $\square$

Def 3.1 If  $M, N$  are  $R$ -modules,  $M$  is called primary or a primary submodule if whenever  $r \in R$ ,  $x \in N \subset M$  and  $rx \in M$ , then  $r^n N \subset M$  for some  $n \in \mathbb{N}$ .

Thm 3.2 Let  $M \subset N$  be a primary  $R$ -submodule.

Then  $\text{Ann}_R(N/M)$  is a primary ideal in  $R$ .

Pf Let  $\mathcal{A} = \text{Ann}_R(N/M) = \{r \in R \mid rN \subset M\}$

Let  $r, s \in R$  with  $rs \in \mathcal{A}$ ,  $s \notin \mathcal{A}$

We need to show  $r^n \in \mathcal{A}$  for some  $n \in \mathbb{N}$ .

Since  $s \notin Q$ , there is some  $x \in N$  with  $sx \notin M$ .

$$\text{But } rs \in Q \Rightarrow rsx \in M$$

Since  $M$  primary,  $r^n N \subset M$  for some  $n \in \mathbb{N}$ . □

Def If  $P$  is the radical of  $\text{Ann}_R(M/M)$ ,  $M$  is called  $P$ -primary.

Lemma 4.3 Let  $M \subset N$  be <sup>Noetherian!</sup>  $R$ -modules, and suppose  $M$  is  $P$ -primary for some prime ideal  $P \subset R$ . Then  $P^n N \subset M$  for some  $n \in \mathbb{N}$ .

PF Let  $I = \text{Ann}_R(N)$  and set  $\bar{R} = R/I$

Note  $I \subset \text{Ann}_R(N/M) \subset P$ , so  $\bar{P} = P/I$  is an ideal in  $\bar{R}$ .

Since  $I$  annihilates  $N$  and  $M$ , they are  $\bar{R}$  modules.

Claim  $M$  is a  $\bar{P}$ -primary  $\bar{R}$ -submodule of  $N$ .

Let  $\bar{r} \in \bar{R}$ ,  $x \in N \setminus M$  such that  $\bar{r}x \in M$ .

We need to show  $\bar{r}^n N \subset M$  for some  $n \in \mathbb{N}$ .

Since  $M$  is a primary  $R$ -submodule of  $N$ ,  $r^n N \subset M$  for some  $n \in \mathbb{N}$ .  
 $\Rightarrow \bar{r}^n N \subset M$

Now observe that Lemma 4.2  $\Rightarrow \bar{R} = R/I$  is a Noetherian ring.

So  $\bar{P} = \bar{p}_1 \bar{R} + \dots + \bar{p}_s \bar{R}$  for some  $\bar{p}_i \in \bar{P}$ .

Since  $M$  is a primary  $\bar{R}$ -submodule of  $N$ ,

for each  $i$ :  $\bar{p}_i^{n_i} N \subset M$  for some  $n_i \in \mathbb{N}$ .

Set  $m = n_1 + \dots + n_s$

Then  $\bar{P}^m N \subset M$ .

Since  $\bar{P} = P/I$  and  $IN = 0$ , we must have  $P^m N \subset M$ . □



#### Thm 4.4 (Krull Intersection Theorem)

Let  $I \subset R$  be an ideal,  $M$  a Noetherian  $R$ -module.

Let  $N = \bigcap_{n=1}^{\infty} I^n M$ . Then  $IN = N$ .

pf Note  $N \subset M$ . If  $IN = M$ , then  $M \subset N$ , so  $N = M = IN$ .

So  $IN$  is a proper submodule, so it has a primary decomposition

$IN = M_1 \cap \dots \cap M_s$ , where  $M_i$  is a  $P_i$ -primary submodule of  $M$ .

Note  $IN \subset M$ , so it suffices to show  $N \subset M_i$  for each  $i$ .

Case 1  $I \subset P_i$

Lemma 4.3  $\Rightarrow P_i^{\infty} M \subset M_i$  for some  $n \in \mathbb{N}$ .

Then  $N = \bigcap_{n=1}^{\infty} I^n M \subset I^n M \subset P_i^n M \subset M_i$ .

Case 2  $I \not\subset P_i$

Then there exists  $r \in I \setminus P_i$ .

Suppose for contradiction  $N \not\subset M_i$ .

Then there exists  $x \in N \setminus M_i$ .

Since  $rx \in IN \subset M_i$  and  $M_i$  primary,  $r^n M \subset M_i$  for some  $n \in \mathbb{N}$ .

$\Rightarrow r \in \text{rad}(\text{Ann}_R(M_0/M_i)) = P_i$   $\downarrow$

Thus  $N \subset M_i$ . □

### Motivation

Let  $(R, \mathfrak{m})$  be a local ring,  $M$  a fin.  $R$ -module.

Then  $M/\mathfrak{m}M$  is a (finite dimensional)  $R/\mathfrak{m}$ -vector space.

What can we say if  $M/\mathfrak{m}M = 0$ ? i.e.  $M = \mathfrak{m}M$ ?

~~Write~~ Write  $M = Rx_1 + \dots + Rx_n$  for some minimal generating set  $\{x_1, \dots, x_n\}$

If  $M \neq 0$ , wlog  $x_1 \neq 0$ , so  $x_1 \in \mathfrak{m}M$

$$x_1 = m_1 x_1 + \dots + m_n x_n \quad \text{for some } m_i \in \mathfrak{m}.$$

$$(1 - m_1)x_1 = m_2 x_2 + \dots + m_n x_n$$

$\uparrow$   
 $\in R^\times$

$$\text{So } x_1 = \frac{m_2}{1-m_1} x_2 + \dots + \frac{m_n}{1-m_1} x_n \quad \downarrow$$

So we had to have  $M = 0$

### Nakayama's Lemma (vi)

Let  $(R, \mathfrak{m})$  be a local ring,  $M$  a fin.  $R$ -module.

Then  $M = 0 \iff M/\mathfrak{m}M = 0$

### Nakayama's Lemma (vii)

Let  $(R, \mathfrak{m})$  be a local ring,  $M$  a fin.  $R$ -module.

Suppose  $\{x_1 + \mathfrak{m}M, \dots, x_n + \mathfrak{m}M\}$  is a basis of  $M/\mathfrak{m}M$ .

Then  $M = Rx_1 + \dots + Rx_n$

pf Let  $N = Rx_1 + \dots + Rx_n \subset M$

~~$M/\mathfrak{m}M = (Rx_1 + \dots + Rx_n)/\mathfrak{m}(Rx_1 + \dots + Rx_n) = (R/\mathfrak{m})x_1 + \dots + (R/\mathfrak{m})x_n$~~

Then  $N/\mathfrak{m}N = M/\mathfrak{m}M$

$$\text{So } 0 = M/\mathfrak{m}M / M/\mathfrak{m}M \cong M/N \implies M = 0.$$

□

What if  $R$  is not local?

Key step:  $1-m \in R^*$

What if  $1-m \in R^*$ ?

If not,  $1-m$  is in some maximal ideal

If  $m$  is in the maximal ideal, so is  $1 \rightarrow$  contradiction!

So we need an ideal contained in every maximal ideal.

