Def 1.1 A <u>ring</u> 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) $a(b+c) = ab + ac$
$(a+b)c = ac + bc$ for all $a, b, c \in R$.

If multiplication is commutative, R is called a <u>commutative ring</u>

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

<u>Ex</u> $\mathbb{Z}$ is a commutative ring with 1.
<u>Ex</u> $\mathbb{Z}_n$ is a commutative ring with 1.
<u>Ex</u> $M_n(\mathbb{R})$ 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 $a_i, b_j \in R$

<u>Pf</u> (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 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
$$\begin{aligned} f(a+b) &= f(a) + f(b) \\ f(ab) &= f(a) f(b) \end{aligned} \quad \text{for all } a, b \in R.$$

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

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

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

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

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

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

<u>Pf</u> (i) If $m \in \operatorname{Ker}\varphi$, $ma = m \cdot 1 \cdot a = 0 \cdot a = 0$ for all $a \in R$.

By assumption, $m > n$. 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 $0 = n \cdot 1 = K r \cdot 1 = K 1 \cdot r \cdot 1$ $\boxed{/\!/}$

§2 Ideals

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

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

<u>Def 2.1</u> Let R be a ring. A <u>subring</u> is a subset that is itself a ring.

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

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

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

<u>Ex</u> $\langle n \rangle$ is an ideal of $\mathbb{Z}$

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

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

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 <u>ideal generated by X</u>.

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

A <u>principal ideal</u> is an ideal generated by a single element.

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

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

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

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

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

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

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

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

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

Then $a_0 b_0 + I = (a-x)(b-y) + I = ab \underbrace{-ay}_{I} \underbrace{-xb}_{I} \underbrace{+xy}_{I} + I = ab + I$. ∎

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 $xa \in \operatorname{Ker}\varphi$ ◻

~~Thm (2.7)~~
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 $\bar{\varphi} : R/\operatorname{Ker}\varphi \to \operatorname{Im}\varphi$, $a + \operatorname{Ker}\varphi \mapsto \varphi(a)$ be the well defined abelian group isomorphism.

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~~

$IJ \subset P \Rightarrow I \subset P$ 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 prime, then R\P is multiplicatively closed, ie. 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 $ab \in P$, 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. $\square$

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 $\square$

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.

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 $1 = (m_1 + ar_1)(m_2 + br_2) = \underbrace{m_1 m_2 + m_1 b r_2 + m_2 a r_1}_{M} + abr_1 r_2$

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 ~~elect~~ 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 ~~[illegible]~~ (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

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

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 $1 \le k \le n$

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

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

Car 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

$x \equiv b_1 \bmod m_1$ ... $x \equiv b_n \bmod m_n$

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 $(a_0, a_1, a_2, \ldots)$ such that $a_i \in R$, only finitely many nonzero

(2) Addition is componentwise

(3) Multiplication given by

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

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

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

Pf need to check multiplication is associative

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

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

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

If $1 \in R$, $(1, 0, 0, \ldots)$ 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) $x^n = (0,0,\dots,0,\underset{\uparrow}{1},0,0,\dots)$

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

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

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 $\varphi(\sum_{i=0}^{n} a_i x^i) = \sum_{i=0}^{n} \varphi_0(a_i)$~~

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) ∎

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

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 $a,b \in R$. ~~If~~ 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~~ 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

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

Ex $\mathbb{Z}$ is a UFD

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

Observe: If R a UFD and x irreducible,

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

so x is prime.

Thm 3.7 Every PID is a UFD.

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

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

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 $x=p_1q_1$ for some irreducible p_1.

$x=p_1p_2q_2$ — p_1,p_2

$x=p_1p_2p_3q_3$

$\vdots$

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 $q, r \in \mathbb{N}$ ~~unique~~ s.t. $a = qb + r$ and $r < b$.

<u>Def 3.8</u> ~~A commutative~~ 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 $\varphi(a) \leq \varphi(ab)$

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

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

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

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

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

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

If $n>m$: $\cancel{f = q\,a_m}$ 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 $f = x^4 + 7x, \quad g = x^2 + 2x + 1$

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

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

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

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

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

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

<u>Ex</u> What is $\mathbb{Q}$? Is $\mathbb{Q} = \mathbb{Z} \times \mathbb{Z}$?

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

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

<u>Ex</u> If R is a ring, $R^\times$ is multiplicative

<u>Ex</u> If R is an integral domain, R^* is multiplicative.

<u>Ex</u> 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 $\frac{1}{st}$)

<u>Thm 4.2</u> 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

<u>Pf</u> 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 same

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

$sadtf - tdesb = 0$

$\underbrace{std}_{s?}(af - be) = 0 \implies (a,b) \sim (e,f)$

$\square$

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 $\gamma \in S$

$tdD\, s(aB-bA) + tbB(cD-dC)=0$

$st((ad+bc)BD - (AD+BC)bd)=0$ ✓

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

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

$st(acBD - bdAC)=0$ ✓

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

s'pose $\frac{0}{s} = \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$, 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 $\mathbb{Q} = \operatorname{frac} \mathbb{Z}$

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

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

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

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

(iii) Suppose $S \subset R^*$ 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

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

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

well defined: suppose $\frac{r}{s} = \frac{r_0}{s_0}$, 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 $\frac{r}{s}, \frac{r_0}{s_0} \in S^{-1}R$

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

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

<u>Thm 4.7</u> 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 $S^{-1}R$.

