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) $\quad a(b+c) = ab + ac$ $\qquad$ for all $a, b, c \in R$.
$\qquad (a+b)c = ac + bc$

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

Thm 1.2 Let R be a ring.

(i) $\quad 0 \cdot a = a \cdot 0 = 0$ $\quad$ for all $a \in R$

(ii) $\quad (-a)b = a(-b) = -(ab)$ for all $a, b \in R$

(iii) $\quad (-a)(-b) = ab$ $\qquad$ for all $a, b \in R$

(iv) $\quad (na)b = a(nb) = n(ab)$ for all $n \in \mathbb{Z}$, $a, b \in R$.

(v) $\quad \left(\sum_{i=1}^{n} a_i \right)\left(\sum_{j=1}^{m} b_j \right) = \sum_{i=1}^{n} \sum_{j=1}^{m} a_i b_j$ $\quad$ 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 $\qquad\qquad\qquad\qquad \blacksquare$

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

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

Ex $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ is also 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 $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in M_2(R)$ is a unit $\left(\text{since } \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right)$

Def 1.5 A commutative ring with $1 \neq 0$ and no zerodivisors is called an __integral domain__. A ring R 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 $f: R \to S$ is called a __homomorphism__ if
$$f(a+b) = f(a) + f(b)$$
$$f(ab) = f(a) f(b)$$
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 $\operatorname{char} R = n$. Otherwise, say R has characteristic 0.

Ex $\operatorname{char} \mathbb{Z}_n = n$

Thm 1.9 Let R be a unital ring with char $R = n > 0$

   (i) Let $\varphi: \mathbb{Z} \to R$ be the map given by $\varphi(m) = m \cdot 1$.
      φ is a homomorphism with kernel $\ker \varphi = \langle n \rangle$

   (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 $m \in \ker \varphi$, $ma = m \cdot 1 \cdot a = 0 \cdot a = 0$ for all $a \in R$.
         By assumption, $m \geq n$. 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 $k \cdot a = k \cdot 1 \cdot a = 0a = 0$ for all $a \in R$.

   (iii) Suppose $n = kr$ for some $k, r \in \mathbb{N}$.
        Then $0 = n \cdot 1 = kr \cdot 1 = k1 \cdot r1$ □

§2 Ideals

   Obyne: If $x, y \in \ker \varphi$, $x+y$, $xy \in \ker \varphi$
   But also   If $a \in R$, $x \in \ker \varphi$, $ax \in \ker \varphi$

Def 2.1 Let R be a ring. A <u>subring</u> is a subset that is itself a ring.
   A left <u>ideal</u> I is a subring satisfying: if $x \in R$, $a \in I$, $xa \in I$
   A <u>right ideal</u> I is a subring satisfying: if $a \in I$, $x \in R$, $ax \in I$
   A (two-sided) <u>ideal</u> is a subring that is both a left and right ideal.

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

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

$\underset{\|}{\underset{0}{}}$

Cor 2.3 The intersection of ideals is an ideal.

Def 2.4 Let $X \subseteq R$ be a subset. Let $\{A_i\}_{i \in \mathbb{Z}}$ be the collection of all ideals containing X.

Then $(X) = \bigcap_{i \in \mathbb{Z}} A_i$ is called the ideal _generated by_ X.

If $X = \{x_1, \ldots, x_n\}$, we write $(x_1, \ldots, x_n)$ and say it is _finitely generated_.

A _principal ideal_ is an ideal generated by a single element.

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

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

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

Thm 2.6 Let I, J be (left) ideals of a ring R.
(i) $I + J = \{x + y \mid x \in I, y \in J\}$ is a (left) ideal
(ii) $IJ = \{\sum x_i y_i \mid x_i \in I, y_i \in J\}$ is a (left) ideal.

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

Pf well-defined: Suppose $a + I = a_0 + I$, $b + I = b_0 + I$
$a = a_0 + x$ for some $x \in I$ $\qquad$ $b = b_0 + y$ for some $y \in J$

Then $a_0 b_0 + I = (a-x)(b-y) + I = ab - ay - xb + xy + I = ab + I$.
$\underset{I}{\uparrow} \quad \underset{I}{\uparrow} \quad \underset{I}{\uparrow}$

$\blacksquare$

Thm 2.8 If $\varphi: R \to S$ 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 $ax \in \ker \varphi$

$\varphi(xa) = \varphi(x)\varphi(a) = \varphi(x) \cdot 0 = 0$, so $xa \in \ker \varphi$ ∎

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

Then $R/\ker\varphi \cong \operatorname{Im}\varphi$

Pf Let $\bar\varphi: R/\ker\varphi \to \operatorname{Im}\varphi$ 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. ∎

Thm 2.13 Let $I \subseteq R$ 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

~~$AB \subseteq P \Rightarrow A \subseteq P$ or $B \subseteq P$ for all ideals~~

$IJ \subseteq P \Rightarrow I \subseteq P$ or $J \subseteq P$ for all ideals $I, J \subseteq R$

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

~~1) If R/P is prime, then R\P is multiplicatively closed, and if ab∈P then a∈P or b∈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 $IJ \subset P$.

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

Let $x \in$ ~~$P \cap J$~~ $I \backslash P$. Let $y \in J$.

Then $xy \in IJ \subset P$, 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__ ~~that so~~ $(a)(b) \subset P$

If $x \in (a)(b)$, $x = a r_1 \, b r_2$ for some $r_1, r_2 \in R$

$= (ab) r_1 r_2 \in P$.

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

__Cor__ Let R be a commutative unital ring. Then ● ~~(003)~~ (0) is prime iff R is an integral domain.

Pf Let $a, b \in R \backslash (0)$. Then (0) is prime iff $ab = 0$ implies $a = 0$ or $b = 0$ iff R is an integral domain. ∎

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

__Thm 2.16__ Let R be a commutative, unital 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 ∎ ∎

(61)

Def 2.17 Let R be a ring. A proper ideal M is called <u>maximal</u> 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 P be the poset of proper ideals of R ordered by inclusion.

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

Claim $C := \bigcup_{i \in \mathcal{I}} C_i$ 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 $a+b, ab \in C_j \subset C$.

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

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

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

Then Zorn $\Rightarrow P$ has a maximal element. $\blacksquare$

Thm 2.19 Let R be a 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
$$1 = m_1 + a r_1 = m_2 + b r_2 \qquad \text{for some } m_1, m_2 \in M, \ r_1, r_2 \in R.$$

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

If $ab \in M$, then $1 \in M$ ⨯ so $ab \notin M$, thus M is prime. $\blacksquare$

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 $\iff R/M$ 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 $(a)+M = R$, so $1 = ar + m$ for some $r \in R$, $m \in M$.
Then $(a+M)(r+M) = ar + M = 1+M$
Thus every nonzero 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 nonzero homomorphism of rings $R \to S$ is injective.

Pf Thm 2.20 gives (i) $\iff$ (iii). Clearly (ii) $\iff$ (iii)
(iv) $\iff$ Either $\ker \varphi = 0$ or $\ker \varphi = R$ $\iff$ (ii)   ∎

(63)

<u>Thm 2.22, 2.23</u> 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.

<u>Thm 2.24</u> Let R be a ring, $I_1, \ldots, I_n \subseteq R$ ideals. Suppose

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

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

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

<u>pf</u> $\varphi: I_1 \times \ldots \times I_n \longrightarrow R$ given by $\varphi(x_1, \ldots, x_n) = x_1 + \ldots + x_n$ 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 $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in I_1 \times \ldots \times I_n$

Then $\varphi(a_1, \ldots, a_n) \varphi(b_1, \ldots, b_n) = (a_1 + \ldots + a_n)(b_1 + \ldots + b_n)$

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

$$= \varphi((a_1, \ldots, a_n)(b_1, \ldots, b_n))$$ □

<u>Thm 2.25</u> ("Chinese Remainder Theorem" — Sun-Tsze, ~400 AD)

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

and $I_i + I_j = R$ for all $i \ne j$; ($I_1, \ldots, I_n$ called <u>pairwise comaximal</u>)

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

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

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

(64)

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

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

$m = 2$: $R = I_1 + I_2$ ✓

$m > 2$: By induction, $R = I_1 + (I_2 \wedge \ldots \wedge I_{m-1})$

$$R^2 = (I_1 + (I_2 \wedge \ldots \wedge I_{m-1}))(I_1 + I_m) \subset I_1 + (I_2 \wedge \ldots \wedge I_m)$$

Since $R \supset R^2 + I_1$, $R = I_1 + (I_2 \wedge \ldots \wedge I_m)$

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

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 $r_k \equiv b_k \mod I_k$ and $r_k \equiv 0 \mod I_i$ for all $i \neq k$.

Let $b = r_1 + \ldots + r_k$.   Then $b \equiv r_k \equiv b_k \mod I_k$ ∎

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

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

$$x \equiv b_1 \mod m_1 \quad \ldots \quad x \equiv b_n \mod m_n$$

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

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

i.e. $\mathbb{Z} = (m_i) + (m_j)$.   ∎

Apply thm 2.25.

§5 Polynomial rings

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

(1) the set of all sequences $(a_0, a_1, a_2, \dots)$ such that $a_i \in R$, only finitely many nonzero

(2) Addition is componentwise

(3) Multiplication given by
$$(a_0, a_1, \dots) \cdot (b_0, b_1, \dots) = (a_0 b_0, \ a_0 b_1 + a_1 b_0, \ a_0 b_2 + a_1 b_1 + a_2 b_0, \ \dots)$$
$$\left(n^{th} \text{ component is } \sum_{i+j=n} a_i b_j \right)$$

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

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

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

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) $x^n = (0,0,\dots,0,1,0,0,\dots)$

$\quad\quad\quad\quad\quad\quad\quad\uparrow$
$\quad\quad\quad\quad\quad n+1\text{-st spot}$

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

(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 denoted $R[x,y]$ (or more generally, $R[x_1,\dots,x_n]$)

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

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

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

Thm 5.5 Let $\varphi_0 : R \to S$ be a homomorphism of commutative unital rings. with $\varphi(1)=1$. Let $s_1,\dots,s_n \in S$. then there is a unique homomorphism

$$\varphi : R[x_1,\dots,x_n] \longrightarrow S \quad\quad\text{s.t. } \varphi|_R = \varphi_0 \text{ and } \varphi(x_i) = s_i.$$

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

Pf ~~$\varphi\left(\sum a_i x^i\right) \in R[x]$ set $\varphi\left(\sum a_i x^i\right) = \sum \varphi_0(a_i)$~~

Suffices to assume $n=1$.

If $\sum_{i=0}^{n} a_i x^i \in R[x]$, set $\varphi\left(\sum_{i=0}^{n} a_i x^i \right) = \sum_{i=0}^{n} \varphi_0(a_i) s^i$

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

This is called the <u>evaluation map</u> or <u>substitution map</u>

§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 & b are called _associates_

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

(i) $a|b \iff (b) \subseteq (a)$

(ii) a and b are associates $\iff (a) = (b)$

(iii) $u \in R^* \iff u|r$ for all $r \in R$.

(iv) $u \in R^* \iff (u) = R$

(v) If R is a domain, a and b are associates $\iff a = bu$ for some $u \in R^*$

Pf   (i) $a|b \iff \bullet b \in (a) \iff (b) \subseteq (a)$

(ii) Immediate from (i)

(iii) $\implies r = u(u^{-1}r)$
   $\impliedby$ If $u|1$, $1 = ux$ for some $x \in R$, i.e. $u \in R^*$

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

(v) $\impliedby$ (Domain not needed) $a = bu \implies b|a$, $b = au^{-1} \implies a|b$
   $\implies a = bx$ and $b = ay$
   then $a = ayx \iff a(1-yx) = 0$ $\implies x, y \in R^*$ ∎

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 • $R = \mathbb{k}[x,y]/(x^2 - y^3)$

y is irreducible

But $y(y^2) = x^2$, so $y | x^2$. 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 $\iff$ (x) is a prime ideal

(ii) x is irreducible $\iff$ (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 $\iff$ x is irreducible.

(v) Associates of primes are prime. Associates of irreducibles are irreducible.

(vi) If x is irreducible and $a|x$, either $a \in R^*$ or $x|a$ (i.e., a is an associate).

Pf (i) Immediate

(ii) $\Rightarrow$ Suppose $(x) \subseteq (y)$. 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 $a, b \in R$. $\cancel{\text{If suppose}}$ then $(x) \subseteq (a)$, 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 $x|ab$, so wolog $x|a$. 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 $k[x,y]/(x^2-y^3)$: $x^2 = y^3$

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 UFD

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

Observe: If R a UFD and x irreducible,

$x | ab \Rightarrow x | a$ or $x | b$ (factor into irreducibles)

so x is prime.

__Thm 3.7__ Every PID is a UFD.

__Lemma 3.6__ A PID is Nötherian, 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 $(x) \subset (a_n) \subset I = (x)$. ∎

__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

$x = p_1 p_2 q_2$ $- p_1 p_2$

$x = p_1 p_2 p_3 q_3$

$\vdots$

(15)

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

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

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

Since R a PID, (p_1) is maximal, so $R/(p_1)$ a field.