Lemma 4.5 (Nakayama) Let  $I \subset R$  be an ideal. TFAE

(i)  $I$  is contained in every maximal ideal of  $R$

(ii) If  $m \in I$ , then  $1-m \in R^*$

(iii) If  $M$  is a fin.  $R$ -module with  $IM = M$ , then  $M = 0$

(iv) If  $N$  is a fin.  $R$ -module with  $M = IM + N$ , then  $M = N$

Prop 4.6 Let  $I \subset R$  be an ideal. Then  $I$  is contained in every maximal ideal of  $R$  if and only if for every Noetherian  $R$ -module  $M$ ,  $\bigcap_{n=1}^{\infty} I^n M = 0$

PF  $\Rightarrow$  Let  $N = \bigcap_{n=1}^{\infty} I^n M$ . Krull intersection  $\Rightarrow IN = N$   
Nakayama  $\Rightarrow N = 0$ .

$\Leftarrow$  Let  $\mathfrak{m} \subset R$  be a maximal ideal.

Then  $R/\mathfrak{m}$  is a field, hence a simple  $R$ -module, so Noetherian.

On  $N$  the  $\bigcap_{n=1}^{\infty} I^n N = 0$ .

Since  $IN$  is a submodule of  $N$ , either  $IN = N$ , hence  $I^n N = N \Rightarrow \bigcap_{n=1}^{\infty} I^n N = N \nrightarrow$   
or  $IN = 0 \Rightarrow I \subset \mathfrak{m}$  since  $N = R/\mathfrak{m}$ .

Cor 4.7 Let  $(R, \mathfrak{m})$  be a Noetherian local ring. Then  $\bigcap_{n=1}^{\infty} \mathfrak{m}^n = 0$

Prop 4.8 (Kaplansky, 1958) Let  $(R, \mathfrak{m})$  be a local ring,  $P$  a finitely generated projective module. Then  $P$  is free.

PF Let  $n$  be the minimal number of generators of  $P$ .

$$0 \rightarrow K \rightarrow F \xrightarrow{\pi} P \rightarrow 0$$

$$F = R^n \oplus \dots \oplus R^n$$

$$K = \ker \pi$$

Claim  $K \subset \mathfrak{m}F$

Suppose not: There exists  $K \in K \setminus \mathfrak{m}F$

$$K = r_1 x_1 + \dots + r_n x_n$$

$r_i \in R$  and wlog,  $r_i \notin \mathfrak{m}$ .  
So  $r_i \in R^\times$ .

$$\text{Then } x_1 - r_1^{-1} K = r_1^{-1} r_2 x_2 + \dots + -r_1^{-1} r_n x_n$$

$$\pi(x_1) = \cancel{0} = \sum_{i=2}^n r_1^{-1} r_i \pi(x_i)$$

Then  $P$  is generated by  $\{\pi(x_2), \dots, \pi(x_n)\}$  contradicting minimality.

Now with  $K \oplus P = F$  (since  $P$  projective)

$$F = K + P \subset \mathfrak{m}F + P$$

Then  $F/P \subset \mathfrak{m}F/P \subset \mathfrak{m}(F/P)$ , so  $F/P = \mathfrak{m}(F/P)$

Nakayama  $\Rightarrow F/P = 0$ , i.e.  $F \cong P$ .



Thm 4.1 (Hilbert's Basis Theorem) If  $R$  is Noetherian, then  $R[x_1, \dots, x_n]$  is Noetherian.

pf It suffices to show  $R[x]$  is Noetherian.

Let  $I \subset R[x]$  be an ideal. We will show  $I$  is f.g.

Let  $I_n = \left\{ \frac{f^{(n)}(u)}{n!} \mid f \in I \right\}$  = leading coefficients of deg  $n$  polys from  $I$   
(for  $n > 0$ ; if  $n = 0$ ,  $I_0 = I \cap R$ )

$I_n \subset R$  is an ideal

Note if  $r \in I_n$ ,  $r = \frac{f^{(n)}(u)}{n!} = \frac{(xf)^{(n+1)}(u)}{(n+1)!} \in I_{n+1}$

$I_0 \subset I_1 \subset I_2 \subset \dots$

$R$  Noetherian  $\Rightarrow I_n = I_t$  for all  $n \geq t$  for some fixed  $t$ .

Write  $I_n = r_{n,1}R + \dots + r_{n,i_n}R$  for some  $r_{n,j} \in I_n$  for each  $n \in \mathbb{N}$ .

Write  $r_{n,j} = \frac{f_{n,j}^{(n)}(u)}{n!}$  for some  $f_{n,j} \in I$

Claim  $I = \underbrace{\sum_{n=0}^t \sum_{j=1}^{i_n} f_{n,j} R}_{\text{call this } J}$

pf  $\supset \checkmark$

$\subset$  We prove by induction  $\{f \in I \mid \deg f \leq k\} \subset J$

$k=0$ : Note  $f_{0,j} = r_{0,j}$ , so  $\{f \in I \mid \deg f = 0\} \subset \sum_{j=1}^{i_0} r_{0,j}R = \sum_{j=1}^{i_0} f_{0,j}R \subset J$

$t \geq k > 1$ : Let  $f \in I$  have ~~deg~~  $\deg f = k$  and set  $r = \frac{f^{(k)}(u)}{k!} \in I_k \setminus \{0\}$

Write  $r = r_{k,1}s_1 + \dots + r_{k,i_k}s_{i_k}$  for some  $s_j \in R$ .

Set  $\tilde{f} = f - (f_{k,1}s_1 + \dots + f_{k,i_k}s_{i_k})$

Then  $\deg \tilde{f} < \deg f$ , so by inductive hypothesis  $\tilde{f} \in J \Rightarrow f \in J$ .

$K \geq 1$  Let  $f \in \mathcal{I}$  have degree  $K$ , let  $r = \frac{f^{(K)}(c)}{K!} \in \mathcal{I}_K \setminus \{0\}$

write  $r = r_{k,1} s_1 + \dots + r_{k,m} s_m$  for  $s_i \in \mathcal{R}$ .

Set  $\tilde{f} = f - x^{K-b} (r_{k,1} s_1 + \dots + r_{k,m} s_m)$

Then  $\deg \tilde{f} < \deg f$ , so induction  $\Rightarrow \tilde{f} \in \mathcal{J}$ , so  $f \in \mathcal{J}$ .  $\square$

Prop 4.10 If  $R$  is Noetherian, so is  $R[[x]]$

Def Let  $K/\mathbb{R}$  be a field extension.  $u \in K$  is called algebraic over  $\mathbb{R}$  if there exists  $f \in \mathbb{R}[x] \setminus \{0\}$  with  $f(u) = 0$ . Otherwise,  $u$  is called transcendental.  
If every element of  $K$  is algebraic,  $K$  is called an algebraic extension of  $\mathbb{R}$ .  
Otherwise,  $K$  is called a transcendental extension.

Ex  $\sqrt{2} \in \mathbb{R}$  is algebraic over  $\mathbb{Q}$

Ex  $\pi \in \mathbb{R}$  is transcendental (over  $\mathbb{Q}$ )

Ex  $\mathbb{R}$  is a transcendental extension of  $\mathbb{Q}$ .

Ex  $\mathbb{C}$  is an algebraic extension of  $\mathbb{R}$

(if  $a \in \mathbb{C} \setminus \mathbb{R}$ ,  $a$  is a root of  $(x-a)(x-\bar{a}) \in \mathbb{R}[x]$ )

Thm Let  $\mathbb{A}$  be a field. TFAE

(i) Every nonconstant polynomial  $f \in \mathbb{A}[x]$  has a root in  $\mathbb{A}$ .

