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

(1) $(R, +)$ is an abelian group

(2) $(R, \cdot)$ is a semigroup

(3) $a(b+c) = ab + ac$ for all $a, b, c \in \mathbb{R}$.
$(a+b)c = ac + bc$

If multiplication is commutative, R is called a commutative ring

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

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

Thm 1.2 Let R be a ring.

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

(ii) $(-a)b = a(-b) = -(ab)$ for all $a, b \in \mathbb{R}$

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

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

(v) $\left(\sum_{i=1}^{n} a_i\right)\left(\sum_{j=1}^{m} b_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j$ for all $a_i, b_j \in R$

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

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

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

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

(v) Distributive property ∎

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

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

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

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

Ex $\mathbb{Z}$ is an integral domain.

Def 1.7 Let R, S be rings. A function $f: R \to S$ is called a *homomorphism* if

$$\left.\begin{aligned} f(a+b) &= f(a) + f(b) \\ f(ab) &= f(a) f(b) \end{aligned}\right\} \text{ for all } a, b \in R.$$

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 [redacted] $\varphi : \mathbb{Z} \to R$ be the map given by $\varphi(m) = m\cdot 1$.

φ is a homomorphism with ~~Kernel~~ $\operatorname{Ker}\varphi = \langle n \rangle$

(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 $m \in \operatorname{Ker}\varphi$, $ma = m\cdot 1\cdot a = 0\cdot a = 0$ 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 $0 = n\cdot 1 = K r \cdot 1 = K 1 \cdot r \cdot 1$ ◻

[redacted]

§2 Ideals

Observe: If $x, y \in \operatorname{Ker}\varphi$, $x+y, xy \in \operatorname{Ker}\varphi$

But also If $a \in R$, $x \in \operatorname{Ker}\varphi$, $ax \in \operatorname{Ker}\varphi$

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

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

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

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

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

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

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

Cor 2.3 The intersection of ideals is an ideal.

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

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

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

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

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

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

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

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

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

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

Pf well defined: Suppose $a+I = a_0+I$, $b+I = b_0+I$

$a = a_0 + x$ for some $x \in I$ $\quad$ $b = b_0 + y$ for some $y \in I$

Then $a_0b_0 + I = (a-x)(b-y) + I = ab \underset{\underset{I}{\Uparrow}}{-ay} \underset{\underset{I}{\Uparrow}}{-xb} \underset{\underset{I}{\Uparrow}}{+xy} + I = ab + I.$ ∎

Thm 2.8 If $\varphi: R \to S$ is a ring homomorphism, $\operatorname{Ker}\varphi$ is an ideal

Pf If $a, b \in \operatorname{Ker}\varphi$, $\varphi(a+b) = \varphi(a) + \varphi(b) = 0 + 0 = 0$, so $a+b \in \operatorname{Ker}\varphi$

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

$\varphi(xa) = \varphi(x)\varphi(a) = \varphi(x)0 = 0$, so $xa \in \operatorname{Ker}\varphi$ ☒

~~[illegible]~~

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

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

Pf Let $\bar{\varphi}: R/\operatorname{Ker}\varphi \to \operatorname{Im}\varphi$ be the well defined abelian group isomorphism.

$a + \operatorname{Ker}\varphi \mapsto \varphi(a)$

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

$\bar{\varphi}(ab + \operatorname{Ker}\varphi) = \varphi(ab)$ so $\bar{\varphi}$ is a ring isomorphism. ☒

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

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

~~[illegible]~~ for all ideals $I, J \subset R$

$IJ \subset P \Rightarrow I \subset P$ or $J \subset P$

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

~~1) If R is prime, then R\P is multiplicatively closed, i.e. if ab∈P then a∈P or b∈P.~~

~~2) If R is commutative & 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 $ab \notin P$, 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 $x \in I \setminus P$. 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 $(a)(b) \subset P$

If $x \in (a)(b)$, $x = ar_1 br_2$ 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 (0) is prime iff R is an integral domain.

Pf Let $a, b \in R \setminus (0)$. Then (0) is prime iff $ab = 0$ implies $a = 0$ or $b = 0$ 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 ■ □

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

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

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

(1) C is a proper ideal: Let $a, b \in C$, so $a \in C_i$, $b \in C_j$.

Since $\mathcal{C}$ is a chain, WLOG $C_i \subset C_j$, so $a+b, ab \in C_j \subset C$.

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

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

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

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

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

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

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

$$1 = m_1 + ar_1 = m_2 + br_2 \quad \text{for some } m_1, m_2 \in M,\ r_1, r_2 \in R.$$

Then $1 = (m_1 + ar_1)(m_2 + br_2) = \underbrace{m_1 m_2 + m_1 b r_2 + m_2 a r_1}_{\Uparrow \, M.} + ab r_1 r_2$

If $ab \in M$, then $1 \in M$ ↯ so $ab \notin M$, thus M is prime. ☒

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 $R \longrightarrow S$ 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) $\blacksquare$

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

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

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

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

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

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

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

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

Then
$$\begin{aligned}\varphi(a_1,\dots,a_n)\varphi(b_1,\dots,b_n) &= (a_1+\dots+a_n)(b_1+\dots+b_n)\\ &= a_1b_1+\dots+a_nb_n\\ &= \varphi((a_1,\dots,a_n)(b_1,\dots,b_n))\end{aligned}$$ ∎

Thm 2.25 ("Chinese Remainder Theorem" – Sun-Tsze, ~ 400 AD)

Let $I_1,\dots,I_n\subset R$ be ideals such that $R^2+I_i=R$ for all i and $I_i+I_j=R$ for all $i\neq j$ ($I_1,\dots,I_n$ called pairwise comaximal)

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

$b\equiv b_i \bmod I_i$ for each $1\le i\le n$.

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

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

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

$m=2$: $R = I_1 + I_2$ ✓

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

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

Since $R = R^2 + I_1$, $R = I_1 + (I_2 \cap \dots \cap I_m)$

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

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

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

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

Cor 2.26 Let $m_1, \dots, m_n$ be pairwise coprime positive integers. Let $b_1, \dots, b_n \in \mathbb{Z}$. Then there is a solution to

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

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

Pf Let $I_i = (m_i)$. 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 *ring of polynomials over R*, denoted $R[x]$ is

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

(2) Addition is component wise

(3) Multiplication given by

$$(a_0, a_1, \dots)\cdot(b_0, b_1, \dots) = (a_0b_0,\ a_0b_1 + a_1b_0,\ a_0b_2 + a_1b_1 + a_2b_0,\ \dots$$

(n^{th} component is $\sum_{i+j=n} a_ib_j$

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

Pf Need to check multiplication is associative

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

$$(a_i)\left(\left((b_i)\cdot(c_i)\right)\right) = (a_i)\cdot\left(\sum_{j+k=i} b_jc_k\right)$$

$$= \left(\sum_{r+s=i} a_r \sum_{j+k=s} b_jc_k\right)$$

$$= \left(\sum_{r+j+k=i} a_rb_jc_k\right)$$

$$\left((a_i)\cdot(b_i)\right)\cdot(c_i) = \left(\sum_{j+k=i} a_jb_k\right)\cdot(c_i)$$

$$= \left(\sum_{r+s=i}\left(\sum_{j+k=r} a_jb_k\right)c_s\right)$$

$$= \left(\sum_{j+k+s=i} a_jb_kc_s\right)$$

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) $x^n = (0,0,\dots,0,\underset{\substack{\uparrow \\ n+1\text{-st spot}}}{1},0,0,\dots)$