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

q_1, p_1 are associate

Then since a domain, cancel, $p_2 \ldots p_r = q_2 \ldots q_s$. Induct. ☐

— ✗ —

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

Def 3.8 ~~Associator~~ An integral domain R is called a __Euclidean domain__ if there exists a function $\varphi : R\backslash\{0\} \to \mathbb{N}$ such that

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

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

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

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

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

Ex $\dfrac{3+4i}{1+2i} = \dfrac{(3+4i)(1-2i)}{5} = \dfrac{11}{5} - \dfrac{2}{5}i$

$\varphi(1+2i) = 2 + \dfrac{1}{5} - \dfrac{2}{5}i$

$(3+4i) = 2(1+2i) + (\dfrac{1}{5} - \dfrac{2}{5}i)(1+2i)$

$= 2(1+2i) + 1$

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

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

With $ac+bd = q_1 \varrho(\beta) + r_1$, $\quad (bc-ad)e = q_2 \varrho(\beta) + r_2$

with $|r_1| \leq \frac{1}{2}\varrho(\beta)$ $\qquad$ with $|r_2| \leq \frac{1}{2}\varrho(\beta)$

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

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

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

Ex $k[x]$ is Euclidean with $\varrho(f) = \deg f$

Do Ex first!

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

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

If $n = m$, $\quad f = \dfrac{a_n}{b_m} g + \sum\limits_{i=0}^{m-1}\left(a_i - \dfrac{a_n}{b_m} b_i\right)x^i$

$\qquad\qquad\qquad\qquad \uparrow q \qquad\qquad\qquad \uparrow r$

If $n > m$: $\quad$ Let $q = \dfrac{a_n}{b_m} x^{n-m}$,

$\qquad$ then $\deg(f - qg) < \deg f$.

$\qquad$ If $\deg(f - qg) < \deg g$, done. $\quad$ Else, $f - qg = q_0 g + r$ $\quad$ ($\deg r < \deg g$ by induction)

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

(72)

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

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

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

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

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

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

Thn 3.9   Euclidean rings are PIDs.

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

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

~~that $qy + r = x - qy \in I$~~ $\implies r = 0$

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 $\mathbb{Q} = \mathbb{Z} \times \mathbb{Z}$?

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

<u>Def 4.1</u> A nonempty subset $S \subset R$ is called <u>multiplicative</u> if it is ~~multiplicatively closed~~
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^+ is multiplicative.

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

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

<u>Thm 4.2</u> Let R be a commutative ring, and $S \subset R$ multiplicative
Define $\sim$ on $R \times S$ by
$\quad (a,b) \sim (c,d)$ if $s(ad - bc) = 0$ for some $s \in S$.

$\sim$ is an equivalence relation

Pf   Reflexive + symmetric ✓
Transitive: Suppose $(a,b) \sim (c,d)$ and $(c,d) \sim (e,f)$ for some $s, t \in S$
$\qquad s(ad - bc) = 0 \qquad\qquad t(cf - de) = 0$

$\qquad\qquad sad = sbc \qquad\qquad\qquad tcf = bde$
$\qquad\qquad\qquad\qquad$ make same

$\qquad sad(tf) = sbc \, tf \qquad sb \, tcf = tde(sb)$

$\qquad\qquad s a d t f - t d e \, s b = 0$
$\qquad\qquad \underline{s t d (af - be) = 0} \qquad\qquad \Rightarrow (a,b) \sim (e,f)$
$\qquad\qquad\qquad\quad ?$
$\qquad\qquad\qquad\quad s$

☐

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

Typically write $\frac{a}{b}$ for elements of $R \times S/\sim$. Write $S'R$ for $R \times S/\sim$.

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

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

(iii) If $0 \in S$, then $S'R = \{0\}$

Thm 4.3 (i) $S'R$ is a commutative unital ring with operations
$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \qquad \text{and} \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

(ii) If R is an integral domain and $0 \notin S$, then $S'R$ is an integral domain.

(iii') If R is an integral domain and $S = R^*$, then $S'R$ is denoted frac R (or sometimes quot R), the <u>field of fractions</u> of R, is a field.

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

$$s(aB-bA)=0 \quad \text{and} \quad t(cD-dC)=0 \text{ for some } s,t \in S$$

then want: $\frac{ad+bc}{bd} = \frac{AD+BC}{BD}$, so $\big((ad+bc)BD - (AD+BC)bd\big)\gamma=0$ for some $\gamma \in S$

$$tdD\, s(aB-bA) + tbB(cD-dC)=0$$
$$st\big((ad+bc)BD - (AD+BC)bd\big)=0 \quad \checkmark$$

want: $\frac{ac}{bd} = \frac{AC}{BD}$ so $(acBD-ACbd)\gamma=0$ for some $\gamma \in S$.

$$(t\,cD)s(aB-bA) + (sbA)(t)(cD-dC)=0$$
$$st(acBD - bdAC)=0 \quad \checkmark$$

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

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

$sac = 0$

$\Rightarrow a = 0$ or $c = 0$

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

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

(note $\frac{s}{s} \in \bar{S}^1 R$ is mult. identity for any $s \in S$). ∎

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

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

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

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

__Thm 4.41__ Let R be commutative, $S \subset R$ multiplicative.

(i) the map $\varphi : R \longrightarrow \bar{S}^1 R$ is a well defined homomorphism

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

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

(ii) If $0 \notin S$ and S contains no zero divisors, φ 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 φ is an isomorphism.

(76)

<u>Pf</u> (i) well defined: need $\frac{rs}{s} = \frac{rt}{t}$ for any $s, t \in S$

• $rst - rst = 0$ ✓

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

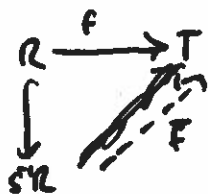$$\varphi(ab) = \frac{abs^2}{s^2} = \frac{as}{s} \cdot \frac{bs}{s} = \varphi(a)\varphi(b)$$

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

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

(ii) s'pose $\varphi(a) = \frac{as}{s} = 0$. Then $as = 0$, so $as = 0$ ⇓ ⇔ $a = 0$.
Thus φ is injective.

(iii) s'pose $S \subset R^+$ and $\frac{r}{s} \in S^{-1}R$. Then $\varphi(\textcircled{r}) rs^{-1}) = \frac{rs \cdot s}{s} = \frac{r}{s}$

<u>Thm 4.5</u> Let R be commutative, $S \subset R$ multiplicative. Let T be a commutative unital ring. Let $f: R \to T$ be a homomorph with $f(S) \subset T^\times$. Then there exists a unique homomorph $\bar{f}: S^{-1}R \to T$ s.t. diagram commutes

$$
\begin{array}{ccc}
R & \xrightarrow{f} & T \\
\downarrow & \nearrow & \\
S^{-1}R & \bar{f} &
\end{array}
$$

<u>Pf</u> Define $\bar{f}(\frac{r}{s}) = f(r) f(s)^{-1}$

well defined: s'pose $\frac{r}{s} = \frac{r_0}{s_0}$, so $t(r s_0 - s r_0) = 0$ for some $t \in S$

$f(t)(f(r) f(s_0) - f(s) f(r_0)) = 0$

$f(r) f(s_0) - f(s) f(r_0) = 0 \cdot f(t)^{-1} = 0$

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

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

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

(77)

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

$\frac{f(\tfrac{r}{s})}{}$

$\tilde{f}\left(\frac{r r_0}{s s_0}\right) = f(r r_0)\, f(s s_0)^{-1} = f(r)f(s)^{-1} f(r_0)f(s_0)^{-1} = \tilde{f}\left(\frac{r}{s}\right)\tilde{f}\left(\frac{r_0}{s_0}\right)$

$\tilde{f}\left(\frac{r}{s} + \frac{r_0}{s_0}\right) = \tilde{f}\left(\frac{r s_0 + r_0 s}{s s_0}\right) = f(r s_0 + r_0 s)\, f(s)^{-1} f(s_0)^{-1}$

$\qquad = \left(f(r) f(s_0) + f(r_0) f(s) \right) f(s)^{-1} f(s_0)^{-1}$

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

$\qquad = \tilde{f}\left(\frac{r}{s}\right) + \tilde{f}\left(\frac{r_0}{s_0}\right)$

Thm 4.7 Let R be commutative, $S \subseteq R$ multiplicative.
  If $I \subseteq R$ is an ideal, then $S^{-1}I = \left\{ \frac{a}{s} \mid a \in I,\, s \in S \right\}$ is an ideal of $S^{-1}R$.

pf Let $\frac{a}{s}, \frac{b}{t} \in S^{-1}I$ (so $a, b \in I$, $s, t \in S$)
  then $\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st} \in S^{-1}I$ since $at + bs \in I$
  If $\frac{x}{u} \in S^{-1}R$, $\frac{x}{u} \cdot \frac{a}{s} = \frac{xa}{us} \in S^{-1}I$ since $xa \in I$.   ∎

Thm 4.8 Let R be commutative, unital ring, $S \subseteq R$ multiplicative, $I \subseteq R$ 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.
  $\Longleftarrow$ If $s \in S \cap I$, then $1 = \frac{s}{s} \in S^{-1}I$, so $S^{-1}I = S^{-1}R$
  $\Longrightarrow$ ~~homomorphism~~
  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 $a \in I$, $t \in S$
  $\qquad\qquad\qquad\qquad t_0(st - as) = 0$ for some $t_0 \in S$
  $\qquad\qquad\qquad\qquad$ Then $\underset{I}{\underset{\uparrow}{a s t_0}} = t_0 \underset{S}{\underset{\uparrow}{s t}}$ $\in I \cap S$.   ∎

Lemma 4.9 Let R be commutative, unital, $S \subset R$ multiplicative.

(i) Every ideal in $S^{-1}R$ is of form $S^{-1}I$ for some ideal $I \subset R$.

(ii) If $P \subset R$ is a prime ideal, and $S \cap P = \emptyset$, then $S^{-1}P$ is a prime ideal.

Pf (i) Let $J \subset S^{-1}R$ be an ideal. Fix some $e \in S$, so $\frac{e}{e}$ is identity in $S^{-1}R$.

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

(i) I is an ideal: Let $r, s \in I$. Then $\frac{re}{e}, \frac{se}{e} \in J$, so $\frac{re}{e} + \frac{se}{e} = \frac{re^2 + se^2}{e^2} = \frac{(r+s)e^2}{e^2} = \frac{(r+s)e}{e} \in J$, so $r+s \in I$.

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

(ii) $J = S^{-1}I$:

If $\frac{a}{s} \in J$, then $\frac{a}{s} \cdot \frac{se}{e} = \frac{ae}{e} \in J$, so $a \in I$ and $\frac{a}{s} \in S^{-1}I$.

If $\frac{a}{s} \in S^{-1}I$, $a \in I$, so $\frac{ae}{e} \in J$, then $\frac{ae}{e} \cdot \frac{s}{s^2} = \frac{a}{s} \cdot \frac{s}{s} = \frac{a}{s} \in J$

(ii) Let $\frac{a}{s}, \frac{b}{t} \in S^{-1}R \setminus S^{-1}P$, so $a, b \in R$, so $a, b \in R \setminus P$.

Need to show $\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st} \notin S^{-1}P$.

Suppose $\frac{ab}{st} \in S^{-1}P$: we claim $ab \in P$.

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

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

$\underbrace{abuv}_{\not\in P} = \underbrace{cstv}_{P} \longrightarrow$ requires $S \cap P = \emptyset$

Thus $ab \in P$.   This contradicts P being prime.   ∎

Thm 4.10 Let R be commutative, unital, and let $S \subseteq R$ 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 $I \subseteq R$.

> **claim** I is prime.
>
> Let $a, b \in R \setminus I$.
>
> Then $\frac{as}{s}, \frac{bs}{s} \in S^{-1}R \setminus Q$
>
> So $\frac{as}{s} \cdot \frac{bs}{s} = \frac{abs^2}{s^2} = \frac{abs}{s} \in \underset{S^{-1}R \setminus S^{-1}I}{\underbrace{S^{-1}R \setminus Q}}$ since Q prime
>
> Then $ab \notin I$.

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

Def Let R be a commutative, unital ring, $P \subseteq R$ 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 $I \subseteq R$ is an ideal, $S^{-1}I$ is denoted I_P

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

Thm 4.11 Let R be commutative, unital, $P \subseteq R$ 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) (c) 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 is $\mathfrak{m}$, we write $\underline{(R, \mathfrak{m}) \text{ is local}}$

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) $R \backslash R^\times$ is a max ideal
  (iii) $R \backslash R^\times$ is an ideal

Pf (i) $\Rightarrow$ (ii)   Note $\mathfrak{m} \subset R \backslash R^\times$
                 If $x \in R \backslash R^\times$, $(x) \neq R$, so $(x) \subset \mathfrak{m}$
                 Thus $R \backslash R^\times \subset \mathfrak{m}$,   so $R \backslash R^\times = \mathfrak{m}$.

  (ii) $\Rightarrow$ (iii) ✓
  (iii) $\Rightarrow$ (i)   Any proper ideal must be contained in $R \backslash R^\times$ □

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 $R \times M \longrightarrow M$ satisfying

for all $r, s \in R$ $a, b \in M$

1) $r \cdot (a+b) = r \cdot a + r \cdot b$

2) $(r+s) \cdot a = ra + sa$

3) $r(sa) = (rs)a$

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

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

1) $f(a+b) = f(a) + f(b)$ for all $a, b \in M$

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

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

The map $\varphi : R[x] \longrightarrow R[x]$ is a module homomorphism but not a ring homomorphism

$$f \longmapsto xf$$

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

Ex   A ring is a module over itself. ~~Does soundrat or any arritys.~~ Its submodules are its ideals

Ex $x^2 R$ 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~~ the submodule
generated by their union is called the __sum__ of the B_i. If I is finite,
it is denoted $B_1 + \cdots + B_n$.