(ii) Every irreducible polynomial in  $\mathbb{A}[x]$  has degree one.

(iii) Every polynomial  $f \in \mathbb{A}[x]$  splits, i.e. factors as a product of linear polynomials.

(iv) There is no algebraic extension of  $\mathbb{A}$  (except  $\mathbb{A}$  trivially).

Such a field  $\mathbb{A}$  is called algebraically closed.

Pf (i)  $\Rightarrow$  (ii)  $\Rightarrow$  (iii)  $\Rightarrow$  (iv)

Part (i)  $\Rightarrow$  Part (iv) : If  $f \in \mathbb{A}[x]$  has no root in  $\mathbb{A}$ ,  $K = \text{Frac } \mathbb{A}[x]/(f)$  is an algebraic extension of  $\mathbb{A}$ .

Def Let  $\mathbb{A}$  be a field. An extension  $K$  is called an algebraic closure of  $\mathbb{A}$  if it is an algebraically closed algebraic extension.

Thm Every field has a unique algebraic closure.

Ex  $\mathbb{C}$  is the algebraic closure of  $\mathbb{R}$  (FTA)

## § VI.1

Def 1.1 Let  $K/k$  be a field extension.  $S \subset K$  is called algebraically dependent (over  $k$ ) if there is a polynomial  $f \in k[x_1, \dots, x_n]$  and  $s_1, \dots, s_n \in S$  with  $f(s_1, \dots, s_n) = 0$ . Otherwise  $S$  is called algebraically independent.

Thm 1.2 Let  $K/k$  be a field extension, and  $\{s_1, \dots, s_n\}$  an algebraically independent subset of  $K$ . Then  $k(s_1, \dots, s_n) \cong k(x_1, \dots, x_n)$

Pf ~~Bijective~~ ~~isomorphism~~  $\cong$   $k[x_1, \dots, x_n] \rightarrow k[s_1, \dots, s_n]$   
 $x_i \mapsto s_i$

extends to ~~bijective~~ ~~isomorphism~~  $\cong$   $k(x_1, \dots, x_n) \rightarrow k(s_1, \dots, s_n)$

Def 1.4 Let  $K/k$  be a field extension. A transcendence basis of  $K$  over  $k$  is a maximal algebraically independent subset.

Ex Let  $K = k(x)$ .  $\{x\}$  is a transcendence basis of  $K$ .  
 For any  $\frac{f}{g} \in K$ ,  $\{x, \frac{f}{g}\}$  is algebraically dependent:  $g(x) \cdot \frac{f}{g} - f(x) = 0$

More generally,  $\{x_1, \dots, x_n\}$  is a transcendence basis of  $k(x_1, \dots, x_n)$  over  $k$ .

Thm 1.5 Let  $K/k$  be a field extension,  $S \subset K$  algebraically independent, and let  $u \in K \setminus k(S)$ . Then  $S \cup \{u\}$  is algebraically independent over  $k$  if and only if  $u$  is transcendental over  $k(S)$ .

Pf  $\Leftarrow$  Suppose  $u$  is transcendental over  $S$ .

Suppose for contradiction that  $S \cup \{u\}$  is algebraically dependent.

Then there exists  $s_1, \dots, s_n \in S$ ,  $f \in k[x_1, \dots, x_{n+1}]$  with  $f(s_1, \dots, s_n, u) = 0$  and  $\deg_{x_{n+1}} f > 0$ .

Let  $g(x_{n+1}) = f(s_1, \dots, s_n, x_{n+1}) \in k(S)[x_{n+1}]$  so  $\deg g > 0$ .

Then  $g(u) = 0$ , so  $u$  is algebraic over  $k(S)$   $\square$



$\Rightarrow$  Suppose  $S \cup \{u\}$  is algebraically independent.

Let  $f \in k(S)[x]$  be such that  $f(u) = 0$

we will show  $f = 0$ .

$$f = \sum_{i=0}^n \frac{f_i(s_1, \dots, s_n)}{g(s_1, \dots, s_n)} x^i = \frac{1}{g(s_1, \dots, s_n)} \sum_{i=0}^n \tilde{f}_i(s_1, \dots, s_n) x^i.$$

$$\text{Let } h = \sum_{i=0}^n \tilde{f}_i(x_1, \dots, x_n) x_{n+1}^i \in k[x_1, \dots, x_{n+1}].$$

$$\text{We have } f(u) = 0 \Rightarrow h(s_1, \dots, s_n, u) = 0 \Rightarrow \tilde{f}_i = 0 \text{ for all } i \Rightarrow f = 0$$

$\uparrow$   
 $S \cup \{u\}$  algebraically independent

Cor 1.6 Let  $K/k$  be a field extension,  $S \subset K$  algebraically independent.

Then  $S$  is a transcendence basis if and only if  $K$  is algebraic over  $k(S)$ .

Pf  $\Rightarrow$  Let  $u \in K \setminus k(S)$ . Then  $S \cup \{u\}$  is algebraically dependent  $\Rightarrow$   $u$  is algebraic over  $k(S)$ .

$\Leftarrow$   $K$  algebraic over  $k(S) \Leftrightarrow S \cup \{u\}$  is algebraically dependent for all  $u \in K \setminus k(S)$   
 $\Leftrightarrow S$  is a transcendence basis.  $\square$

Cor 1.7 Let  $K/k$  be a field extension. If  $K$  is algebraic over  $k(x)$  for some  $x \in K$ , then  $x$  contains a transcendence basis of  $K$  over  $k$ .

Pf Let  $S \subset x$  be maximal among algebraically independent subsets of  $x$ .

Then  $k(x)$  is algebraic over  $k(S)$ , so  $K$  is algebraic over  $k(S)$ .

Then Cor 1.6  $\Rightarrow S$  is a transcendence basis.  $\square$

Def Any two transcendence bases of a field extension have the same cardinality. This is called the transcendence degree of the extension.

## § 5 Ring Extensions

Def 51 Let  $S$  be a (commutative, unital) ring, and  $R \subset S$  a subring with  $1 \in R$ .  
Then  $S$  is called a ring extension of  $R$ .

Ex  $\mathbb{R} \subset \mathbb{R}[x]$  is a ring extension.

Ex  $\mathbb{Z} \subset \mathbb{Z}$  is not a ring extension.

Def 52 Let  $R \subset S$  be a ring extension. An element  $s \in S$  is called integral (over  $R$ ) if there is a monic polynomial  $f(x) \in R[x]$  with  $f(s) = 0$ .  
If every element of  $S$  is integral,  $S$  is called an integral extension.

Ex If  $K/\mathbb{Q}$  is an algebraic field extension, it is an integral ring extension.

Ex  $\mathbb{Z} \subset \mathbb{Q}$ .  $a \in \mathbb{Q}$  is integral  $\iff a \in \mathbb{Z}$ .

Ex  $\mathbb{Z} \subset \overline{\mathbb{Q}}$ .  $\frac{1}{\sqrt{3}}$  is algebraic but not integral (over  $\mathbb{Z}$ )  
However,  $\frac{1}{\sqrt{3}}$  is integral over  $\mathbb{Q}$ .

