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

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

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

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

If multiplication is commutative, R is called a commutative ring

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

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

Thm 1.2 Let R be a ring.

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

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

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

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

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

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

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

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

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

(v) Distributive property ∎

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

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

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

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

Ex $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in M_2(R)$ is a unit (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 $f(a+b) = f(a) + f(b)$, $f(ab) = f(a)f(b)$ for all $a, b \in R$.

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

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

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

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

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

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

Pf (i) If $m \in \ker \varphi$, $ma = m \cdot 1 \cdot a = 0 \cdot a = 0$ for all $a \in R$.
By assumption, $m > n$. Write $m = kn + r$ for some $0 \le r < n$.
Then $ra = 0$ for all $a \in R$, so $r = 0$, i.e. $m \in \langle n \rangle$.

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

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

§2 Ideals

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

Def 2.1 Let R be a ring. A subring is a subset that is itself a ring.
An ideal I is a subring satisfying if $x \in R$, $a \in I$, $xa \in I$
A left ideal I is a subring satisfying if $a \in I$, $x \in R$, $ax \in I$
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 $I = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \mid a, b \in \mathbb{R} \right\} \subset M_2(\mathbb{R})$. This is a left-sided ideal but not a right ideal.

Ex For any ring R, $\{0\}$ ($=0$) 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 $X = \{x_1, \ldots, x_n\}$, we write $(x_1, \ldots, x_n)$ and say it is finitely generated.

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

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

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

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

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

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

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

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

Pf well-defined: 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 $y \in J$

Then $a_0 b_0 + I = (a - x)(b - y) + I = ab - ay - xb + xy + I = ab + I$.
($ay \in I$, $xb \in I$, $xy \in I$) ∎

Thm 2.8 If $\varphi: R \to S$ is a ring homomorphism, $\ker\varphi$ is an ideal

Pf If $a, b \in \ker\varphi$, $\varphi(a+b) = \varphi(a)+\varphi(b) = 0+0=0$, so $a+b \in \ker\varphi$

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

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

Thm 2.9 (First Isomorphism Theorem) Let $\varphi: R \to S$ be a ring homomorphism.
Then $R/\ker\varphi \cong \operatorname{Im}\varphi$

Pf Let $\bar{\varphi}: R/\ker\varphi \longrightarrow \operatorname{Im}\varphi$, $a + \ker\varphi \longmapsto \varphi(a)$ be the well-defined abelian group isomorphism.

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

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

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

Thm 2.13 Let $I \subset R$ 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

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

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

1) If R is commutative, then $R \setminus P$ is multiplicatively closed, i.e. if $ab \in R \setminus P$ then $a \notin P$ or $b \notin P$.

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

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 $\iff$ If $ab \in R$ with $ab \in P$, either $a \in P$ or $b \in P$

Pf (i) Let $I, J \subset R$ be ideals with $IJ \subset P$.
Suppose $I \not\subset P$ (so we will show $J \subset P$).
Let $x \in I \setminus P$. 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 **maximal** if it is not contained in any other proper ideal.

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

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

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

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

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

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

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

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 commutative unital ring. Every maximal ideal is a prime ideal

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

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

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

Then $1 = (m_1 + ar_1)(m_2 + br_2) = \underbrace{m_1 m_2 + m_1 br_2 + m_2 ar_1}_{\in M} + abr_1 r_2$

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 $R \to S$ is injective.

Pf Thm 2.20 gives (i) $\Leftrightarrow$ (iii). Clearly (ii) $\Leftrightarrow$ (iii)

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

Thm 2.22, 2.23 Let $\{R_i\}_{i\in I}$ be a collection of rings. Then $\prod_{i\in I} R_i$ is a ring (with componentwise multiplication) that is the 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 $\varphi(a_1, \dots, a_n)\varphi(b_1, \dots, b_n) = (a_1 + \dots + a_n)(b_1 + \dots + b_n)$

$= a_1 b_1 + \dots + a_n b_n$

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

Thm 2.25 ("Chinese Remainder Theorem" – Sun-Tsze, ~4th 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

$b \equiv b_i$ mod 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 $1 \leq k \leq n$

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

$n=2$: $R = I_1 + I_2$ ✓

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

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

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

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

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

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

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

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

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

i.e. $\mathbb{Z} = (m_i) + (m_j)$. ∎

Apply Thm 2.25.