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

Thm 1.5   Let R be a $\overset{\text{unital}}{\text{arbitrary}}$ M an 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 ~~for the~~ $\{B_i\}_{i \in I}$ is a family of submodules, the sum
is $\left\{ \sum_{k=1}^{s} b_{i_k} \mid s \in \mathbb{N}, b_{i_k} \in B_{i_k} \right\}$

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

Pf M/N is an abelian group.

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

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

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

If I is finite these coincide and are denoted $M_1 \oplus M_2 \oplus \ldots \oplus M_n$.

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

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

$$\ldots \xrightarrow{f_{i-1}} A_{i-1} \xrightarrow{f_i} A_i \xrightarrow{f_{i+1}} A_{i+1} \xrightarrow{f_{i+2}} \ldots \quad \text{is called } \underline{\text{exact}} \text{ if}$$

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
$$0 \to M \to M \oplus N \to N \to 0 \text{ is exact.}$$

Ex If $N \subset M$ is a submodule

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

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

$$0 \to \operatorname{Ker} f \to M \xrightarrow{f} N \to \operatorname{Coker} f \to 0 \quad \text{is exact.}$$

$$\| \atop N/\operatorname{Im} f$$

Lemma 1.17 (Short Five Lemma) Let

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0 \qquad \text{be a commutative diagram}$$
$$\quad \downarrow \alpha \quad , \quad \downarrow \beta \quad , \quad \downarrow \gamma$$
$$0 \to A' \xrightarrow{f'} B' \xrightarrow{g'} C' \to 0$$

Suppose the rows are both exact.

(i) If α and γ are both injective, so is β.

(ii) If α and γ are both surjective, so is β

(iii) If α and γ are both isomorphisms, so is β.

Pf "Diagram chasing"

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

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

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

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

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

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

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

(ii) Let $x \in B'$.

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

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

$$\text{\& } \gamma g(z) = g'\beta(z)$$
$$\overset{"}{\gamma(y)} = g'(x)$$

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

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

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

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

$$x - \beta(z) = \beta f(v)$$
$$x = \beta(z + f(v)) \qquad \blacksquare$$

Def If case (iii) occurs, we say the exact sequences are isomorphic.

Sequence of Remodules

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

(1) The sequence is right split: There exists $h: C \to B$ with $gh = id$

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

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

Pf (1) ⟹ (3)

$$0 \to A \overset{i}{\to} A \oplus C \overset{\pi}{\to} C \to 0$$
$$\quad\; \downarrow id \qquad \downarrow f+h \qquad \downarrow id$$
$$0 \to A \overset{f}{\to} B \overset{g}{\to} C \to 0$$

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

$$f(id(a)) = f(a) \quad \checkmark$$

(86)

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

$$g\left((f+h)(a,c)\right) = g\left(f(a)+h(c)\right) = g(f(a)) + g(h(c)) = 0 + c = c$$

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

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

$(ii) \Rightarrow (iii)$

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

$$\downarrow id \qquad \downarrow (K,g) \qquad \downarrow id$$

$$0 \longrightarrow A \xrightarrow{i} A \oplus C \xrightarrow{\pi} C \longrightarrow 0$$

Let $a \in A$: $(K,g)(f(a)) = (Kf(a), gf(a)) = (a, 0)$

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

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.

$(iii) \Rightarrow (i, ii)$

$$0 \longrightarrow A \xrightarrow{i_1} A \oplus C \underset{i_2}{\overset{\pi_2}{\rightrightarrows}} C \longrightarrow 0$$

$$\downarrow \quad \pi_1 \qquad \downarrow \varphi \qquad \downarrow$$

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

Let $h = \varphi \, i_2$

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

§2   Free modules

Def: Let M be an R-module, $X \subseteq M$ a subset. X is called __linearly independent__
if whenever $x_1, \ldots, x_n \in X$, $r_1, \ldots, r_n \in R$,

$$r_1 x_1 + \ldots + r_n x_n = 0 \implies r_1 = \ldots = r_n = 0.$$

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 nonempty basis X

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

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

commutes

Pf: (1) $\Rightarrow$ (3)   Let X be a basis, $i: X \to F$ the inclusion map.
Since X is linearly independent, every $u \in F$ can be written uniquely
$$u = r_1 x_1 + \ldots + r_n x_n \quad \text{for some } r_i \in R, \ x_i \in X$$

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

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

(3) $\Rightarrow$ (2)

note $\tilde{f}$ has inverse map $\sum_{x \in X} xR \to F$
$$x \mapsto i(x)$$

$(2) \Rightarrow (1)$ If X linearly dependent, this violates direct sum   (Thm 1.15)

Clearly X generates F. ∎

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

__Cor 2.2__ 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.
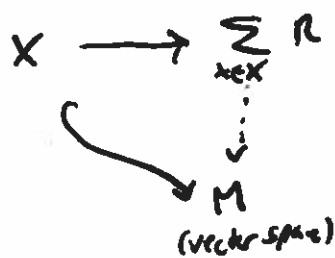
__Thm 2.4__ Every module over a field (or division ring) is free, ~~i.e. a vector space~~.

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

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

Then X is a basis of N.

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

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

    not all $r_{n+1} \neq 0$ (since X linearly independent),

    So $a = -\frac{1}{r_{n+1}} (r_1 x_1 + \cdots + r_n x_n) \in N$ ↯

Claim contradicts maximality, so $M = N$.

__Pf of Thm 2.4__   Let $S = \{ X \subseteq M \mid X \text{ is linearly independent}\}$.

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

Rmk

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

Def 2.6 Let R be unital. If for every free module F, two bases of F have the same cardinality, we say R has the <u>invariant basis number (IBN) property</u> or the <u>invariant dimension property</u>. The <u>rank</u> (<u>dimension</u>) 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, WLOG suppose X is infinite.

     ● **Claim** Y is infinite.

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

         write $y_1 = a_{11} x_1 + \ldots + a_{1m} x_m$

         $\vdots$ $\Rightarrow \{x_1, \ldots, x_m\}$ span V

         $y_n = a_{n1} x_1 + \ldots + a_{nm} x_m$ $\Rightarrow X$ linearly dependent. ⨍

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

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

     Then $\left| \bigcup_{i \in S} E_i \right| = |I| = |Y|$ and $\bigcup_{i \in I} E_i$ spans V.

     If $|X| > |Y|$, there exists $x \in X \setminus \bigcup_{i \in S} E_i$

         Since $\bigcup_{i \in I} E_i$ spans, $x = b_1 x_1 + \ldots + b_n x_n$ for some $x_i \in X$

           $\Rightarrow X$ linearly dependent

     So $|X| \leq |Y|$.
(Similarly, $|Y| \leq |X|$ (90)   ∎

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

Lemma 2.10 Let R be unital, $I \subset R$ an ideal (proper). Let F be a free module with basis X, and $\pi: F \to F/IF$ 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 $u = \sum_{j=1}^{n} r_i x_i$ for some $r_i \in R$.

So $u + IF = \left(\sum_{j=1}^{n} r_i x_i \right) + IF = \sum_{j=1}^{n} (r_j x_j + IF) = \sum_{j=1}^{n} (r_j + IF)(x_j + IF)$

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

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.

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

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

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

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

After reindexing, since X linearly independent we must have $r_j = \tilde{s}_j \in I$, $x_j = \tilde{x}_j$,

So $r_j + I = I$ for all j.

Claim 3 π is injective

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

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

$$\parallel$$

$$x_1 + x_2 + IF \qquad \text{with } \tilde{s}_i \in I$$

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

Prop 2.11   Let $f: R \to S$ 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 $|X| = |Y|$ ☐

Cor 2.12   Let R be a commutative, unital ring. Then R has IBN property
Pf.   Let $m \subset R$ be a maximal ideal. Then $\pi: R \to R/m$
      is a nonzero surjection, and R/m is a field, thus has IBN.   ☐

§3 Projective and Injective modules

Motivations

1) Projective modules are almost as nice as free modules
   (i) Direct summands of free modules
   (2) Locally free

2) Algebraic analogue of vector bundles — locally trivial
   (Ex Infinity loss Möbius strip)

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

$$\begin{array}{ccc} & & P \\ & {}^{h}\swarrow & \downarrow f \\ A \xrightarrow{g} & B & \to 0 \end{array}$$
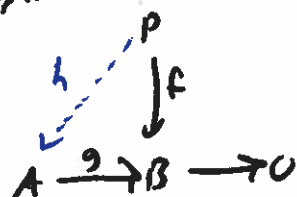
Thm 3.2 Free modules are projective.

Pf Let F be a free module, and suppose

$$\begin{array}{ccc} & & X \\ & {}^{h_0}\swarrow & \downarrow F \\ & \swarrow {}_{g}^{h} & \downarrow f \\ A \xrightarrow{g} & B & \to 0 \end{array}$$
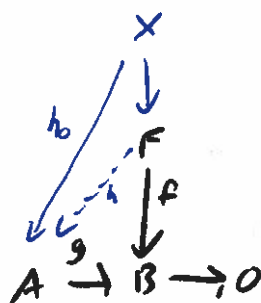
Let X be a basis for F. For each $x \in X$, choose $y_x \in A$ with $g(y_x) = f(x)$

Define $h_0: X \to A$ 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 $0 \to A \to B \to P \to 0$ splits
    (so $B \cong A \oplus P$)

(3) There is a free module F and a (projective) module K
    such that $F \cong K \oplus P$.

Pf (i) $\Rightarrow$ (ii)

$$0 \longrightarrow A \longrightarrow B \longrightarrow P \longrightarrow 0$$

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

$$0 \longrightarrow K \longrightarrow F \longrightarrow P \longrightarrow 0$$

$\hookrightarrow K =$ Kernel of the map.

Then $F \cong K \oplus P$

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

$F \cong K \oplus P$ F projective !

$$A \longrightarrow B \longrightarrow 0$$

□

Ex $\mathbb{Z}_2$ and $\mathbb{Z}_3$ are $\mathbb{Z}_6$ modules
$\mathbb{Z}_6 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3$, $\mathbb{Z}_6$ a 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

$\sum P_i$

P_i

Then P_i is projective

$$A \longrightarrow B \longrightarrow 0$$

$\Leftarrow$ Suppose P_i each projective

$$P_i \downarrow$$
$$\Sigma P_i \downarrow$$
$$A \to B \to 0$$

Since we have maps $P_i \to A$ for all $i \in I$, we get a map $\sum\limits_{i \in I} P_i \to A$ $\quad\blacksquare$

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

$$0 \to A \xrightarrow{g} B$$
$$f \downarrow \quad \swarrow h$$
$$J$$

there exists $h: B \to J$ s.t. $hg = f$.

Prop 3.7 A direct product of R-modules $\prod\limits_{i \in I} J_i$ 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 $I \to J$ extends to a homomorphism $R \to J$.

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

$$0 \to I \to R$$
$$\downarrow \quad \swarrow$$
$$J$$

(45)

$\Longleftarrow$ Suppose we are given $0 \to A \xrightarrow{g} B$

$$\downarrow f$$
$$J$$

Let $S = \{ h: C \to J \mid \text{Im} g \subseteq C \subseteq B, \ hg = f \}$

S is nonempty, since $A \cong \text{Im} g$, so $fg^{-1}: \text{Im} g \to J$

S is partially ordered by extension / restriction

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

<u>Claim</u> $H = B$ (If true, then J is injective!)

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

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

Then $\varphi: I \longrightarrow J$
$$r \longmapsto h(rb)$$

Observe: If $a \in R$, $\varphi(ar) = h(arb) = a h(rb) = a\varphi(r)$

So φ is an R-module homomorphism

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

Let $K = H + Rb$

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

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 $\quad\quad$ $\downarrow$ $\quad$ $\square$

~~Divisible~~ ~~Groups~~

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 $\begin{array}{c} D \longrightarrow D \\ x \longmapsto nx \end{array}$ is surjective.

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

Easy Lemma Homomorphic image of a divisible group is divisible.

Lemma 3.9 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 $f : \langle n \rangle \longrightarrow D$ by $f(n) = y$ (since $\{n\}$ is a basis)

$$0 \longrightarrow \langle n \rangle \longrightarrow \mathbb{Z}$$

with $f : \langle n \rangle \downarrow$, h (diagonal), D below.

Since D injective, there exists $h : \mathbb{Z} \to D$
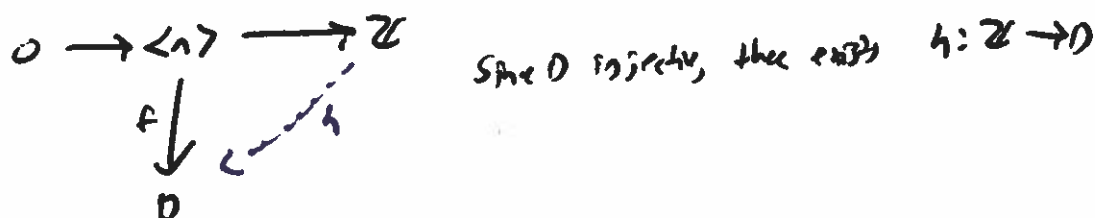
Now $nh(1) = h(n) = f(n) = y$. $\quad$ Thus D is divisible.

$\Rightarrow$ Suppose D is divisible. Let $f : \langle n \rangle \longrightarrow D$ be a homomorphism [ideal of $\mathbb{Z}$]. Choose $x \in D$ with $nx = f(n)$, and define $h : \mathbb{Z} \longrightarrow D$ by $h(1) = x$. Then h extends f, so by Lemma 3.8 D is injective. $\quad$ $\square$

<u>Lemma 3.10</u> Every abelian group can be embedded in a divisible abelian group.

<u>Pf</u> Let A be an abelian group.