Thm 5.3 Let  $R \subset S$  be a ring extension,  $s \in S$ . TFAE

(i)  $s$  is integral over  $R$

(ii)  $R[s]$  is a f.g.  $R$ -module

(iii) There exists  $\underbrace{T}_{\text{ring extension}}$  with  $R[s] \subset T \subset S$  s.t.  $T$  is a f.g.  $R$ -module.

(iv) There is a  $R[s]$ -submodule  $B \subset S$  s.t.

(a)  $B$  is a f.g.  $R$ -module

(b)  $\text{Ann}_{R[s]} B = 0$

Pf (i)  $\Rightarrow$  (ii)  $S$  integral  $\Rightarrow S^n = \sum_{i=0}^n a_i s^i$  for some  $a_i \in R$ .

$$\Rightarrow R[S] = R + Rs + \dots + Rs^{n-1}$$

(ii)  $\Rightarrow$  (iii)  $T = R[S]$  suffices

(iii)  $\Rightarrow$  (iv) Let  $B = T$ . If  $\alpha \in \text{Ann}_{R[S]} B$ ,  $\alpha \cdot 1 = 0 \Rightarrow \alpha = 0$ ,  
since  $B = T$  is a ring extension

(iv)  $\Rightarrow$  (i) Write  $B = Rb_1 + \dots + Rb_n$

Since  $B$  is an  $R[S]$ -module, can write  $Sb_i = r_{i,1}b_1 + \dots + r_{i,n}b_n$  for some  $r_{i,j} \in R$ .

$$\text{Let } \vec{b} = \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} \text{ and } A = (r_{i,j}) \in M_n(R)$$

$$\text{then } (sI - A) \cdot \vec{b} = 0$$

$$\text{so } \det(sI - A) \cdot I \cdot \vec{b} = 0 \text{ i.e. } \det(sI - A) b_i = 0 \text{ for each } i$$

$$\text{so } \det(sI - A) \in \text{Ann}_{R[S]} B = 0$$

But  $\det(sI - A)$  ~~is not~~ is a monic polynomial in  $S$ .  $\square$

Cor 5.4 Let  $R \subset S$  be a ring extension. If  $S$  is a f.g.  $R$ -module, then  $S$  is integral over  $R$ .

Thm 5.5 Let  $R \subset S$  be a ring extension,  $s_1, \dots, s_n \in S$  integral over  $R$ .  
Then  $R[s_1, \dots, s_n]$  is a f.g.  $R$ -module and hence is integral over  $R$ .

Pf  $R \subset R[s_1] \subset R[s_1, s_2] \subset \dots \subset R[s_1, \dots, s_n]$

Since each  $s_i$  integral over  $R$ , integral over  $R[s_1, \dots, s_{i-1}]$

Thus  $R[s_1, \dots, s_i]$  is a f.g.  $R[s_1, \dots, s_{i-1}]$  module

$\Rightarrow R[s_1, \dots, s_i]$  is a f.g.  $R$ -module. for each  $i$ .  $\square$

Thm 5.6 Let  $R \subset S \subset T$  be ring extensions. If  $T$  is integral over  $S$ , and  $S$  is integral over  $R$ , then  $T$  is integral over  $R$ .

Pf Let  $t \in T$ . Since  $t$  is integral over  $S$ ,  $t$  is a root of  $f = \sum_{i=0}^n s_i x^i$   
with  $f \in R[s_0, \dots, s_{n-1}][x]$ , so  $t$  is integral over  $R[s_0, \dots, s_{n-1}]$ ,  
so  $R[s_0, \dots, s_{n-1}, t]$  is a f.g.  $R[s_0, \dots, s_{n-1}]$  module  
Since  $S$  integral over  $R$ ,  $R[s_0, \dots, s_{n-1}]$  is a f.g.  $R$ -module  
 $\Rightarrow R[s_0, \dots, s_{n-1}, t]$  is a f.g.  $R$ -module  
 $\bigcup_{R \subset T} \Rightarrow t$  integral by Thm 5.3.

Thm 5.7 Let  $R \subset S$  be a ring extension. Let  $\bar{R} = \{s \in S \mid s \text{ is integral over } R\}$ , called the integral closure of  $R$  in  $S$ . Then  $\bar{R}$  is integral over  $R$ , and is maximal among integral extensions of  $R$  contained in  $S$ .

Pf Only need to show  $R \subset \bar{R}$  is a ring extension.  
If  $s, t \in \bar{R}$ ,  $s, t \in R[s, t]$  so  $st, s \in R[s, t] \subset \bar{R}$   
Since  $s, t$  integral,  $R[s, t] \subset \bar{R}$

Def If  $R \subset S$  is a ring extension and  $R = \bar{R}$ ,  $R$  is called integrally closed in  $S$ .  
 If  $R$  is an integral domain that is integrally closed in its fraction field,  $R$  is called integrally closed.

Ex  $\mathbb{Z}$  is integrally closed (since  $\mathbb{Z}$  integrally closed in  $\mathbb{Q}$ )  
 $\mathbb{Z}$  is not integrally closed in  $\mathbb{Q}$ , since  $i$  is integral over  $\mathbb{Z}$ .

Ex If  $R \subset S$  is integral,  $\bar{R}$  is integrally closed in  $S$ .

Ex Every UFD is integrally closed. In particular,  $k[x_1, \dots, x_n]$  is integrally closed.

Let  $R$  be a UFD,  $\frac{a}{b} \in \text{frac } R$  integral with  $(a, b) = 1$ .

$$\left(\frac{a}{b}\right)^n + c_{n-1}\left(\frac{a}{b}\right)^{n-1} + \dots + c_1\left(\frac{a}{b}\right) + c_0 = 0 \quad \text{for some } n, c_i \in R.$$

$$\begin{aligned} a^n &= -c_{n-1}a^{n-1}b - \dots - c_1ab^{n-1} - c_0b^n \\ &= b(-c_{n-1}a^{n-1} - \dots - c_1ab^{n-1} - c_0b^{n-1}) \end{aligned}$$

Every irreducible component of  $b$  must divide  $a$ , but  $(a, b) = 1$ , so  $b \in R^*$   
 i.e.  $\frac{a}{b} \in R$ .

Thm 5.8 Let  $R$  be an integral domain,  $S \subset R$  multiplicative.

If  $R$  is integrally closed, so is  $S^{-1}R$ .

pf Note  $\text{frac}(S^{-1}R) = \text{frac}(R)$

Let  $\frac{a}{b} \in \text{frac}(S^{-1}R) = \text{frac}(R)$  be integral over  $S^{-1}R$

$$\left(\frac{a}{b}\right)^n + \frac{s_{n-1}}{s_1}\left(\frac{a}{b}\right)^{n-1} + \dots + \frac{s_1}{s_1}\left(\frac{a}{b}\right) + \frac{s_0}{s_0} = 0$$

for some  $\frac{s_i}{s_j} \in S^{-1}R$  (so  $s_i \in S, p_i \in R$ )

Let  $S = s_0 \dots s_{n-1} \in S$ , multiply through by  $S^n$ .

$$\left(\frac{s_0 a}{b}\right)^n + \frac{s_{n-1}}{s_1}\left(\frac{s_0 a}{b}\right)^{n-1} + \dots + \frac{s_1^n}{s_1}\left(\frac{s_0 a}{b}\right) + \frac{s_0^n}{s_0} = 0 \quad \text{so } \frac{s_0 a}{b} \text{ is integral over } R.$$

Thus  $\frac{s_0 a}{b} \in R \subset S^{-1}R$ , so  $\frac{1}{s_0} \cdot \left(\frac{s_0 a}{b}\right) = \frac{a}{b} \in S^{-1}R$ .