§ 5 Polynomial rings

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

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

(2) Addition is componentwise

(3) Multiplication given by

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

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

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

pf Need to check multiplication is associative

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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 $\varphi_0(1) = 1$.
Let $s_1, \dots, s_n \in S$. Then there is a unique homomorphism

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

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

Pf Suffices to assume $n = 1$.
If $\sum_{i=0}^{n} a_i x^i \in R[x]$, set $\varphi\left(\sum_{i=0}^{n} a_i x^i\right) = \sum_{i=0}^{n} \varphi_0(a_i)\, s^i$
(This is the only choice that makes φ a homomorphism)
∎

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

§3 Factorization in commutative rings

Def 3.1 Let R be commutative. We say $a \mid b$ (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 $a = ayx \iff a(1 - yx) = 0 \Rightarrow x, y \in R^*$ ∎

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

Y is irreducible

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

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

(i) x is prime $\iff$ (x) is a prime ideal

(ii) x is irreducible $\iff$ (x) is maximal among proper principal ideals

(iii) If x is prime then x is irreducible.

(iv) If R is a PID, then x is prime $\iff$ x is irreducible.

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

(vi) If x is irreducible and $a \mid x$, 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 $\mathbb{Z}[x,y]/(x^2-y^3)$: $x^2=y^3$

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

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

Ex $\mathbb{Z}$ is a UFD

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

Observe: If R a UFD and x irreducible, [illegible]

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

so x is prime.

Thm 3.7 Every PID is a UFD.

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

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

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

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

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

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

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

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

$= p_1 p_2 q_2$ - p_1, p_2

$= p_1 p_2 p_3 q_3$

$\vdots$

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

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

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

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

— x —

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

Def 3.8 ~~Accurate~~ An integral domain R is called a **Euclidean domain** if there exists a function $\varphi: R \setminus \{0\} \to \mathbb{N}$ such that

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

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

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

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

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

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

$= 2 + \frac{1}{5} - \frac{2}{5}i$

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

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

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

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

With $ac+bd = q_1\varphi(\beta)+r_1$ with $|r_1| \le \frac{1}{2}\varphi(\beta)$ $\quad (bc-ad)\beta = q_2\varphi(\beta)+r_2$ 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 $\varphi\left(\frac{(r_1+r_2 i)\beta}{\varphi(\beta)}\right) = \varphi\left(\frac{r_1+r_2 i}{\beta}\right)\cdot\frac{\varphi(r_1+r_2 i)}{\varphi(\beta)} = \frac{r_1^2+r_2^2}{\varphi(\beta)} \le \frac{(\frac{1}{2}\varphi(\beta))^2+(\frac{1}{2}\varphi(\beta))^2}{\varphi(\beta)} = \frac{1}{2}\varphi(\beta)$

Ex $\mathbb{R}[x]$ 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 $n=m$, $\quad f = \underbrace{\frac{a_m}{b_m}}_{q}\, g + \underbrace{\sum_{i=0}^{m-1}\left(a_i - \frac{a_m}{b_m}b_i\right)x^i}_{r}$

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

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

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

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

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

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

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

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

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

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

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

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

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 multiplicative if it is 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 $s, t \in S$

$sad = sbc$ $\quad tcf = bde$

(make sense)

$sad(tf) = sbctf$ $\quad sb\,tcf = tde(sb)$

$sadtf - tdesb = 0$

$\underbrace{std}_{\in S}(af - be) = 0 \Rightarrow (a,b) \sim (e,f)$

□

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

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 called frac R (or sometimes $\operatorname{Quot} R$), the <u>field of fractions</u> of R, is a field.

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

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

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 $s \in S$.

