

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

- (1) $(R, +)$ is an abelian group
- (2) (R, \cdot) is a semigroup
- (3) $a(b+c) = ab+ac$ for all $a, b, c \in R$.
 $(a+b)c = ac+bc$

If multiplication is commutative, R is called a commutative ring

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

Ex \mathbb{Z} is a commutative ring with 1.

Ex \mathbb{Z}_n is a commutative ring with 1.

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

Thm 1.2 Let R be a ring.

- (i) $0 \cdot a = a \cdot 0 = 0$ for all $a \in R$
- (ii) $(-a)b = a(-b) = -(ab)$ for all $a, b \in R$
- (iii) $(-a)(-b) = ab$ for all $a, b \in R$
- (iv) $(na)b = a(nb) = n(ab)$ for all $n \in \mathbb{Z}$, $a, b \in R$.
- (v) $\left(\sum_{i=1}^n a_i\right)\left(\sum_{j=1}^m b_j\right) = \sum_{i=1}^n \sum_{j=1}^m a_i b_j$ for all $a_i, b_j \in R$

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

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

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

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

(v) Distributive property

□

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

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

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

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

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

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

Ex \mathbb{Z} is an integral domain.

Def 1.7 Let R, S be rings. A function $f: R \rightarrow S$ is called a homomorphism if $f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$ for all $a, b \in R$.

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

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

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

ϕ is a homomorphism with $\text{Ker } \phi = \langle n \rangle$

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

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

Pf (i) If $m \in \text{Ker } \phi$, $ma = 0 \cdot m \cdot 1 \cdot a = 0 \cdot a = 0$ for all $a \in R$.

By assumption, $m > n$. Write $m = Kn + r$ for some $0 \leq r < n$.

Then $ra = 0$ for all $a \in R$, so $r = 0$, i.e. $m \in \langle n \rangle$.

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

(iii) Suppose $n = Kr$ for some $K, r \in \mathbb{N}$.

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

□

~~Section 2~~

§2 Ideals

Observe: If $x, y \in \text{Ker } \phi$, $x+y, xy \in \text{Ker } \phi$

But also If $a \in R$, $x \in \text{Ker } \phi$, $ax \in \text{Ker } \phi$

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

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

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

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

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

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

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

Cor 2.3 The intersection of ideals is an ideal.

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

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

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

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

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

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

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

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

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

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

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

Thm 2.8 If $\varphi: R \rightarrow S$ is a ring homomorphism, $Ker \varphi$ is an ideal.

pf If $a, b \in Ker \varphi$, $\varphi(a+b) = \varphi(a) + \varphi(b) = 0 + 0 = 0$, so $a+b \in Ker \varphi$

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

$\varphi(xa) = \varphi(x)\varphi(a) = \varphi(x)0 = 0$, so $xa \in Ker \varphi$ \square

~~Thm 2.9~~

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

Then $R/Ker \varphi \cong Im \varphi$

pf Let $\bar{\varphi}: R/Ker \varphi \rightarrow Im \varphi$ be the well-defined abelian group isomorphism.
 $a + Ker \varphi \mapsto \varphi(a)$

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

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

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

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

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

~~$RS \subset P \Rightarrow R \subset P$ or $S \subset P$~~

$IS \subset P \Rightarrow I \subset P$ or $S \subset P$ for all ideals $I, S \subset R$

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

~~1) If R is prime, then $R \setminus P$ is multiplicatively closed, or if $a, b \in R$ then $ab \in P$ or $b \in P$.~~

~~2) If R is commutative and P is prime,~~

1) If $R \setminus P$ is multiplicatively closed, then P is prime.

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

Remark $R \setminus P$ multiplicatively closed \Leftrightarrow If $a, b \in R$ with $ab \in P$, either $a \in P$ or $b \in P$

PF (i) Let $I, J \subset R$ be ideals with $I \subset J \subset P$.

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

Let $x \in I \setminus P$. Let $y \in J$.

Then $xy \in I \subset P$, so $y \in P$ (since $x \notin P$).

This holds for all $y \in J$, so $J \subset P$.