□

Big Idea! Integral extensions play nice with prime ideals

Let  $R \subset S$  be a ring extension. If  $J \subset S$  is a proper ideal,  
 $I = J \cap R$  is a proper ideal of  $R$ . We say  $J$  lies over  $I$ .

If  $Q \subset S$  is a prime ideal,  $Q \cap R$  is a prime ideal of  $R$ .

Thm 5.9 (Lying over theorem) Let  $R \subset S$  be an integral extension,  $P \subset R$  a prime ideal.  
 There is a prime ideal  $Q \subset S$  lying over  $P$  (i.e.  $Q \cap R = P$ ).

PF Let  $C = \{I \subset S \mid I \cap (R \setminus P) = \emptyset\}$

~~then  $C$  has a maximal element~~  
 Thm 7.2  $\Rightarrow C$  has a maximal element  $Q$  which is a prime ideal of  $S$ .

Since  $Q \cap (R \setminus P) = \emptyset$ ,  $Q \cap R \subset P$

Suppose for contradiction there exists  $u \in P$  with  $u \notin Q$ .

Then  $Q \subset Q + uS$  ~~proper~~, so  $Q + uS \notin C$

Thus there exists  $c \in (Q + uS) \cap R \setminus P$

write  $c = q + us$  for some  $q \in Q, s \in S$ .

Substn  $\Rightarrow s^n + r_1 s^{n-1} + \dots + r_n s + r_{n+1} = 0$  for some  $r_i \in R$

$$(sq)^n + (r_1 u)(sq)^{n-1} + \dots + (r_n u^n)(sq) + (r_{n+1} u^n) = 0$$

Substitute  $sq = c - q$ ;  $sq$  is mod  $Q$ , we see (since  $q \in Q$ )

$$v := c^n + (r_1 u) c^{n-1} + \dots + (r_n u^n) c + (r_{n+1} u^n) \in Q.$$

Since  $c, u, r_i \in R$ , we have  $v \in Q \cap R = P$

Then  $u \in P \Rightarrow c^n \in P \Rightarrow c \in P$  since  $P$  prime.  $\downarrow \square$

Cor S.10 (Going-up Theorem) Let  $R \subset S$  be an integral extension, and  $P_1 \subset P \subset R$  two prime ideals. If  $Q \subset S$  lies over  $P_1$ , then there exists a prime ideal  $Q'$  lying over  $P$  with  $Q' \subset Q$ .

pf  $R/P_1 \subset S/Q_1$  is integral.

Lying over  $\Rightarrow$  there exists prime ideal  $Q'/Q_1$  lying over  $P/P_1$ .  
Then  $Q'$  lies over  $P$ .

Thm S.11 Let  $R \subset S$  be an integral extension,  $P \subset R$  prime. Suppose  $Q_1, Q_2 \subset S$  are prime ideals lying over  $P$ . If  $Q_1 \subset Q_2$ , then  $Q_1 = Q_2$ .

pf Let  $\mathcal{C} = \{I \subset S \mid I \text{ lies over } P\}$ . Suffices to prove:

Claim If  $Q \in \mathcal{C}$  is prime, then  $Q$  is maximal in  $\mathcal{C}$ .

pf Suppose not: there exists  $I \in \mathcal{C}$  with  $Q \subsetneq I$ .

Let  $u \in I \setminus Q$ . ~~Since  $S$  is integral~~

~~$u^n + r_{n-1}u^{n-1} + \dots + r_1u + r_0 = 0$  for some  $r_i \in R$~~

~~which is not in  $Q$~~

~~Now  $r_0 \in I \cap R = P \subset Q$ .~~

~~Then~~

Let  $f \in \{g \in R[x] \mid g \text{ monic, } g(u) \in Q\}$ . Nonempty since  $S$  integral.  
have minimal degree

$f(u) = u^n + r_{n-1}u^{n-1} + \dots + r_1u + r_0 \in Q \subset I$  for some  $r_i \in R$

Since  $u \in I$ , we have  $r_0 \in I \cap R = P \subset Q$ .

Then  $u(u^{n-1} + r_{n-1}u^{n-2} + \dots + r_1) \in Q$

Since  $u^{n-1} + r_{n-1}u^{n-2} + \dots + r_1$  has smaller degree than  $f$ , not in  $Q$ .

then  $Q$  prime  $\Rightarrow u \in Q \nmid$



Thm 5.12 Let  $R \subset S$  be an integral extension, and suppose  $P \subset R$  is prime, and  $Q \subset S$  is prime lying over  $P$ . Then  $Q$  is a maximal ideal of  $S$  if and only if  $P$  is a maximal ideal of  $R$ .

pf  $\Rightarrow$  Suppose  $Q$  is a maximal ideal.

Let  $M \subset R$  be a maximal ideal containing  $P$ .

(going up  $\Rightarrow$ ) There is a prime ideal  $Q' \subset S$  lying over  $M$  with  $Q \subset Q'$ , so  $Q = Q'$ .  
Then  $P = Q \cap R = Q' \cap R = M$ , so  $P$  is maximal.

$\Leftarrow$  Suppose  $P$  is a maximal ideal.

Let  $N \subset S$  be a maximal ideal containing  $Q$ .

Then  $P = Q \cap R \subset N \cap R$ , and since  $P$  is maximal,  $P = N \cap R$ .

Thus  $N$  and  $Q$  lie over  $P$  with  $Q \subset N \Rightarrow Q = N$  i.e.  $Q$  is maximal.  $\square$

Thm 7.2 (Noether Normalization Lemma) Let  $k$  be a field,  $R = k[u_1, \dots, u_n]$  a fin. dim. l.d.g.  
Assume  $R$  is an integral domain, and let  $r$  be transcendence degree of  $\text{frac } R$  over  $k$ .  
Then there exists an algebraically independent subset  $\{t_1, \dots, t_r\} \subset R$   
such that  $R$  is integral over  $k[t_1, \dots, t_r]$

pf For  $\text{frac } R = k(u_1, \dots, u_n)$ . If  $\{u_1, \dots, u_n\}$  is algebraically independent over  $k$ , then  $r = n$ , and  $R$  is trivially integral over  $k[u_1, \dots, u_n]$ .  
So assume  $\{u_1, \dots, u_n\}$  algebraically dependent over  $k$ . (so  $r < n$ )

$$\sum_{(i_1, \dots, i_n) \in I} K_{i_1, \dots, i_n} u_1^{i_1} \dots u_n^{i_n} = 0 \quad \text{for some finite set } I, \quad K_{i_1, \dots, i_n} \in k^*$$

Let  $c \in \mathbb{N}$  such that  $c > i_j$  for all  $j$ ,  $(i_1, \dots, i_n) \in I$ .

Consider  $J = \{i_1 + ci_2 + \dots + c^{n-1}i_n \mid (i_1, \dots, i_n) \in I\}$

Claim  $|J| = |I|$

pf Suppose  $i_1 + ci_2 + \dots + c^{n-1}i_n = j_1 + cj_2 + \dots + c^{n-1}j_n$  for some  $(i_1, \dots, i_n), (j_1, \dots, j_n) \in I$ .