(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 $f = \sum_{i=0}^{n}\left(\sum_{j=0}^{m} a_{ij} x^j\right) y^i = \sum_{j=0}^{m}\left(\sum_{i=0}^{n} a_{ij} y^i\right) x^j$ $\blacksquare$

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

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

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

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

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) $\blacksquare$

This is called the evaluation map or substitution map

HW1 (6,7)

§3 Factorization in commutative rings

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

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

(i) $a \mid b \iff (b) \subset (a)$

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

(iii) $u \in R^* \iff u \mid r$ 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) $a \mid b \iff b \in (a) \iff (b) \subset (a)$

(ii) Immediate from (i)

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

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

(iv) Note (iii) says $u \in R^* \iff u \mid 1 \iff R \subset (u)$ by (i)

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

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

Then $a = ayx \iff a(1 - yx) = 0$ $\Rightarrow x, y \in R^*$ $\blacksquare$

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 $x \mid ab$, then $x \mid a$ or $x \mid b$.

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

Ex $R = k[x,y]/(x^2-y^3)$

y is irreducible

But $y(y^2) = x^2$, so $y \mid x^2$. But $y \nmid x$, so y is <u>not</u> 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 $a \mid x$, either $a \in R^*$ or $x \mid a$ (i.e. a is an associate).

Pf (i) Immediate

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

If $a \in R^*$, then $(x) = (y)$. If $y \in R^*$, then $(y) = R$.

$\Leftarrow$ Suppose $x = ab$ for some $a, b \in R$. Then $(x) \subset (a)$,

So $(x) = (a)$ (i.e. $b \in R^*$) or $(a) = R$ (i.e. $a \in R^*$).

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

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

<u>Def 3.5</u> An integral domain is called a <u>unique factorization domain</u> if every element factors uniquely (up to units) as a product of irreducibles

<u>Ex</u> $\mathbb{Z}$ is a UFD

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

Observe: If R a UFD and x irreducible, ~~[illegible] is a unit.~~ ~~[illegible] irreducible.~~

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

so x is prime.

<u>Thm 3.7</u> Every PID is a UFD.

<u>Lemma 3.6</u> A PID is Nötherian, i.e. every chain of ideals

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

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

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

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

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

<u>Pf</u> (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

$x = p_1 p_2 p_3 q_3$

$\vdots$

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

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

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

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

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

Then since a domain, cancel, $p_2 \cdots p_r = q_2 \cdots q_s$. Induct. $\boxtimes$

— x —

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 An integral domain R is called a <u>Euclidean domain</u> if there exists a function $\varphi : R \setminus \{0\} \to \mathbb{N}$ such that

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

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

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

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

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

<u>Ex</u>
$$\frac{3+4i}{1+2i} = \frac{(3+4i)(1-2i)}{\underset{\varphi(1+2i)\nearrow}{5}} = \frac{11}{5} - \frac{2}{5}i$$
$$= 2 + \frac{1}{5} - \frac{2}{5}i$$

$$(3+4i) = 2(1+2i) + \left(\tfrac{1}{5} - \tfrac{2}{5}i\right)(1+2i)$$
$$= 2(1+2i) + 1$$

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

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

Write $ac+bd = q_1\varphi(\beta)+r_1$ with $|r_1| \le \frac{1}{2}\varphi(\beta)$ $\quad (bc-ad) = q_2\varphi(\beta)+r_2$ with $|r_2| \le \frac{1}{2}\varphi(\beta)$

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

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

Now $\varphi\left(\frac{(r_1+r_2 i)\beta}{\varphi(\beta)}\right) = \varphi\left(\frac{r_1+r_2 i}{\bar{\beta}}\right) = \frac{\varphi(r_1+r_2 i)}{\varphi(\beta)} = \frac{r_1^2+r_2^2}{\varphi(\beta)} \le \frac{(\frac{1}{2}\varphi(\beta))^2+(\frac{1}{2}\varphi(\beta))^2}{\varphi(\beta)} \ge \frac{1}{2}\varphi(\beta)$

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

Do Ex first!

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

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

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

If $n>m$: [illegible] Let $q = \frac{a_m}{b_m} x^{n-m}$

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

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

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

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

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

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

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

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

Thm 3.9 Euclidean rings are PIDs.

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

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

~~Then $x = qy$~~ $r = x - qy \in I \Rightarrow r = 0$

So $x = qy$

Thus $I = (y)$. ∎

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

§4 Rings of quotients + localization

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

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

Def 4.1 A nonempty subset $S\subset R$ is called <u>multiplicative</u> if it is ~~multiplicatively close~~ 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, $R\setminus P$ is multiplicative

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

Thm 4.2 Let R be a commutative ring, and $S\subset R$ multiplicative
Define $\sim$ on $R\times S$ by
$(a,b)\sim(c,d)$ 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 $(c,d)\sim(e,f)$

$s(ad-bc)=0$ $\quad t(cf-de)=0$ for some $s,t\in S$

$$\begin{tikzcd} sad = sbc \arrow[r, bend right, leftrightarrow, "\text{make same}"'] & tcf = bde \end{tikzcd}$$

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

$sadtf - tdesb = 0$ $\implies (a,b)\sim(e,f)$

$\underbrace{std}_{\overset{?}{S}}(af-be)=0$

$\square$

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

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

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

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

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

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

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

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

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

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

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

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

$$(tcD)s(aB-bA) + (sbA)(t)(cD-dC) = 0$$

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

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

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

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

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

(note $\frac{s}{s} \in S^{-1}R$ is 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 $S = \{1, x, x^2, \dots\} \subset \mathbb{C}[x]$

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

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

(i) the map $\varphi : R \longrightarrow S^{-1}R$, $r \longmapsto \frac{rs}{s}$ for any $s \in S$ is a well defined homomorphism

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

(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.

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

$rst - rst = 0$ ✓

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

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

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

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 $\varphi(rs^{-1}) = \frac{rs^{-1} \cdot s}{s} = \frac{r}{s}$

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

$$\begin{tikzcd} R \arrow[r, "f"] \arrow[d, hook] & T \\ S^{-1}R \arrow[ur, dashed, "\bar{F}"'] & \end{tikzcd}$$

Pf Define $\bar{F}\left(\frac{r}{s}\right) = f(r)f(s)^{-1}$

well defined: s'pose $\frac{r}{s} = \frac{r_0}{s_0}$, so $t(rs_0 - sr_0) = 0$ for some $t \in S$

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

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

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

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

$$\bar{F}\left(\frac{r}{s}\right) = \bar{F}\left(\frac{r_0}{s_0}\right)$$

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

$$\bar{f}\left(\frac{rr_0}{ss_0}\right) = f(rr_0)f(ss_0)^{-1} = f(r)f(s)^{-1}f(r_0)f(s_0)^{-1} = \bar{f}\left(\frac{r}{s}\right)\bar{f}\left(\frac{r_0}{s_0}\right)$$

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

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

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

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, $S \subset R$ multiplicative, $I \subset R$ an ideal
Then $S^{-1}I = S^{-1}R$ iff $S \cap I \neq \emptyset$

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

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

$\Rightarrow$

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

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

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

Then $\underset{\underset{I}{\uparrow}}{as}t_0 = t_0 s\underset{\underset{S}{\uparrow}}{t}$ $\in I \cap S$. ∎

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, ~~[illegible]~~ and ~~[illegible]~~ $S \cap P = \emptyset$, 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 $I := J \cap R = \{ r \in R \mid \frac{re}{e} \in J \}$

(1) 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 ~~[illegible]~~ $\frac{ae}{e} \cdot \frac{re}{e} = \frac{are^2}{e^2} = \frac{are}{e} \in J$, so $ar \in I$.