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

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

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

Then $A \cong F/K \xleftarrow{} f(F)$

$A \cong F/K \cong f(F)/f(K) \longrightarrow \sum \mathbb{Q}/f(K)$

$\uparrow$ Homomorphic image of a divisible group, thus divisible. ∎

<u>Lemma 3.11</u> Let R be unital, J a divisible abelian group.

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

<u>Pf</u> Let $I \subseteq R$ be an ideal, and $f : I \longrightarrow \text{Hom}_{\mathbb{Z}}(R, J)$

Define $g : I \longrightarrow J$ by $g(a) = (f(a))(1)$

Since J injective,

$$0 \longrightarrow I \longrightarrow R$$
$$g \downarrow \quad \swarrow \tilde{g}$$
$$J$$

Now define $h : R \longrightarrow \text{Hom}_{\mathbb{Z}}(R, J)$
$\qquad r \longmapsto h(r)$

$h(r) : R \longrightarrow J$
$\qquad x \longmapsto \tilde{g}(xr)$

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

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

Check: Is h a homomorphism?

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

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

$$\boxed{\text{CHK}}\ [rh(s)](x) = [h(s)](xr) = \tilde{g}(xrs)$$

↑ R-module structure of $\text{Hom}_{\mathbb{Z}}(R, J)$ Def'n obb

check: Does h extend f ?

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

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

$$= [xf(r)](1)$$ since $\text{Hom}_{\mathbb{Z}}(R,J)$ an R-mod

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

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

So h extends f, and Lemma 3.8 shows $\text{Hom}_{\mathbb{Z}}(R,J)$ is injective. ∎

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 a $\overset{\text{injective}}{\underset{↑}{\text{group}}}$ homomorphism $f: A \to J$

This induces a map $\bar{f}: \text{Hom}_{\mathbb{Z}}(R, A) \to \text{Hom}_{\mathbb{Z}}(R, J)$

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

$\begin{array}{ccc} R & \to & A \\ \downarrow & \nearrow f & \\ J & & \end{array}$

Note: $\bar{f}$ injective since if $fg = 0$, then $\text{Img} \subset \ker f = \{0\}$ Since f injective.

$\bar{f}$ is an R-module homomorphism

Also observe $\text{Hom}_R(R, A) \subset \text{Hom}_{\mathbb{Z}}(R, A)$

And $A \hookrightarrow \text{Hom}_R(R, A)$
$$a \longmapsto f_a$$
where $f_a(r) = ra$

Injective! ↓

So $A \hookrightarrow \text{Hom}_R(R,A) \hookrightarrow \text{Hom}_{\mathbb{Z}}(R,A) \hookrightarrow \text{Hom}_{\mathbb{Z}}(R, J)$

(99)

<u>Prop 3.13</u> Let R be unital, J an R-module. TFAE

(i) J is injective

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

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

<u>Pf</u> (i) ⇒ (ii)

$$0 \to J \longrightarrow B \longrightarrow C \to 0$$

$$\downarrow \quad \swarrow$$

$$J$$

(ii) ⇒ (iii) Suppose J is a submodule of B

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

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

Prop 3.7 ⇒ J is injective. ∎

(100)

§4 Hom

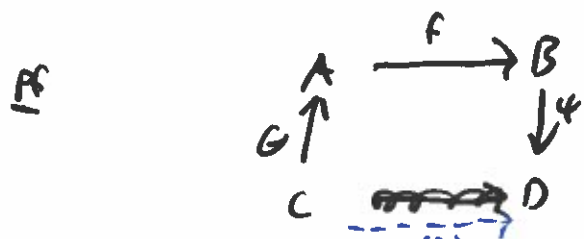**Def** Let A, B be R-modules.
$$\text{Hom}_R(A,B) = \{ f: A \to B \mid f \text{ is an } R\text{-module homomorphism}\}$$

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

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

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

Pf

If $f, g \in \text{Hom}_R(A,B)$ $\Theta(f+g) = \psi(f+g)\varphi = \psi \circ (f\varphi + g\varphi) = \psi f \varphi + \psi g \varphi = \Theta(f) + \Theta(g)$

If $r \in R$, $\Theta(rf) = \psi \circ (rf) \varphi = r \psi f \varphi = r \Theta(f)$. ∎

Two important examples:

(1) $A = C$, $\Theta = id$ ~~$\text{Hom}(A,B)$~~   A map $\psi: B \to D$ gives a map $\text{Hom}_R(A,B) \to \text{Hom}_R(A,D)$, $f \mapsto \psi f$

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

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

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

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

ie. A Let $0 \to A \xrightarrow{\varphi} B \xrightarrow{\psi} C$ ~~-----~~ be a sequence of R-modules.

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

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

Pf $\Rightarrow$

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

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

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

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

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

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

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

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

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

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

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

$$D \xrightarrow{g} \bullet \text{Im}\,g \underset{\subset B}{\subset} \text{Im}\,\varphi \xrightarrow{\varphi^{-1}} A$$

$\leftarrow$ Since φ injective.

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

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

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

$\Leftarrow$ (i) we first show φ is injective

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

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

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

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

(ii) **Claim** $\text{Im } \tilde{\varphi} \supseteq \text{Ker } \tilde{\psi}$.

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

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

For other containment,

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

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

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

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

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

So $\text{Ker } \psi \subseteq \text{Im } \varphi$ ∎

Prop 4.3 $\text{Hom}_R(-, D)$ is ~~left~~ **left exact**

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

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

$$0 \to \text{Hom}_R(C,D) \xrightarrow{\tilde{\psi}} \text{Hom}_R(B,D) \xrightarrow{\tilde{\theta}} \text{Hom}_R(A,D) \text{ is exact.}$$

Pf $\Rightarrow$ (i) First show $\tilde{\psi}$ is injective.

Let $f \in \text{Ker } \tilde{\psi}$, so $0 = \tilde{\psi}(f) = f\psi$

Now let $y \in C$. The ψ surjective $\Rightarrow y = \psi(x)$ for some $x \in B$

Then $f(y) = f\psi(x) = 0$. Thus $f = 0$

So $\tilde{\psi}$ is injective.

(ii) **Claim** $\text{Im } \tilde{\psi} = \text{Ker } \tilde{\theta}$

Let $f \in \text{Ker } \tilde{\theta}$. We want to construct $g \in \text{Hom}_R(C,D)$ with $f = \tilde{\psi}(g)$

so that $f \in \text{Im } \tilde{\psi}$.

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

$$\downarrow f$$

$$D$$

$$B/\text{Ker }\xi \underset{\bar{\varphi}}{\overset{\bar{\xi}}{\rightleftarrows}} C \rightarrow 0$$

$$\downarrow \bar{f}$$

$$0$$

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

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

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

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

Thus $\text{Ker } \bar{\Theta} \subset \text{Im } \bar{\xi}$.

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

Then $\bar{\Theta}(g) = g\Theta = f\xi\Theta = 0$ since $\xi\Theta = 0$

Thus $\text{Im } \bar{\xi} \subset \text{Ker } \bar{\Theta}$.

$\Longleftarrow$ (i) First we show ξ is surjective.

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

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

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

(ii) **Claim** $\text{Im } \Theta = \text{Ker } \xi$

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

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

Now $\bar{\Theta}(\pi) = \pi\Theta = 0$, so $\pi \in \text{Ker } \bar{\Theta} = \text{Im } \bar{\xi}$.

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

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

Thus $\text{Ker } \xi \subset \text{Im } \Theta$

(104)

By assumption, $0 \to \text{Hom}(C,c) \xrightarrow{\bar{\zeta}} \text{Hom}(B,c) \xrightarrow{\bar{\theta}} \text{Hom}(A,c)$ is exact.

The $\underset{0}{\underbrace{\bar{\theta}\bar{\zeta}}}(\omega) = \theta \cdot 0$, so $\text{Im}\,\theta \subseteq \ker \zeta$. ☑

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

Pf $\Rightarrow$ Suppose P is projective.

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

Consider $0 \to \text{Hom}_R(P,A) \xrightarrow{\bar{\alpha}} \text{Hom}_R(P,B) \xrightarrow{\bar{\psi}} \text{Hom}_R(P,C) \to 0$

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

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

$$
\begin{array}{ccc}
 & & P \\
 & {}^{g}\swarrow & \downarrow f \\
B & \xrightarrow{\psi} C & \to 0
\end{array}
$$

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

$\Leftarrow$ Suppose

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

The $0 \to \text{Hom}(P,K) \to \text{Hom}(P,B) \to \text{Hom}(P,C) \to 0$ 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-module. J is injective if and only if $\text{Hom}(-, J)$ is (right) exact.

Pf $\Rightarrow$ Suppose J is injective.

Let $0 \to A \xrightarrow{\varphi} B \xrightarrow{\psi} C \to 0$ be exact.

consider $0 \to \text{Hom}(C, J) \xrightarrow{\bar{\psi}} \text{Hom}(B, J) \xrightarrow{\bar{\varphi}} \text{Hom}(A, J) \to 0$

By Prop 4.3, it suffices to show $\bar{\varphi}$ is surjective

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

$$0 \to A \xrightarrow{\varphi} B$$
$$f \downarrow \quad \swarrow g$$
$$J$$

Since J injective, there exists $g \in \text{Hom}(B, J)$ with $f = g\varphi = \bar{\varphi}(g)$

$\Leftarrow$ Suppose

$$0 \to A \to B \to B/\text{Im} \to 0$$
$$f \downarrow$$
$$J$$

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

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

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

Pf Define $\varphi : \text{Hom}_R(R, A) \to A$
$$f \mapsto f(1)$$

$\psi : A \to \text{Hom}_R(R, A)$
$$a \mapsto (r \mapsto ra)$$

check $\varphi\psi = id$ ☐

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

§5 Tensor Products

Motivation Let R be commutative, with 1 ring.

How are $R[x]$, $R[y]$, $R[x,y]$ related as modules?

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

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

$R[x] \oplus R[y]$ free on $\{1, x, y, x^2, y^2, x^3, y^3, \ldots\}$ **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

$$(m_1 + m_2, n) - (m_1, n) - (m_2, n)$$

$$(m, n_1 + n_2) - (m, n_1) - (m, n_2)$$

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

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

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

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__ $f: A \times B \longrightarrow C$ is a function satisfying

(i) $f(a_1 + a_2, b) = f(a_1, b) + f(a_2, b)$

(ii) $f(a, b_1 + b_2) = f(a, b_1) + f(a, b_2)$

(iii) $f(ra, b) = f(a, rb) = r f(a, b)$

for all $a, a_1, a_2 \in A$
$b, b_1, b_2 \in B$
$r \in R$

Ex There is a canonical bilinear map

$$M \times N \longrightarrow M \otimes N$$
$$(m, n) \longmapsto m \otimes n$$

"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 $g: M \times N \longrightarrow L$ a bilinear map. There is a unique R-module homomorphism $\bar{g}: M \otimes_R N \longrightarrow L$

Pf

Suffices to show $K \subset \ker g_0$

But this is precisely the bilinearity of g!

$\square$

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

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

Cor 5.3 Let $f: M \longrightarrow M'$, $g: N \longrightarrow N'$ be R-module homomorphisms. There is a unique homomorphism $M \otimes N \longrightarrow M' \otimes N'$ such that $m \otimes n \longmapsto f(m) \otimes g(n)$

This homomorphism is denoted $f \otimes g$.

Pf The map $M \times N \longrightarrow M \otimes N'$
$(m, n) \longmapsto f(m) \otimes g(n)$ is a bilinear

Then by Thm 5.6 obtain unique homomorphism $M \otimes N \longrightarrow M' \otimes N'$

<u>Prop 5.4</u> The tensor product is right exact, i.e. if

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

$$K \otimes_R L \xrightarrow{id \otimes f} K \otimes_R M \xrightarrow{id \otimes g} K \otimes_R N \to 0 \quad \text{is exact.}$$

<u>PF</u> <u>Claim 1</u> $id \otimes g$ is surjective.

Suffices to show $k \otimes n \in Im(id \otimes g)$ for all $k \in K$, $n \in N$.

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

The $k \otimes n = k \otimes g(m) = (id \otimes g)(k \otimes m) \in Im(id \otimes g)$

<u>Claim 2</u> $Im(id \otimes f) \subset Ker(id \otimes g)$

Note $(id \otimes g) \circ (id \otimes f) = id \otimes (g \circ f) = id \otimes 0 = 0$ since $g \circ f = 0$.