(ii) Let $a, b \in R$ with $ab \in P$

Claim ~~(a) or (b) \subset P~~

If $x \in (a)(b)$, $x = ar_1br_2$ for some $r_1, r_2 \in R$
 $= (ab)r_1r_2 \in P$.

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

Cor Let R be a commutative unit ring. Then (0) is prime iff R is an integral domain.

PF Let $a, b \in R \setminus (0)$. Then (0) is prime iff $ab=0$ implies $a=0$ or $b=0$ i.e. R is an integral domain. \square

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

Thm 2.16 Let R be a commutative unit ring. An ideal P is prime iff R/P is an integral domain.

PF \Rightarrow Let $a+P, b+P \in R/P$.
If $(a+P)(b+P) = 0+P$, $ab+P = P$, i.e. $ab \in P$.
Then $a \in P$ or $b \in P$, so $a+P = 0+P$ or $b+P = 0+P$.
Thus R/P is an integral domain.

\Leftarrow Suppose R/P is an integral domain. Let $a, b \in R$ with $ab \in P$.
Then $(a+P)(b+P) = 0+P$, so $a+P = 0+P$ or $b+P = 0+P$
i.e. $a \in P$ or $b \in P$.

Thus P is prime \square

Def 2.17 Let R be a ring. A proper ideal M is called maximal if it is not contained in any other proper ideal.

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

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

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

Let $\mathcal{C} = \{C_i \mid i \in I\}$ be a chain of ^{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 $a, b \in C_j \subset C$.

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

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

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

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

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

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

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

$$1 = m_1 + ar_1 = m_2 + br_2$$

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

$$\text{Then } 1 = (m_1 + ar_1)(m_2 + br_2) = \underbrace{m_1 m_2 + m_1 br_2 + m_2 ar_1}_{\in M} + ab r_1 r_2$$

If $ab \in M$, then $1 \in M$ \downarrow so $ab \notin M$, $\therefore M$ is prime. \square

Thm 2.20 Let R be a unital ring.

(i) If R/M is a division ring, then M is maximal.

(ii) If R is commutative, then M is maximal $\Leftrightarrow R/M$ is a field.

PF (i) Let N be an ideal with $M \subsetneq N$.

Let $a \in N \setminus M$. Then there exists $b \in N \setminus M$ with $(a+M)(b+M) = 1+M$

so $ab - 1 \in M \subset N$. But $ab \in N$, so $1 \in N$, i.e. $N = R$.

Thus M is maximal.

(ii) \Leftarrow Follows from (i)

\Rightarrow Suppose M is maximal. Then M is prime, so R/M is an integral domain.

Let $a+M \neq 0+M$, (so $a \notin M$).

Then $(a+M)R/M = R/M$, so $1 = ar + m$ for some $r \in R, m \in M$.

Then $(a+M)(r+M) = ar + M = 1+M$

Thus every non-zero element of R/M has a multiplicative inverse,

So R/M is a field.

Cor 2.21 Let R be a commutative unital ring. TFAE

(i) R is a field

(ii) R has exactly two ideals, 0 and R .

(iii) 0 is a maximal ideal

(iv) Every non-zero homomorphism of rings $R \rightarrow S$ is injective.

PF Thm 2.20 gives ~~(i) \Leftrightarrow (ii)~~ (i) \Leftrightarrow (iii). Clearly (ii) \Leftrightarrow (iii)

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

□

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

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

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

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

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

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

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

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

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

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

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

□

Thm 2.25 ("Chinese Remainder Theorem" - Sun-Tsz'e, ~400 AD)

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

and $I_i + I_j = R$ for all $i \neq j$ (I_1, \dots, I_n called pairwise comaximal)

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

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

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

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

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

$n=2$: $R = I_1 + I_2$ ✓

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

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

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

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

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

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

Let $b = r_1 + \dots + r_n$. Then $b \equiv r_k \equiv b_k \pmod{I_k}$ □

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

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

$$x \equiv b_1 \pmod{m_1} \quad \dots \quad x \equiv b_n \pmod{m_n}$$

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

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

(1) The set of all sequences (a_0, a_1, a_2, \dots) such that $a_i \in R$, only finitely many non-zero

(2) Addition is component wise

(3) Multiplication given by

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

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

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

PF need to check multiplication is associative

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

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

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

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

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

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

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

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

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

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

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

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

Thm 5.5 Let $\phi_0: R \rightarrow S$ be a homomorphism of commutative unital rings with $\phi_0(1) = 1$. Let $s_1, \dots, s_n \in S$. Then there is a unique homomorphism

$\phi: R[x_1, \dots, x_n] \rightarrow S$ s.t. $\phi|_R = \phi_0$ and $\phi(x_i) = s_i$.