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

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 $\frac{a}{s}, \frac{b}{t} \in S^{-1}R \setminus S^{-1}P$ ~~$s \in S$ $a, b \in R$~~, 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 $v \in S$

$$ab\underbrace{uv}_{\notin P} = \underbrace{cstv}_{\in P}$$

requires $S \cap P = \emptyset$

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

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

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

Pf Our proof of 4.9 (i) shows this is injective.

Let Q be a prime ideal of $S^{-1}R$. Then $Q = S^{-1}I$ for some ideal $I \subset R$.

claim I is prime.

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

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

So $\frac{as}{s} \cdot \frac{bs}{s} = \frac{abs^2}{s^2} = \frac{abs}{s} \in \underset{S^{-1}R \setminus S^{-1}I}{\underset{\shortparallel}{S^{-1}R \setminus Q}}$ 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, $P \subset R$ a prime ideal. The <u>localization of R at P</u>, denoted R_P, is the ring $S^{-1}R$ for the set $S = R \setminus P$.

If $I \subset R$ is an ideal, $S^{-1}I$ is denoted I_P

Idea from algebraic geometry! R represents regular functions from variety $V \longrightarrow \overset{\text{field}}{k}$

To restrict attention locally, need functions that don't vanish $\Leftrightarrow$ can be inverted.

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

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

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

Pf (i) follows from 4.10.

(ii) (i) implies P_p is maximal.

Suppose $M \subset R_p$ is some other maximal ideal. By (i), $M = Q_p$ for some prime ideal $Q \subset P$. But $Q \subset P \Rightarrow Q_p \subset P_p$ and Q_p maximal $\Rightarrow Q_p = P_p$.

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

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

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

Maximal ideal is (p)

Thm 4.13 Let R be a commutative unital ring. TFAE

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

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

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

Pf (i) $\Rightarrow$ (ii) Note $\mathfrak{m} \subset R \setminus R^*$

If $x \in R \setminus R^*$, $(x) \neq R$, so $(x) \subset \mathfrak{m}$

Thus $R \setminus R^* \subset \mathfrak{m}$, so $R \setminus R^* = \mathfrak{m}$.

(ii) $\Rightarrow$ (iii) ✓

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

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 $r \cdot m = \varphi(r) \cdot m$ for all $r \in R$, $m \in M$.

Def 1.2 Let M, N be R-modules. An <u>R-module homomorphism</u> is a function $f: M \to N$

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 $\begin{aligned} \varphi: R[x] &\longrightarrow R[x] \\ f &\longmapsto xf \end{aligned}$ is a module homomorphism but not a ring homomorphism

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. 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 $B_1 + \dots + B_n$.

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

Thm 1.5 Let R be a unital ring, M an R-module.

(i) If $a \in M$, 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

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

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

$$\left\{ \sum_{k=1}^{s} b_{i_k} \;\middle|\; s \in \mathbb{N},\ b_{i_k} \in B_{i_k} \right\}$$

(Finite sums of elements of B_i's)

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

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

Pf M/N is an abelian group.
Check multiplication well defined: Suppose $a+N = b+N$, so $a-b=n \in N$.

Then $ra + N = r(b+n) + N = rb + N$.

Straightforward to check submodule properties.

Remark Straightforward to verify that isomorphism theorems hold for modules.

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

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

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

If I is finite 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

$$\cdots \xrightarrow{f_{i-1}} A_{i-1} \xrightarrow{f_i} A_i \xrightarrow{f_{i+1}} A_{i+1} \xrightarrow{f_{i+2}} \cdots$$

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

Ex If M, N are R-modules

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

Ex If $N \subset M$ is a submodule

$$0 \to N \to M \to M/N \to 0$$ is exact.

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

$$\begin{tikzcd} 0 \arrow[r] & \operatorname{Ker} f \arrow[r] & M \arrow[r, "f"] & N \arrow[r] & \operatorname{Coker} f \arrow[r] \arrow[d, equal] & 0 \\ & & & & N/\operatorname{Im} f & \end{tikzcd}$$ is exact.

Lemma 1.17 (Short Five Lemma) Let

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "f"] \arrow[d, "\alpha"] & B \arrow[r, "g"] \arrow[d, "\beta"] & C \arrow[r] \arrow[d, "\gamma"] & 0 \\ 0 \arrow[r] & A' \arrow[r, "f'"] & B' \arrow[r, "g'"] & C' \arrow[r] & 0 \end{tikzcd}$$

be a commutative diagram

Suppose the rows are both exact.

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

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

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

Pf "Diagram chasing"

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

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 $g(z) = y$

$$\text{So } \begin{array}{c} \gamma g(z) = g'\beta(z) \\ \shortparallel \\ \gamma(y) = g'(x) \end{array}$$

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

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

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

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

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

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

∎

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

Thm 1.18 Let $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ be exact $\overset{\text{sequence of } R\text{-modules}}{\wedge}$. 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)

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "i"] \arrow[d, "id"] & A \oplus C \arrow[r, "\pi"] \arrow[d, "f+h"] & C \arrow[r] \arrow[d, "id"] & 0 \\
0 \arrow[r] & A \arrow[r, "f"] & B \arrow[r, "g"] & C \arrow[r] & 0
\end{tikzcd}$$

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

$f(id(a)) = f(a)$ ✓

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

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

$$id(\pi(a,c)) = id(c) = c \quad ✓$$

So the diagram commutes. Five lemma => $f+h$ is an isomorphism

(ii) => (iii)

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "f"] \arrow[d, "id"] & B \arrow[r, "g"] \arrow[d, "(K,g)"] & C \arrow[r] \arrow[d, "id"] & 0 \\
0 \arrow[r] & A \arrow[r, "i"] & A \oplus C \arrow[r, "\pi"] & C \arrow[r] & 0
\end{tikzcd}$$

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

$i(id(a)) = i(a) = (a,0)$ ✓

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

$id(g(b)) = g(b)$ ✓

So the diagram commutes. Five lemma => (K,g) is an isomorphism.