Then  $c | \hat{u}_1 - j_1$ , but  $c > \hat{c}_1$ ,  $c > \hat{j}_1$ , so  $\hat{c}_1 = \hat{j}_1$ .

$$\text{then } \hat{c}_2 + \dots + \hat{c}^{n-1} \hat{c}_n = \hat{c}_2 + \dots + \hat{c}^{n-1} \hat{j}_n$$

$$\hat{c}_2 + \dots + \hat{c}^{n-2} \hat{c}_n = \hat{j}_2 + \dots + \hat{c}^{n-2} \hat{j}_n$$

Same argument  $\Rightarrow \hat{c}_2 = \hat{j}_2, \dots, \hat{c}_n = \hat{j}_n$ .

Let  $j_1 + c j_2 + \dots + c^{n-1} j_n \in J$  be ~~maximal~~ maximum element.

$$\text{Set } v_2 = u_2 - u_1^c, \quad v_3 = u_3 - u_1^{c^2}, \quad \dots, \quad v_n = u_n - u_1^{c^{n-1}}$$

$$\sum_{(i_1, \dots, i_n) \in \Sigma} K_{i_1, \dots, i_n} u_1^{i_1} (v_2 + u_1^c)^{i_2} (v_3 + u_1^{c^2})^{i_3} \dots (v_n + u_1^{c^{n-1}})^{i_n} = 0$$

$$K_{i_1, \dots, i_n} u_1^{j_1 + c j_2 + c^2 j_3 + \dots + c^{n-1} j_n} + \underbrace{f(u_1, v_2, \dots, v_n)}_{\deg_{u_1} f < j_1 + c j_2 + c^2 j_3 + \dots + c^{n-1} j_n} = 0$$

$\Rightarrow u_1$  is integral over  $k[v_2, \dots, v_n]$

~~So  $k[u_1, v_2, \dots, v_n]$  is integral over  $k[v_2, \dots, v_n]$~~

So  $k[u_1, v_2, \dots, v_n]$  is integral over  $k[v_2, \dots, v_n]$

Also  $u_2, \dots, u_n$  integral over  $k[u_1, v_2, \dots, v_n]$

Then  $k[u_1, \dots, u_n]$  is integral over  $k[v_2, \dots, v_n]$

IF  $\{v_2, \dots, v_n\}$  is algebraically independent, result follows as des.

Otherwise: Let  $R_1 = k[v_2, \dots, v_n]$

Repeat to produce  $R_1$  integral over  $k[v_3, \dots, v_n]$ .

IF  $\{v_3, \dots, v_n\}$  is algebraically independent done. otherwise, repeat...




## § 7 Hilbert's Nullstellensatz

Let  $k$  be a field throughout.


Def If  $S \subset k[x_1, \dots, x_n]$ , the variety set of  $S$  is

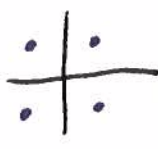
$$V(S) = \{ (a_1, \dots, a_n) \in k^n \mid f(a_1, \dots, a_n) = 0 \text{ for all } f \in S \}.$$

It is called an algebraic set

Ex  $V(y - x^2)$  

Ex  $V(y^2 - x^2)$   "reducible"

Ex  $V(\{x-2, y-1\})$  

Ex  $V(\{x^2 + y^2 - 8, y^2 - x^2\})$  

Ex  $V(k^2) = V(\emptyset)$

Remark If  $I = (S)$  is ideal generated by  $S$ , then  $V(S) = V(I)$   
 $\Rightarrow$  Every algebraic set is variety set of a finite set of poly's.

Conversely: Given  $Y \subset k^n$ , define

$$I(Y) = \{ f \in k[x_1, \dots, x_n] \mid f(a_1, \dots, a_n) = 0 \text{ for all } a_1, \dots, a_n \in Y \}.$$

Note  $I(Y)$  is always an ideal

Lemma 7.1 Let  $k$  be algebraically closed,  $S, T \subset k[x_1, \dots, x_n]$ ,  $x, y' \in k^*$

(i)  $V(k[x_1, \dots, x_n]) = \emptyset$

$I(k^*) = 0$

$I(\emptyset) = k[x_1, \dots, x_n]$

(ii)  $S \subset T \Rightarrow V(S) \supset V(T)$

$x \subset y' \Rightarrow I(x) \supset I(y')$

(iii)  $S \subset I(V(S))$  and  $x \subset V(I(x))$

(iv)  $V(S) = V(I(V(S)))$  and  $I(x) = I(V(I(x)))$

PF (iv) (iii)  $\Rightarrow V(S) \subset V(I(V(S)))$   
 Also,  $S \subset I(V(S))$ , so  $V(S) \supset V(I(V(S)))$

(iii)  $\Rightarrow I(x) \subset I(V(I(x)))$

Also,  $x \subset V(I(x)) \Rightarrow I(x) \supset I(V(I(x)))$

Observation If  $X = V(S)$  is an algebraic set,  $V(I(X)) = X$ .

Q: For what kind of ideals  $J$  is  $I(V(J)) = J$ ?

A: Nullstellensatz  $\Rightarrow$  radical ideals!

Lemma 7.3 (Weak Nullstellensatz) Let  $k$  be algebraically closed,  $I \subset k[x_1, \dots, x_n]$  a proper ideal. Then  $V(I) \neq \emptyset$ .

PF Let  $P \supset I$  be prime. Suffices to show  $V(P) \neq \emptyset$ , since  $V(P) \subset V(I)$ .

Let  $R = k[x_1, \dots, x_n]/P = k[u_1, \dots, u_n]$

Weak Nullstellensatz  $\Rightarrow R$  integral over  $k[t_1, \dots, t_r]$  and  $\{t_1, \dots, t_r\}$  are independent and

Let  $M = (t_1, \dots, t_r) \subset S$ , a maximal ideal.

There is a maximal ideal  $N \subset R$  lying over  $M$ .

Let  $\gamma: R \rightarrow R/\mathfrak{p}$  be quotient; note  $\gamma(R) \cong R/\mathfrak{p}$  is a field.

Then  $R \cong k[t_1, \dots, t_r]/\mathfrak{p} = k[t_1, \dots, t_r]/N \cap k[t_1, \dots, t_r] \cong \frac{(k[t_1, \dots, t_r] + \mathfrak{p})}{N} = \gamma(k[t_1, \dots, t_r])$   
 $\uparrow$   
 Second Isom.

Since  $R$  integral over  $k[t_1, \dots, t_r]$ ,  $\gamma(R)$  algebraic over  $\gamma(k[t_1, \dots, t_r])$

$\Rightarrow \gamma(R) = \gamma(k[t_1, \dots, t_r]) = k$ .

$$k[x_1, \dots, x_n] \xrightarrow{\varphi} R \xrightarrow{\gamma} k$$

Call this composition  $\varphi$ .

Then  $(\varphi(x_1), \dots, \varphi(x_n)) \in V(\mathfrak{p})$ , since for all  $f \in \mathfrak{p}$ ,  $\varphi(f) = f(\varphi(x_1), \dots, \varphi(x_n)) = 0$ .