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

pf ~~$\phi(\sum_{i=0}^n a_i x^i) = \sum_{i=0}^n \phi(a_i) \phi(x^i)$~~

It suffices to assume $n=1$.

If $\sum_{i=0}^n a_i x^i \in R[x]$, set $\phi(\sum_{i=0}^n a_i x^i) = \sum_{i=0}^n \phi_0(a_i) s^i$

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

This is called the evaluation map or substitution map □

§3 Factorization in commutative rings

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

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

- (i) $a|b \Leftrightarrow (b) \subset (a)$
- (ii) a and b are associates $\Leftrightarrow (a) = (b)$
- (iii) $u \in R^* \Leftrightarrow u|r$ for all $r \in R$.
- (iv) $u \in R^* \Leftrightarrow (u) = R$
- (v) If R is a domain, a and b are associates $\Leftrightarrow a = bu$ for some $u \in R^*$

pf (i) $a|b \Leftrightarrow \exists b \in (a) \Leftrightarrow (b) \subset (a)$

(ii) Immediate from (i)

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

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

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

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

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

then $a = ayx \Leftrightarrow a(1 - yx) = 0 \Rightarrow x, y \in R^*$ \square

Def Let R be commutative, unit. Let $x \in R \setminus R^*$ be nonzero.

(i) x is called irreducible if whenever $x = ab$, then $a \in R^*$ or $b \in R^*$.

(ii) x is called prime if whenever $x|ab$, then $x|a$ or $x|b$.

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

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

y is irreducible

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

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

- (i) x is prime $\Leftrightarrow (x)$ is a prime ideal
- (ii) x is irreducible $\Leftrightarrow (x)$ is maximal among proper principal ideals
- (iii) If x is prime then x is irreducible.
- (iv) If R is a PID, then x is prime $\Leftrightarrow x$ is irreducible.
- (v) Associates of primes are prime. Associates of irreducibles are irreducible.
- (vi) If x is irreducible and $a \mid x$, either $a \in R^*$ or $x \mid a$ (i.e. a is an associate).

Pf (i) Immediate

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

\Leftarrow Suppose $x = ab$ for some $a, b \in R$. ~~It follows that~~ $(x) \subset (a)$,
so $(x) = (a)$ (i.e. $b \in R^*$) or $(a) = R$ (i.e. $a \in R^*$).

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

Then $a = xy$, so $x = (xy)b$. Then $x(1 - yb) = 0$, so $b \in R^*$.

(iv) Assume R is a PID, let $x \in R$ be irreducible. Then by (ii) (x) is a maximal ideal, hence prime.

(v) Follows from (i) & (ii). Since associates generate the same ideal.

(vi) Definition

Q: When are prime + irreducible the same?

Problem with $\mathbb{Z}[x]/(x^2 - y^3)$: $x^2 = y^3$

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

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

Ex \mathbb{Z} is a UFO

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

Observe: If R a UFO and x irreducible, x is prime.

~~Top is irreducible.~~

$x|ab \Rightarrow x|a$ or $x|b$ (factor into irreducibles)
so x is prime.

Thm 3.7 Every PID is a UFO.