<u>Pf</u> 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 $xa \in I$. ∎

<u>Thm 4.8</u> Let R be commutative, unital ring, $S \subset R$ multiplicative, $I \subset R$ an ideal
Then $S^{-1}I = S^{-1}R$ iff $S \cap I \neq \emptyset$

<u>Pf</u> 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 $S^{-1}I = S^{-1}R$

$\Rightarrow$ ~~[illegible]~~
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 $\underset{\substack{\uparrow\\ I}}{ast_0} = t_0\underset{\substack{\uparrow\\ S}}{s}t \in I \cap S$. ∎

<u>Lemma 4.9</u> 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.

<u>Pf</u> (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 $ar \in I$.

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

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

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

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

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

$$\underbrace{ab\,uv}_{\notin P} = \underbrace{cstv}_{\in P}$$ 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 $\frac{as}{s} \cdot \frac{bs}{s} = \frac{abs^2}{s^2} = \frac{abs}{s} \in S^{-1}R \setminus Q$ since Q prime
$\qquad\qquad S^{-1}R \setminus S^{-1}I$

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 $\Rightarrow$ can be inverted.

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

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

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

Pf (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 the maximal ideal is $\mathfrak{m}$, often write <u>$(R, \mathfrak{m})$ is local</u>

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

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

Ex A ring is a module over itself. ~~[illegible]~~. 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 <u>submodule generated by X</u> is the intersection of all submodules containing X.
If X is finite, the module it generates is called <u>finitely generated</u>.

Def If $\{B_i\}_{i \in I}$ is a family of submodules, ~~[illegible]~~ the submodule generated by their union is called the <u>sum</u> 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 ~~[illegible]~~ $\{B_i\}_{i \in I}$ 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 $M_1 \oplus M_2 \oplus \dots \oplus M_n$.

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

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

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

Ex If M, N are R-modules

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

Ex If $N \subset M$ is a submodule

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

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

$$0 \to \operatorname{Ker} f \to M \xrightarrow{f} N \to \underset{\substack{\| \\ N/\operatorname{Im} f}}{\operatorname{Coker} f} \to 0$$ 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 $g(z) = y$

$$\text{So } \gamma g(z) = g'\beta(z)$$

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

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 $\alpha(v) = w$.

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

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

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

∎

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

<u>Thm 1.18</u> Let $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ be exact sequence of R-modules. 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 $0 \to A \to A \oplus C \to C \to 0$

<u>Pf</u> (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 $(a,c) \in A \oplus C$

$$g((f+h)(a,c)) = g(f(a)+h(c)) = g(f(a)) + g(h(c)) = 0 + c = c$$
$$id(\pi(a,c)) = id(c) = c \quad \checkmark$$

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

(ii) $\Rightarrow$ (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 $a \in A$: $(K,g)(f(a)) = (Kf(a), gf(a)) = (a,0)$
$i(id(a)) = i(a) = (a,0) \quad \checkmark$

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)

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

Let $h = \varphi i_2$

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

$\boxtimes$

§2 Free modules

<u>Def</u> Let M be an R-module, $X \subset M$ a subset. X is called <u>linearly independent</u> 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 <u>basis</u>

<u>Thm 2.1</u> 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 $\tilde{f} : F \to M$

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

commutes

<u>Pf</u> (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)

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

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

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

$\blacksquare$

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

<u>Cor 2.2</u> Let R be unital, M an R-module. Then M is the homomorphic image of a free module

<u>Pf</u> Let X be a generating set for M.

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

<u>Thm 2.4</u> Every module (vector space) over a field (or division ring) is free, ~~[illegible]~~.

$\blacksquare$

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

<u>Pf</u> Let X be a maximal linearly independent set, let $N = \sum_{x\in X} kx$.
Then X is a basis of N.
Suppose $a \in M \setminus N$. <u>Claim</u> $X \cup \{a\}$ is linearly independent.
IC $r_1x_1 + \dots + r_nx_n + r_{n+1}a = 0$ for some $r_i \in k$, not all zero
note $r_{n+1} \neq 0$ (since X linearly independent),
So $a = \frac{-1}{r_{n+1}}(r_1x_1 + \dots + r_nx_n) \in N$ $\lightning$

Claim contradicts maximality, so $M = N$.

<u>Pf of Thm 2.4</u> Let $S = \{X \subset M \mid X$ is linearly independent$\}$.
If $\{C_i \mid i \in I\}$ is a chain in S, $C = \bigcup_{i\in I} C_i$ is lin indep, so in S.
Zorn $\Rightarrow$ S has a maximal element, which is a basis by Lemma 2.3.

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

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

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

Def 2.8 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 $\left|\bigcup_{i \in I} E_i\right| = |I| = |Y|$ and $\bigcup_{i \in I} E_i$ spans V.

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

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 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 $u = \sum_{j=1}^{n} r_j x_j$ 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.

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

So $$\sum_{j=1}^{n} r_j x_j = \sum_{k=1}^{m} s_k u_k \quad \text{for some } s_k \in I,\ u_k \in F.$$
$$= \sum_{i=1}^{p} \tilde{s}_i \tilde{x}_i \quad \text{for some } \tilde{s}_i \in I,\ \tilde{x}_i \in X \quad \text{since } X \text{ a basis of } F.$$

After reindexing, since X linearly independent we must have $r_j = \underset{\in I}{\tilde{s}_j}$, $x_j = \tilde{x}_j$,
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 $(1+I)\,\pi(x_1) - (1+I)\,\pi(x_2) = 0$

$$\begin{gathered} \| \\ x_1 + x_2 + IF \end{gathered}$$

with $\tilde{s}_i \in I$

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

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

Pf Let $I = \operatorname{Ker} f$, 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 $\pi: R \longrightarrow R/m$
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 Infinity 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 $F = K \oplus P$.