<u>Claim 3</u> $Ker(id \otimes g) \subset Im(id \otimes f)$

Since $Im(id \otimes f) \subset Ker(id \otimes g)$

Suffices to show α is an isomorphism

Define $\beta : K \times N \longrightarrow K \otimes_R M / Im(id \otimes f)$ by

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

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

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

Then $k \otimes (m - m_0) \in Im(id \otimes f)$, so $\pi(k \otimes (m - m_0)) = 0$

so $\pi(k \otimes m) = \pi(k \otimes m_0)$

Straightforward to verify that β is bilinear, so we obtain

$$\bar{\beta}: K \otimes_R N \longrightarrow K \otimes_R M / \mathrm{Im}(\mathrm{id} \otimes f)$$

For any generator $k \otimes n \in K \otimes_R N$
$$\alpha \bar{\beta}(k \otimes n) = \alpha \beta(k, n) = \alpha \pi(k \otimes m) = (\mathrm{id} \otimes g)(k \otimes m) = k \otimes n.$$

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

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

$$\bar{\beta} \alpha (\overline{G(k \otimes m)}) = \bar{\beta}(\mathrm{id} \otimes g)(k \otimes m) = \bar{\beta}(k \otimes g(m)) = \beta(k, g(m)) = \pi(\overline{k \otimes m}) \qquad \blacksquare$$

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

Pf Define bilinear map $A \times R \longrightarrow a$
$$(a, r) \longmapsto ra$$

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

Construct $\beta: A \longrightarrow A \otimes_R R$ check $\beta \alpha = \mathrm{id}$, $\alpha \beta = \mathrm{id}$. $\qquad \blacksquare$
$$a \longmapsto a \otimes 1 .$$

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 $\lambda_x: M \times N \longrightarrow (L \otimes_R M) \otimes N$ by
$$(m, n) \longmapsto (x \otimes m) \otimes n$$

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

Now define $\alpha: L \times (M \otimes_R N) \longrightarrow (L \otimes_R M) \otimes N$ by
$$(x, \gamma) \longmapsto \bar{\lambda}_x(\gamma).$$

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

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

Construct inverse in same way. $\blacksquare$

Thm 5.9 Let L, M, N be R-modules.
$$(L \oplus M) \otimes N \cong (L \otimes N) \oplus (M \otimes N)$$

Pf Construct $\alpha_1: L \otimes N \longrightarrow (L \oplus M) \otimes N$ by $\alpha_1 = i_1 \otimes id$

$\quad\quad\quad\quad \alpha_2: M \otimes N \longrightarrow (L \oplus M) \otimes N$ by $\alpha_2 = i_2 \otimes id$

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

Define $\beta_0: (L \oplus M) \times N \longrightarrow (L \otimes N) \oplus (M \otimes N)$

$\quad\quad\quad\quad ((l, m), n) \longmapsto (l \otimes n, m \otimes n)$

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

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

$\alpha\beta((l, m) \otimes n) = \alpha(l \otimes n, m \otimes n)$
$\quad\quad\quad\quad = (l, 0) \otimes n + (0, m) \otimes n$
$\quad\quad\quad\quad = ((l, 0) + (0, m)) \otimes n$
$\quad\quad\quad\quad = (l, m) \otimes n$

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

$$\beta_1(\ell \otimes n_1, m \otimes n_2) = \beta\big((\ell,0)\otimes n_1 + (0,m)\otimes n_2\big)$$

$$= \beta\big((\ell,0)\otimes n_1\big) + \beta\big((0,m)\otimes n_2\big)$$

$$= (\ell \otimes n_1, 0 \otimes n_1) + (0 \otimes n_2, m \otimes n_2)$$

$$= (\ell \otimes n_1, 0) + (0, m \otimes n_2)$$

$$= (\ell \otimes n_1, m \otimes n_2)$$

β_1 identity on generators, so $\beta_1 = id$. $\boxed{}$

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

for $f \in \text{Hom}_R(L \otimes M, N)$, $\alpha(f) : L \longrightarrow \text{Hom}(M, N)$

$$\big[\alpha(f)(\ell)\big](m) = f(\ell \otimes m)$$

(1) Is $\alpha(f)(\ell)$ a homomorphism $M \to N$?

$$\big[\alpha(f)(\ell)\big](m_1 + m_2) = f(\ell \otimes (m_1 + m_2)) = f(\ell \otimes m_1) + f(\ell \otimes m_2)$$
$$= \big[\alpha(f)(\ell)\big](m_1) + \big[\alpha(f)(\ell)\big](m_2)$$

$$\big[\alpha(f)(\ell)\big](rm) = f(\ell \otimes rm) = f(r(\ell \otimes m)) = rf(\ell \otimes m) = r\big[\alpha(f)(\ell)\big](m)$$

(2) Is $\alpha(f)$ a homomorphism?

$$\big[\alpha(f+g)(\ell)\big](m) = (f+g)(\ell \otimes m) = f(\ell \otimes m) + g(\ell \otimes m) = \big[\alpha(f)(\ell)\big](m) + \big[\alpha(g)(\ell)\big](m)$$

$$\big[\alpha(rf)(\ell)\big](m) = (rf)(\ell \otimes m) = r(f(\ell \otimes m)) = r\big[\alpha(f)(\ell)\big](m)$$

$(\cdots)$

(1) Is f a homomorphism?

(2) Is $\alpha(f)$ a homomorphism?

$$[\alpha(f)(\ell_1 + \ell_2)](m) = f((\ell_1 + \ell_2) \otimes m) = f(\ell_1 \otimes m + \ell_2 \otimes m)$$
$$= f(\ell_1 \otimes m) + f(\ell_2 \otimes m)$$
$$= [\alpha(f)(\ell_1)](m) + [\alpha(f)(\ell_2)](m)$$

$$[\alpha(f)(r\ell)](m) = f(r\ell \otimes m) = f(r(\ell \otimes m)) = r f(\ell \otimes m)$$
$$= r[\alpha(f)(\ell)](m)$$

Define $\beta : \text{Hom}(L, \text{Hom}(M,N)) \longrightarrow \text{Hom}(L \otimes M, N)$

If $g \in \text{Hom}(L, \text{Hom}(M,N))$

$$[\beta(g)](\ell \otimes m) = [g(\ell)](m)$$

(4) Is β a homomorphism?

$$[\beta(g_1 + g_2)](\ell \otimes m) = [(g_1 + g_2)(\ell)](m) = [g_1(\ell) + g_2(\ell)](m)$$
$$= [g_1(\ell)](m) + [g_2(\ell)](m)$$
$$= [\beta(g_1)](\ell \otimes m) + [\beta(g_2)](\ell \otimes m).$$

$$[\beta(rg)](\ell \otimes m) = [(rg)(\ell)](m) = [r g(\ell)](m)$$
$$= r[g(\ell)](m)$$
$$= r[\beta(g)](\ell \otimes m)$$

(5) Is $\beta\alpha$ identity?

$$[\beta\alpha(f)](\ell \otimes m) = [\alpha(f)(\ell)](m) = f(\ell \otimes m), \quad \text{so } \beta\alpha(f) = f$$

(6) Is $\alpha\beta$ identity?

$$[\alpha\beta(g)(\ell)](m) = [\beta(g)](\ell \otimes m) = [g(\ell)](m), \quad \text{so } \alpha\beta(g) = g.$$

§7 Algebras

<u>Def 7.1</u> Let R be a commutative, unital ring. For R A ring A is called an
     <u>R-algebra</u> if
     1) A is an R-module
     2) $r \cdot (ab) = (r \cdot a)b = a(r \cdot b)$ for all $r \in R$, $a, b \in A$.

<u>Ex</u> $R[x]$ is an R-algebra.

<u>Ex</u> $\mathbb{Q}$ is a $\mathbb{Z}$-algebra

<u>Ex</u> $\mathbb{C}$ is an $\mathbb{R}$-algebra.

<u>Thm</u> 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)

<u>Pf</u> $A \otimes_R M$ is an abelian group since it is an R-module
     Let $a \in A$, $\sum a_i \otimes m_i \in A \otimes_R M$.
     Then $a \cdot \sum a_i \otimes m_i = \sum (a a_i) \otimes m_i$

<u>Ex</u> $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}[x] = \mathbb{Q}[x]$

<u>Ex</u> If S is a R-algebra, $S \otimes_R R^n \cong S^n$

<u>Ex</u> $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}^n \cong \mathbb{C}^n$

§6 Modules over a PID

__Thm 6.1__ Let R be a PID, F a free R-module, $G \subseteq F$ a submodule.
Then G is a free R-module and rank $G \leq$ 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
$$\overline{F_{(j)}} = \sum_{i < j} Rx_i \quad \text{and} \quad F_{(j)} = \sum_{i \leq j} Rx_i = \overline{F_{(j)}} \oplus Rx_j \quad \text{for all } j \in J.$$

Note if $x \in F_{(j)}$, $x = b + rx_j$ for some $b \in \overline{F_{(j)}}$, $r \in R$.

Define $\quad f_j : F_{(j)} \cap G \longrightarrow R$
$$b + rx_j \longmapsto r$$

Note $\ker f_j = \overline{F_{(j)}} \cap G$, so we have an exact sequence

$$0 \to \overline{F_{(j)}} \cap G \longrightarrow F_{(j)} \cap G \xrightarrow{f_j} \operatorname{Im} f_j \to 0$$

Note $\operatorname{Im} f_j \subseteq R$ is an ideal, so $\operatorname{Im} f_j = (r_j)$ for some $r_j \in R$.
Moreover, if $r_j \neq 0$, there exists $c_j \in F_{(j)} \cap G$ with $f_j(c_j) = r_j$.

__Claim__ $C = \{ c_j \mid j \in J, r_j \neq 0 \}$ is a basis of G.

(i) Linear independence: Suppose $s_1 c_{j_1} + \ldots + s_n c_{j_n} = 0$ for some $j_1 < \ldots < j_n$
then $0 = f_{j_n}(s_1 c_{j_1} + \ldots + s_n c_{j_n}) = s_n f_{j_n}(c_{j_n}) = s_n r_{j_n}$
Thus $s_n = 0$. By induction, all $s_i = 0$.

(ii) 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 $\bar{F}_{(i)} \cap G \longrightarrow F_{(i)} \cap G$ is equality,

so $a \in \bar{F}_{(i)} \cap G$.

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 $f_i(a) = s r_i$ for some $s \in R$.

Let $b = a - s c_i$. Since $a \notin \text{span}(C)$, $b \in \text{span}(C)$.

Also, $f_i(b) = f_i(a) - f_i(s c_i) = 0$, so $b \in \bar{F}_{(i)} \cap G$.

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 $N \subseteq M$ be a submodule.

$$\pi : R^n \longrightarrow M$$

$\pi^{-1}(N)$ is a submodule of R^n, hence free with basis $\{x_1, \ldots, x_m\}$, $m \leq n$.

Then N is generated by $\{\pi(x_1), \ldots, \pi(x_m)\}$ ◻

Cor 6.3 A projective module over a PID is free

pf Let M be a ~~projective~~ projective R-module.

$$0 \to K \to F \to M \to 0 , \quad \text{so} \quad F \cong M \oplus K$$

i.e. M is isomorphic to a submodule of F, hence is free. ◻

Thm 6.4 Let R be a PID, A an R-module.

(i) $O_a := \{r \in R \mid ra = 0\}$ is an ideal of R. For each $a \in A$.

This is called the order ideal of $a \in A$
If $O_a = (r)$, a is said to have order r.

(ii) $A_{tor} = \{a \in A \mid O_a \neq 0\}$ is a submodule of A.

This is called the torsion submodule of A.
If $A = A_{tor}$, A is called a torsion module. If $A_{tor} = 0$, A is called torsion free.

(iii) For each $a \in A$, $R/O_a \cong Ra = \{ra \mid r \in R\}$ as R-modules.

(iv) Let $p \in R$ be prime. If $(p^i) \subset O_a$, then $O_a = (p^j)$ for some $0 \le j \le i$.

(v) Let $p \in R$ be prime. If $(p^i) = O_a$, then $p^j \notin O_a$ for all $0 \le j < i$.

Pf (i) Let $a \in A$.
If $r_1, r_2 \in O_a$, $r_1 a = 0$, $r_2 a = 0$, so $(r_1 + r_2)a = r_1 a + r_2 a = 0 + 0 = 0$, so $r_1 + r_2 \in O_a$
If $s \in R$, $(s r_1)a = s(r_1 a) = s \cdot 0 = 0$, so $s r_1 \in O_a$.

(ii) Let $a_1, a_2 \in A_{tor}$. 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 $a_1 + a_2 \in A_{tor}$

If $r \in R$, then $r_1(r a_1) = r(r_1 a_1) = r \cdot 0 = 0$, so $r a_1 \in A_{tor}$.

(iii) Define $\varphi : R \xrightarrow{\ a\ } Ra$ $\quad \varphi$ is surjective.
$\qquad\qquad r \longmapsto ra$

Note $\ker \varphi = O_a$, so $R/O_a \cong Ra$

(iv) Since R a PID, $O_a = (r)$ for some $r \in R$.
Then since $p^i \in O_a = (r)$, $r \mid p^i$.
Since R a UFD, $r = p^j u$ for some $u \in R^*$, $j \le i$. Then $O_a = (r) = (p^j)$.

(v) Suppose for contradiction that $p^j \in Q_a$ for some $0 \leq j < i$.

Then $p^j = p^i \gamma$ ~~are prime.~~ with $j < i$, contradicts unique factorization. ∎

Thm 6.6 Let ~~Abbox~~ R be a PID, A an f.g. R-module. Then $A = A_{tor} \oplus F$
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. torsion free R-module generated by a finite set X.

Since A torsion free, Rx is a free submodule of A for each $x \in X$.

Let $S = \{x_1, \ldots, x_k\} \subset X$ be a maximal$_\text{linearly independent sub.}$ subset, for which

$$F = Rx_1 + \cdots + Rx_k \quad \text{is a free submodule.}$$

If $y \in X \backslash S$, then $ry \in F$ for some$_\text{non zero}$ $r \in R$. (otherwise, $S \cup \{y\}$ is linearly independent)

Taking a (finite) product of these r's for each $y \in X \backslash S$, obtain nonzero $r \in R$

s.t. $rX \subset F$.

Since X generates A, $rA \subset F$.