(iii) => (i, ii)

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "i_1"] \arrow[d] & A \oplus C \arrow[r, "\pi_2"] \arrow[d, "\varphi"] \arrow[l, bend left, "\pi_1"] & C \arrow[r] \arrow[d] \arrow[l, bend left, "i_2"] & 0 \\
0 \arrow[r] & A \arrow[r, "f"] & B \arrow[r, "g"] & C \arrow[r] & 0
\end{tikzcd}$$

Let $h = \varphi i_2$

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

∎

§2 Free modules

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

$$r_1x_1 + \dots + r_nx_n = 0 \Rightarrow r_1 = \dots = r_n = 0.$$

A linearly independent generating set is called a basis

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

(1) F has a 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 $\tilde{f} : F \to M$

$$\begin{tikzcd} X \arrow[r, "i"] \arrow[dr, "f"'] & F \arrow[d, dotted, "\tilde{f}"] \\ & M \end{tikzcd}$$

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

$$u = r_1x_1 + \dots + r_nx_n \quad \text{for some } r_i \in R,\ x_i \in X$$

Define $\tilde{f} : F \to M$ by $\tilde{f}(r_1x_1 + \dots + r_nx_n) = r_1f(x_1) + \dots + r_nf(x_n)$

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

(3) $\Rightarrow$ (2)

$$\begin{tikzcd} X \arrow[r, "i"] \arrow[dr, "f"'] & F \arrow[d, dotted, "\tilde{f}"] \\ & \sum_{x\in X} xR \end{tikzcd}$$

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

(2) ⇒ (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 $\{1, x, x^2, x^3, \dots\}$

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.

$$\begin{tikzcd} X \arrow[r] \arrow[dr, bend right] & \sum_{x\in X} R \arrow[d, dotted] \\ & M \end{tikzcd}$$

∎

Thm 2.4 Every module (vectorspace) over a field (or division ring) is free.

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

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

Then X is a basis of N.

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

If $r_1x_1 + \dots + r_nx_n + r_{n+1}a = 0$ for some $r_i \in k$, not all zero,
note $r_{n+1} \neq 0$ (since X linearly independent),
so $a = -\frac{1}{r_{n+1}}(r_1x_1 + \dots + r_nx_n) \in N$ ↯

Claim contradicts maximality, so $M = N$.

Pf of Thm 2.4 Let $S = \{X \subset M \mid X \text{ is linearly independent}\}$.
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 ⇒ S has a maximal element, which is a basis by Lemma 2.3.

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

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

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

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

Ex $\mathbb{Z}$ has IBN property.

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

Pf If X, Y both finite: row reduction + count pivots

Now, WLOG suppose X is infinite.

Claim 1 Y is infinite.

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

write
$$\begin{aligned} y_1 &= a_{11}x_1 + \dots + a_{1m}x_m \\ &\vdots \\ y_n &= a_{n1}x_1 + \dots + a_{nm}x_m \end{aligned}$$
$\Rightarrow \{x_1,\dots,x_m\}$ span V

$\Rightarrow X$ linearly dependent. ↯

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

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

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

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

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

$\Rightarrow X$ linearly dependent

So $|X| \le |Y|$.

(Similarly, $|Y| \le |X|$ ∎

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

Lemma 2.10 Let R be unital, $I \subset R$ a proper ideal. Let F be a free module with basis X, and $\pi: F \longrightarrow F/IF$ 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 $u + IF = \left(\sum_{j=1}^{n} r_i x_i\right) + IF = \sum_{j=1}^{n}(r_i x_j + IF) = \sum_{j=1}^{n}(r_j + IF)(x_j + IF)$

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

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.

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

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

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

$= \sum_{i=1}^{p} \tilde{s}_i \tilde{x}_i$ 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 $r_j = \overset{\in I}{\tilde{s}_j}$, $x_j = \tilde{x}_j$,

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

__Claim 3__ π is injective

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

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

$$\begin{gathered} (1+I)\pi(x_1) - (1+I)\pi(x_2) \\ \parallel \\ x_1 + x_2 + IF \end{gathered}$$

So $x_1 - x_2 = \sum \tilde{s}_i \tilde{x}_i$ as above, with $\tilde{s}_i \in I$ 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
   (1) Direct summands of free modules
   (2) Locally free
2) Algebraic analogue of vector bundles - locally trivial
   (Ex Infinitely long Möbius strip)

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

$$\begin{tikzcd} & P \arrow[dl, dashed, "h"'] \arrow[d, "f"] & \\ A \arrow[r, "g"] & B \arrow[r] & 0 \end{tikzcd}$$

Thm 3.2 Free modules are projective.

Pf Let F be a free module, and suppose

$$\begin{tikzcd} & X \arrow[d] \arrow[ddl, "h_0"'] & \\ & F \arrow[dl, dashed, "h"'] \arrow[d, "f"] & \\ A \arrow[r, "g"] & B \arrow[r] & 0 \end{tikzcd}$$

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 $F = K \oplus P$.

Pf (i)=>(ii)

$$\begin{tikzcd} & & & P \arrow[d] \arrow[dl, dashed] & \\ 0 \arrow[r] & A \arrow[r] & B \arrow[r] & P \arrow[r] & 0 \end{tikzcd}$$

(ii)=>(iii) There is free module F

$$\begin{tikzcd} 0 \arrow[r] & K \arrow[r] & F \arrow[r] & P \arrow[r] & 0 \end{tikzcd}$$

Let K = Kernel of this map.

Then $F \cong K \oplus P$

(iii)=>(i) Suppose $F \cong K \oplus P$ F projective!

$$\begin{tikzcd} & F \cong K\oplus P \arrow[d, shift right, "\pi"'] \arrow[ddl, dashed] & \\ & P \arrow[u, shift right, "i"'] \arrow[d] & \\ A \arrow[r] & B \arrow[r] & 0 \end{tikzcd}$$

∎

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 => Suppose $\sum_{i\in I} P_i$ is projective

$$\begin{tikzcd} & \sum P_i \arrow[d, shift right, "\pi"'] \arrow[ddl, dashed] & \\ & P_i \arrow[u, shift right, "i"'] \arrow[d] & \\ A \arrow[r] & B \arrow[r] & 0 \end{tikzcd}$$

Thus P_i is projective

$\Leftarrow$ Suppose P_i each projective

$$\begin{tikzcd} & P_i \arrow[d] \arrow[ddl] & \\ & \sum P_i \arrow[d] & \\ A \arrow[r] & B \arrow[r] & 0 \end{tikzcd}$$

Since we have maps $P_i \to A$ for all $i \in I$, we get a map $\sum_{i\in I} P_i \longrightarrow A$ ∎

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

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "g"] \arrow[d, "f"'] & B \arrow[dl, dashed, "h"] \\ & J & \end{tikzcd}$$

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

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

Pf Reverse arrows in proof of Prop 3.5

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

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

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

$$\begin{tikzcd} 0 \arrow[r] & I \arrow[r] \arrow[d] & R \arrow[dl, dashed] \\ & J & \end{tikzcd}$$

$\Leftarrow$ Suppose we are given

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "g"] \arrow[d, "f"] & B \\ & J & \end{tikzcd}$$

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

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

S is partially ordered by extension / restriction

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

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

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

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

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

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

so φ is an R-module homomorphism

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

Let $K = H + Rb$

Define $\bar{h} : K \longrightarrow J$ by $\bar{h}(a + rb) = h(a) + K(r)$ 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 $h(a_1) - h(a_2) = h((r_2 - r_1) b) = K(r_2 - r_1) = K(r_2) - K(r_1)$

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

Then $\bar{h} \in S$ extends h, contradicting maximality ↯ $\boxed{/}$

[illegible]

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)

$$\begin{tikzcd}
0 \arrow[r] & \langle n \rangle \arrow[r] \arrow[d, "f"'] & \mathbb{Z} \arrow[dl, dashed, "h"] \\
 & D &
\end{tikzcd}$$

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

Now $n h(1) = h(n) = f(n) = y$. 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. $\boxed{/}$

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

Pf Let A be an abelian group.