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

$sac = 0$

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

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

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

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

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

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

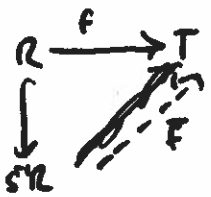
$$q(a+b) = \frac{(a+b)s^2}{s^2} = \frac{as}{s} + \frac{bs}{s} = q(a) + q(b)$$

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

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

(iii) Suppose $S \subseteq R^\times$ and $\frac{r}{s} \in S^{-1}R$. Then $q(\quad) rs^{-1}) = \frac{rs^{-1} \cdot s}{s} = \frac{r}{s}$

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



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

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

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

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

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

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

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

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

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

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

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

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

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

Thm 4.8 Let R be commutative, unital ring, $S \subseteq R$ multiplicative, $I \subseteq R$ an ideal
Then $\bar{S}^{-1}I = \bar{S}^{-1}R$ 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 $1 = \frac{s}{s} \in \bar{S}^{-1}I$, so $\bar{S}^{-1}I = \bar{S}^{-1}R$

$\Rightarrow$

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

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

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

Then $as t_0 = t_0 s t \in I \cap S$. ∎

($a \in I$, $t_0 s t \in S$)

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

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

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

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

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

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

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

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

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

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

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 $v \in S$

$abuv = cstv$ → requires $S \cap P = \emptyset$

$\in P$ (since $c \in P$)

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

so $\frac{a}{s} \cdot \frac{b}{s} = \frac{ab}{s^2} = \frac{ab}{s} \in \underset{S^{-1}R \setminus S^{-1}I}{S^{-1}R \setminus Q}$ 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 **localization of R at P**, denoted R_P, is the ring $S^{-1}R$ for the set $S = R \setminus P$.

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

Idea from algebraic geometry! R represents regular functions from variety $V \longrightarrow k$ (field)

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

Thm 4.11 Let R be commutative, unital, and $P \subset R$ 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 <u>local ring</u> 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 an 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 $\mathbb{R}[x]/(x^n)$ 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 $R \times M \to M$ satisfying, for all $r, s \in R$ and $a, b \in M$:

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

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

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 $\varphi: R[x] \to R[x]$, $f \longmapsto xf$ is a module homomorphism but not a ring homomorphism

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

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

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

Def 1.4 Let M be an R-module. Let $X \subseteq M$ be a subset.
The **submodule generated by X** is the intersection of all submodules containing X.
If X is finite, the module it generates is called **finitely generated**.

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

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

Thm 1.5 Let R be a unital ring, M an R-module.
(i) If $a \in R$, the submodule generated by $\{a\}$ is $Ra = \{ra \mid r \in R\}$
(ii) If $X \subseteq M$ is a set, the submodule generated by X is
$$RX = \left\{ \sum_{i=1}^{s} r_i a_i \mid s \in \mathbb{N}, r_i \in R, a_i \in X \right\}$$
(iii) If $\{B_i\}_{i \in I}$ is a family of submodules, the sum is
$$\left\{ \sum_{k=1}^{s} b_{i_k} \mid s \in \mathbb{N}, b_{i_k} \in B_{i_k} \right\}$$
(finite sums of elements of B_i's)

Thm 1.6 Let M be an R-module and $N \subseteq M$ a submodule.
Then M/N is an R-module with multiplication
$$r \cdot (a+N) = ra+N \quad \text{for all } r \in R.$$

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 $M_1 \oplus M_2 \oplus \cdots \oplus M_n$.

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

Def A sequence of R-module homomorphisms $A \xrightarrow{f} B \xrightarrow{g} C$ is called exact (at B) if $\operatorname{Im} f = \ker g$. 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
$$0 \to M \to M \oplus N \to N \to 0 \text{ is exact.}$$

Ex If $N \subset M$ is a submodule

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

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

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

$$\operatorname{coker} f = N/\operatorname{Im} f$$

Lemma 1.17 (Short Five Lemma) Let

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

be a commutative diagram

Suppose the rows are both exact.