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

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

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

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

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

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

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

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

$$x = p_1 p_2 q_2 \quad - p_1, p_2$$

$$x = p_1 p_2 p_3 q_3$$

\vdots

(70)

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

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

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

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

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

q_1, p_1 are associates

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

— x —

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

Def 3.8 ~~Approximate~~ An integral domain R is called a Euclidean domain if there exists a function $\phi: R \setminus \{0\} \rightarrow \mathbb{N}$ such that

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

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

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

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

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

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

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

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

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

With $ac+bd = q_1 q(\beta) + r_1$ with $|r_1| \leq \frac{1}{2}q(\beta)$ $(bc-ad)i = q_2 q(\beta) + r_2$ with $|r_2| \leq \frac{1}{2}q(\beta)$

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

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

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

Ex $\mathbb{A}[x]$ is Euclidean with $q(f) = \deg f$

Do Ex first:

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

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

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

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

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

If $\deg(f - qg) < \deg g$, done.

Else, $f - qg = q_0 g + \overset{\deg < \deg g}{\downarrow \text{int}} r$

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

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

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

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

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

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

Th 3.9 Euclidean rings are PIDs.

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

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

$$\text{Then } x - qy = r \in I \Rightarrow r = 0$$

So $x = qy$

Thus $I = (y)$. □

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

§4 Rings of quotients + localization

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

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

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

Ex If R is a ring, R^\times is multiplicative

Ex If R is an integral domain, R^\times is multiplicative.

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

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

Thm 4.2 Let R be a commutative ring, and $S \subset R$ multiplicative. Define \sim on $R \times S$ by

$$(a, b) \sim (c, d) \text{ if } s(ad - bc) = 0 \text{ for some } s \in S.$$

\sim is an equivalence relation

pf Reflexive & symmetric ✓

Transitive: Suppose $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$

$$s(ad - bc) = 0$$

$$t(cf - de) = 0$$

for some $s, t \in S$

$$sad = sbc$$

$$tcf = bde$$

make sense

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

$$sadtf - tdesb = 0$$

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

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

□

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

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

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

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

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

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

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

(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 a field.
 $\text{frac } R$ (or sometimes $\text{quot } R$), the field of fractions of R , is a field.

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

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

we want: $\frac{ad+bc}{bd} = \frac{Ad+Bc}{BD}$, so $((ad+bc)BD - (Ad+Bc)bd) \neq 0$ for some $y \in S$

$$tdDs(aB-bA) + tBb(cD-dC)=0$$

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

we want: $\frac{ac}{bd} = \frac{Ac}{Bd}$ so $(acBD - Acbd) \neq 0$ for some $y \in S$.

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

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

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

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

$$sac = 0$$

$$\Rightarrow a=0 \text{ or } c=0$$

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

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

(note $\frac{s}{s} \in S^{-1}R$ is m.u. identity for any $s \in S$).

□

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

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

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

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

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

(i) the map $Q: R \longrightarrow S^{-1}R$

is a well defined homomorphism

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

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

(ii) If $0 \notin S$ and S contains no zero divisors, Q is injective.

In particular, every integral domain may be embedded in its field of fractions

(iii) If R is unital and $S \subset R^*$, then Q is an isomorphism.

pf (i) well defined: need $\frac{rs}{s} = \frac{r' b}{t}$ for any $s, t \in S$

$$\bullet \quad rs - r's = 0 \quad \checkmark$$

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

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

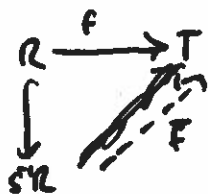
$$\varphi(a+b) = \frac{(a+b)s^2}{s^2} = \frac{as}{s} + \frac{bs}{s} = \varphi(a) + \varphi(b)$$

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

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

(iii) Suppose $s \in R^* \cap S$ and $\frac{r}{s} \in S^{-1}R$. Then $\varphi(\frac{r}{s}) = \frac{rs^2}{s^3} = \frac{r}{s}$

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



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

well defined: suppose $\frac{r}{s} = \frac{r_0}{s_0}$, so $t(rs_0 - sr_0) = 0$ for some $t \in S$
 $f(t)(f(r)f(s_0) - f(s)f(r_0)) = 0$
 $f(r)f(s_0) - f(s)f(r_0) = 0 \cdot f(t)^{-1} = 0$

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

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

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

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

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

Thm 4.7 Let R be commutative, SCR multiplicative.

If $I \subset R$ is an ideal, then $S^{-1}I = \left\{ \frac{a}{s} \mid a \in I, s \in S \right\}$ is an ideal of $S^{-1}R$.