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

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

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

Then ~~$A \cong F/K \hookrightarrow f(F)$~~

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

↑ Homomorphic image of a divisible group, thus divisible.

Lemma 3.11 Let R be unital, J a divisible abelian group. Then $\mathrm{Hom}_{\mathbb{Z}}(R, J)$ is an injective R-module.

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

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

Since J injective,

$$\begin{tikzcd}
0 \arrow[r] & I \arrow[r] \arrow[d, "g"'] & R \arrow[dl, dashed, "\tilde{g}"] \\
& J &
\end{tikzcd}$$

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

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

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

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

Check: Is h a homomorphism?

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

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

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

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

Check: Does h extend f ?

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

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

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

$= f(r)(1x)$

$= f(r)(x)$

So h extends f, and Lemma 3.8 shows $\mathrm{Hom}_{\mathbb{Z}}(R,J)$ 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 injective group homomorphism $f: A \to J$

$$\begin{tikzcd} R \arrow[r] \arrow[d] & A \arrow[dl, "f"] \\ J & \end{tikzcd}$$

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

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

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

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

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

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

$a \longmapsto f_a$

where $f_a(r) = ra$

Injective!

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

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

(i) J is injective

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

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

Pf (i) $\Rightarrow$ (ii)

$$\begin{tikzcd} 0 \arrow[r] & J \arrow[r] \arrow[d] & B \arrow[r] \arrow[dl, dashed] & C \arrow[r] & 0 \\ & J & & & \end{tikzcd}$$

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

Prop 3.7 $\Rightarrow$ J is injective. ∎

§4 Hom

Def Let A, B be R-modules.

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

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

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

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

Pf

$$\begin{tikzcd} A \arrow[r, "f"] & B \arrow[d, "\psi"] \\ C \arrow[u, "\varphi"] \arrow[r, dashed, "\theta(f)"'] & D \end{tikzcd}$$

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

If $r \in R$, $\theta(rf) = \psi \circ (rf) \circ \varphi = r \psi f \varphi = r\theta(f)$. $\boxed{}$

Two important examples:

(1) $A = C$, $\theta = \mathrm{id}$ A map $\psi : B \to D$ gives a map $\operatorname{Hom}_R(A,B) \to \operatorname{Hom}_R(A,D)$, $f \longmapsto \psi f$

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

(2) $B = D$, $\psi = \mathrm{id}$ A map $\theta : C \to A$ gives a map $\operatorname{Hom}_R(A,B) \to \operatorname{Hom}_R(C,B)$, $f \longmapsto f\theta$

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

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

i.e. 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 $0 \to \mathrm{Hom}_R(D,A) \xrightarrow{\bar{\varphi}} \mathrm{Hom}_R(D,B) \xrightarrow{\bar{\psi}} \mathrm{Hom}_R(D,C)$ is exact.

Pf $\Rightarrow$

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

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

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

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

So $\ker \bar{\varphi} = 0$

(ii) Claim $\mathrm{Im}\,\bar{\varphi} = \ker \bar{\psi}$

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

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

Thus $g \in \ker \bar{\psi}$. So $\mathrm{Im}\,\bar{\varphi} \subset \ker \bar{\psi}$.

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

In other words, $\mathrm{Im}\, g \subset \ker \psi = \mathrm{Im}\,\varphi$

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

$\leftarrow$ 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 $g \in \mathrm{Im}\,\bar{\varphi}$

Thus $\ker \bar{\psi} \subset \mathrm{Im}\,\bar{\varphi}$

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

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

Let $i \in \mathrm{Hom}(\ker\varphi, A)$ be the inclusion map $\ker\varphi \overset{i}{\hookrightarrow} A$

Then $\bar{\varphi}(i) = \varphi i = 0$ (since $\mathrm{Im}\, i = \ker\varphi$)

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

(ii) <u>Claim</u> $\operatorname{Im}\varphi > \operatorname{Ker}\psi$.

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

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

For other containment,

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

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

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

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

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

So $\operatorname{Ker}\psi \subset \operatorname{Im}\varphi$ ∎

<u>Prop 4.3</u> $\operatorname{Hom}_R(-, D)$ is <u>left</u> 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,

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

<u>Pf</u> $\Rightarrow$ (i) First show $\bar\psi$ is injective.

Let $f \in \operatorname{Ker}\bar\psi$, so $0 = \bar\psi(f) = f\psi$

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

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

So $\bar\psi$ is injective.

(ii) <u>Claim</u> $\operatorname{Im}\bar\psi = \operatorname{Ker}\bar\theta$

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

so that $f \in \operatorname{Im}\bar\psi$.

$$\begin{tikzcd}
\operatorname{Ker}\xi \arrow[r, hook] & B \arrow[r, "\xi"] \arrow[d, "f"] & C \arrow[r] & 0 \\
& D & &
\end{tikzcd}
\qquad
\begin{tikzcd}
B/\operatorname{Ker}\xi \arrow[r] \arrow[d, "\bar{f}"] & C \arrow[r] \arrow[l, bend left, "\varphi"] & 0 \\
0 & &
\end{tikzcd}$$

<u>Claim</u> $\operatorname{Ker}\xi \subset \operatorname{Ker} f$

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

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

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

Thus $\operatorname{Ker}\bar{\theta} \subset \operatorname{Im}\bar{\xi}$.

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

Then $\bar{\theta}(g) = g\theta = f\xi\theta = 0$ Since $\xi\theta = 0$

Thus $\operatorname{Im}\bar{\xi} \subset \operatorname{Ker}\bar{\theta}$.

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

By assumption, $0 \to \operatorname{Hom}(C, C/\operatorname{Im}\xi) \xrightarrow{\bar{\xi}} \operatorname{Hom}(B, C/\operatorname{Im}\xi) \xrightarrow{\bar{\theta}} \operatorname{Hom}(A, C/\operatorname{Im}\xi)$ is exact.

Let $\pi : C \to C/\operatorname{Im}\xi$ be quotient map.

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

(ii) <u>Claim</u> $\operatorname{Im}\theta = \operatorname{Ker}\xi$

By assumption $0 \to \operatorname{Hom}(C, B/\operatorname{Im}\theta) \xrightarrow{\bar{\xi}} \operatorname{Hom}(B, B/\operatorname{Im}\theta) \xrightarrow{\bar{\theta}} \operatorname{Hom}(A, B/\operatorname{Im}\theta)$ is exact.

Let $\pi : B \to B/\operatorname{Im}\theta$ be quotient map

Note $\bar{\theta}(\pi) = \pi\theta = 0$, so $\pi \in \operatorname{Ker}\bar{\theta} = \operatorname{Im}\bar{\xi}$.

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

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

Thus $\operatorname{Ker}\xi \subset \operatorname{Im}\theta$

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

Then $\underset{0}{\underset{\shortparallel}{\bar{\theta}\bar{\psi}}}(\mathrm{id}) = \psi\theta$, so $\mathrm{Im}\,\theta \subset \mathrm{Ker}\,\psi$. $\boxtimes$

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

Pf $\Rightarrow$ Suppose P is projective.