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

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

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

Pf "Diagram chasing"

(i) Let $x \in \ker \beta$

Then $\gamma g(x) = g'\beta(x) = g'(0) = 0$, i.e. $g(x) \in \ker \gamma$

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

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

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

So $y \in \ker \alpha$, 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 $g(z) = y$

so $\gamma g(z) = g'\beta(z)$

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

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

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

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

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

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

$x = \beta(z + f(v))$ ∎

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

sequence of R-modules

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

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

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

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

Pf (1) $\Rightarrow$ (3)

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

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

$f(id(a)) = f(a)$ ✓

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

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

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

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

(ii) $\Rightarrow$ (iii)

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

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

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

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

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

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

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

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

Let $h = \varphi i_2$

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

□

§2 Free modules

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

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

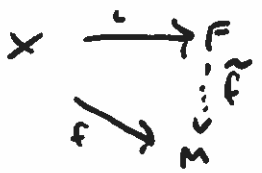
A linearly independent generating set is called a basis

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 $\tilde{f}: F \to M$



commutes

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

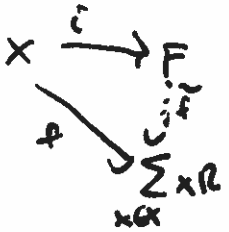
Since X is linearly independent, every $u \in F$ can be written uniquely

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

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

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

(3) $\Rightarrow$ (2)



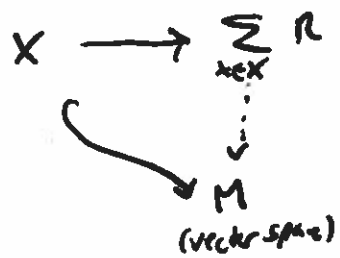
Note $\tilde{f}$ has some map $\sum_{x \in X} xR \to F$, $x \mapsto i(x)$

(2) $\Rightarrow$ (1) If X linearly dependent, this violates direct sum (Thm 1.15)
Clearly X generates F. ∎

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

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.



∎

Thm 2.4 Every module over a field (or division ring) is free, ~~a vector space~~.

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

Pf Let X be a maximal linearly independent set, let $N = \sum_{x \in X} kx$.
Then X is a basis of N.
Suppose $a \in M \setminus N$. Claim $X \cup \{a\}$ is linearly independent.
If $r_1 x_1 + \cdots + r_n x_n + r_{n+1} a = 0$ for some $r_i \in k$, not all zero
and $r_{n+1} \neq 0$ (since X linearly independent),
so $a = -\frac{1}{r_{n+1}}(r_1 x_1 + \cdots + r_n x_n) \in N$ ↯

Claim contradicts maximality, so $M = N$.

Pf of Thm 2.4 Let $S = \{X \subset M \mid X \text{ is linearly independent}\}$.
If $\{C_i \mid i \in I\}$ is a chain in S, $C = \bigcup_{i \in I} C_i$ is an independent set in S.
Zorn $\Rightarrow$ S has a maximal element, which is a basis by Lemma 2.3.

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

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

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

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

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

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

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

Now, WLOG suppose X is infinite.

Claim 1 Y is infinite.

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

write $y_1 = a_{11}x_1 + \dots + a_{1m}x_m$
$\vdots$
$y_n = a_{n1}x_1 + \dots + a_{nm}x_m$

$\Rightarrow \{x_1, \dots, x_m\}$ spans 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 $|X| > |Y|$, then exists $x \in X \setminus \bigcup_{i \in I} E_i$

Since $\bigcup_{i \in I} E_i$ spans, $x = b_1 x_1 + \dots + b_m x_m$ for some $x_i \in X$
$\Rightarrow X$ linearly dependent

So $|X| \leq |Y|$.