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

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

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

Thm 4.8 Let R be commutative, unit ring, SCR multiplicative, $I \subset R$ an ideal

Then $S^{-1}I = S^{-1}R$ iff $S \cap I \neq \emptyset$

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

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

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

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

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

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

$$\text{Then } \underbrace{as}_{\in I} \underbrace{t_0}_{\in S} = \underbrace{t_0}_{\in S} \underbrace{st}_{\in S} \in I \cap S. \quad \square$$

Lemma 4.9 Let R be commutative, unital, SCR multiplicative.

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

(ii) If $P \subset R$ is a prime ideal, ~~$S \not\cap P$~~ and ~~$S \cap P \neq \emptyset$~~ , then $\tilde{S}'P$ is a prime ideal.
 $S \cap P = \emptyset$

Pr (i) Let $J \subset \tilde{S}'R$ be an ideal. Fix some $e \in S$, so $\frac{e}{e}$ is identity in $\tilde{S}'R$.

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

(i) I is an ideal: Let $r, s \in I$

$$\text{Then } \frac{re}{e}, \frac{se}{e} \in J, \text{ so } \frac{re}{e} + \frac{se}{e} = \frac{re^2 + se^2}{e^2} = \frac{(r+s)e^2}{e^2} = \frac{(r+s)e}{e} \in J, \\ \text{so } r+s \in I.$$

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

(ii) $J = \tilde{S}'I$:

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

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

(ii) Let $\frac{a}{s}, \frac{b}{t} \in \tilde{S}'R \setminus \tilde{S}'P$, ~~$a, b \in R$~~ , so $a, b \in R \setminus P$.

$$\text{Need to show } \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st} \notin \tilde{S}'P.$$

Suppose $\frac{ab}{st} \in \tilde{S}'P$: we claim $ab \in P$.

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

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

$$\underbrace{ab} \underbrace{uv} = \underbrace{cst} \underbrace{v} \quad \begin{array}{l} \uparrow \\ P \end{array} \quad \text{requires } S \cap P = \emptyset$$

thus $ab \in P$. This contradicts P being prime. \square

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

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

PF Our proof of 4.9 (i) shows this is injective.
 Let Q be a prime ideal of $S^{-1}R$. Then $Q = S^{-1}I$ for some ideal $I \subset R$.

claim I is prime.

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

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

so $\frac{a}{s} \cdot \frac{b}{s} = \frac{ab}{s^2} = \frac{ab}{s} \in S^{-1}R \setminus Q$ since Q prime
 $\frac{ab}{s} \in S^{-1}R \setminus S^{-1}I$
 then $ab \notin I$.

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

Def Let R be a commutative, unital ring, $P \subset R$ a prime ideal.
 The localization of R at P , denoted R_P , is the ring $S^{-1}R$ for the set $S = R \setminus P$.
 If $I \subset R$ is an ideal, $S^{-1}I$ is denoted I_P .

Idea from algebraic geometry! R represents regular functions from variety $V \rightarrow \mathbb{A}^n$
 To restrict attention locally, need functions that don't vanish \Rightarrow can be inverted.

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

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

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

Pf (c) follows from 4.10.

(ii) (i) implies P_p is maximal.

Suppose $M \subset R_p$ is some other maximal ideal. By (i), $M = Q_p$

for some prime ideal $Q \subset P$. But $Q \subset P \Rightarrow Q_p \subset P_p$

and Q_p maximal $\Rightarrow Q_p = P_p$.

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

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

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

Maximal ideal is (p)

Thm 4.13 Let R be a commutative unital ring. TFAE

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

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

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

Pf (i) \Rightarrow (ii) Take $\mathfrak{m} \subset R \setminus R^*$
If $x \in R \setminus R^*$, $x \notin R$, so $x \in \mathfrak{m}$
Thus $R \setminus R^* \subset \mathfrak{m}$, so $R \setminus R^* = \mathfrak{m}$.

(ii) \Rightarrow (iii) \checkmark

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

Ex $\mathbb{C}[[x]]$ is local

Ex $k[x]/(x^n)$ is local