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

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

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

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

$$\begin{tikzcd}
 & P \arrow[dl, dashed, "g"'] \arrow[d, "f"] & \\
B \arrow[r, "\psi"] & C \arrow[r] & 0
\end{tikzcd}$$

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

$\Leftarrow$ Suppose

$$\begin{tikzcd}
 & & & P \arrow[d, "f"] & \\
0 \arrow[r] & K \arrow[r] & B \arrow[r] & C \arrow[r] & 0
\end{tikzcd}$$

Then $0 \to \mathrm{Hom}(P,K) \to \mathrm{Hom}(P,B) \to \mathrm{Hom}(P,C) \to 0$ is exact

Then $f \in \mathrm{Hom}(P,C)$ lifts to $g \in \mathrm{Hom}(P,B)$ $\boxtimes$

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

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "\varphi"] \arrow[d, "f"'] & B \arrow[dl, dashed, "g"] \\
& J &
\end{tikzcd}$$

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

$\Leftarrow$ Suppose

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] \arrow[d, "f"] & B \arrow[r] & B/\text{Im} \arrow[r] & 0 \\
& J & & &
\end{tikzcd}$$

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

Then $f \in \text{Hom}(A, J)$ 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 $\varphi : \text{Hom}_R(R, A) \longrightarrow A$, $f \longmapsto f(1)$

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

Check $\varphi\psi = id$ ☒

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

§5 Tensor Products

Motivation Let R be commutative, with 1 rings

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

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

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

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

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

Def Let M, N be R-modules.

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

Let $K \subset F$ be generated by

$$(m_1+m_2, n) - (m_1, n) - (m_2, n)$$
$$(m, n_1+n_2) - (m, n_1) - (m, n_2)$$
$$r(m,n) - (rm, n)$$
$$r(m,n) - (m, rn)$$

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

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

Def Let A, B, C be R-modules. A __bilinear map__ $f: A \times B \longrightarrow C$ 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) $f(ra, b) = f(a, rb) = rf(a,b)$

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 $\bar{g} : M \otimes_R N \longrightarrow L$

$$\begin{tikzcd}
M \times N \arrow[r, "g"] \arrow[d] & L \\
M \otimes N \arrow[ur, dashed, "\bar{g}"'] &
\end{tikzcd}$$

Pf

$$\begin{tikzcd}
M \times N \arrow[r, "g"] \arrow[d] & L \\
F \arrow[ur, "g_0"] \arrow[d] & \\
F/K = M \otimes N \arrow[uur, "\bar{g}"'] &
\end{tikzcd}$$

Suffices to show $K \subset \operatorname{Ker} g_0$. But this is precisely the bilinearity of g! □

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 5.7 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 bilinear.

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

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

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

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

Pf **Claim 1** $id \otimes g$ 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 $m \in M$.

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

Claim 2 $Im(id \otimes f) \subset Ker(id \otimes g)$

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

Claim 3 $Ker(id \otimes g) \subset Im(id \otimes f)$

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

$$\begin{tikzcd}
K \otimes_R M \arrow[r, "id \otimes g"] \arrow[d, "\pi"'] & K \otimes_R N \\
K \otimes_R M / Im(id \otimes f) \arrow[ur, "\alpha"'] &
\end{tikzcd}$$

Suffices to show α is an isomorphism

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

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

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

Then $g(m - m_0) = 0$, 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 $\pi(k \otimes m) = \pi(k \otimes m_0)$

(cont)

Straightforward to verify that β is bilinear, so we obtain

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

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

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

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

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

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

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

Pf Define bilinear map

$$A \times R \longrightarrow a$$
$$(a, r) \longmapsto ra$$

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

Construct

$$\beta : A \longrightarrow A \otimes_R R$$
$$a \longmapsto a \otimes 1 .$$

check $\beta\alpha = id$, $\alpha\beta = id$. ∎

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

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

Pf Fix $x \in L$. Define $\lambda_x : M \times N \longrightarrow (L \otimes_R M) \otimes N$ 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 $\bar{\alpha} : L \otimes_R (M \otimes_R N) \longrightarrow (L \otimes_R M) \otimes_R N$.

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

Construct inverse in same way. ∎

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 $\alpha_1 = i_1 \otimes id$

$\alpha_2 : M \otimes N \longrightarrow (L \oplus M) \otimes N$ 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 $\beta_0 : (L \oplus M) \times N \longrightarrow (L \otimes N) \oplus (M \otimes N)$

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

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

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

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

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

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

$\beta\alpha$ identity on generators, so $\beta\alpha = id$. $\boxed{}$

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

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

Pf Define $\alpha : \mathrm{Hom}_R(L\otimes M, N) \longrightarrow \mathrm{Hom}(L, \mathrm{Hom}(M,N))$ by

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

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

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

- $[\alpha(f)(\ell)](m_1+m_2) = f(\ell\otimes(m_1+m_2)) = f(\ell\otimes m_1) + f(\ell\otimes m_2) = [\alpha(f)(\ell)](m_1) + [\alpha(f)(\ell)](m_2)$
- $[\alpha(f)(\ell)](rm) = f(\ell\otimes rm) = f(r(\ell\otimes m)) = rf(\ell\otimes m) = r[\alpha(f)(\ell)](m)$

(2) Is α([illegible]) a homomorphism?

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

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

~~(3) Is f a homomorphism~~?

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

$$[\alpha(f)(l_1+l_2)](m) = f((l_1+l_2)\otimes m) = f(l_1\otimes m + l_2\otimes m)$$
$$= f(l_1\otimes m) + f(l_2\otimes m)$$
$$= [\alpha(f)(l_1)](m) + [\alpha(f)(l_2)](m)$$

$$[\alpha(f)(rl)](m) = f(rl\otimes m) = f(r(l\otimes m)) = rf(l\otimes m)$$
$$= r[\alpha(f)(l)](m)$$

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

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

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

(4) Is β a homomorphism?

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

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

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

$[\beta\alpha(f)](l\otimes m) = [\alpha(f)(l)](m) = f(l\otimes m)$, so $\beta\alpha(f) = f$

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

$[\alpha\beta(g)(l)](m) = [\beta(g)](l\otimes m) = [g(l)](m)$, so $\alpha\beta(g) = g$.

∎

§7 Algebras

Def 7.1 Let R be a commutative, unital ring. ~~An R~~ A ring A is called an **R-algebra** if

1) A is an R-module
2) $r\cdot(ab) = (r\cdot a)b = a(r\cdot b)$ for all $r \in R$, $a, b \in A$.

Ex $R[x]$ is an R-algebra.

Ex $\mathbb{Q}$ is a $\mathbb{Z}$-algebra

Ex $\mathbb{C}$ is an $\mathbb{R}$-algebra.

Thm Let A be an R-algebra, and M an R-module.
Then $A \otimes_R M$ is an A-module
(This is called change of base)

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

Ex $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}[x] = \mathbb{Q}[x]$

Ex If S is an R-algebra, $S \otimes_R R^n \cong S^n$

Ex $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}^n \cong \mathbb{C}^n$

§6 Modules over a PID

Thm 6.1 Let R be a PID, F a free R-module, $G \subset F$ a submodule.
Then G is a free R-module and rank $G \leq$ rank F.