(Similarly, $|Y| \leq |X|$

∎

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

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

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

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

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

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

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

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

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

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

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

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 $r_j = \tilde{s}_j \in I$, $x_j = \tilde{x}_j$,

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

Claim 3 π is injective

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

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

$\|$

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

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

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

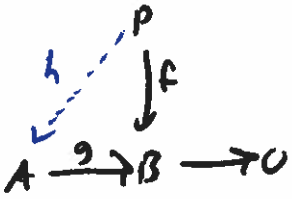
Pf. Let $m \subset R$ be a maximal ideal. Then $\pi: R \to R/m$
is a nonzero surjection, and R/m is a field, thus has IBN. ∎

§3 Projective and Injective modules

Motivations

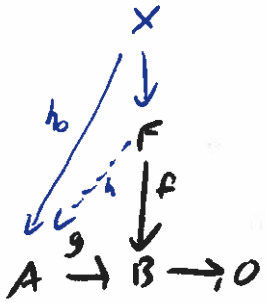
1) Projective modules are almost as nice as free modules
   (1) Direct summands of free modules
   (2) Locally free
2) Algebraic analogue of vector bundles - locally trivial
   (Ex Infinitely long Möbius strip)

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. $f = gh$



Thm 3.2 Free modules are projective.

Pf Let F be a free module, and suppose



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

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

Apply universal property of F. ∎

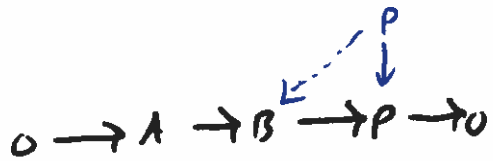
Thm 3.4 Let P be an R-module. TFAE

(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) $\Rightarrow$ (ii)



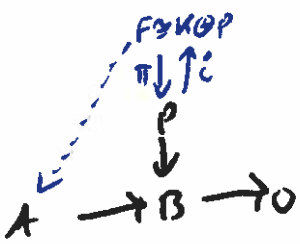
(ii) $\Rightarrow$ (iii) There is free module F

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

Let K = Kernel of this map.

Then $F \cong K \oplus P$

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



F projective!

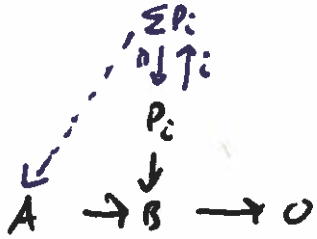
□

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

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

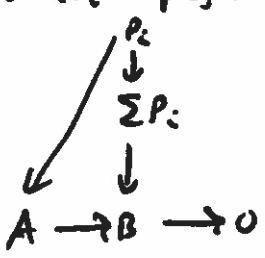
Prop 3.5 A direct sum of R-modules $\sum_{i \in I} P_i$ is projective if and only if each P_i is projective

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



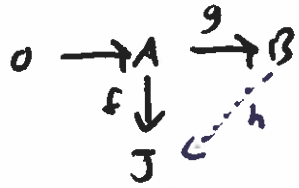
Then P_i is projective

$\Leftarrow$ Suppose P_i each projective



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

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



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

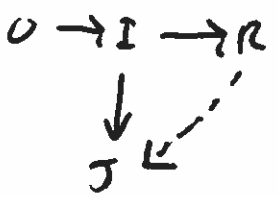
Prop 3.7 A direct product of R-modules $\prod_{i \in I} J_i$ is injective if and only if each J_i is injective.

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 a ring, J an R-module. J is injective iff for every (left) ideal $I \subset R$, every R-module homomorphism $I \to J$ extends to a homomorphism $R \to J$.

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



$\Leftarrow$ Suppose we are given $0 \to A \xrightarrow{g} B$, $A \xrightarrow{f} J$

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

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

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 $\varphi: I \to J$, $r \mapsto h(rb)$

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

so φ is an R-module homomorphism

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

Let $K = H + Rb$

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

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

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 ↯ □

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 $\begin{array}{ccc} D & \longrightarrow & D \\ x & \longmapsto & nx \end{array}$ 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 ⇐ 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)

$$\begin{array}{ccccc} 0 & \longrightarrow & \langle n \rangle & \longrightarrow & \mathbb{Z} \\ & & \downarrow f & \swarrow h & \\ & & D & & \end{array}$$

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

Now $nh(1) = h(n) = f(n) = y$. This D is divisible.

⇒ Suppose D is divisible. Let $f : \langle n \rangle \longrightarrow D$ be a homomorphism. ($\langle n \rangle$: 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. □