Define $\varphi_r : A \longrightarrow A$ Clearly $\text{Im } \varphi_r = rA \subset F$ is a free module
$\qquad\qquad\quad a \longmapsto ra$

But since A torsion free, φ_a is injective, so $A \cong \text{Im } \varphi_r$ ∎

PF of 6.6 Set $F = A/A_{tor}$, free by Thm 6.5

$$0 \longrightarrow A_{tor} \longrightarrow A \longrightarrow F \longrightarrow 0 \quad \text{is exact, splits since } F \text{ free, hence projective.}$$

Thus $A \cong A_{tor} \oplus F$ ∎

Thm 6.12 Let M be a f.g. module over a PID R.

$$\text{Then } M \cong R^{\hat{}} \oplus \underbrace{Rx_1 \oplus \cdots \oplus Rx_n}_{M_{tor}} \quad \text{where } x_i \text{ has order } p_i^{s_i} \text{ for some prime } p_i, \text{ positive integer } s_i$$

Thm 6.7 Let R be a PID, M a torsion R-module. For $p \in M$ a prime, set

$$M(p) = \{a \in M \mid a \text{ has order } a\, p^s \text{ for some } s\}$$

(i) $M(p)$ is a submodule for each prime $p \in M$

(ii) $M = \sum_{\substack{p \in R \\ prime}} M(p)$. 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 $0 \le i \le k$ (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 $0 \le j \le k$

Thus, $xa \in M(p)$

(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 $r = p_1^{n_1} \cdots p_u^{n_u}$ for u distinct primes p_i

Let $r_i = p_1^{n_1} \cdots p_{i-1}^{n_{i-1}} p_{i+1}^{n_{i+1}} \cdots p_u^{n_u}$.

Then $r_1, \ldots, r_u$ are coprime, so $\gcd(r_1, \ldots, r_u) = 1$

Then $1 = s_1 r_1 + \cdots + s_u r_u$ for some $s_i \in R$.

$$a = s_1 r_1 a + \cdots + s_u r_u a$$

Note $p_i^{n_i}(s_i r_i a) = s_i r a = 0$ for each i, so $s_i r_i a \in M(p_i)$.

Then $a \in M(p_1) + \cdots + M(p_u)$

Claim 2 the sum is direct

Fix $p \in R$ a prime, and let M_1 be submodule generated by $M(q)$ for primes $q \neq p$.

we need to show $M(p) \cap M_1 = 0$

Suppose $a \in M(p) \cap M_1$, so $p^k a = 0$ for some $k \in \mathbb{N}$.

Also, $a = a_1 + \cdots + a_6$ 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 $(q_1^{k_1} \cdots q_\ell^{k_\ell}) a = 0$ Let $d = q_1^{k_1} \cdots q_\ell^{k_\ell}$.

Note p^k, d coprime, so $1 = r p^k + s d$ for some $r, s \in R$.

Then $a = r p^k a + s d a = 0$

Claim 3 If M is f.g., this sum is finite.

Suppose $M = R x_1 + \cdots + R x_n$

~~is generated by $M(p_i)$ ...~~

Then $x_i \in M(p_{i_1}) \oplus \cdots \oplus M(p_{i_m})$ for some primes $p_{i_1}, \ldots, p_{i_m} \in R$.

$\Rightarrow$ $M = \overset{\wedge}{\underset{\delta=1}{\oplus}} M(p_{i_1}) \oplus \cdots \oplus M(p_{i_m})$ $\square$

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 $j \leq n$ 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 $\quad 0 = \rho^n c = \rho^{n-j}(\rho^j c) \cdot \rho^{n-j}(\rho^k ra)$, $\quad$ so $n-j+k \geq n$, ths $k \geq j \geq 1$

Set $\quad b = \rho^{j-1} c - r\rho^{k-1} a$

Note $\rho^{j-1} c \notin Ra$, so $b \neq 0$, and $\rho b = \rho^j c - r\rho^k a = 0 - 0 = 0$

We claim $Ra \cap Rb = 0$.

If not, then exists $s \in R$ with $sb \in Ra$ and $sb \neq 0$.

Since $sb \neq 0$, $\rho \nmid s$, so s and ρ^n are coprime

Thus $\quad sx + \rho^n y = 1$ $\quad$ for some $x, y \in R$.

Then $\quad b = sxb + \rho^n yb = sxb \in Ra$ $\quad$ since $\rho^n M = 0$

Then $\quad \rho^{j-1} c = b + r\rho^{k-1} a \in Ra$

Recall j was __minimal__ s.t. $\rho^j c \in Rc$, so we must have $j-1 > 0$, so $c \in Ra$ $\quad \downarrow$

(ii) wlog, $M \neq Ra$.

$\quad$ Let $S = \{ B \subset M \mid Ra \cap B = 0 \}$

Zorn $\Rightarrow$ S has a maximal element $C \in M$ with $Ra \cap B = 0$

Since $Ra \cap C = 0$, suffices to show $M = Ra + C$.

$\quad$ __Claim__ $M/C = R(a+c)$

$\qquad$ Since $\rho^n A = 0$, $\quad \rho^n(A/c) = 0$

$\qquad$ But $\rho^{n-1}(a+c) = \rho^{n-1} a + C \neq C$, since $\rho^{n-1} a + c = c \Rightarrow \rho^{n-1} a \in C \cap Ra = 0$

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ and $\rho^{n-1} a \neq 0$ by $\in$ Shaph.

$\qquad$ So $\rho^{n-1}(A/c) \neq 0$, and we can apply part (i) to A/c

$\qquad$ So either $M/C = R(a+c)$, or there exists $b+c \in M/C$ with $R(a+c) \cap R(b+c) = C$

$\qquad$ Spse latter

$\qquad$ Then $Ra \cap (Rb + C) = 0$. But $C \subsetneq Rb+C$, contradicting maximality

$\qquad$ Thus $M/C = R(a+c)$, so $M = Ra + C$ $\qquad\qquad$ ▢

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 $M = Ra_1 \oplus \cdots \oplus Ra_k$, where a_i has order p^{n_i} for some $n_i \in \mathbb{N}$.

Pf Suppose $M = Ra_1 + \cdots + Ra_k$. Induct 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 $\pi : M \to C$ be quotient map,

C is generated by $\pi(a_2), \ldots, \pi(a_k)$

Moreover, $p^{n_i} \pi(a_i) = \pi(p^{n_i} a_i) = \pi(0) = 0$, so $O_{\pi(a_i)} = (p^{j_i})$ for some $j_i \leq n_i$.

Now apply induction hypothesis $\Rightarrow$ $C = Ra_{(2)} \oplus \cdots \oplus Ra_{(k)}$ ∎

Thm 6.12 Let R be a PID, M a f.g. R-module.
$$M = R^n \oplus Ra_1 \oplus \cdots \oplus Ra_u$$
where a_i has order $p_i^{n_i}$ for some prime $p \in R$.

Pf By Thm 6.6, $M = R^n \oplus M_{tor}$

By Thm 6.7, $M_{tor} = M_{tor}(P_1) \oplus \cdots \oplus M_{tor}(P_u)$

By Thm 6.9, $M_{tor}(P_i) = Ra_{i_1} \oplus \cdots \oplus Ra_{i_u}$ ∎

Ch. 8 Commutative Rings and Modules

Assume all rings are commutative unital.

§1 Chain Conditions

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

M is called <u>Artinian</u> if every chain of submodules
$$M_1 \supset M_2 \supset M_3 \ldots \quad \text{stabilizes} \quad \text{(Descending chain condition)}$$

Def 1.2 A ring is Noetherian (or 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
$$(m) \subset (n) \iff n | m \quad ,$$
$$\text{While} \quad (2) \supset (4) \supset (8) \supset (16) \supset \ldots$$

Ex Every PID is Noetherian

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

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

PF: ⇒ Submodules of L are submodules of M, so L is Noetherian

Let $N_1 \subset N_2 \subset \cdots$ be a chain of submodules of N.

Then $g^{-1}(N_1) \subset g^{-1}(N_2) \subset \cdots$ is a chain of submodules of M

So $g^{-1}(N_i) = g^{-1}(N_n)$ for all $i \geq n$ for some $n \in \mathbb{N}$

then $N_i = g\,g^{-1}(N_i) = g\,g^{-1}(N_n) = N_n$ for all $i \geq n$, so N is Noetherian.

⇐ Suppose L, N Noetherian

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

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

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

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

For $i \geq n$:

$$0 \to L_n \to M_n \to N_n \to 0$$
$$\downarrow id \qquad \downarrow i \qquad \downarrow id$$
$$0 \to L_i \to M_i \to N_i \to 0$$

Five Lemma ⇒ $M_n = M_i$ for all $i \geq n$. $\qquad$ ∎

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 $M_1, \ldots, M_n$ be modules. Then $M_1 \oplus \cdots \oplus M_n$ is Noetherian (resp. Artinian) iff all M_i are Noetherian (resp. Artinian)

PF $\qquad 0 \to (M_1 \oplus \cdots \oplus M_{n-1}) \to M_1 \oplus \cdots \oplus M_n \to M_n \to 0$

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, $N \subset M$ a submodule.
       Let $S = \{ L \subset N \mid L \text{ is finitely generated} \}$.

       note: if $L_1 \subset L_2 \subset L_3 \subset \ldots$ is a chain in L,
             then $\bigcup_{i=1}^{\infty} L_i = \bigcup_{i=1}^{n} L_i = L_n$ for some n, once $L_{n+k} = L_n$.
                                                                   $\therefore \bigcup_{i=1}^{\infty} L_i \in S$.

       Zorn $\Rightarrow$ S has a maximal element K
       If $K \neq N$, let $x \in N \setminus K$. Then $K + Rx$ is f.g., and $K \subsetneq K + Rx$ $\frac{1}{2}$.
       So $K = N$, i.e. N is f.g.

$\Leftarrow$ Let $M_1 \subset M_2 \subset M_3 \subset \ldots$ be a chain of submodules of M.

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

       Let m be minimal s.t. $x_1, \ldots, x_n \in M_m$.
       Then $M_m \supset N = \bigcup_{i=1}^{\infty} M_i$, so $M_i = M_m$ for all $i \geq m$. $\square$

Ex $k[x_1, x_2, \ldots]$ is not Noetherian

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

§2 Prime and primary ideals

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

Then $d = p_1^{n_1} \cdots p_k^{n_k}$ for some primes $p_i \in R$

so $(d) = (p_1^{n_1}) \cap \cdots \cap (p_k^{n_k})$

↑
Not a prime ideal!

But if $ab \in (p_1^n)$ and $a \notin (p_1^n)$, then $b^K \in (p_1^n)$ 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 Let $I \subset R$ be an ideal. The __radical of I__ is

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

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

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

Suppose $r^n \in I$, and $P \supseteq I$ is prime. Then $r^n \in P$, so $r \in P$.
Thus $r \in rad(I)$

Conversely, suppose $r \in rad(I)$, 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 $P \supseteq I$)

Note P is prime: If $x, y \notin P$, then $r^n \in P + xR$ for some $n \in \mathbb{N}$
$\qquad\qquad r^m \in P + yR$ for some $m \in \mathbb{N}$,
and $r^{n+m} \in P + xyR$, so $xy \in P$
(as $xy \notin P \Rightarrow r^{n+m} \notin P$, contradicts $P \in S$)

But P prime, $P \supseteq I \Rightarrow r \in P$ ↯

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 $(r^n)^m \in I$

$$r^{nm} \implies r \in \text{rad}(I).$$

  (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 $r^{n+m} \in I \cap J$, so $r \in \text{rad}(I \cap J)$

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

    ~~if $r \in \text{rad}(IJ)$, $r^n \in IJ$ 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 $Q \subset R$ is called **primary** if whenever $ab \in Q$ and $a \notin Q$, then $b^n \in Q$ for some $n \in \mathbb{N}$

Ex If R 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 $\bar{a}\bar{b} \in (x^2)$

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

$\bar{b} = b_0 + b_1 x + x^2 \tilde{b}(x)$ $b_0, b_1 \in \mathbb{R}$

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

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

$\bar{a}\bar{b} = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + x^2(*)$

So $a_0 b_0 = 0$ and $a_0 b_1 + a_1 b_0 = 0$

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 $b_0 = 0$ ⟵

(More generally, $(x^2, y^3) \subset \mathbb{R}[x, y]$ is primary)

___

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

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

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

So $a^n b^n$

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

b^{nm}

So $b \in \mathrm{rad}(Q)$.

Thus Q is prime.

___

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

P is called the <u>associated prime ideal</u> of Q

Q is called P-primary.

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

(i) $Q \subset P \subset \mathrm{rad}\, Q$ 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 $b \in P \subset \mathrm{rad}\, Q$, so $b^n \in Q$ for some $n \in \mathbb{N}$. Thus Q is primary.

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

Let $b \in \mathrm{rad}\, Q$, 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 $P = \mathrm{rad}\, Q$.

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

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

Pf Suppose ~~Q_1-2, Q_1~~ Q_1, Q_2 are P-primary.

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

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. $\blacksquare$

Def Let $I \subseteq R$ be an ideal. A <u>minimal prime</u> over I is a prime ideal $P \supseteq I$ s.t. if Q prime and $I \subseteq Q \subseteq P$, then $Q = P$.

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

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

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

I contained in a maxideal, so $S \neq \emptyset$

If $P_1 \supseteq P_2 \supseteq \dots$ 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, $I \subseteq P$, there is a minimal prime P_0 with $I \subseteq P_0 \subseteq P$)

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 min'l prime over $I + fR$ or $I + gR$.

$\Rightarrow I + fR$ (or $I + gR$) is a bigger counterexample ↯ ∎

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 $n \geq N$.

<u>Claim</u> $I = J_N \cap (I + (b^N))$

<u>Pf</u> $\subseteq$ ✓

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

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

$\Rightarrow b^N y \in I$

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

<s>So again</s>
Now I irreducible $\Rightarrow$ $I = J_N$ or $I = I + (b^N)$

<u>Case 1</u> $I = I + (b^N)$ $\Rightarrow$ $b^N \in I$

<u>Case 2</u> $I = J_N \supset J_1 \supset J_0 = I$, so $J_1 = I$

But $a \in J_1$, so $a \in I$.   ∎

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

<u>Pf</u> By lemma, it suffices to show every ideal is a finite intersection of irreducible ideals.