Pf Let $\{x_j \mid j \in J\}$ be a basis of F, so $F = \sum_{j \in J} R x_j$
By the well ordering principle, assume J is well ordered (every nonempty set has a minimal element)

Set

$$\overline{F}_{(j)} = \sum_{i < j} R x_i \quad \text{and} \quad F_{(j)} = \sum_{i \leq j} R x_i = \overline{F}_{(j)} \oplus R x_j \quad \text{for all } j \in J.$$

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

Define

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

Note $\operatorname{Ker} f_j = \overline{F}_{(j)} \cap G$, so we have an exact sequence

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

Note $\operatorname{Im} f_j \subset R$ is an ideal, so $\operatorname{Im} f_j = (r_j)$ for some $r_j \in R$.
Moreover, ~~there exists~~, 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 $s_1 c_{j_1} + \dots + s_n c_{j_n} = 0$ for some $j_1 < \dots < j_n$

then $0 = f_{j_n}(s_1 c_{j_1} + \dots + s_n c_{j_n}) = s_n f_{j_n}(c_{j_n}) = s_n r_{j_n}$

Thus $s_n = 0$. By induction, all $s_i = 0$

(ii) Generates:

Let $i \in J$ be smallest such that $a \in F_{(i)} \cap G$ is not generated by C.

Let $J' = \{j \mid r_j \neq 0\}$ (so $C = \{c_j \mid j \in J'\}$)

Suppose $i \notin J'$: Then the map $\overline{F}_{(i)} \cap G \longrightarrow F_{(i)} \cap G$ is equality,

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

But then there is a $k < i$ with $a \in F_{(k)} \cap G$, contradicting minimality of i.

So we must have $i \in J'$. write $f_i(a) = s r_i$ 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 $b \in \overline{F}_{(i)} \cap G$.

This contradicts minimality of i $\square$

Cor 6.2 Let R be a PID. If M is a finitely generated R-module generated by n elements, then every submodule of M is generated by at most n elements

Pf Let $N \subset M$ be a submodule.

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

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

Then N is generated by $\{\pi(x_1), \dots, \pi(x_m)\}$ $\square$

Cor 6.3 A projective module over a PID is free

Pf Let M be a projective R-module.

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

i.e. M is isomorphic to a submodule of F, hence is free. $\square$

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

(i) $\mathcal{O}_a := \{r \in R \mid ra = 0\}$ is an ideal of R for each $a \in A$.

This is called the <u>order ideal of $a \in A$</u>

If $\mathcal{O}_a = (r)$, a is said to have <u>order r</u>.

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

This is called the <u>torsion submodule</u> of A.

If $A = A_{tor}$, A is called a <u>torsion module</u>. If $A_{tor} = 0$, A is called <u>torsion free</u>.

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

(iv) Let $p \in R$ be prime. If $(p^i) \subset \mathcal{O}_a$, then $\mathcal{O}_a = (p^j)$ for some $0 \leq j \leq i$.

(v) Let $p \in R$ be prime. If $(p^i) = \mathcal{O}_a$, then $p^j \notin \mathcal{O}_a$ for all $0 \leq j < i$.

<u>Pf</u> (i) Let $a \in A$.

If $r_1, r_2 \in \mathcal{O}_a$, $r_1 a = 0$, $r_2 a = 0$, so $(r_1 + r_2)a = r_1 a + r_2 a = 0 + 0 = 0$, so $r_1 + r_2 \in \mathcal{O}_a$

If $s \in R$, $(sr_1)a = s(r_1 a) = s \cdot 0 = 0$, so $sr_1 \in \mathcal{O}_a$.

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

[illegible] If $r \in R$, then $r_1 (ra_1) = r(r_1 a_1) = r \cdot 0 = 0$, so $ra_1 \in A_{tor}$.

(iii) Define

$$\varphi : R \xrightarrow{\varphi} Ra \qquad r \longmapsto ra$$

φ is surjective.

Note $\ker \varphi = \mathcal{O}_a$, so $R/\mathcal{O}_a \cong Ra$

(iv) Since R a PID, $\mathcal{O}_a = (r)$ for some $r \in R$.

Then since $p^i \in \mathcal{O}_a = (r)$, $r \mid p^i$.

Since R a UFD, $r = p^j u$ for some $u \in R^*$, $j \leq i$. then $\mathcal{O}_a = (r) = (p^j)$.

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

Then $\rho^j = \rho^i \gamma$ ~~[illegible]~~ with $j < i$, contradicting unique factorization. $\boxtimes$

<u>Thm 6.6</u> Let ~~[illegible]~~ R be a PID, A an f.g. R-module. Then $A = A_{tor} \oplus F$ for some free module F.

<u>Thm 6.5</u> Every f.g. torsion free module over a PID is free.

<u>Pf</u> 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 $S = \{x_1, \dots, x_k\} \subset X$ be a maximal linearly independent i.e. subset, for which $F = Rx_1 + \dots + Rx_k$ is a free submodule.

If $y \in X \setminus S$, then $ry \in F$ for some nonzero $r \in R$. (otherwise, $S \cup \{y\}$ is linearly independent)

Taking a (finite) product of these r's for each $y \in X \setminus S$, obtain nonzero $r \in R$ s.t. $rX \subset F$.

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

Define $\varphi_r : A \longrightarrow A$, $a \longmapsto ra$. Clearly $\operatorname{Im} \varphi_r = rA \subset F$ is a free module

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

<u>Pf of 6.6</u> Set $F = A/A_{tor}$, free by Thm 6.5

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

Thus $A \cong A_{tor} \oplus F$ $\boxtimes$

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

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

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

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

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

(ii) $M = \sum_{\substack{p \in R \\ \text{prime}}} M(p)$. If M is f.g., this sum is finite.

Pf (i) Let $a, b \in M(p)$. Then $\mathcal{O}_a = (p^r)$, $\mathcal{O}_b = (p^s)$ for some $r, s \in \mathbb{N}$

Setting $k = \max(r,s)$, we see $p^k(a+b) = 0$, so $(p^k) \subset \mathcal{O}_{a+b}$, hence $\mathcal{O}_{a+b} = (p^i)$ for some $0 \le i \le k$ (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 $r = p_1^{n_1} \cdots p_k^{n_k}$ for distinct primes p_i

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

Then $r_1, \dots, r_k$ are coprime, so $\gcd(r_1, \dots, r_k) = 1$

Then $1 = s_1 r_1 + \dots + s_k r_k$ for some $s_i \in R$.

$a = s_1 r_1 a + \dots + s_k r_k a$

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 $a \in M(p_1) + \dots + M(p_k)$

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, $a = a_1 + \dots + a_t$ 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 $(q_1^{k_1} \cdots q_t^{k_t}) a = 0$ Let $d = q_1^{k_1} \cdots q_t^{k_t}$.

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

Then $a = rp^k a + sda = 0$

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

Suppose $M = Rx_1 + \dots + Rx_n$

~~generated by $M(p_t)$, ...~~

Then $x_i \in M(p_{i_1}) \oplus \dots \oplus M(p_{i_k})$ for some primes $p_{i_1}, \dots, p_{i_k} \in R$.

$\Rightarrow M = \bigoplus_{i=1}^{n} M(p_{i_1}) \oplus \dots \oplus M(p_{i_k})$ ☒

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 maximal $k \geq 0$, so $p \nmid r$

Then $0 = p^n c = p^{n-j}(p^j c) = p^{n-j}(p^k r a)$, so $n-j+k \geq n$, thus $k \geq j \geq 1$

Set $b = p^{j-1}c - rp^{k-1}a$

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

We claim $Ra \cap Rb = 0$.