Ex  $I_n \subset \mathbb{R}[x]$ ,  $V(x^2+1) = \emptyset$ , but in  $\mathbb{C}[x]$ ,  $V(x^2+1) = \{i, -i\}$

Hilbert's Nullstellensatz Let  $k$  be algebraically closed,  $J \subset k[x_1, \dots, x_n]$  a proper ideal.  
 Then  $I(V(J)) = \text{rad}(J)$ .

PG  $\supset$  Let  $f \in \text{rad}(J)$ , so  $f^m \in J$  for some  $m \geq 1$ .

If  $(a_1, \dots, a_n) \in V(J)$ , then  $0 = f^m(a_1, \dots, a_n) = (f(a_1, \dots, a_n))^m \Leftrightarrow f(a_1, \dots, a_n) = 0$

Thus  $f \in I(V(J))$

$\subset$  Let  $f \in I(V(J))$ . wlog,  $f \neq 0$

Define  $L \subset k[x_1, \dots, x_n, y]$  by  $L = (J, yf-1)$  "Rabinowitsch trick"

Claim  $V(L) \subset k^{n+1}$  is empty.

If  $(a_1, \dots, a_n, b) \in V(L)$ , then  $(a_1, \dots, a_n) \in V(J)$ , so  $f(a_1, \dots, a_n) = 0$

$$\Rightarrow b f(a_1, \dots, a_n) - 1 = -1 \neq 0$$

$\Rightarrow L = k[x_1, \dots, x_n, y]$

Then  $1 = \sum_{i=1}^b g_i f_i + g_{b+1}(yf-1)$  for some  $g_i \in k[x_1, \dots, x_n, y]$   
 $f_i \in I$ .

w/Nullstellensatz

Note that  $y^b - 1$  is irreducible, hence prime

fractional field  
↓

$$k[x_1, \dots, x_n, y] \rightarrow k[x_1, \dots, x_n, y] / (y^b - 1) \cong k[x_1, \dots, x_n, \frac{1}{f}] \rightarrow k(x_1, \dots, x_n)$$

Apply this map

$$1 = \sum_{i=1}^b g_i(x_1, \dots, x_n, \frac{1}{f}) f_i(x_1, \dots, x_n)$$

Fix  $m = \max \{ \deg_y g_i \}$ , so  $f^m(x_1, \dots, x_n) g_i(x_1, \dots, x_n, \frac{1}{f}) \in k[x_1, \dots, x_n]$  for each  $i$ .

$$\text{Then } f^m = \sum_{i=1}^b (f^m g_i(x_1, \dots, x_n, \frac{1}{f})) f_i(x_1, \dots, x_n) \in \mathcal{I}$$

So  $f \in \text{rad}(\mathcal{I})$ .

□

## Algebraic Sets $\longleftrightarrow$ Radical Ideals

Def An algebraic set  $X$  is called irreducible if whenever  $X = X_1 \cup X_2$  for algebraic sets  $X_1, X_2$ , then  $X = X_1$  or  $X = X_2$ .

Lemma An algebraic set  $X$  is irreducible if and only if  $\mathcal{I}(X)$  is prime.

Pf  $\Leftarrow$  Let  $P \subset \mathcal{I}(X)$  be prime. Note  $X = V(\mathcal{I}(X)) = V(P)$ .

Suppose  $X = X_1 \cup X_2$ , and  $X \neq X_1$  (we will show  $X = X_2$ ).

$$\text{Then } P = \mathcal{I}(V(P)) = \mathcal{I}(X_1 \cup X_2) = \mathcal{I}(X_1) \cap \mathcal{I}(X_2).$$

Let  $\lambda \in \mathcal{I}(X_1)$  but  $\lambda \notin \mathcal{I}(X_2)$ . If  $\mathcal{I}(X) \supset \mathcal{I}(X_1)$ , then  $X = V(\mathcal{I}(X)) = V(\mathcal{I}(X_1)) = X_1$   $\downarrow$  so let  $f \in \mathcal{I}(X) \setminus \mathcal{I}(X_1)$ .

Now, for any  $g \in \mathcal{I}(X_2)$ ,  $fg \in \mathcal{I}(X_1) \cap \mathcal{I}(X_2) = P$ , so  $P \text{ prime} \Rightarrow g \in P$ .

Thus  $\mathcal{I}(X_2) \subset P \subset \mathcal{I}(X_2)$ , so  $\mathcal{I}(X) \supset P = \mathcal{I}(X_2) \Rightarrow X = X_2$ .

$\Rightarrow$  Suppose  $X$  is irreducible. Let  $f, g \in R$  with  $fg \in \mathcal{I}(X)$ .

$$\text{Then } X \subset V(fg) = V(f) \cup V(g)$$

$$\text{so } X = (X \cap V(f)) \cup (X \cap V(g))$$

$X$  irreducible  $\Rightarrow$

$$X = X \cap V(f) \Rightarrow X \subset V(f) \Rightarrow f \in I(X)$$

OR  $X = X \cap V(g) \Rightarrow X \subset V(g) \Rightarrow g \in I(X)$

Def An irreducible algebraic set is called an affine variety.

Affine varieties  $\longleftrightarrow$  Prime ideals of  $k[x_1, \dots, x_n]$

Observe: (1) A finite union of algebraic sets is an algebraic set (since  $V(I_1) \cup \dots \cup V(I_n) = V(I_1 \cap \dots \cap I_n)$ )  
(2) An arbitrary intersection of algebraic sets is an algebraic set (since  $\bigcap V(I_i) = V(\bigcup I_i)$ )  
(3)  $\emptyset$  and  $k^n$  are algebraic sets

Def  $A^n_k$  is the topological space on the set  $k^n$  with algebraic sets being closed sets. This topology is called the Zariski topology.

## Morphisms

Ex  $\theta: A^1 \rightarrow A^1$

For  $f \in k[x_1, \dots, x_n]$ , define  $\theta(a_1, \dots, a_n) = f(a_1, \dots, a_n)$

Proper closed set in  $A^1$   $\{p\}$

$$\theta^{-1}(\{p\}) = \{(a_1, \dots, a_n) \in A^1 \mid f(a_1, \dots, a_n) = p\} = \{(a_1, \dots, a_n) \in A^1 \mid f(a_1, \dots, a_n) - p = 0\} = V(f-p)$$

So  $\theta$  is continuous

Similarly, if  $f_1, \dots, f_m \in k[x_1, \dots, x_n]$ ,

$$A^n \rightarrow A^m$$

$$(a_1, \dots, a_n) \mapsto (f_1(a_1, \dots, a_n), \dots, f_m(a_1, \dots, a_n)) \text{ is continuous.}$$

Def Let  $X \subset A^n$  and  $Y \subset A^m$  be affine varieties.

A map  $q: X \rightarrow Y$  is called a morphism

if there exist  $f_1, \dots, f_m \in k[x_1, \dots, x_n]$  s. t.

$$q(a_1, \dots, a_n) = (f_1(a_1, \dots, a_n), \dots, f_m(a_1, \dots, a_n))$$

for all  $(a_1, \dots, a_n) \in X$ .