Let $S = \{ I \subset R \mid I$ is <u>not</u> a finite intersection of irreducible ones $\}$.

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
(otherwise I is irreducible)

Note WLOG $J_1 \in S$ (if J_1, K_1 both not in S, their intersection is not in S!)
Let $I_1 = J_1$.

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

This contradicts R being Noetherian!

So S had to be empty.   ∎

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

<u>pf</u> Let $I \subset R$ be radical.

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

Then $I = rad(I) = rad(Q_1 \cap \dots \cap Q_n) = rad(Q_1) \cap \dots \cap rad(Q_n)$
$$\underset{\text{all prime!}}{\uparrow \qquad \qquad \nearrow}$$

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

$$(\dots)$$

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

Pf $\Rightarrow$ R Noetherian $\Rightarrow$ _every_ ideal finitely generated.

$\Leftarrow$ Let $S = \{ I \subset R \mid I$ 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 $P + aR = (p_1 + ar_1, \ldots, p_n + ar_n)$ $\qquad p_i, q_i \in P$

$\qquad P + bR = $ ~~(..........)~~

$\qquad\qquad (q_1 + bs_1, \ldots, q_m + bs_m)$ $\qquad r_i, s_i \in R$

Now set $J = Ann_{R/P}(\{a\}) = \{ r \in R \mid ra \in P \}$, an ideal ("annihilator")

observe $(q_i + bs_i) a = q_i a + ab s_i \in P$, ~~not~~
$\qquad\qquad\qquad\qquad \underset{\in P}{\cap} \quad \underset{\in P}{\cap}$

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

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

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

Then $x = \overset{n}{\underset{i=1}{\sum}} (p_i + ar_i) y_i$ for some $y_i \in R$

Rearranging, $a \overset{n}{\underset{i=1}{\sum}} r_i y_i = x - \overset{n}{\underset{i=1}{\sum}} p_i y_i \in P$

So by definition $\overset{n}{\underset{i=1}{\sum}} r_i y_i \in J$, so $\overset{n}{\underset{i=1}{\sum}} r_i y_i = \overset{k}{\underset{i=1}{\sum}} j_i z_i$ for some $z_i \in R$.

Then $x = \overset{n}{\underset{i=1}{\sum}} p_i y_i + \overset{k}{\underset{i=1}{\sum}} j_i z_i a$

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

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

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

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 $M = Rx_1 + \cdots + Rx_n$

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

we have an injective map $\Theta : R/I \longrightarrow R/I_1 \oplus \cdots \oplus R/I_n$

claim $R/I_i \cong Rx_i$
$$r + I_i \longrightarrow rx_i$$

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

Injective: if $rx_i = 0$, $r \in I_i$

Surjective $1 + I_i \longrightarrow x_i$

M Noetherian $\Rightarrow$ Rx_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. ∎

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

Thm 3.2 Let $M \subseteq N$ be a primary R-submodule. Then $\text{Ann}_R(N/M)$ is a primary ideal in R.

Pf Let $Q = \text{Ann}_R(N/M) = \{r \in R \mid rN \subseteq M\}$
Let $r, s \in R$ with $rs \in Q$, $s \notin Q$
we need to show $r^n \in Q$ for some $n \in \mathbb{N}$.

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

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

$$\text{Since } M \text{ primary}, \ r^n N \subseteq M \text{ for some } n \in \mathbb{N}. \qquad \blacksquare$$

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

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

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

Note $I \subseteq \text{Ann}_R(N/M) \subseteq P$, 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 $\bar{r}^n N \subseteq M$ for some $n \in \mathbb{N}$.

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

$$\implies \bar{r}^n N \subseteq M$$

Now observe that Lemma 4.2 $\implies$ $\bar{R} = R/I$ 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 $\bar{P}_i^{n_i} N \subseteq M$ for some $n_i \in \mathbb{N}$.

Set $m = n_1 + \dots + n_s$

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

Since $\bar{P} = P/I$ and $IN = 0$, we must be $P^m N \subseteq M$. $\qquad \blacksquare$

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 $N \subseteq M$. If $IN = M$, then $M \subseteq N$, 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 $IN \subseteq N$, so it suffices to show $N \subseteq M_i$ for each i.

__Case 1__ $I \subset P_i$

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

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

__Case 2__ $I \not\subset P_i$

There exists $r \in I \setminus P_i$

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

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

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

$\Rightarrow$ $r \in \operatorname{rad}\left(\operatorname{Ann}_R (M/M_i)\right) = P_i$ ⨎

Thus $N \subset M_i$. ☑

<u>Motivation</u> Let (R, m) be a local ring, M ~~an submodule~~ a f.g. R-module.

Then M/mM is a (finite dimensional) R/m-vector space.

what can we say if $M/mM = 0$? i.e. $M = mM$?

~~we~~ 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 $x_1 \in mM$

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

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

$$\nearrow$$
$$\in R^*$$

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

So we had to have $M = 0$

<u>Nakayama's Lemma (v1)</u> Let (R, m) be a local ring, M a f.g. R-module.

Then $M = 0 \iff M/mM = 0$

<u>Nakayama's Lemma (v2)</u> Let (R, m) be a local ring, M a f.g. R-module.

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

Then $M = Rx_1 + \dots + Rx_n$

<u>Pf</u> Let $N = Rx_1 + \dots + Rx_n \subseteq M$

Then $N/mM = M/mM$

So $0 = \dfrac{M/mM}{N/mM} \cong M/N \implies M = 0.$ ∎

What if R is not local?

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

when is $1 - m \in R^*$?

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

If m in this max ideal, so is $1 \to$ contradiction!

So we need an ideal contained in every maximal ideal.

Lemma 4.5 (Nakayama) Let $I \subseteq R$ 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 f.g. R-module with $IM \supseteq M$, then $M = 0$

(iv) If N is a f.g. R-module with $M \supseteq IM + N$, then $M \supseteq N$

•

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

Pf $\Rightarrow$ Let $N = \bigcap_{n \geq 1}^{\infty} I^n M$. Krull intersection $\Rightarrow IN = N$

Nakayama $\Rightarrow N = 0$.

$\Leftarrow$ Let $m \subseteq R$ be a maximal ideal.
Then R/m is a field, hence a simple R-module, so Noetherian.
So $N \overset{!!}{=} \overset{R/m}{}$ then $\bigcap_{n \geq 1}^{\infty} I^n N = 0$.
Since IN is a submodule of N, either $IN = N$, hence $I^n N = N \Rightarrow \bigcap_{n \geq 1}^{\infty} I^n N = N$ ⨯
or $IN = 0 \Rightarrow I \subseteq m$ s.t. $N = R/m$.

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

Prop 4.8 (Kaplansky, 1958) Let (R, 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.

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

$F = R_1 \oplus \cdots \oplus R_n$
$K = \ker \pi$

Claim $K \subset mF$

Suppose not: There exists $\kappa \in K \setminus mF$

$$\kappa = r_1 x_1 + \cdots + r_n x_n \qquad r_i \in R \text{ and WLOG, } r_1 \notin m.$$
$$\text{So } r_i \in R^x$$

Then $x_1 - r_1^{-1}\kappa = -r_1^{-1}r_2 x_2 + \cdots - r_1^{-1}r_n x_n$

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

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

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

$$F = K + P \subset mF + P$$

Then $F/P \subset mF/P \subset m(F/P)$, so $F/P = m(F/P)$

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

Thm 4.1 (Hilbert's Basis Theorem) If R is Noetherian, then $R[x_1, \ldots, x_n]$ 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 $I_n = \left\{ \frac{f^{(n)}(0)}{n!} \mid f \in I \right\} =$ 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 $r \in I_n$, $r = \frac{f^{(n)}(0)}{n!} = \frac{(xf)^{(n+1)}(0)}{(n+1)!} \in I_{n+1}$

$$I_0 \subset I_1 \subset I_2 \subset \ldots$$

R Noetherian $\Rightarrow$ $I_n = I_\ell$ for all $n \geq \ell$ for some fixed ℓ.

Write $I_n = r_{n,1} R + \ldots + r_{n,i_n} R$ for some $r_{n,j} \in I_n$ for all $n \leq \ell$.

Write $r_{n,j} = \frac{f_{n,j}^{(n)}(0)}{n!}$ for some $f_{n,j} \in I$

Claim $I = \sum_{n=0}^{\ell} \sum_{j=1}^{i_n} f_{n,j} R$

$\underbrace{\qquad\qquad}_{\text{Call this } J}$

Pf $\supseteq$ ✓

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

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

$\ell \geq K > 1$: Let $f \in I$ have degree K and set $r = \frac{f^{(K)}(0)}{K!} \in I_K \setminus \{0\}$

Write $r = r_{K,1} s_1 + \ldots + r_{K,i_K} s_{i_K}$ for some $s_j \in R$.

Set $\tilde{f} = f - (f_{K,1} s_1 + \ldots + f_{K,i_K} s_{i_K})$

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

···

$K \geq \ell$ Let $f \in J$ have degree K, let $r = \frac{f^{(K)}(0)}{K!} \in J_K \setminus \{0\}$

write $r = f_{K,1} S_1 + \dots + f_{K,i_K} S_{i_K}$ for some $S_j \in R$.

Set $\tilde{f} := f - x^{K-b}\left(f_{K,1} S_1 + \dots + f_{K,i_K} S_{i_K} \right)$

The $\deg \tilde{f} < \deg f$, so induction $\Rightarrow$ $\tilde{f} \in J$, so $f \in J$. $\blacksquare$

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

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

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

Thm Let k be a field. TFAE
   (i) Every nonconstant polynomial $f \in k[x]$ has a root in k.
   (ii) Every irreducible polynomial in $k[x]$ has degree one.
   (iii) Every polynomial $f \in k[x]$ splits, i.e. factors as a product of linear polynomials
   (iv) There is no algebraic extension of k (except k, trivially)

Such a field k is called <u>algebraically closed</u>.

Pf (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (iv)
   Not (i) $\Rightarrow$ Not (iv): If $f \in k[x]$ has no root in k, $K = \operatorname{Frac} k[x]/f$ is an algebraic extension of k.

Def Let k be a field. An extension K is called an <u>algebraic closure</u> of k 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 $f \in k[x_1, \ldots, x_n]$ and $s_1, \ldots, s_n \in S$ with $f(s_1, \ldots, s_n) = 0$. Otherwise S is called *algebraically independent*.

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

Pf ~~Bijective~~ Bijective map
$$k[x_1, \ldots, x_n] \longrightarrow k[s_1, \ldots, s_n]$$
$$x_i \longmapsto s_i$$

extends to ~~bijective~~ bijective map
$$k(x_1, \ldots, x_n) \longrightarrow k(s_1, \ldots, s_n)$$

Def 1.4 Let K/k be a field ~~extension~~ 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, $\{x_1, \ldots, x_n\}$ is a transcendence basis of $k(x_1, \ldots, x_n)$ 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 $s_1, \ldots, s_n \in S$, $f \in k[x_1, \ldots, x_{n+1}]$ with $f(s_1, \ldots, s_n, u) = 0$ and $\deg_{x_{n+1}} f > 0$.

Let ~~g~~ $g(x_{n+1}) = f(s_1, \ldots, s_n, x_{n+1}) \in K(S)[x_{n+1}]$ so $\deg g > 0$.
Then $g(u) = 0$, so u algebraic over $K(S)$ by

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

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

$$f = \sum_{i=0}^{n} \frac{f_i(s_1, \ldots, s_n)}{g(s_1, \ldots, s_n)} x^i = \frac{1}{g(s_1, \ldots, s_n)} \sum_{i=0}^{n} \tilde{f}_0(s_1, \ldots, s_n) x^i.$$

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

Now $f(u) = 0 \Rightarrow h(s_1, \ldots, s_n, u) = 0 \Rightarrow \tilde{f}_i = 0$ for all $i \Rightarrow f = 0$

$\uparrow$ Since $S \cup \{u\}$ algebraically independent $\qquad \blacksquare$

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 $u \in K(k(S))$. Then S transcendence basis $\Rightarrow S \cup \{u\}$ algebraically dependent~~

~~$\Rightarrow$ u algebraic over $k(S)$~~

$\Leftarrow$ K algebraic over $k(S)$ $\iff$ $S \cup \{u\}$ is algebraically dependent for all $u \in K \setminus k(S)$

$\iff$ ~~$S \subseteq$~~ S a transcendence basis. $\qquad \blacksquare$

Cor 1.7 Let K/k be a field extension. If K is algebraic over $k(X)$ for some $X \subset K$, 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. $\qquad \blacksquare$

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

§5 Ring Extensions

Def 5.1 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 $k \subset k[x]$ is a ring extension.

Ex $2\mathbb{Z} \subset \mathbb{Z}$ is __not__ a ring extension.

Def 5.2 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/k is an algebraic field extension, it is an integral ring extension.

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

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 a $\overset{\text{subring}}{T}$ 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) => (ii) s integral => $s^n = \sum_{i=0}^{n-1} a_i s^i$ for some $a_i \in R$.

$$\Rightarrow R[s] = R + Rs + \cdots + Rs^{n-1}$$

(ii) => (iii) $T = R[s]$ suffices

(iii) => (iv) Let $B = T$. If $\alpha \in Ann_{R[s]} B$, $\alpha \cdot 1 = 0 \Rightarrow \alpha = 0$.

since $B = T$ a ring extension
↓

(iv) => (i) Write $B = Rb_1 + \cdots + Rb_n$

Since B is a $R[s]$-module, can write $sb_i = r_{i1} b_1 + \cdots + r_{in} b_n$ for some $r_{0,j} \in R$.