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

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

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

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

Then $p^{j-1}c = b + rp^{k-1}a \in Ra$

Recall j was <u>minimal</u> s.t. $p^j c \in Ra$, so we must have $j-1=0$, so $c \in Ra$ ↯

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

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

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

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

<u>Claim</u> $M/C = R(a+C)$

Since $p^n A = 0$, $p^n(A/C) = 0$

But $p^{n-1}(a+C) = p^{n-1}a + C \neq C$, since $p^{n-1}a + C = C \Rightarrow p^{n-1}a \in C \cap Ra = 0$ and $p^{n-1}a \neq 0$ by assumption

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

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

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

Thus $M/C = R(a+C)$, so $M = Ra + C$ ∎

Thm 6.9 Let R be a PID, M a f.g. R-module such that every element has order a power of p for some fixed prime $p \in R$. Then $M = Ra_1 \oplus \dots \oplus Ra_k$, where a_i has order p^{n_i} for some $n_i \in \mathbb{N}$.

Pf Suppose $M = Ra_1 + \dots + Ra_k$. 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 $\pi : M \longrightarrow C$ be quotient map,

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

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

Now apply induction hypothesis $\Rightarrow$ $C = R\pi(a_2) \oplus \dots \oplus R\pi(a_k)$ $\square$

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

$M = R^n \oplus Ra_1 \oplus \dots \oplus Ra_k$

where a_i has order $p_i^{n_i}$ for some prime $p \in R$.

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

By Thm 6.7, $M_{tor} = M_{tor}(p_1) \oplus \dots \oplus M_{tor}(p_k)$

By Thm 6.9, $M_{tor}(p_i) = Ra_{i_1} \oplus \dots \oplus Ra_{i_k}$ $\square$

Ch. 8 Commutative Rings and Modules

Assume all rings are commutative unital.

§1 Chain Conditions

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

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

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

Ex $\mathbb{Z}$ is Noetherian, but not Artinian

$(m) \subset (n) \iff n \mid m$,

Note $(2) \supset (4) \supset (8) \supset (16) \supset \dots$

Ex Every PID is Noetherian

Ex An Artinian integral domain R is a field.

Let $a \in R$. Then $(a) \supset (a^2) \supset (a^3) \supset \dots$ stabilizes, so $(a^n) = (a^{n+1})$ for some $n \in \mathbb{N}$.

Then $a^n \in (a^{n+1})$, so $a^n = ba^{n+1}$ for some $b \in R$, so $1 = ba$.

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

Pf $\Rightarrow$ 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.

$\Leftarrow$ 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 $i \geq n$:

$$\begin{tikzcd}
0 \arrow[r] & L_n \arrow[r] \arrow[d, "id"] & M_n \arrow[r] \arrow[d, "i"] & N_n \arrow[r] \arrow[d, "id"] & 0 \\
0 \arrow[r] & L_i \arrow[r] & M_i \arrow[r] & N_i \arrow[r] & 0
\end{tikzcd}$$

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

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

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

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

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

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

Pf Let M be a 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 $L_1 \subset L_2 \subset L_3 \subset \dots$ is a chain in L,

then $\bigcup_{i=1}^{\infty} L_i = \bigcup_{i=1}^{n} L_n = L_n$ for some n, ~~[illegible]~~.

so $\bigcup_{i=1}^{\infty} L_i \in S$.

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 $K \subsetneq K + Rx$ ↯.

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

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

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

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

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

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

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

§2 Prime and primary ideals

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

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

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

$\uparrow$ Not a prime ideal!

But if $ab \in (p_1^{n_1})$ and $a \notin (p_1^{n_1})$, then $b^k \in (p_1^{n_1})$ 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

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

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

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

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

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

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

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

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

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

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

$r^m \in P + yR$ for some $m \in \mathbb{N}$,

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

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

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

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

(i) $\mathrm{Rad}(\mathrm{Rad}\, I) = \mathrm{Rad}\, I$

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

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

Pf (i) Let $r \in \mathrm{Rad}(\mathrm{Rad}\, I)$, so $r^n \in \mathrm{rad}\, I$, so $(r^n)^m \in I$

$$\underset{r^{nm}}{\underset{\shortparallel}{(r^n)^m}} \implies r \in \mathrm{rad}(I).$$

(ii) Let $r \in \mathrm{Rad}(I) \cap \mathrm{Rad}(J)$, 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 $r \in \mathrm{rad}(IJ)$

and $r^{n+m} \in I \cap J$, so $r \in \mathrm{rad}(I \cap J)$

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

~~If $r \in \mathrm{rad}(IJ)$, $r^n \in IJ$ for some $n \in \mathbb{N}$~~

Also $IJ \subset I$, $IJ \subset J$, so $\mathrm{rad}(IJ) \subset \mathrm{rad}(I) \cap \mathrm{rad}(J)$ $\blacksquare$

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

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

Ex Every prime ideal is radical

Def 2.8 An ideal $\mathfrak{Q} \subset R$ is called _primary_ if whenever $ab \in \mathfrak{Q}$ and $a \notin \mathfrak{Q}$, then $b^n \in \mathfrak{Q}$ 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 $a_0, a_1 \in k$ $\tilde{a}, \tilde{b} \in k[x]$

$\bar{b} = b_0 + b_1 x + x^2 \tilde{b}(x)$ b_0, b_1

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, $(x^i, y^j) \subset k[x,y]$ 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~~ $\overset{\shortparallel}{a^n b^n}$

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

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 associated prime ideal of Q

Q is called P-primary.

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

(i) $Q \subset P \subset \text{rad } Q$ and

(ii) If $ab \in Q$ and $a \notin Q$, then $b \in P$.

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

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

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

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

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

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

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

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

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

Pf S'pose Q_1, Q_2 are P-primary.

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

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

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

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

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

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

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

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

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

I contained in a max'l ideal, so $S \neq \emptyset$

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

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

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

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

Pf Suppose not. Since R Noetherian, there is [illegible] a maximal counterexample ideal I.

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

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

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

$\Rightarrow$ $I + fR$ (or $I + gR$) is a bigger counterexample ↯ ☒

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

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

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

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

Pf $\subset$ ✓

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

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

and $cb^N \in I$

So $\underset{I}{\underset{\cap}{cb^N}} = \underset{I}{\underset{\cap}{xb^N}} + b^{2N} y \Rightarrow b^{2N} y \in I$, so $y \in J_{2N} = J_N$

$\Rightarrow b^N y \in I$

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

~~So either~~

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

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

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

But $a \in J_1$, so $a \in I$. ∎

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

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

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

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

We must have $I_0 = J_1 \cap K_1$ for some ideals J_1, K_1 different from I (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

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

This contradicts R being Noetherian!

So S had to be empty. $\square$

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

Pf Let $I \subset R$ be radical.

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

Then $$I = \mathrm{rad}(I) = \mathrm{rad}(Q_1 \cap \dots \cap Q_n) = \underset{\uparrow}{\mathrm{rad}(Q_1)} \cap \dots \cap \underset{\nearrow}{\mathrm{rad}}(Q_n)$$

all prime!

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