Ex Let  $X = V(y - x^2) \subset A^2$

$$q: A^2 \rightarrow A^1$$

$(x, y) \mapsto x$  is a morphism

$$\psi: A^1 \rightarrow A^2$$

$t \mapsto (t, t^2)$  is a morphism

Def Let  $X = V(P) \subset \mathbb{A}^n$  be an affine variety. The coordinate ring of  $X$ , denoted  $\Gamma(X)$  or  $k[X]$ , is the ring of regular functions on  $X$ , i.e. morphisms  $X \rightarrow \mathbb{A}^1$   $\Gamma(X) = \text{Hom}(X, \mathbb{A}^1)$

If  $\varphi_1, \varphi_2: X \rightarrow \mathbb{A}^1$  are two morphisms, given by poly's  $f_1, f_2 \in k[x_1, \dots, x_n]$

$$\varphi_1 = \varphi_2 \iff f_1(a_1, \dots, a_n) = f_2(a_1, \dots, a_n) \text{ for all } (a_1, \dots, a_n) \in V(P)$$

$$\iff (a_1, \dots, a_n) \in V(f_1 - f_2) \text{ for all } (a_1, \dots, a_n) \in V(P)$$

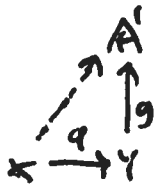
$$\iff V(P) \subset V(f_1 - f_2)$$

$$\iff f_1 - f_2 \in P$$

$$\text{So } \Gamma(X) = k[x_1, \dots, x_n] / P$$

Prop Let  $X, Y$  be affine varieties. Then  $\text{Hom}(X, Y) \cong \text{Hom}_k(\Gamma(Y), \Gamma(X))$

pf Let  $\varphi: X \rightarrow Y$  be a morphism. Let  $g \in \Gamma(Y) = \text{Hom}(Y, \mathbb{A}^1)$



then  $g \circ \varphi \in \text{Hom}(X, \mathbb{A}^1) = \Gamma(X)$

Suppose  $\lambda \in \text{Hom}_k(\Gamma(Y), \Gamma(X))$ . write  $X = V(P) \subset \mathbb{A}^n$ ,  $Y = V(Q) \subset \mathbb{A}^m$

$$\lambda: k[x_1, \dots, x_m] / Q \rightarrow k[x_1, \dots, x_n] / P$$

$$\text{Choose } f_i \in k[x_1, \dots, x_n] \text{ with } \lambda(x_i + Q) = f_i + P$$

$$\text{Set } \lambda^*: X \rightarrow Y \\ (f_1, \dots, f_m)$$

$\lambda^*$  is well defined on  $X = V(P)$

$$\begin{aligned} \text{If } g \in Q = I(Y), \text{ and } (a_1, \dots, a_n) \in X, \text{ then } g(\lambda^*(a_1, \dots, a_n)) &= g(f_1(a_1, \dots, a_n), \dots, f_m(a_1, \dots, a_n)) \\ &= g(\lambda(x_1 + Q)|_{a_1, \dots, a_n}, \dots, \lambda(x_m + Q)|_{a_1, \dots, a_n}) \\ &= \lambda(g + Q)|_{a_1, \dots, a_n} \\ &= \lambda(0 + Q) \\ &= 0 \end{aligned}$$



Prop There is a contravariant functor between affine varieties and finitely generated integral domains over  $k$ .

Ex Consider  $Q: A[x, y, z] \rightarrow A[t]$   
 $(t^3, t^4, t^5 + t)$

Then  $Q^*: A' \rightarrow A'$   
 $t \mapsto (t^3, t^4, t^5 + t)$

Ex Suppose  $\text{char } k = p > 0$

Define  $Q: A' \rightarrow A'$   
 $t \mapsto t^p$

This is a bijection. But  $Q^*: A[x] \rightarrow A[x]$   
 $x \mapsto x^p$  is not surjective!

So  $Q$  is not an isomorphism of varieties.

Ex  $Q: \mathbb{C} \rightarrow \mathbb{C}^2$   
 $t \mapsto (t^2, t^3)$

Then  $Q^*: \mathbb{C}[x, y] \rightarrow \mathbb{C}[t]$   
 $(t^2, t^3)$  so  $\text{Im } Q^* = \mathbb{C}[t^2, t^3] \neq \mathbb{C}[t]$

Really  $Q: \mathbb{C} \rightarrow V(x^3 - y^2)$  is a bijection, but not an isomorphism

$Q^*: \mathbb{C}[t^2, t^3] \rightarrow \mathbb{C}[t]$

## Dimension

Def If  $X$  is a variety, the function field of  $X$  is  $k(X) = \text{frac } \Gamma(X)$

Def If  $X$  is a variety, the dimension of  $X$  is  $\text{trdeg}_k k(X)$ .

If  $k$  is algebraically closed, TFAE

- (1)  $\dim X = 0$
- (2)  $k(X) = k$
- (3)  $X$  is a point

Prop Let  $Y \subset X$  be a proper (closed) subvariety. Then  $\dim Y < \dim X$

Lemma Let  $R$  be an integral  $d$ -domain,  $P \subset R$  prime. Then  
 $\text{trdeg } R \geq \text{trdeg } R/P$ , with equality only if  $P=0$  or  $\dim R$  is infinite.

Pr Assume  $P \neq 0$ ,  $\text{trdeg } R = n < \infty$ .

Suppose for contradiction  $\text{trdeg } R/P = n$ .

Then exist  $x_1, \dots, x_n \in R$  s.t.  $\bar{x}_1, \dots, \bar{x}_n \in R/P$  are algebraically independent.

For any  $p \in P \setminus \{0\}$ ,  $p, x_1, \dots, x_n$  must be al. dep.

Then  $f(p, x_1, \dots, x_n) = 0$  for some (nonzero irreducible)  $f \in k[y_0, \dots, y_n]$

Then  $\bar{f}(0, \bar{x}_1, \dots, \bar{x}_n) = 0$  in  $R/P \Rightarrow \bar{f} = 0$ , i.e.  $f \in (y_0) \Rightarrow f = y_0 \cdot g$   
 $\Rightarrow p = 0$   $\square$

Def If  $Y \subset X$ , the codimension of  $Y$  in  $X$  is  $\dim X - \dim Y$

Thm Let  $X$  be an affine variety,  $g \in \Gamma(X)$  non-zero. Then  $V(g) \subset X$  has codimension 1.

Krull's Principal Ideal Theorem Let  $R$  be a f.g.  $k$ -algebra and an integral domain.

If  $f \in R^{(n)}$  and  $P$  is a minimal prime over  $(f)$ , then  $\text{trdeg}_k R/P = \text{trdeg}_k R - 1$

Def Let  $\varphi: X \rightarrow Y$  be a morphism of affine varieties.

$\varphi$  is called finite if  $\Gamma(X)$  is integral over  $\varphi^*(\Gamma(Y))$ .

Prop Let  $\varphi: X \rightarrow Y$  be a finite morphism of affine varieties

1)  $\varphi$  maps closed sets to closed sets

2) For all  $y \in Y$ ,  $\varphi^{-1}(y)$  is finite.

3)  $\varphi$  is surjective if and only if  $\varphi^*: \Gamma(Y) \rightarrow \Gamma(X)$  is injective.

pf  ~~$\varphi$  maps closed sets to closed sets,  $\varphi^{-1}(y)$  is finite, and  $\varphi$  is surjective~~

(10/11)

Noether Normalization Lemma

Let  $X$  be an affine variety of dimension  $n$ .

Then there is a finite surjective morphism  $X \rightarrow \mathbb{A}^n$ .