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

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

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

so $\det(sI - A) \in Ann_{R[s]} B = 0$

But $\det(sI - A)$ ~~eq R[s]~~ is a monic polynomial in S. ∎

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

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

Pf
$$R \subseteq R[s_1] \subseteq R[s_1, s_2] \subseteq \ldots \subseteq R[s_1, \ldots, s_n]$$

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

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

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

Thm 5.6 Let $R \subseteq S \subseteq T$ 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 $f = \sum_{i=0}^{n} s_i x^i$

Note $f \in R[s_0, \ldots, s_{n-1}][x]$, so t is integral over $R[s_0, \ldots, s_{n-1}]$,
so $R[s_0, \ldots, s_{n-1}, t]$ is a f.g. $R[s_0, \ldots, s_{n-1}]$ module

Since S integral over R, $R[s_0, \ldots, s_{n-1}]$ is a f.g. R-module

$\Rightarrow R[s_0, \ldots, s_{n-1}, t]$ is a f.g. R-module

$\underset{R[t]}{\cup} \quad \Rightarrow t$ integral by Thm 5.3.

Thm 5.7 Let $R \subseteq S$ be ring extension. Let $\bar{R} = \{s \in S \mid s \text{ is integral over } R\}$, called the <u>integral closure</u> 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 $R \subseteq \bar{R}$ is a ring extension.
If $s, t \in \bar{R}$, $\quad s, t \in R[s, t]$ so $s+t, st \in R[s,t] \subseteq \bar{R}$
Since s, t integral, $R[s,t] \subseteq \bar{R}$ ∎

(147)

Def If $R \subseteq S$ 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 $\bar{\mathbb{Q}}$, since i is integral over $\mathbb{Z}$.

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

Ex Every UFD is integrally closed. In particular, $k[x_1, \ldots, x_n]$ is integrally closed.
Let R be a UFD, $\frac{a}{b} \in \text{frac } R$ integral. with $(a,b)=1$

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

$$a^n = -c_{n-1}a^{n-1}b - \ldots - c_1 ab^{n-1} - c_0 b^n$$
$$= b(-c_{n-1}a^{n-1} - \ldots - c_1 ab^{n-2} - c_0 b^{n-1})$$

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, $S \subseteq R$ 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 $S^{-1}R$

$$\left(\frac{a}{b}\right)^n + \frac{r_{n-1}}{s_{n-1}}\left(\frac{a}{b}\right)^{n-1} + \ldots + \frac{r_1}{s_1}\left(\frac{a}{b}\right) + \frac{r_0}{s_0} = 0 \qquad \text{for some } \frac{r_i}{s_i} \in S^{-1}R \quad (\text{so } s_i \in S, \ r_i \in R)$$

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

$$\left(\frac{sa}{b}\right)^n + \frac{s r_{n-1}}{s_{n-1}}\left(\frac{sa}{b}\right)^{n-1} + \ldots + \frac{s^n r_1}{s_1}\left(\frac{sa}{b}\right) + \frac{s^n r_0}{s_0} = 0 \qquad \text{so } \frac{sa}{b} \text{ is integral over } R.$$

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

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 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... these ~~

Thm 2.2 $\Rightarrow$ 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 $Q \subset Q + uS \notin C$, so $Q + uS \notin C$

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

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

S integral $\Rightarrow$

$$ s^n + r_{m-1} s^{m} + \dots + r_1 s + r_0 = 0 \qquad \text{for some } r_i \in R $$

$$ (su)^n + (r_{m-1} u)(su)^{m} + \dots + (r_1 u^{m-1})(su) + (r_0 u^n) = 0 $$

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

$$ c^n + (r_{m-1} u) c^{m-1} + \dots + (r_1 u^{m-1})c + (r_0 u^n) \in Q. $$

$$ v := c^n + (r_{m-1} u) c^{n-1} + \dots + (r_1 u^{m-1})c + (r_0 u^n) $$

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. ↯ ☑

<u>Cor 5.10</u> (Going-up Theorem) Let $R \subseteq S$ be an integral extension, and $P_1 \subseteq P \subseteq R$ two prime ideals If $Q_1 \subseteq S$ lies over P_1, there exists a prime ideal Q lying over P with $Q_1 \subseteq Q$

<u>Pf</u> $R/P_1 \subseteq S/Q_1$ is integral.

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

Then Q lies over P.

<u>Thm 5.11</u> Let $R \subseteq S$ be an integral extension, $P \subseteq R$ prime. Suppose $Q, Q' \subseteq S$ are prime ideals lying over P. If $Q_1 \subseteq Q_2$, then $Q_1 = Q_2$.

<u>Pf</u> Let $\mathcal{C} = \{ I \subseteq S \mid I \text{ lies over } P \}$. Suffices to prove:

<u>Clm</u> If $Q \in \mathcal{C}$ is prime, then Q is maximal in $\mathcal{C}$.

<u>Pf</u> Suppose not: there exists $I \in \mathcal{C}$ with $Q \subsetneq I$

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

~~$u^n + r_{n-1} u^{n-1} + \dots + r_1 u + r_0 = 0$~~ ~~for some $r_i \in R$~~

~~Therefore, this integral~~

~~Now~~ ~~$r_0 \in r_0 \subseteq I$,~~ ~~so that $I \cap R = P \subseteq Q$.~~

~~Then~~

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

$f(u) = u^n + r_{n-1} u^{n-1} + \dots + r_1 u + r_0 \in Q \subseteq I$ for some $r_i \in R$

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

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 $\Rightarrow u \in Q$ ⨯   ▨

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 $\Rightarrow$) Then 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 maximal, $P = N \cap R$.

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

Thm 7.2 (Noether Normalization Lemma) Let k be a field, $R = k[u_1, \ldots, u_n]$ a fin. generated k-algebra. Assume R is an integral domain, and let r be transcendence degree of Frac R over k. Then there exists an algebraically independent subset $\{t_1, \ldots, t_r\} \subset R$ such that R is integral over $k[t_1, \ldots, t_r]$.

Pf Note Frac $R \supset k(u_1, \ldots, u_n)$. If $\{u_1, \ldots, u_n\}$ is algebraically independent over k, then $r = n$, and R is trivially integral over $k[u_1, \ldots, u_n]$. (so $r \leq n$)

So assume $\{u_1, \ldots, u_n\}$ algebraically dependent over k.

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

for all j, $(i_1, \ldots, i_n) \in I$.

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

Consider $J = \{ i_1 + c i_2 + \cdots + c^{n-1} i_n \mid (i_1, \ldots, i_n) \in I \}$

Claim $|J| = |I|$

Pf Suppose $i_1 + c i_2 + \cdots + c^{n-1} i_n = j_1 + c j_2 + \cdots + c^{n-1} j_n$ for some $(i_1, \ldots, i_n), (j_1, \ldots, j_n) \in I$.

Then $c \mid i_1 - j_1$, but $c > i_1$, $c > j_1$, so $i_1 = j_1$.

Then
$$c i_2 + \dots + c^{n-1} i_n = c j_2 + \dots + c^{n-1} j_n$$
$$i_2 + \dots + c^{n-2} i_n = j_2 + \dots + c^{n-2} j_n$$

Same argument $\Rightarrow$ $i_2 = j_2$, $\dots$, $i_n = j_n$.

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

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

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

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

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

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

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

IF $\{v_2, \dots, v_n\}$ is algebraically independent, result reduces one dim.

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

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

IF $\{v_3, \dots, v_n\}$ als independent done. Otherwise, repeat ...

$\square$

§7 Hilbert's Nullstellensatz

Let k be a field throughout.

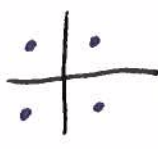**Def** If $S \subset k[x_1, \ldots, x_n]$, the _vanishing set_ of S is

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

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 $V(k^2) = V(x)$

Remark If $I = (S)$ is ideal generated by S, then $V(S) = V(I)$

$\Rightarrow$ Every algebraic set is vanishing set of a finite set of poly's.

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

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

Note $I(Y)$ is always an _ideal_

Lemma 7.1 Let k be algebraically closed, $S, T \subset k[x_1, \ldots, x_n]$, $X, Y \subset k^n$

(i) $V(k[x_1, \ldots, x_n]) = \emptyset$
$I(k^n) = 0$
$I(\emptyset) = k[x_1, \ldots, x_n]$

(ii) $S \subset T \implies V(S) \supset V(T)$
$X \subset Y \implies I(X) \supset I(Y)$

(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) $\implies V(S) \subset V(I(V(S)))$
Also $S \subset I(V(S))$, so $V(S) \supset V(I(V(S)))$

(iii) $\implies I(X) \subset I(V(I(X)))$
Also, $X \subset V(I(X)) \implies I(X) \supset I(V(I(X)))$

Observe 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 $\implies$ radical ideals!

Lemma 7.3 (weak Nullstellensatz) Let k be algebraically closed, $I \subset k[x_1, \ldots, x_n]$ 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 $R = k[x_1, \ldots, x_n]/P = k[u_1, \ldots, u_n]$

Noether Normalization $\implies$ R integral over $k[t_1, \ldots, t_r]$ and $\{t_1, \ldots, t_r\}$ alg independent.

Let $M = (t_1, \ldots, t_r) \subset S$, a maximal ideal.
There is a maximal ideal $N \subset R$ lying over M.

Let $J: R \longrightarrow R/N$ be quotient; note $J(R) \cong R/N$ is a field.

Then $R \cong \mathscr{k}[b_{1,\dots}, b_r]/M = \mathscr{k}[b_{1,\dots}, b_r]/N \cap \mathscr{k}[b_{1,\dots}, b_r] \cong (\mathscr{k}[b_1 + \dots + b_r] + N)/N = J(\mathscr{k})[b_{1,\dots}, b_r]$

$\underset{\text{Second Iso Thm}}{\uparrow}$

Since R integral over $\mathscr{k}[b_{1,\dots}, b_r]$, $J(R)$ algebraic over $J(\mathscr{k}[b_{1,\dots}, b_r])$

$\Rightarrow J(R) = \mathscr{k}[\overline{b_1}, \dots, \overline{b_r}] = \mathscr{k}.$

$$\mathscr{k}[x_{1,\dots}, x_n] \xrightarrow{\pi} R \xrightarrow{J} \mathscr{k}$$

Call this composition φ.

Then $(\varphi(x_1), \dots, \varphi(x_n)) \in V(P)$, since for all $f \in P$, $\varphi(f) = f(\varphi(x_1), \dots, \varphi(x_n)) = 0$.

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

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

__Pf.__ $\supset$ Let $f \in \mathrm{rad}(J)$, so $f^m \in J$ for some $n \geq 1$.

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

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

Define $L \subset \mathscr{k}[x_1, \dots, x_n, Y]$ by $L = (J, Yf - 1)$ "Rabinowitsch trick"

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

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

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

Weak Nullstellensatz $\Rightarrow L = \mathscr{k}[x_1, \dots, x_n, Y]$

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

Note that $Yf-1$ is irreducible, hence prime

fractional field
↓

$$k[x_1,\ldots,x_n,Y] \longrightarrow k[x_1,\ldots,x_n,Y]\!\Big/\!_{(Yf-1)} \cong k[x_1,\ldots,x_n,\tfrac{1}{f}] \longrightarrow k(x_1,\ldots,x_n)$$

Apply this map

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

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

Then $\quad f^m = \sum_{i=1}^{b} \left(f^m g_i(x_1,\ldots,x_n,\tfrac{1}{f})\right) f_i(x_1,\ldots,x_n) \in J$

So $f \in \mathrm{rad}(J)$. ∎

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 $I(X)$ is prime

Pf $\Leftarrow$ Let $P = I(X)$ be prime. Note $X = V(I(X)) = V(P)$.
Suppose $X = X_1 \cup X_2$, and $X \neq X_1$ (we will show $X = X_2$)
Then $P = I(V(P)) = I(X_1 \cup X_2) = I(X_1) \cap I(X_2)$.
If $I(X) \supsetneq I(X_1)$, then $X = V(I(X)) = V(I(X_1)) = X_1$ ↯ so let $f \in I(X) \setminus I(X_1)$
Now, for any $g \in I(X_2)$, $fg \in I(X_1) \cap I(X_2) = P$, so P prime $\Rightarrow g \in P$.
Thus $I(X_2) \subset P \subset I(X_2)$, so $I(X) \supset P = I(X_2) \Rightarrow X = X_2$.

$\Rightarrow$ Suppose X is irreducible. Let $f, g \in R$ with $fg \in I(X)$.
Then $X \subset V(fg) = V(f) \cup V(g)$
so $X = (X \cap V(f)) \cup (X \cap V(g))$

(156)

X irreducible $\Rightarrow$

$\qquad X = X \wedge V(f) \qquad \Rightarrow X \subset V(f) \Rightarrow f \in I(x)$

$OR \quad x = x \wedge V(g) \qquad \Rightarrow x \subset V(g) \Rightarrow g \in I(x)$

Def An irreducible algebraic set is called an <u>affine variety</u>.

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

Observe: (1) A finite union of algebraic sets is a algebraic set $\quad (s_{in} \ V(I_1) \cup \dots \cup V(I_n) = V(I_1 \dots I_n)$

$\qquad$ (2) An arbitrary intersection of algebraic sets is a algebraic set $(s_{in} \cap V(I_k) = V(\cup I_k))$

$\qquad$ (3) $\emptyset$ and k^n are algebraic sets

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